МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

Кафедра іноземної філології

ENGLISH FOR CYBERSECURITY

Методичні вказівки
з англійської мови професійного спрямування для самостійної роботи
здобувачів вищої освіти спеціальності *125 Кібербезпека*
першого (бакалаврського) рівня вищої освіти
(*Частина II*)

Обговорено і рекомендовано
на засіданні кафедри іноземної філології
протокол № 2 від 19.02. 2024 р.

Чернігів 2024

English for Cybersecurity. Методичні вказівки з англійської мови професійного спрямування для самостійної роботи здобувачів вищої освіти спеціальностей *125 Кібербезпека* першого (бакалаврського) рівня вищої освіти *(Частина II)* / Укл.: В.А. Пермінова, А. І. Сікалюк, Г.А. Дивнич. Чернігів : НУ «Чернігівська політехніка», 2024. 73 с.

Укладачі: В. А. Пермінова, кандидат педагогічних наук, доцент, доцент кафедри іноземної філології,
Сікалюк А.І., кандидат педагогічних наук, доцент кафедри іноземної філології Національного університету «Чернігівська політехніка»,
Г.А. Дивнич, кандидат державного управління, доцент кафедри іноземної філології

Відповідальна за випуск: Литвин С. В., кандидат педагогічних наук, доцент, завідувачка кафедри іноземної філології
Національного університету «Чернігівська політехніка»

Рецензент: О. Б. Шендерук, кандидат педагогічних наук, доцент, доцент кафедри іноземної філології

ВСТУП

"English for Cybersecurity" (Частина II) – комплексний курс, покликаний забезпечити здобувачів освіти мовними навичками та спеціалізованими знаннями, необхідними для ефективної комунікації у сфері кібербезпеки.

Курс складається з восьми модулів, які охоплюють основні поняття, технічну термінологію, комунікаційні стратегії та тематичні дослідження, пов'язані з кібербезпекою. Ці модулі ретельно структуровані для поступового розвитку мовних навичок та одночасного поглиблення розуміння концепцій кібербезпеки.

У кожному модулі ви знайдете добірку матеріалів для читання. Тексти підібрані таким чином, щоб ознайомити студентів з автентичною мовою, яка використовується в контексті кібербезпеки, надаючи цінну інформацію про специфічні мовні нюанси галузі.

Перед початком роботи з матеріалами для читання студентам будуть запропоновані завдання для підготовки до читання, які активізують відповідну лексику та концепції. Завдання для післячитання заохочують до роздумів, осмислення та застосування набутих знань на практиці.

Інтерактивні вправи та запитання, що спонукають до роздумів, інтегровані в усі модулі для покращення мовних навичок та критичного мислення. Ці елементи покликані сприяти залученню, спільному навчанню та практичному застосуванню мовних концепцій кібербезпеки.

У кожному модулі є спеціальний розділ, присвячений тематичним дослідженням, що дозволяє студентам застосувати мовні навички в реальних сценаріях кібербезпеки. Тематичні дослідження ретельно розроблені, щоб імітувати автентичні ситуації, розвиваючи вміння вирішувати проблеми та посилюючи засвоєння мови.

Для викладачів та фасилітаторів надаються вичерпні методичні рекомендації щодо планування уроків, проведення дискусій та оцінювання прогресу учнів. Ці нотатки містять додаткову інформацію, запропоновані вправи та поради щодо адаптації матеріалу до різних навчальних середовищ.

Щоб допомогти здобувачам освіти опанувати спеціалізовану лексику з кібербезпеки, до посібника включено вичерпний глосарій. Цей ресурс слугує швидким довідником для ключових термінів і технічної мови, що зустрічаються в модулях.

Introduction

"English for Cybersecurity" (Part II) is a comprehensive course designed to equip students with the language skills and specialised knowledge necessary for effective communication in the field of cybersecurity.

The course consists of eight modules covering basic concepts, technical terminology, communication strategies and case studies related to cybersecurity. These modules are carefully structured to gradually develop your language skills while deepening your understanding of cybersecurity concepts.

Each module contains a selection of reading materials. The texts are selected to introduce students to authentic language used in the context of cybersecurity, providing valuable insights into the specific linguistic nuances of the industry.

but a comprehensive glossary. This resource serves as a quick reference for key terms and technical language encountered in the modules.

Before starting with the reading materials, students will be given pre-reading activities that activate relevant vocabulary and concepts. The post-reading activities encourage reflection, reflection and application of the knowledge gained.

Interactive exercises and thought-provoking questions are integrated throughout the modules to improve language skills and critical thinking. These elements are designed to promote engagement, collaborative learning and practical application of cybersecurity language concepts.

Each module has a special section dedicated to case studies, allowing students to apply language skills in real-life cybersecurity scenarios. The case studies are carefully designed to simulate authentic situations, developing problem-solving skills and reinforcing language acquisition.

Comprehensive teaching notes are provided for teachers and facilitators to plan lessons, lead discussions and assess learner progress. These notes include additional information, suggested activities and tips for adapting the material to different learning environments.

A comprehensive glossary is included to help learners master specialised cybersecurity vocabulary. This resource serves as a quick reference for key terms and technical language used in the modules.

Table of Contents

MODULE 5
CHOOSING A BROWSER

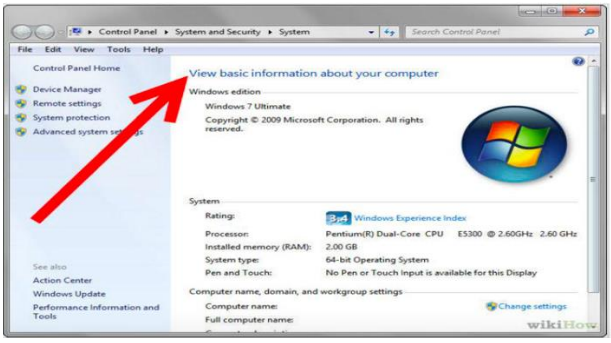
UNIT 17
BROWSER REQUIREMENTS

Pre-Reading Questions on Browser Requirements:

1. **Current Browser Usage:**
   - What browser(s) are you currently using, and why have you chosen them?
   - Have you experienced any limitations or issues with your current browser(s)?
2. **Prior Knowledge on Browser Security:**
   - How concerned are you about security when using a web browser?
   - Can you name any security features that browsers commonly offer?
3. **Expectations from a Browser:**
   - What features or capabilities do you expect a modern web browser to have?
   - Are there specific requirements you look for in a browser for your daily activities?
4. **Compatibility Considerations:**
   - How important is browser compatibility for your online experience?
   - Have you ever encountered issues with website compatibility based on your browser choice?
5. **Interest in Browser Updates:**
   - How often do you update your browser? What motivates you to do so?
   - Are you aware of the latest updates and features in your browser?
6. **Browsing Preferences:**
   - Do you have specific preferences regarding the user interface or design of a web browser?
   - Are there particular features that significantly influence your choice of a browser?
7. **Awareness of Alternative Browsers:**
   - Are you familiar with alternative browsers to mainstream ones (e.g., Chrome, Firefox, Safari)?
   - What factors might influence someone to choose an alternative browser?

Browser Requirements

Browsers are the key to the Internet these days, at least for most tasks. There are many, many browsers for every platform and operating system, so the choice can be tough. However, this should help narrow the search.



View basic information about your computer

Windows edition

Windows 7 Ultimate

Copyright © 2009 Microsoft Corporation. All rights reserved.

System

Rating: 3.4 Windows Experience Index

Processor: Pentium(R) Dual-Core CPU E5300 @ 2.60GHz 2.60 GHz

Installed memory (RAM): 2.00 GB

System type: 64-bit Operating System

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:

Full computer name:

Step 1: Determine the age of your computer. How old is your computer? Is it a mobile device? Know your systems specifications as this may be more suited to some browsers than others.

Step 2: Think about your ideal browser; what would it be able to do? You may want it to be quite simple, handling only the bare necessities. You may want some basic features like web feed reading, bookmarking (favorites), or search boxes. Some browsers have a lot more, and that's where it starts to get confusing.

Step 3: Make sure you know what platform you are on. Some browsers are only available to a certain operating system, or not available to one operating system.

Step 4: Research browsers. Tabbed browsers include Safari (runs on OS X, iPhone and is new to Windows), Firefox (general purpose with the most plug-ins), Opera(supports torrents, handles e-mail and runs on mobile devices), Konqueror (dual purpose file manager), Seamonkey (includes HTML editor and e-mail client), Off By One (tiny) and Flock (social networking).

Step 5: See the features of all browsers you have found, and compare with what you want.

Step 6: Consider alternative lower-memory browsers, if you have low computer memory. Consider Off by One, Dillo, SkipStone and NetSurf.

Step 7: Consider a text-based browser, if you want an even faster-than-fast(maximum speed/hyperdrive) experience. Consider ELinks.

Step 8: Find out if you can add features you may want or if there is an easy method to doing so such as an existing plugin or extension in the case of Firefox.

Step 9: Download and install your new browser!

Activities

1. **Research and Compare**: Research different web browsers (such as Google Chrome, Mozilla Firefox, Safari, etc.) and compare their system requirements. Create a chart or a list highlighting the minimum and recommended specifications for each browser.

2. **Browser Compatibility Test**: Test the compatibility of different websites on various browsers. They can choose a few popular websites and access them using different browsers to see if all the features and functionalities work properly. Write a report or create a presentation discussing their findings.

3. **Browser Features Analysis**: Choose a specific feature of a web browser (such as tab management, privacy settings, extensions, etc.) and research how different browsers handle that feature. Create a comparison chart or write a detailed analysis of the strengths and weaknesses of each browser in relation to that feature.

RECOMMENDED VIDEOS:

https://www.youtube.com/watch?v=sr7mgYD2tAc
https://www.youtube.com/watch?v=-jHs-RYD7gc
https://www.youtube.com/watch?v=gNiz4kfSZnw

UNIT 18
SAFE BROWSING

1. What does safe browsing mean to you?

2. Have you ever encountered any online security threats while browsing the internet?
3. What precautions do you usually take to ensure safe browsing?
4. Can you name a few common online threats or scams?

Internet security is a matter of great concern for internet users. It is important to **know if a website is secure** or not while surfing the internet19. A **secure website** creates a safe connection between the website and the web browser so that entered data, such as personal information, credit card details, banking information, etc, is not accessible to unauthorized entities. When the browser opens a secured connection, "https" can be seen in the URL instead of just http. To **know if a website is secure** or not, look for the locked yellow colour padlock symbol on the lower right corner of the browser window.

Some web sites use a secure connection between the web site and your browser. This may be important to you, for instance, if you want to pay online for a product or a service and have to enter credit card information or other personal information. To know if your browser is viewing a secure web site, you can look in the lower right part of the window. There is a small box in the frame of the window to the left of the area that describes which zone you are in (usually the Internet zone, with a globe icon). If you see a yellow padlock icon, the web site you are viewing is a "secure web site." If the box is empty, the web site does not have a secure connection with your browser.

Shopping online can be cheaper and more convenient for you and for businesses. However, make sure you understand your rights and the risks before you shop online or bid in an online auction.

I. **Pay securely:** Don’t make any payment unless:

- You are on a secure website, and
- You can make a secure payment.

This will protect you against fraud and unauthorized credit card transactions. A secure website address will always:

- begin with „https://‟, not „http://‟
- display the image of a closed padlock (usually in the bottom right corner of your browser window).

Only make a payment if you can see both of these things. Never give out your bank account details, credit card number or other personal details if you are not certain that the business is a reputable trader.

II. Know the business: Only buy from websites you know and trust. Check that the company has a physical street address and landline phone number. If the company operates from overseas, you might have trouble getting a refund or repair.

III. Know the product: Make sure you check whether:

- the product is legal
- the product will work in Australia
- any warranties or guarantees offered are valid in Australia
- the product has an authorised repairer nearby.

IV. **Check the contract:** Make sure you read and understand:

- the terms and conditions of sale
- the refund policy
- the delivery details
- returns and repairs policies, including any associated costs.

V. **Check the full cost:** Be aware of the full cost of your purchase. Additional costs may include:

- currency conversion
- taxes

- postage and delivery fees
- packaging.

It might end up being cheaper to buy the product at a local shop.

VI. **Protect your privacy:** Only buy online if you are comfortable with a business's privacy policy. Do not give out information unless they require it to complete the sale. Remember, if a deal sounds too good to be true, it probably is.

VII. **Keep records**: Always write down any reference numbers and print out copies of:
the order form (both before and after you confirm the order)
receipts (can come by email or in a pop-up window).

Always make sure all charges are correct by checking the receipt against your:

- credit card statement
- merchant account statement (such as PayPal)
- bank statement.

The charges may be converted from another currency.

VIII. **Online auction sites:** Most online auction sites (like eBay) offer a dispute resolution process for buyers and sellers. This should be your first step to resolve a dispute if:

- you did not receive the items you bought
- you did not receive payment for items you sold
- you received items that were significantly different from their description.

The eBay website has an example of this facility.

Your internet browser's cache stores certain information (snapshots) of webpages you visit on your computer or mobile device so that they'll load more quickly upon future visits and while navigating through websites that use the same images on multiple pages so that you do not download the same image multiple times21. Occasionally, however your cache can prevent you from seeing updated content, or cause functional problems when stored content conflicts with live content. You can fix many browser problems simply by clearing your cache.

1. What are some essential tips for safe browsing that you learned from the reading?
2. How can you identify a secure website while browsing?
3. What are some common signs of a phishing email or website?
4. How can you protect your personal information while browsing the internet?
5. What are the potential consequences of not practicing safe browsing habits?

Activities:

1. Research and create a list of the top five antivirus software programs to protect against online threats.
2. Create a poster or infographic highlighting the dos and don'ts of safe browsing.
3. Role-play different scenarios where someone encounters a potential online threat and discuss the appropriate actions to take.

UNIT 19
WIRELESS LAN

1. What is a wireless LAN and how does it work?

2. What are some advantages of using a wireless LAN compared to a wired network?
3. Can you think of any potential disadvantages or challenges of using a wireless LAN?
4. Have you ever used a wireless LAN before? If so, what was your experience like?
5. How do you think a wireless LAN can benefit businesses or individuals in their daily lives?

The Wireless LAN or WLAN is becoming a popular way to connect devices such as computers these days. In offices and homes, WLAN has become an alternative way of communication compared to wired LAN. The convenience to connect different devices is both cost effective and easily maintainable. The Wikipedia says: “Wireless LANs have become popular in the home due to ease of installation, and the increasing to offer wireless access to their customers; often for free.”

The other factors why WLANs are becoming more acceptable are:

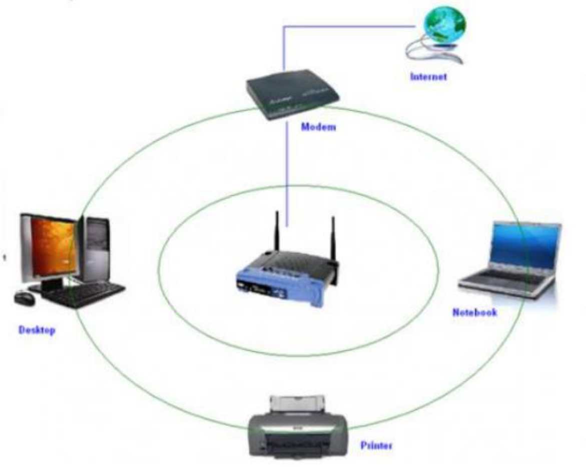
1. No need to be connected physically with each other through any medium such as cables. You can roam around freely in office premises, home or around.

2. WLANs are cost effective. Cabling all the way in the offices, hotels etc. are not needed. So it’s cheap and provides same quality of service.

3. Unreachable spots where a cable is hardly accessible, WLAN signals can reach out such as big installations like airports. Also surfing outdoors is also convenient. Just install the device called Access Points (AP) and you are done.

4. Less interruption and easy trouble shooting in case of failures as compared to cabled networks.

5. More secure as most of APs support best encryption methods which protect them from sniffing and other attacks.



A typical Wireless network

Activities:

1. Research and create a presentation comparing the advantages and disadvantages of wireless LANs versus wired networks.
2. Conduct a survey among your peers or colleagues to gather their experiences and opinions on using wireless LANs.
4. Write a short essay discussing the future trends and advancements expected in wireless LAN technology.

Create a poster or infographic illustrating the key components and working principles of a wireless LAN.

UNIT 20
SECURE WLAN. WI-FI. AT HOME

1. What is the significance of having a secure WLAN (Wireless Local Area Network) at home?
2. Can you list some potential risks and threats associated with unsecured Wi-Fi networks?
3. How familiar are you with different encryption protocols used for securing Wi-Fi connections?
4. What are some common methods attackers use to exploit vulnerabilities in home Wi-Fi networks?
5. Have you ever experienced or heard of any security issues related to home Wi-Fi networks?

Secure WLAN

- Wireless Security mainly depends on these 3 factors:
- How much is your wireless network secured in terms of encryption being used.
- Monitoring for suspicious and unusual activities.
- User awareness and education.

These are the combination of various approaches ranging from corporate to home networks. These are also for users how to remain safe while surfing.

Wi-Fi at home

Using a Wi-Fi at home is not a luxury anymore it has become a necessity. However, when the question of security comes into the scene, the first thought that would arise in my mind is how you can protect something which you cannot see, neither can you feel it? Protecting a home wireless network is altogether a different side of the coin as compared to wired networks. Most of wireless network device vendor‟s and Internet Service provider do not provide any security settings by default and leave the customer to fend for herself. So make sure, your network is secured from being maliciously used.

There is no silver bullet that will protect your wireless network infrastructure. These are, however, some countermeasures listed below that should be used in conjunction with each other to secure your wireless network to the highest level:

1. Use most secure possible encryption: The first and most necessary step- use industry standard encryptions. The old (however generally used) WEP-Wired Equivalent Privacy, has been known to be broken. Even you use complex passwords it can be broken and decrypted within minutes or hours. WEP uses 40 bit or 128 bits RC4 ciphers to encrypt the channel.

Instead use secure protocols such as WPA 2 – Wi-Fi Protected Access- 2, which uses strong 128 bits AES ciphers and is typically considered more robust encryption strategy available.

Attacks mitigated: WEP Key cracking, Sniffing, Capturing/Eavesdropping

2. Use Firewall: All the wireless routers come with built-in firewalls. Enable them with all the security features. You should block any anonymous ping requests and place restrictions on website browsing, if required. Define additional security policies and apply them.

Attacks mitigated: Fingerprinting, System compromise

3. Have a monitoring system in place: There‟s a saying- prevention is better than a cure. If you are able to detect some suspicious activities before it penetrates your network, you can block them or take precautionary measures. Deploy WIPS/WIDS for monitoring suspicious activities.

Attacks mitigated: Scanning, DoS

4. Don't use default credentials: Every wireless router comes with a set of default username/password. Sometimes, people don't change them and keep using them for long time. Username and passwords are used by computers or other devices to connect to wireless router. If any hacker is able to guess them, he can connect to your network easily. Studies show that majority of users use the same combination of username/passwords as set by manufacturers. Some default username combinations are: admin/admin, admin/password or admin/ " ".

Attacks mitigated: Unauthorized access, War driving

5. Disable Auto-connect feature: Some devices or the computers/laptops have „Let this tool manage your wireless networks‟ or „Connect automatically to available network‟. Such users having this auto-connect feature enabled are prone to Phishing attack or Rogue AP attack. Attackers keep their APs alive and kicking for such kind of unsuspecting users. They also use luring names as „HotSpot‟, „SecureConnect‟, ‟GovtNetworks‟ etc. The user will never suspect them and keep surfing the wireless network happily. Also if you have not changed the default password of your router, the attacker will try to use this feature on their machine and automatically connect using the easily guessable default passwords.

Attacks mitigated: Phishing, Sniffing, Rouge AP association

6. Don't use public Wi-Fi spots to surf sensitive websites: Free and open wireless networks available on airports, cafes, railway stations are not very secure by nature. They do not use any encryption to secure the channel between your laptop to the router. So any information which is not by default going on HTTPS from your laptop/smart phone is susceptible to sniffing and even more your session could be hijacked because the unencrypted channel may leak the active session ID used by your website. Recently to demonstrate these types of attacks one researcher developed a tool Firesheep [http://codebutler.github.com/firesheep/]. All the attacker needs to do is to just install this tool in Firefox and start sniffing the communications on a public unencrypted Wi-Fi. Some applications like Facebook encrypts the login page [HTTPS] but internal pages are served on unencrypted [HTTP] channel so your session ID can be leaked.

Attacks mitigated: Sniffing, Session Hijacking

7. Change the default SSID: Although this will not prevent hackers breaking into a network, using a default SSID acts as an indication that the user is careless. So he may be an obvious target to explore further to see if he still uses the default passwords as well?

Attacks mitigated: War driving

8. Restrict access by assigning static IP addresses and MAC filtering: Disable automatic IP assigning feature and use private static IPs to the legitimate devices you want to connect. This will help you in blocking unwanted devices from being connected to your network. Also, enable MAC filtering- router remembers MAC of each and every device connected to it and saves it as list. You can use this facility to restrict access. Only a set of trusted devices can be allowed to connect. However MAC spoofing is still possible but it raises an extra bar for your wireless network. **Turn off your router when not in use:** Last but not least, a little obvious, but it will save your network from all the attacks for that time period.

1. How does securing your home Wi-Fi network contribute to overall online safety?
2. What steps can you take to enhance the security of your Wi-Fi password?
3. How do different encryption standards contribute to the security of a Wi-Fi network?
4. What measures can be implemented to safeguard against unauthorized access to your home network?

5. How can users stay informed about the latest security threats and updates for their Wi-Fi routers?

Activities:

1. Conduct a security audit of your own home Wi-Fi network, implementing any recommended changes.
2. Develop a step-by-step guide for securing a home Wi-Fi network, suitable for non-technical users.
3. Create a presentation or infographic highlighting the importance of securing home Wi-Fi networks.

Conduct a simulated phishing exercise to test the email security awareness of yourself or your team.
Create an infographic or poster highlighting the dos and don'ts of email security for general users.
Write a reflective essay discussing the evolving landscape of email security and its implications for individuals and businesses.

RECOMENDED VIDEOS

https://www.youtube.com/watch?v=_WHynHcXm7c
https://www.youtube.com/watch?v=Jmszt__J204
https://www.youtube.com/watch?v=aktovPyT0iM
https://www.youtube.com/watch?v=CStMHLQWa_8
https://www.youtube.com/watch?v=a9q-tDRCTtc
https://www.youtube.com/watch?v=xex1h93fnI8
https://www.youtube.com/watch?v=a9q-tDRCTtc

MODULE 6
EMAIL AND SOCIAL MEDIA SECURITY

UNIT 21

1. What does safe browsing mean to you, and why is it important, especially on social networking sites?
2. Can you identify common risks and challenges associated with online activities, particularly on social media?
3. How do you currently manage your privacy settings on social networking sites?
4. What are your experiences or concerns regarding online security and personal information protection?
5. Have you ever encountered phishing attempts or scams while using social media platforms?

SAFE BROWSING

Online communities have existed since the invention of the internet. First there were bulletin boards and email lists, which gave people around the world opportunities to connect, to communicate and to share information about particular subjects. Today, social networking websites have greatly expanded the range of possible interactions, allowing you to share messages, pictures, files and even up-to-the-minute information about what you are doing and where you are. These functions are not new or unique – any of these actions can also be performed via the internet without joining a social networking site.

Although these networks can be very useful, and promote social interaction both online and offline, when using them you may be making information available to people who want to abuse it. Think of a social networking site as being like a huge party. There are people there that you know, as well as some that you don't know at all. Imagine walking through the party with all your personal details, and up-to-the-minute accounts of what you are thinking, written on a big sign stuck on your back so that everyone can read it without you even knowing. Do you really want everyone to know all about you?

Remember that social networking sites are owned by private businesses, and that they make their money by collecting data about individuals and selling that data on, particularly to third party advertisers. When you enter a social networking site, you are leaving the freedoms of the internet behind and are entering a network that is governed and ruled by the owners of the site. Privacy settings are only meant to protect you from other members of the social network, but they do not shield your data from the owners of the service. Essentially you are giving all your data over to the owners and trusting them with it.

If you work with sensitive information and topics, and are interested in using social networking services, it is important to be very aware of the privacy and security issues that they raise. Human rights advocates are particularly vulnerable to the dangers of social networking sites and need to be extremely careful about the information they reveal about themselves AND about the people they work with.

Before you use any social networking site it is important to understand how they make you vulnerable, and then take steps to protect yourself and the people you work with. This guide will help you understand the security implications of using social networking sites.

General Tips on using Social Networking platforms safely

Social media have become an evident part of our life. We share out updates with our friends, family and anyone who is concerned using social media. But the hackers can use this information to steal sensitive data and hack your account. Given below are some of the general tips on using social media.

Always ask the questions:

- Who can access the information I am putting online?
- Who controls and owns the information I put into a social networking site?
- What information about me are my contacts passing on to other people?
- Will my contacts mind if I share information about them with other people?
- Do I trust everyone with whom I'm connected?

Always make sure you use **secure passwords** to access social networks. If anyone else does get into your account, they are gaining access to a lot of information about you and about anyone else you are connected to via that social network. Change your passwords regularly as a matter of routine.

Make sure you understand the default **privacy settings** offered by the social networking site, and how to change them.

Consider using **separate accounts/identities**, or maybe different pseudonyms, for different campaigns and activities. Remember that the key to using a network safely is being able to trust its members. Separate accounts may be a good way to ensure that such trust is possible.

Be careful when accessing your social network account in public internet spaces. **Delete your password and browsing history** when using a browser on a public machine.

Access social networking sites using https:// to safeguard your username, password and other information you post. Using https:// rather than http:// adds another layer of security by encrypting the traffic from your browser to your social networking site.

Be careful about putting too much information into **your status updates** – even if you trust the people in your networks. It is easy for someone to copy your information.

Most social networks allow you to integrate information with other social networks. For example you can post an update on your Twitter account and have it automatically posted on your Facebook account as well. Be particularly **careful when integrating your social network accounts**! You may be anonymous on one site, but exposed when using another.

Be cautious about how safe your content is on a social networking site. **Never rely on a social networking site as a primary host for your content** or information. It is very easy for governments to block access to a social networking site within their boundaries if they suddenly find its content objectionable. The administrators of a social networking site may also decide to remove objectionable content themselves, rather than face censorship within a particular country.

Posting Personal Details

Social networking sites ask you for a good deal of data about yourself to make it easier for other users to find and connect to you. Perhaps the biggest vulnerability this creates for users of these sites is the possibility of identity fraud, which is increasingly common. In addition, the more information about yourself you reveal online, the easier it becomes for the authorities to identify you and monitor your activities. The online activities of diaspora activists from some countries have led to the targeting of their family members by the authorities in their homelands.

Ask yourself: is it necessary to post the following information online?

- birth dates
- contact phone numbers
- addresses
- details of family members
- sexual orientation
- education and employment history

Friends, Followers and Contacts

The first thing you will do after filling in your personal details with any social networking application is establish connections to other people. Presumably these contacts are people you know and trust – but you may also be connecting to an online community of like-minded individuals that you have never met. The most important thing to understand is what information you are allowing this online community to have.

When using a social network account such as Facebook, where a lot of information about yourself is held, consider only connecting to people you know and trust not to misuse the information you post.

Status Updates

On Twitter and Facebook and similar networks, the status update answers the questions: What am I doing right now? What's happening? The most important thing to understand about the status update is who can actually see it. The default setting for the status update on most social networking applications is that anyone on the internet can see it. If you only want your contacts to see the updates, you need to tell the social networking application to keep your updates hidden from everyone else.

To do this in Twitter, look for “Protect Your Tweets”. In Facebook, change your settings to share your updates with “Friends Only”. Even if you switch to those settings, consider how easy it is for your information to be reposted by followers and friends. Agree with your network of friends on a common approach to passing on the information posted in your social networking accounts. You should also think about what you may be revealing about your friends that they may not want other people to know; it's important to be sensitive about this, and to ask others to be sensitive about what they reveal about you.

There have been many incidents in which information included in status updates has been used against people. Teachers in the US have been fired after posting updates about how they felt about their students; other employees have lost their jobs for posting about their employers. This is something that nearly everyone needs to be careful about.

Sharing Online Content It's easy to share a link to a website and get your friend's attention. But who else will be paying attention, and what kind of reaction will they have? If you share (or "like") a site that opposes some position taken by your government, for example, agents of that government very might well take an interest and target you for additional surveillance or direct persecution.

If you want your contacts (and of course the administrators of the social networking platform you use) to be the only ones who can see the things you share or mark as interesting, be sure to check your privacy settings. Most social networking sites will display your location if that data is available. This function is generally provided when you use a GPS-enabled phone to interact with a social network, but don't assume that it's not possible if you aren't connecting from a mobile. The network your computer is connected to may also provide location data. The way to be safest about it is to double-check your settings.

Be particularly mindful of location settings on photo and video sharing sites. Don't just assume that they're not sharing your location: double-check your settings to be sure. Most social networking sites will display your location if that data is available. This function is generally provided when you use a GPS-enabled phone to interact with a social network, but don't assume that it's not possible if you aren't connecting from a mobile. The network your computer is connected to may also provide location data. The way to be safest about it is to double-check your settings.

Be particularly mindful of location settings on photo and video sharing sites. Don't just assume that they're not sharing your location: double-check your settings to be sure.

Most social networking sites will **display your location** if that data is available. This function is generally provided when you use a GPS-enabled phone to interact with a social network, but don't assume that it's not possible if you aren't connecting from a mobile. The network your computer is connected to may also provide location data. The way to be safest about it is to double-check your settings.

Be particularly mindful of location settings on photo and video sharing sites. Don't just assume that they're not sharing your location: double-check your settings to be sure.

Sharing Videos and Photos

Photos and videos can reveal people's identities very easily. It's important that you have the consent of the subject/s of any photo or video that you post. If you are posting an image of someone else, be aware of how you may be compromising their privacy. Never post a video or photo of anyone without getting their consent first.

Photos and videos can also reveal a lot of information unintentionally. Many cameras will embed hidden data (metadata tags), that reveal the date, time and location of the photo, camera type, etc. Photo and video sharing sites may publish this information when you upload content to their sites.

Instant Chats

Many social networking sites have tools that allow you to have discussions with your friends in real time. These operate like Instant Messaging and are one of the most insecure ways to communicate on the internet, both because they may reveal who you are communicating with, and what you are communicating about.

Connecting to the site via https is a minimum requirement for secure chatting, but even this is not always a guarantee that your chat is using a secure connection. For example, Facebook chat uses a different channel to HTTPS (and is more prone to exposure).

It is more secure to use a specific application for your chats, such as Pidgin with an Off-the-record plugin, which uses encryption. Read the 'Pidgin – secure instant messaging' hands-on guide.

Joining and Creating Groups, Events and Communities What information are you giving to people if you join a group or community? What does it say about you? Alternatively, what are people announcing to the world if they join a group or community that you have created? How are you putting people at risk?

When you join a community or group online it is revealing something about you to others. On the whole, people may assume that you support or agree with what the group is saying or doing, which could make you vulnerable if you are seen to align yourself with particular political groups, for example. Also if you join a group with a large number of members that you don't know, then this can compromise any privacy or security settings that you have applied to your account, so think about what information you are giving away before joining. Are you using your photo and real name so strangers can identify you?

Alternatively, if you set up a group and people choose to join it, what are they announcing to the world by doing so? For example, perhaps it is a gay and lesbian support group that you have set up to help people, but by joining it people are openly identifying themselves as gay or gay-friendly, which could bring about dangers for them in the real world.

1. How can implementing strong privacy settings on social media contribute to a safer online experience?
2. What are some red flags to look for when identifying potential phishing or scam attempts on social networking sites?
3. How do social media platforms address user concerns regarding data privacy and security?
4. In what ways can users balance sharing personal information on social media while maintaining a level of security?
5. What steps can be taken to educate friends and family about safe browsing habits on social networking sites?

Activities

1. Research and compile a list of common online threats that users might encounter on social networking sites.
2. Explore the privacy settings of popular social media platforms and understand how to customize them for enhanced security.
3. Investigate the concept of two-factor authentication and its implementation on different social networking sites.
4. Look into recent cybersecurity incidents related to social media and their impact on users.
5. Review guidelines and policies provided by social media platforms regarding safe usage.

UNIT 22
E-MAIL SECURITY

1. Why is email security important in today's digital landscape?
2. What are the common threats and risks associated with email communication?
3. How do phishing attacks exploit vulnerabilities in email security?
4. Can you list some best practices for creating strong and secure email passwords?
5. What role do encryption and digital signatures play in email security?

Reading Tasks:

1. Take notes on the key features of a secure email protocol.
2. Identify the steps involved in recognizing and avoiding phishing emails.
3. Look for information on how to configure email clients for enhanced security.
4. Explore the role of secure email gateways in protecting against email-based threats.
5. Pay attention to case studies or examples that highlight the consequences of email security breaches.

Don't open email attachments that you are not expecting, or which have come from someone you do not know. When you open such an email, make sure that your anti-virus software is up-to-date and pay close attention to any warnings from your browser or email program.

You can use anonymity software which can help you hide your chosen email service from anyone who might be monitoring your internet connection. A good, free software program to do this is Tor (Find out more about Tor browser using Google). If you don't want to give away information about your identity through your email, do not register a username or 'Full Name' that is related to your personal or professional life.

You can avoid getting spam (unwanted or junk email) by guarding your email address and distributing it sparingly. Also, never open or reply to any emails you consider to be spam, because spammers will take this as a proof of the legitimacy of the address and will just send you more spam. Consider using a spam filter, but remember that it needs to be monitored as it may mistake a genuine email for spam.

You should try to avoid your emails being mistaken for spam by the recipients. Spam filters will block messages with certain words in the subject heading. It is worth scanning your spam folder for subject lines that are getting blocked.

Beware of email scams. Many scam emails pretend to come from a bank, Ebay, Paypal, or other online shops. If you get an email telling you that your account is in danger of being shut down, or that you need to take immediate action by updating your account information, be very suspicious: these messages are usually scams. Another frequent scam has you receiving an email from someone you know which says that they have had an emergency and asks you to send them money. This person's email account is likely to have been compromised by a scammer.

Pay close attention if your browser suddenly gives you messages about invalid security certificates when you attempt to access a secure webmail account. It could mean that someone is tampering with the communication between your computer and the server in order to intercept your messages.

Post-Reading Questions:

1. How can individuals differentiate between a legitimate email and a phishing attempt?
2. What measures can be taken to secure email communication within an organization?
3. How does end-to-end encryption contribute to the confidentiality of email content?

4. In what ways can users enhance the security of their email accounts through regular maintenance?
5. How can organizations balance convenience and security when implementing email security measures?

Activities

1. What are anonymous accounts? Find some browsers which supports anonymity.
2. After going through the above section, find out whether you were following the above safe practices while handling your social medial account? Find the gaps?
3. Based on the above recommendations, adjust your social media account settings.
4. Conduct a simulated phishing exercise to test the email security awareness of yourself or your team.
5. Write a reflective essay discussing the evolving landscape of email security and its implications for individuals and businesses.

RECOMENDED VIDEOS

https://www.youtube.com/watch?v=EFHfg1bfgVc
https://www.youtube.com/watch?v=tkgLHoaFeFk
https://www.youtube.com/watch?v=QUyla_nMJis
https://www.youtube.com/watch?v=-CeuqCHX7tE
https://www.youtube.com/watch?v=xCHTmzfsGmI

UNIT 23

SMARTPHONE SECURITY

PURSES, WALLETS, SMARTPHONES

1. Why is smartphone security important, especially in the context of purses and wallets?
2. What are the common threats and risks associated with carrying smartphones in purses or wallets?
3. How can smartphone features like biometric authentication enhance security?
4. Are you familiar with the methods used by thieves to target smartphones in public spaces?
5. What measures can individuals take to protect their smartphones from unauthorized access and theft?

Pre-Reading Tasks:

1. Research and compile a list of security features available on modern smartphones.
2. Explore statistics and case studies related to smartphone theft and its impact on personal information.
3. Investigate the role of smartphone security in preventing identity theft and financial fraud.
4. Look into the effectiveness of various smartphone security apps and tools.
5. Familiarize yourself with best practices for securing smartphones in public places.

Advances in technology now mean that mobile phones can provide services and features similar to desktop or laptop computers. These Smartphones offer many new ways to communicate and capture and disseminate media. To provide these new functionalities, the smartphones not only use the mobile network, but also connect to the internet either via a wi-fi connection (similar to a laptop at an internet cafe) or via data connections through the mobile network operator.

So while you can, of course, make phone calls with a smartphone, it is better to view smartphones as small computing devices. This means that the other material in this toolkit is relevant to your use of your smartphone as well as your computer.

Smartphones usually support a wide range of functionality – web browsing, email, voice and instant messaging over the internet, capturing, storing and transmitting audio, videos and photos, enabling social networking, multi-user games, banking and many other activities. However, many of these tools and features introduce new security issues, or increase existing risks. For instance, some smartphones have built-in geo-location (GPS) functionality, which means they can provide your precise location to your mobile network operator by default, and to many applications you use on your phone (such as social networking, mapping, browsing and other applications). As mentioned before, mobile phones already relay your location information to your mobile network operator (as part of the normal functions of the phone). However, the additional GPS functionality not only increases the precision of your location information, it also increases the amount of places where this information might be distributed.

It's worth reviewing all the risks associated with mobile phones discussed in our guide How to use mobile phones as securely as possible as all of them are also relevant to smartphone use. That guide also covers issues of eavesdropping, interception of SMS or phone calls, SIM card related issues, and best practices.

Purses, Wallets, Smartphones

We have an intuitive understanding of the value of keeping our purse or wallet safe, because so much sensitive information is stored in them, and losing them will compromise our privacy and safety. People are less aware of the amount of personal information being carried in their smartphones, and consider losing a phone a nuisance rather than a risk. If you also think that a smartphone is a computing device which is always connected to a network and is continually carried around, it also highlights the important difference between a holder of discrete, passive information (like a wallet), and an active and interactive item like a smartphone.

A simple exercise can help illustrate this:

Empty the content of your wallet or purse, and take account of sensitive items. Typically you may find: - Pictures of loved ones (~5 pictures) - Identification cards (driver's license, membership cards, social security cards) - Insurance and health information (~2 cards) - Money (~5 bills) - Credit/Debit cards (~3 cards)

Now, examine the contents of your smartphone. A typical smartphone user may find some of the above in higher quantities, and in some cases much more valuable items:

- Pictures of loved ones (~100 pictures)
- Email applications and their passwords
- Emails (~500 emails)
- Videos (~50 videos)
- Social networking applications and their passwords
- Banking applications (with access to the bank accounts)
- Sensitive documents
- Sensitive communication records
- A live connection to your sensitive information

The more you use smartphones, the more you need to become aware of the associated risks and take appropriate precautions. Smartphones are powerful amplifiers and distributors of your personal data. They are designed to provide as much connectivity as possible and to link to social networking services by default. This is because your personal data is valuable information that can be aggregated, searched and sold.

It can be disastrous if you lose your phone without having a backup of your most important data (such as your contacts) in a secure location. Besides backing up your data, make sure you also know how to restore the data. Keep a hard copy of the steps you need to take so you can do it quickly in an emergency.

In this chapter we'll start by introducing some smartphone basics – a description of various platforms and some basic setup procedures for securing your information and communication. The remaining parts of this chapter will cover specific precautions related to common uses of smartphones.

Platforms, Setup and Installation

Platforms and Operating Systems

At the time of writing, the most common smartphones in use are Apple's iPhone and Google's Android, followed by Blackberry and Windows phones. The key difference between Android and other operating systems is that Android is, mostly, an Open Source (FOSS) system, which allows the operating system to be audited independently to verify if it properly protects users' information and communication. It also facilitates development of security applications for this platform. Many security-aware programmers develop Android applications with user safety and security in mind. Some of these will be highlighted later in this chapter.

Regardless what type of smartphone you are using, there are issues that you should be aware of when you use a phone which connects to the internet and comes with features such as GPS or wireless networking capacities. In this chapter we focus on devices with the Android platform, because, as mentioned above, it's easier to secure data and communications. Nonetheless, basic setup guides and some applications for devices other than Android phones are provided, too. Blackberry phones have been presented as “secure” messaging and email devices. This is because messages and emails are securely channeled through Blackberry servers, out of the reach of potential eavesdroppers. Unfortunately, more and more governments are demanding access to these communications, citing need for guarding against potential terrorism and organised crime. India, United Arab Emirates, Saudi Arabia, Indonesia and Lebanon are examples of governments which have scrutinized the use of Blackberry devices and demanded access to user data in their countries.

Feature Phones

Another category of mobiles are often called 'feature phones'. Recently, feature phones have increased their functionalities to include those of some smartphones. But generally, feature phones' operating systems are less accessible, therefore there are limited opportunities for security applications or improvements. We do not specifically address feature phones, although many measures discussed here make sense for feature phones too.

Branded and locked smartphones

Smartphones are usually sold branded or locked. Locking smartphones means that the device can only be operated with one carrier, whose SIM card is the only one that will work in the device. Mobile network operators usually brand a phone by installing their own firmware or software. They may also disable some functionalities or add others. Branding is a means for companies to increase revenue by channeling your smartphone use, often also collecting data about how you are using the phone or by enabling remote access to your smartphone.

For these reasons, we recommend that you buy an unbranded smartphone if you can. A locked phone poses a higher risk since all your data is routed through one carrier, which centralizes your data streams and makes it impossible to change SIM cards to disseminate the data over different carriers. If your phone is locked, ask someone you trust about unlocking it.

General Setup

Smartphones have many settings which control the security of the device. It is important to pay attention to how your smartphone is set up. In the Hands-on Guides below we will alert you to certain smartphone security settings that are available but not active by default, as well as those which are active by default and make your phone vulnerable.

Installing and updating applications

The usual way to install new software on your smartphone is to use the iPhone Appstore or Google Play store, log in with your user credentials, and download and install a desired application. By logging-in you associate your usage of the online store with the logged-in user account. The owners of the application store keep records of this user's browsing history and application choices.

The applications which are offered in the official online store are, supposedly, verified by store owners (Google or Apple), but in reality this provides weak protection against what applications will do after being installed on your phone. For example, some applications may copy and send out your address book after you install them on your phone. On Android phones each application needs to request, during the installation process, what it will be permitted to do when it is in use. You should pay close attention to what permissions are requested, and if these permissions make sense for the function of the app you are installing. For example, if you are considering a "news reader" application and you find out that it requests the rights to send your contacts over a mobile data connection to a third party, you should look for alternative applications with appropriate access and rights.)ites. Some users may want to consider these alternative sites to minimize online contact with Google. One of the alternative store is F-Droid ('Free Droid'), which only provides FOSS applications. However please remember that you should trust the site before you download any apps from it. For inexperienced users we recommend that you use Google Play store.

If you don't want to (or are unable to) go online to access apps, you can transfer apps from someone else's phone by sending .apk files (short for 'android application package') via bluetooth. Alternetively you could download the .apk file to your device's Micro SD card or use a usb cable to move it there from a PC. When you have received the file, simply long tap on the filename and you will be prompted to install it. (Note: be especially careful while using Bluetooth.

Communicating Securely (Through Voice and Messages) with a Smartphone

Basic telephony

In order to send or receive any calls or communications to your phone, the signal towers nearest you are alerted by your phone of its presence25. As a result of those alerts and communications the network service provider knows the precise geographic location of your mobile phone at any given time.

About Anonymity: If you are conducting sensitive phone conversations or sending sensitive SMS messages, beware of the above tracking 'feature' of all mobile phones. Consider adopting the steps below:

- Make calls from different locations each time, and choose locations that are not associated with you.
- Keep your phone turned off, with the battery disconnected, go to the chosen location, switch your phone on, communicate, switch the phone off and disconnect the battery. Doing this habitually, each time you have to make a call, will mean that the network cannot track your movements.

- Change phones and SIM cards often. Rotate them between friends or the second-hand market.
- Use unregistered pre-paid SIM cards if this is possible in your area. Avoid paying for a phone or SIM cards using a credit card, which will also create a connection between these items and you.

Sending Messages Securely

You should use precautions when sending SMS and using instant messaging or chatting on your smartphone.

SMS

SMS communication is insecure by default. Anyone with access to a mobile telecommunication network can intercept these messages easily and this is an everyday occurrence in many situations. Don't rely on sending unsecured SMS messages in critical situations. There is also no way of authenticating SMS messages, so it is impossible to know if the contents of a message was changed during delivery or if the sender of the message really is the person they claim to be.

Secure Chat Instant messaging and chatting on your phone can produce a lot of information that is at risk of interception. These conversations might be used against you by adversaries at a later date. You should therefore be extremely wary about what you reveal when you are writing on your phone while instant messaging and chatting. There are ways to chat and instant message securely. The best way is to use end-to-end encryption, as this will enable you to make sure the person on the other end is who you want. We recommend ChatSecure as a secure text chat application for the Android phones. ChatSecure offers easy and strong encryption for your chats with Off-the-Record Messaging protocol. This encryption provides both authenticity (you can verify that you are chatting with the right person) and the independent security of each session so that even if the encryption of one chat session is compromised, other past and future sessions will remain secure. ChatSecure has been designed to work together with Orbot, so your chat messages can be routed through the Tor anonymizing network. This makes it very hard to trace it or even find out that it happened. For iPhones, the ChatSecure client provides the same features, although it is not easy to use it with the Tor network. Whichever application you will use always consider which account you use to chat from. For example when you use Google Talk, your credentials and time of your chatting session are known to Google. Also agree with your conversation partners on not saving chat histories, especially if they aren't encrypted.

1. How can securing your smartphone contribute to overall personal security?
2. What are the potential consequences of losing an unprotected smartphone containing sensitive information?
3. How do biometric authentication methods enhance smartphone security compared to traditional PINs or passwords?
4. What steps can individuals take to minimize the risk of smartphone theft in public places?
5. How important is it to regularly update the security features and software on your smartphone?

Activities:

1. Conduct a security assessment of your own smartphone, implementing any recommended changes.
2. Develop a guide or checklist for others on securing their smartphones in purses and wallets.
3. Create a public service announcement or infographic on the importance of smartphone security.

UNIT 24
SECURE COMMUNIATION

1. Why is secure communication important in today's digital age?
2. What are the potential risks and consequences of insecure communication?
3. How do encryption and decryption play a role in ensuring secure communication?
4. Can you list different methods or technologies used for securing communication channels?
5. How do organizations and individuals benefit from implementing secure communication practices?

Pre-Reading Tasks:

1. Research and compile a list of common cybersecurity threats that can compromise communication security.
2. Explore the history and evolution of encryption techniques in the context of secure communication.
3. Investigate the role of public-key infrastructure (PKI) in ensuring the authenticity and integrity of communication.
4. Look into the differences between symmetric and asymmetric encryption algorithms.
5. Familiarize yourself with secure communication protocols such as SSL/TLS and their applications.

Storing Information on your Smartphone Smartphones come with large data storage capacities. Unfortunately, the data stored on your device can be easily accessible by third parties, either remotely or with physical access to the phone. You can take steps to encrypt any sensitive information on your phone by using specific tools.

Date Encryption Tools The Android Privacy Guard (APG) allows OpenGPG encryption for files and emails. It can be used to keep your files and documents safe on your phone, as well when emailing.

Recording Password Securely You can keep all your needed passwords in one secure, encrypted file by using Keepass. You will only need to remember one master password to access all the others. With Keepass you can use very strong passwords for each account you have, as Keepass will remember them for you, and it also comes with a password generator to create new passwords. You can synchronise Keepass password databases between your phone and your computer. We recommned that you synchronise only those passwords that you will actually use on your mobile phone. You can create a separate smaller password database on the computer and syncronise this one instead of coping an entire database with all the passwords that you use to your smartphone. Also, since all the passwords are protected by your master password, it is vital to use very strong password for your Keepass database.

Sending Email from your Smartphone In this section we will briefly discuss the use of email on smartphones. In the first instance, consider if you really need to use your smartphone to access your email. Securing a computer and its content is generally simpler than doing so for a mobile device such as a smartphone. A smartphone is more susceptible to theft, monitoring and intrusion. If it is absolutely vital that you access your email on your smartphone, there are actions you can take to minimize the risks.

Do not rely on smartphone as your primary means for accessing your email. Downloading (and removing) emails from an email server and storing them only on your smartphone is not advised. You can set up your email application to use only copies of emails.

If you use email encryption with some of your contacts, consider installing it on your smartphone, too. The additional benefit is that encrypted emails will remain secret if the phone falls into wrong hands. Storing your private encryption key on your mobile device may seem risky. But the benefit of being able to send and store emails securely encrypted on the mobile device might outweigh the risks.

Consider creating a mobile-only encrytpion key-pair (using APG) for your use on your smartphone, so you do not copy your encryption private key from your computer to the mobile device. Note that this requires that you ask people you communicate with to also encrypt emails using your mobile-only encryption key.

Capturing Media with your Smartphone Capturing pictures, video or audio with your Smartphone can be a powerful means to document and share important events. However, it is important to be careful and respectful of privacy and safety of those pictured, filmed or recorded. For example, if you take photos or record video or audio of an important event, it might be dangerous to you or to those who appear in the recordings, if your phone fell into the wrong hands. In this case, these suggestions may be helpful:

- Have a mechanism to securely upload recorded media files to protected online location and remove them from the phone instantly (or as soon as you can) after recording.
- Use tools to blur the faces of those appearing in the images or videos or distort the voices of audio or videos recordings and store only blurred and distorted copies of media files on your mobile device.
- Protect or remove meta information about time and place within the media files. Guardian Project has created a FOSS app called ObscuraCam to detect faces on photos and blur them. You can choose the blurring mode and what to blur, of course. Obscuracam also deletes the original photos and if you have set up a server to upload the captured media, it provides easy functionality to upload it.

Accessing the Internet Securely from your Smartphone As discussed in our guide How to keep your Internet communication private and our guide How to remain anonymous and bypass censorship on the Internet, access to content on the Internet, or publishing material online such as photos or videos, leaves many traces of who and where you are and what you are doing. This may put you at risk. Using your smartphone to communicate with the Internet magnifies this risk.

Through Wi-Fi or Mobile Data Smartphones allow you to control how you access the Internet: via a wireless connection provided by an access point (such as an internet cafe), or via a mobile data connection, such as GPRS, EDGE, or UMTS provided by your mobile network operator. Using a WiFi connection reduces the traces of data you may be leaving with your mobile phone service provider (by not having it connected with your mobile phone subscription). However, sometimes a mobile data connection is the only way to get online. Unfortunately, mobile data connection protocols (like EDGE or UMTS) are not open standards. Independent developers and security engineers cannot examine these protocols to see how they are being implemented by mobile data carriers. In some countries mobile access providers operate under different legislation than internet service providers, which can result in more direct surveillance by governments and carriers.

Regardless of which path you take for your digital communications with a smartphone, you can reduce your risks of data exposure through the use of anonymising and encryption tools.

Anonymity of your Smartphone To access content online anonymously, you can use an Android app called Orbot. Orbot channels your internet communication through Tor's anonymity network. Another app, Orweb, is a web browser that has privacy enhancing features like using proxies and not keeping a local browsing history. Orbot and Orweb together circumvent web filters and firewalls, and offer anonymous browsing.

Proxies The mobile version of Firefox – Firefox mobile can be equipped with proxy add-ons, which direct your traffic to a proxy server. From there your traffic goes to the site you are requesting. This is helpful in cases of censorship, but still may reveal your requests unless the connection from your client to the proxy is encrypted. We recommend the Proxy Mobile add-on (also from Guardian Project, which makes proxying with Firefox easy. Is also the only way to channel Firefox mobile communications to Orbot and use the Tor network.

Advanced Smart Phone Security

Get Full Access to your Smartphone Most Smartphones are capable of more than their installed operating system, manufacturers' software (firmware), or the mobile operators' programmes allow. Conversely, some functionalities are 'locked in' so the user is not capable of controlling or altering these functions, and they remain out of reach. In most cases those functionalities are unnecessary for smartphone users. There are however, some applications and functionalities that can enhance the security of data and communications on a smartphone. Also there are some other existing functionalities that can be removed to avoid security risks. For this, and other reasons, some smartphone users choose to manipulate the various software and programs running the smartphone in order to gain appropriate privileges to allow them to install enhanced functionalities, or remove or reduce other ones. The process of overcoming the limits imposed by mobile carriers, or manufacturers of operating systems on a smartphone is called rooting (in case of Android devices), or jailbreaking (in case of iOS devices, like iPhone or iPad). Typically, successful rooting or jailbreaking will result in your having all the privileges needed to install and use additional applications, make modifications to otherwise locked-down configurations, and total control over data storage and memory of the smartphone. WARNING: Rooting or jailbreaking may not be a reversible process, and it requires experience with software installation and configuration. Consider the following:

- There is a risk of making your smartphone permanently inoperable, or 'bricking' it (i.e. turning it into a 'brick').
- The manufacturer or mobile carrier warranty may be voided.
- In some places, this process maybe illegal. But if you are careful, a rooted device is a straightforward way to gain more control over your smartphone to make it much more secure.

Alternative Firmwares Firmware refers to programes that are closely related to the particular device. They are in cooperation with the device's operating system and are responsible for basic operations of the hardware of your smartphone, such as the speaker, microphone, cameras, touchscreen, memory, keys, antennas, etc. If you have an Android device, you might consider installing a firmware alternative to further enhance your control of the phone. Note that in order to install alternative firmware, you need to root your phone. An example of an alternative firmware for an Android phone is Cyanogenmod which, for example, allows you to uninstall applications from the system level of your phone (i.e. those installed by the phone's manufacturer or your mobile network operator). By doing so, you can reduce the number of ways in which your device can be monitored, such as data that is sent to your service provider without your knowledge. In addition, Cyanogenmod ships by default with an OpenVPN application, which can be tedious to install otherwise. VPN (Virtual Private Network) is one of the ways to securely proxy your internet communication (see below). Cyanogenmod also offers an Incognito browsing mode in which history of your communication is not recorded on your smartphone.

Full Device Encryption If your phone is rooted you may consider encrypting it's entire data storage or creating a volume on the Smartphone to protect some information on the phone. Luks Manager allows easy, on-the-fly strong encryption of volumes with an user-friendly interface. We highly recommend that you install this tool before you start storing important data on your Android device and use the Encrypted Volumes that the Luks Manager provides to store all your data.

Virtual Private Network(VPN) Security A VPN provides an encrypted tunnel through the internet between your device and a VPN server. This is called a tunnel, because unlike other encrypted traffic, like https, it hides all services, protocols, and contents. A VPN connection is set up once, and only terminates when you decide. Note that since all your traffic goes through the proxy or VPN server, an intermediary only needs to have access to the proxy to analyze your activities. Therefore it is important to carefully choose amongst proxy services and VPN services. It is also advisable to use different proxies and/or VPNs since distributing your data streams reduces the impact of a compromised service.

1. How does secure communication contribute to the protection of sensitive information and privacy?
2. What are the trade-offs or challenges associated with implementing strong encryption in communication systems?
3. How can individuals ensure secure communication in their day-to-day digital interactions?
4. In what ways can secure communication technologies adapt to evolving cybersecurity threats?
5. How does the balance between security and usability impact the adoption of secure communication practices?

Activities:

1. Develop a guide or checklist for individuals and organizations to follow in order to achieve secure communication.
2. Create a presentation outlining the importance of secure communication in a specific industry or sector.
3. Role-play scenarios where participants practice implementing secure communication measures in various contexts.

RECOMENDED VIDEOS

https://www.youtube.com/watch?v=KCObM4PBTVk
https://www.youtube.com/watch?v=V8bCyRCqK0k

MODULE 7
CYBERSECURITY COLD WAR

UNIT 25

1. What is hacktivism, and how does it differ from traditional hacking or activism?
2. Can you provide examples of notable hacktivist groups and their motivations?
3. What are the potential ethical concerns associated with hacktivism?
4. How does hacktivism impact cybersecurity on a global scale?
5. Are there legal implications for individuals engaging in hacktivism?

Pre-Reading Tasks:

1. Research and compile a list of major hacktivist incidents and their outcomes.
2. Explore the history and evolution of hacktivism as a form of digital activism.
3. Investigate the methods and techniques commonly used by hacktivist groups.
4. Examine case studies where hacktivism has influenced political or social change.
5. Look into the stance of governments and cybersecurity organizations on hacktivism.

There is a war going on right now. Each day, hundreds of millions of attempts are made to gain unauthorized access into digital devices and accounts.Some of these attempts are opportunist, some are targeted but all of them have the purpose of creating political or financial gain over the rightful organizations and people that these assets belong to.

The increase in the number of attempts and the cost of the consequences is botha cause of greatconcern and a driver to improve the security and defenses. As with any war, strategists need to know their enemy. Who are the organizations and people that want to target our digital landscape, what are their goals, how sophisticated are they and how do they operate?The cyber attackers can broadly be considered to consist of 8 different groups.

1. Nation States
2. Terrorist Groups
3. Organized Criminal Groups
4. Hacktivist Communities (Hacktivism)
5. Skilled Professional Hackers
6. Disaffected or Opportunist Insiders
7. Amateur Hackers & Journalists
8. Anyone

Every organizations threatscape is different. According to what you or yourorganization does, you can become more or less attractive to one or more of these groups.

hacktivism – an amalgamation of hacker and activism. Describes any group that uses subversive techniques through digital or electronic means to promotna political agenda. See also hacktivist.

hacktivist – an amalgamation of the words hacker and activist. Describes any individual who operates either independently or as part of a group to use subversive techniques through digital or electronic means to serve a political or social cause that they may see as serving a broader interest.

threatscape –a term that amalgamates threat and landscape. An umbrella term to describe the overall, expected methods (vectors) and types of cyber attackers that an organization or individual might expect to be attacked through or by.

HACKWITISM

Hacktivism, a blend of the words “hacking” and “activism”, uses hacking techniques for political or social causes. It’s a form of civil disobedience, leveraging digital tools to protest or take direct action.

Hacktivists, the individuals involved in hacktivism, often work to promote issues related to freedom of speech, human rights, or information ethics. Hacktivism might employ methods such as website defacement or denial-of-service (DoS) attacks to make statements or disrupt the operations of the organization(s) they oppose. While the ethical implications are a topic of debate, hacktivism is a new frontier in activism, showing digital technologies’ impact on society.

Types of Hacktivism

There are various forms of hacktivism, each with distinct methods and objectives. Let’s explore some of them:

1. Website defacement: This form of hacktivism involves altering the appearance of a website to make a political statement or protest. It’s like digital graffiti, displaying content that reflects the hacktivist’s cause or message.
2. Denial-of-Service attacks (DoS): In a DoS attack, a website’s server is overwhelmed with traffic, rendering it inaccessible to users. This method disrupts operations and draws attention to the cause.
3. Data breaches: Hacktivists infiltrate systems to access and expose confidential information. Their objective is often to reveal hidden secrets or data, functioning as digital whistleblowing.
4. Redirection: Hacktivists manipulate website traffic to redirect users to websites highlighting the issues they advocate for. This approach helps them to reach a larger audience and spreads their message more effectively.
5. Anonymous blogging: Hacktivists may engage in anonymous blogging, providing a platform to share their views and raise awareness about social or political issues.
6. Doxing: Hacktivists sometimes engage in doxing, which involves publicly exposing private information about individuals or organizations to harm their reputation or advance their cause.
7. Geobombing: Geobombing is a form of hacktivism where geographical locations are targeted to create a visual impact. This can be done by manipulating mapping services or changing the names of places to reflect a specific message.
8. Website mirroring: Hacktivists may mirror websites to create copies that preserve the content and make it accessible even if the original website is taken down or blocked. While these methods can raise awareness for social or political issues, they often blur the line between activism and cybercrime, leading to ongoing debates about their ethical and legal implications.

Hackers vs Hacktivists

While “hackers” and “hacktivists” are often used interchangeably, they denote different entities with distinct motivations and methods.

Hackers, at their core, are individuals who are skilled in manipulating computer systems. Not all hackers are malicious. The term can be broken down into three categories: white, black, and gray hat hackers.

- White hat hackers are ethical hackers who use their skills to find and fix vulnerabilities, typically working with organizations to secure their systems.
- Black hat hackers exploit these vulnerabilities for personal gain, often involving illegal activities.
- Gray hat hackers sit in the middle, conducting unsanctioned operations, but usually without malicious intent.

Hacktivists represent a subset of hackers, primarily driven by political or social motives rather than personal gain. They use their skills to advance a cause, addressing issues they feel are ignored or mishandled. Hacktivism operates in a gray area of ethics and legality. While the intentions may be noble, the methods employed often involve unauthorized access and can infringe upon laws.

In summary, while all hacktivists are hackers, not all hackers are hacktivists. The key difference lies within their motivations and how they apply their skills.

The Ethics of Hacktivism

The ethics of hacktivism are a complex and contentious issue. Hacktivism is viewed as a powerful tool for promoting transparency, accountability, and freedom of information in the digital age. This perspective sees hacktivism as a form of activism that allows individuals or groups to express dissent, draw attention to important issues, and push for change.

From this standpoint, hacktivism represents a response to perceived injustices or wrongdoings, providing a means for marginalized voices to be heard. Examples include hacktivist actions that expose corporate misconduct, government abuses, or human rights injustices. Such actions can serve as essential checks in the digital space, promoting open dialogue and democratic values.

However, the opposing view considers hacktivism a form of cybercrime. Critics argue that regardless of the motives behind it, hacking is illegal and infringes upon individuals' or organizations' right to privacy. Hacktivists' methods, such as DoS attacks or data breaches, can cause significant harm and disruption. They can violate privacy, damage reputations, and lead to financial loss.

Moreover, critics believe that hacktivism can be used to cover for malicious intent, pointing to instances where information disclosed through hacktivist actions has been exploited for harmful purposes. Additionally, concerns are raised about the lack of accountability and the potential for unchecked power within the hacktivist community.

The debate around the ethics of hacktivism revolves around balancing the potential for positive social impact against the risks of harm, legality, and potential misuse. Attempts to regulate hacktivism pose additional challenges, given the global and decentralized nature of the internet and the difficulty in establishing universal ethical guidelines for digital behavior. As such, the discourse on the ethics of hacktivism continues to evolve alongside the ever-changing digital landscape.

The History of Hacktivism

The roots of hacktivism can be traced back to the 1980s when the concept of "phreaking" emerged. Phreaking was an early form of hacking that involved manipulating telephone networks to make free calls. However, the term "hacktivism" itself was coined in 1996 by Omega, a member of the hacking group Cult of the Dead Cow.

In the 1990s, alongside the adoption of personal computers and the internet, hacktivism experienced significant growth, with hacktivists using the digital realm to protest against various issues.

One of the earliest instances of hacktivism occurred in 1994 when a group called the Zippies launched an attack against the UK government in protest of a proposed law restricting open-air raves.

In the 2000s, the hacktivist landscape became more diverse and sophisticated with the formation of groups such as Anonymous and LulzSec. These groups carried out several high-profile attacks, often targeting corporations, governments, and other entities they perceived as oppressive or unethical.

The 2010s saw the rise of hacktivism in resistance to censorship and surveillance. Significant events include the Arab Spring and the Occupy movement, where hacktivism played a role in facilitating communication and coordinating protests.

Throughout its history, hacktivism has evolved in tandem with technological and societal changes. It remains a prominent force in the digital age, with its ethical and legal implications continually subject to debate. While the tactics and targets of hacktivism have diversified over time, the underlying motivation to use hacking as a means of protest and activism remains consistent.

Famous Examples of Hacktivism Events

1. Operation Payback (2010): Operated by the hacktivist group known as Anonymous, Operation Payback was a series of retaliatory attacks against various major organizations involved in anti-piracy operations. The operation gained significant attention when the group targeted companies that withdrew support from WikiLeaks.
2. Arab Spring (2010-2012): The Arab Spring was a wave of anti-government protests, uprisings, and armed rebellions that spread across much of the Arab world. Hacktivists played a key role in this movement, using their skills to bypass government censorship, disseminate information, and coordinate protests.
3. Hacking Team Exposure (2015): A yet-unidentified hacktivist leaked 400 gigabytes of data from Hacking Team, an Italian company selling intrusion and surveillance capabilities to governments, law enforcement agencies, and corporations. The leaked data exposed the company’s controversial clients, which included oppressive governments.
4. The Ashley Madison Data Breach (2015): A group known as The Impact Team breached the system of Ashley Madison, a dating website designed for extramarital affairs, leaking user data online. While the action was illegal and caused harm to individuals, the group claimed moral high ground, criticizing the company’s business practices and user fraud.
5. Panama Papers (2016): An anonymous hacktivist leaked over 11.5 million documents from the Panamanian law firm Mossack Fonseca, revealing how wealthy individuals worldwide used offshore firms to evade taxes. The act was deemed a form of hacktivism due to its political significance and the use of digital means to execute it.

These are just a few examples of the numerous hacktivism events throughout history, showcasing the broad range of motivations and targets within the hacktivist community.

Preventing Hacktivism

Preventing hacktivism involves a combination of technical, legal, and ethical strategies.

From a technical standpoint, organizations can protect themselves by maintaining robust cybersecurity measures. This includes regular system updates, strong encryption practices, intrusion detection systems, and the use of firewalls and/or DDoS protection. Regular audits of these systems can help identify and fix potential vulnerabilities before they are exploited. Employee education around phishing attempts and safe online practices is also crucial.

From a legal perspective, laws and regulations need to keep pace with the evolving landscape of cyber threats. Ensuring firm legal consequences for unauthorized hacking activities can serve as a deterrent for would-be hacktivists. International cooperation and shared standards can also help in preventing cross-border cyber attacks.

Ethically, organizations can reduce their risk of becoming targets by operating responsibly and transparently. Many hacktivism attacks are motivated by perceived injustices or unethical practices. Organizations can lessen the chances of becoming a target by addressing potential grievances, respecting privacy rights, and being transparent about data use.

It is important to note that while these measures can significantly reduce the risk, they cannot eliminate the possibility of hacktivism attacks. Maintaining vigilance and preparedness against cyber threats is necessary in an increasingly digital world.

1. In what ways can hacktivism be considered a double-edged sword for promoting social or political change?

2. How do hacktivist activities shape public opinion and influence policy decisions?
3. What measures can organizations take to defend against hacktivist threats?
4. Are there situations where hacktivism could be justified from an ethical standpoint?
5. How has the threat landscape evolved with the rise of hacktivism?

Activities:

1. Write a reflective essay discussing the ethical implications of hacktivism and its potential impact on society.
2. Create a presentation highlighting the tactics and techniques used by prominent hacktivist groups.

UNIT 26
INTTERNET OF THINGS

1. What is the Internet of Things (IoT), and how would you define it in your own words?
2. Can you name some everyday devices that are part of the Internet of Things?
3. What are the potential benefits and challenges associated with the widespread adoption of IoT?
4. How does IoT impact privacy and security concerns?
5. In what ways can IoT technology be applied in different industries?

Pre-Reading Tasks:

1. Research and compile a list of examples where IoT is currently being used in real-world applications.
2. Investigate the communication protocols commonly used in IoT devices.
3. Explore the evolution of IoT technology and its historical context.
4. Look into the potential environmental impact of IoT devices and their disposal.
5. Familiarize yourself with key IoT terminology and concepts.

What is the internet of things (IoT)?

The internet of things, or IoT, is a network of interrelated devices that connect and exchange data with other IoT devices and the cloud. IoT devices are typically embedded with technology such as sensors and software and can include mechanical and digital machines and consumer objects.

Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, deliver enhanced customer service, improve decision-making and increase the value of the business.

With IoT, data is transferable over a network without requiring human-to-human or human-to-computer interactions. IoT devices share the sensor data they collect by connecting to an IoT gateway, which acts as a central hub where IoT devices can send data. Before the data is shared, it can also be sent to an edge device where that data is analyzed locally. Analyzing data locally reduces the volume of data sent to the cloud, which minimizes bandwidth consumption.

Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices -- for example, to set them up, give them instructions or access the data.

The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IoT applications deployed.

IoT can also use artificial intelligence and machine learning to aid in making data collection processes easier and more dynamic.

A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low, or any other natural or man-made object that can be assigned an Internet Protocol address and is able to transfer data over a network.

How does IoT work?

An IoT ecosystem consists of web-enabled smart devices that use embedded systems -- such as processors, sensors and communication hardware -- to collect, send and act on data they acquire from their environments.

IoT helps people live and work smarter. Consumers, for example, can use IoT-embedded devices -- such as cars, smartwatches or thermostats -- to improve their lives. For example, when a person arrives home, their car could communicate with the garage to open the door; their thermostat could adjust to a preset temperature; and their lighting could be set to a lower intensity and color.

In addition to offering smart devices to automate homes, IoT is essential to business. It provides organizations with a real-time look into how their systems really work, delivering insights into everything from the performance of machines to supply chain and logistics operations.

IoT enables machines to complete tedious tasks without human intervention. Companies can automate processes, reduce labor costs, cut down on waste and improve service delivery. IoT helps make it less expensive to manufacture and deliver goods, and offers transparency into customer transactions.

IoT is one of the most important technologies and it continues to advance as more businesses realize the potential of connected devices to keep them competitive.

What are the pros and cons of IoT?

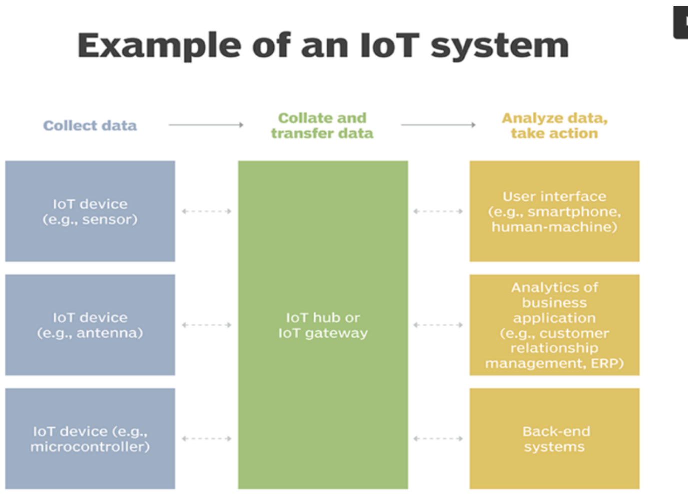
Some of the advantages of IoT include the following:

- Enables access to information from anywhere at any time on any device.
- Improves communication between connected electronic devices.
- Enables the transfer of data packets over a connected network, which can save time and money.
- Collects large amounts of data from multiple devices, aiding both users and manufacturers.
- Analyzes data at the edge, reducing the amount of data that needs to be sent to the cloud.
- Automates tasks to improve the quality of a business's services and reduces the need for human intervention.
- Enables healthcare patients to be cared for continually and more effectively.

Some disadvantages of IoT include the following:

- Increases the attack surface as the number of connected devices grows. As more information is shared between devices, the potential for a hacker to steal confidential information increases.
- Makes device management challenging as the number of IoT devices increases. Organizations might eventually have to deal with a massive number of IoT devices, and collecting and managing the data from all those devices could be challenging.
- Has the potential to corrupt other connected devices if there's a bug in the system.

- Increases compatibility issues between devices, as there's no international standard of compatibility for IoT. This makes it difficult for devices from different manufacturers to communicate with each other.


Example of an IoT system
Collect data
Collate and transfer data
Analyze data, take action
IoT device (e.g., sensor)
IoT device (e.g., antenna)
IoT device (e.g., microcontroller)
IoT hub or IoT gateway
User interface (e.g., smartphone, human-machine)
Analytics of business application (e.g., customer relationship management, ERP)
Back-end systems

1. How has your understanding of the Internet of Things evolved after reading about its applications and challenges?
2. What are the most significant security and privacy concerns associated with IoT, and how can they be mitigated?
3. In what ways can IoT contribute to improving efficiency and sustainability in various industries?
4. How might the integration of IoT impact our daily lives and routines?
5. What ethical dilemmas or considerations arise with the widespread adoption of IoT technology?

Activities:

1. Develop a concept map or diagram illustrating the interconnectedness of different IoT devices and their applications.
2. Create a hypothetical scenario where IoT technology is used to address a specific social or environmental challenge.
3. Write a persuasive essay discussing the potential benefits and drawbacks of IoT in a specific industry or domain.

UNIT 27
CYBERSECURITY RISKS

1. What is your current understanding of cybersecurity and its importance in today's digital world?
2. Can you name some common types of cybersecurity threats and attacks?
3. How do you think individuals and organizations can be vulnerable to cyber threats?
4. Are you familiar with any recent cybersecurity incidents or breaches that made headlines?

5. What measures do you currently take to secure your personal digital devices and online accounts?

Pre-Reading Tasks:

1. Research and compile a list of major cybersecurity threats, including malware, phishing, ransomware, etc.
2. Investigate the role of cybersecurity in protecting critical infrastructure and national security.
3. Explore cybersecurity best practices for individuals, businesses, and governments.
4. Look into recent cybersecurity trends and emerging threats in the digital landscape.
5. Familiarize yourself with common cybersecurity terms and concepts, such as encryption, firewalls, and multi-factor authentication.

What should be evident from all of the case studies is that any organization that is caught out by substantial breaches in their cybersecurity did not have a clear understanding of the risks they were taking. These organizations self-evidently lacked a connected and informed view of their active risks.

Effective cybersecurity management relies on accurate capture and escalation of priority risks. If issues or problems are not consistently captured at an individual level and appropriately escalated when they are significant, the management layer will be operating in an uninformed environment, with no sense of the true gaps and their comparative priorities. In this chapter we cover:

- What is a cybersecurity risk?
- How do you capture and manage individual risks?

How do you deal with measuring, monitoring, managing clusters of

- risks using:
- Risk Registers
- Risk Assessments
- How to apply risk-based cybersecurity management.

Managing risks individually, although important, will still create issues if the big picture view is not possible. When organizations suffer from major financial losses through intrusions and data losses, it is always the case that a chain of separate and unresolved risks were in place. We will refer to this as stacked risks and will cover this topic in greater detail during the Cyber Risk Register section of this chapter. stacked risk –a chain of related problems that have the potential to cause greater financial impact together than their individual information may suggest.

Before we look at what risk is, it is useful to consider the general problems and prejudices that people have in understanding any type of risk. Consider the following items and what order of threat to life you think they would pose, based on the number of deaths they cause annually in North America:

- Vending machines
- Brown bear attacks.
- Soft toys.
- Being left handed.

Without any metrics or analysis, we can easily have a distorted impression of the reality. In fact, vending machines kill more people in the US each year (by falling on people when they rock them to recover loose items) than brown bears. Soft toys are responsible for more deaths that either brown bears or vending machines.

Being left handed is thought to be the biggest killer, through accidents caused by left-handed people using equipment designed for right-handed people. (A much debated study in 1991 by Halpern and Coren showed a significant difference in life expectancy for left-handed people. The study was later dismissed by many as likely to contain some statistical anomalies. However, there is consensus that left-handed people using right-handed equipment does cause asubstantially greater number of accidents for them.)

- There were 11 deaths recorded in the US in 2012 due to soft toys, according to the US Consumer Product Safety Commission.
- 2 or 3 people die in the US each year due to vending machines.
- An average of one person is killed in North America each year due to brown bear attacks.
- The number of fatalities due to being left-handed is unrecorded.

How is this relevant to cybersecurity? We have the same issue in cybersecurity that without an accurate understanding of the numbers that sit behind risks, we can and do make mistakes regarding where to focus our security efforts and budget. Without a full picture of the risks, as a cybersecurity manager, I might be tempted to prioritize spending on encrypting data because it covers a lot of the potential attack surface. However, if I had full visibility of the issues and comparative countermeasure costs and benefits, I could easily discover that there were twenty or more, higher priority, higher impact and lower cost items to address first. It is the largest, unresolved risks that create the most damage. You need to have a comprehensive and connected view of your overall risks to be able to accurately understand where the cybersecurity priorities are. When risks are presented in isolation, it is not possible to understand their comparative priority.

Before we get to the big, joined up view, we still need to understand the **basics of capturing and managing individual risks.**

What is a Cybersecurity Risk?

Anything that has the potential to cause detrimental impact to the electronic devices we use, or the information they store or transact, can be considered a cybersecurity risk. Remember, that can include processes and other non-technical items that directly affect our security status. For example, if there is a problem that Security awareness training is not being regularly provided, that can still be a risk to cybersecurity because it has a high potential to lead to poor usage practices by staff that will create increased, successful malware attacks. Earlier in the book, we have looked at threats, vulnerabilities and other gaps. Each of these can also be considered, when they have (i) enough probability of occurring and (ii) potential detrimental impact if they do, can also be considered sources of risk.

That is because the only 2 critical ingredients to a risk are:

1) Probability (also referred to as potential, likelihood or chance) of the problem occurring.

2) Impact of a sufficient magnitude to be of material concern.

There are a number of ways to measure probability. The most effective method is to ensure all expressions of likelihood or the chances of something happening are translated into a percentage value. It is not possible or essential for the initial probability percentage assigned to a risk to be exactly correct. That is because the percentage value assigned to each risk will be improved as the information about the risk grows. materiality –to have a level of significance or magnitude to be of concern.

Generally, the larger the organization, the greater the financial impact must be before something is considered to have enough materiality to be recorded and managed as a risk.

If I have identified an individual, critical vulnerability in a single application, it is only likely to be considered a risk if it could (on its' own) create substantial impact to my organization. I will still need to ensure it is managed to closure through normal processes, but I will not need to ask for it to be tracked as a risk. However, I may also determine that the same critical vulnerability could be present in a large number of other applications and needs urgent investigation. In that case, I would escalate it as a risk if I thought the collective impact was significant.

Each organization defines their materiality threshold, usually as a financial amount. If a gap or problem has the potential to cause the organization more than $x of financial risk (where x is the materiality threshold determined by the organization) it should be captured into the risk management process. There is more about materiality in the Risk Register section of this chapter. These activities aim to provide students with hands-on experience, critical thinking opportunities, and insights into the multifaceted nature of computer forensics in the realm of digital investigations.

1. How has your perception of cybersecurity changed after learning about various risks and threats?
2. What are the potential consequences of not taking cybersecurity seriously at the individual and organizational levels?
3. How do cybersecurity risks impact our daily lives, both online and offline?
4. What role do individuals play in maintaining a secure digital environment, and what responsibilities do organizations have in safeguarding user data?
5. How can awareness and education help mitigate cybersecurity risks on a broader scale?

Activities:

1. Conduct a risk assessment of your own digital habits and devices, identifying potential cybersecurity vulnerabilities.
2. Create a cybersecurity checklist for individuals to follow in order to enhance their online security.
3. Develop a presentation or infographic illustrating the most common cybersecurity threats and how to protect against them.

UNIT 28
THE CYBER RISK REGISTER

1. What is a Cyber Risk Register, and why is it essential for organizations?
2. How does the identification and assessment of cyber risks contribute to overall cybersecurity?
3. Can you list some common types of cyber risks that organizations might face?
4. What role does the Cyber Risk Register play in the risk management process?
5. How often should a Cyber Risk Register be updated, and why?

Pre-Reading Tasks:

1. Research the key components of a Cyber Risk Register and how they are structured.
2. Investigate real-world examples of organizations that have faced significant cyber risks and analyze the impact on their operations.
3. Explore the various methodologies used for assessing and quantifying cyber risks.

4. Look into regulatory requirements and standards related to maintaining a Cyber Risk Register.
5. Identify common vulnerabilities and threats that organizations might need to include in their Cyber Risk Register.

A risk register is a tool in risk management. It is used to identify potential risks in a particular project or across a company, sometimes to fulfill regulatory compliance but generally to stay on top of potential issues that can derail company objectives. As mentioned, a specialized cyber risk register tool is used to identify and organize the risks distinctive to cybersecurity. Cybersecurity is unique in its nature, covering physical, technical, and operational risks.

A cyber risk register is a form of reporting that organizes an inventory of potential risks, logging relevant details for each that can be used for prioritizing and decision making. Each detail logged serves to highlight a difference aspect of the risk.

Why is a cyber risk register important?

Doing your due diligence means you’ll have a plan in place before risks can open you up to threats and vulnerabilities. Being organized boosts efficiency and productivity which in turn will overall be financially beneficial to your company.

Unlike other areas of business, cyber security is inherently about securing systems, networks, databases and information, ultimately through reducing the risks involved. The huge array of risks connected to cybersecurity need a high level of organization and focused proven remediation steps.

A risk register is a tool in risk management. It is used to identify potential risks in a particular project or across a company, sometimes to fulfill regulatory compliance but generally to stay on top of potential issues that can derail company objectives. As mentioned, a specialized cyber risk register tool is used to identify and organize the risks distinctive to cybersecurity. Cybersecurity is unique in its nature, covering physical, technical, and operational risks.

A cyber risk register is a form of reporting that organizes an inventory of potential risks, logging relevant details for each that can be used for prioritizing and decision making. Each detail logged serves to highlight a difference aspect of the risk.

Why is a cyber risk register important?

Doing your due diligence means you’ll have a plan in place before risks can open you up to threats and vulnerabilities. Being organized boosts efficiency and productivity which in turn will overall be financially beneficial to your company.

Unlike other areas of business, cyber security is inherently about securing systems, networks, databases and information, ultimately through reducing the risks involved. The huge array of risks connected to cybersecurity need a high level of organization and focused proven remediation steps.

What to include in a cyber risk register?

- **Risk Description**: This is the risk itself, including details of how it may threaten the organization.
- **Impact**: This is the result of the event occurring, a measure of the impact it will have on your organization.
- **Likelihood:** This logs how likely it is for the potential event to occur. This will be key in prioritizing the remediation efforts.
- **Outcome:** This measures the effect on the organization after the event occurs. This is actionable information that helps leaders understand whether they are likely to achieve what

they have set out to achieve. They can determine whether that likelihood is acceptable and decide what actions are needed, if any.

- **Risk Level:** Taking all factors into account, based on your risk matrix, it measures how much of a priority is any particular risk.
- **Cost:** Mitigation measures and remediating risks may save money in the long run but will cost money to implement. This can evaluate both sides of the coin.
- **Mitigation actions:** What are the steps to remediate or at least mitigate the risk? Creating a task for each risk will make it easier to put into action and to measure progress.
- **Roles and responsibilities**: To whom is the risk assigned? Risk management is a team effort. Assigning responsibilities clarifies who needs to take care of the risk and maximizes accountability, usually producing productive results.

The Challenges of a Traditional Risk Register

Most companies have kept their risk registers in spreadsheets. This was once the best way to do it but times have moved on. Traditional risk registers suffer from human error, time wasted on input, updates are very difficult to track accurately, and since the spreadsheet is siloed from real-time events, you end up with an isolated list that isn't working in sync with the rest of the company activities in this area. It has also been difficult to measure the multi-facets of risk simultaneously, including the financial impact, technical effect, damage to business objectives, effect on continuity, amongst others.

When Centraleyes released platform update version 4.0, it included a one of its kind capability – an Automated Risk Register.

The new addition to the platform's unique cyber risk management features is a state-of-the-art organizational risk register that automatically creates a set of 64 primary risks and generates both an inherent and a residual risk score, as well as the linkage to the affected assets and mitigating controls. This feature alone can save tens to hundreds of hours of manual work, when creating and maintaining a risk register. The risk register will continuously update itself based on control measurement the platform does in real time.

The 64 primary risks are based on a unique combination of the OWASP, NIST and MITRE ATT&CK framework, which include physical, adversarial and non-adversarial risks.

An additional and significant advanced attribute is the Financial Impact, which is calculated under 6 elements of loss, automatically tagging the risk with a financial attribute.

The addition of this cutting-edge new capability Automated Risk Register is another unique and proprietary feature that positions the Centraleyes platform as the leading solution for cyber risk and compliance management.

1. How does maintaining a Cyber Risk Register align with an organization's overall risk management strategy?
2. What challenges might organizations face when trying to assess and quantify cyber risks for the register?
3. In what ways can a well-maintained Cyber Risk Register contribute to incident response and recovery?
4. How can organizations ensure that their Cyber Risk Register remains up-to-date in the face of evolving cyber threats?
5. How might stakeholders, including employees and customers, benefit from the transparency provided by a Cyber Risk Register?

Activities:

1. Create a presentation or infographic highlighting the importance of Cyber Risk Registers for various stakeholders.
2. Role-play a scenario where an organization's leadership team discusses the findings of their Cyber Risk Register and makes decisions based on the identified risks.

MODULE 8
CYBERSECURITY AND BUSINESS ORGANIZATIONS.

UNIT 29

FRAMEWORKS TO SECURE BUSINESS

1. What is the significance of having a robust security framework for businesses?
2. Can you name some common cyber threats that businesses often face?
3. How familiar are you with different cybersecurity frameworks used to secure business operations?
4. What role do regulations and compliance standards play in shaping security frameworks for businesses?
5. Have you encountered any real-world examples where a lack of security framework led to a business security breach?

Pre-Reading Tasks:

1. Research and compile a list of prominent cybersecurity frameworks used by businesses globally.
2. Investigate the role of risk assessment in developing a comprehensive security framework for businesses.
3. Explore case studies that highlight successful implementations of security frameworks in businesses.
4. Examine the current regulatory landscape and its impact on cybersecurity frameworks.
5. Look into emerging technologies and trends influencing the evolution of business security frameworks.

Depending on your personal and professional interest, you may want to read more about one or more of those technical defenses.

As an example, the UK Cyber Essentials scheme, one of many frameworks designed to help organizations create better defenses, believes that effective management of just five key areas would protect against 80% of attacks. These areas are:

- Effective firewall positioning and management.
- Secure configuration.
- User Access Controls.
- Malware Protection.
- Timely Patch Management.

secure configuration – ensuring that when settings are applied to any item (device or software), appropriate steps are always taken to ensure (i) default accounts are removed or disabled, (ii) shared accounts are not used and (iii) all protective and defensive control in the item use the strongest appropriate settings.

default accounts – generic user and password permissions, often with administrative access that is provided as standard for some applications andhardware for use during initial set-up.

access controls –the ability to control entry or exit to a physical, virtual or digital area through the use of permissions issued at a personal, electronic or physical level. The permissions can be issued as physical tokens (something you have), secret information (something you know) or biometric information –using part of the human body such as a fingerprint or eye scan to gain access (something you are). See also multi-factor authentication.

patch management –a controlled process used to deploy critical, interim updates to software on digital devices. The release of a software 'patch' is usually in response to a critical flaw or gap that has been identified.

What is noticeable in the list above is that the three bolded items (secure configuration, user access controls and timely patch management), are reliant onhuman procedures. These are not direct technical controls but are processcontrols that need to be applied to networks, systems, devices and applications.

At the highest level, an enterprise governance, risk and compliance system is designed to pull together:

• **Governance information** - is the full range of policies, procedures and specific controls that the executive of an enterprise use to keep their organization working within acceptable boundaries. This will include direct security policies, procedures and controls and also indirect items that can also influence or impact security.

• Compliance information – are the results from processes used to verify that governance items are being followed and to identify any gaps.

• Risk information – is anything that has a possibility to substantially and materially impact the organization. This data can come from multiple sources, including not only identified gaps in compliance but also any new threats (such as changes in regulation or new types of exploits).

Although collecting and synchronizing this highest level information is the best source of creating an informed view of the overall security position, it relies on being able to pull information from more granular sources of security coordination software.

Network operations centers often pull together information about information traffic and attempts at intrusion. Anti-malware coordination suites can monitor assets to ensure their individual anti-malware software is functioning, being updated and collect information about attempted infection rates. Corrective and preventive action systems can operate to measure, manage and monitor identified problems through to closure. There are more than 30 different security control processes that can aggregate information.

Many people still think that getting malware into their system is achieved through email or by intentionally downloading an unknown application on to a device. One of the earliest techniques used was known as phishing.

phishing – using an electronic communication (for example email or instant messaging) that pretends to come from a legitimate source, in an attempt to get sensitive information (for example a password or credit card number) from the recipient.

SSL – is an acronym for Secure Sockets Layer. This is a method (protocol) for providing encrypted communication between a web server (the computer hosting a web service or web site) and a web browser (the program that the recipient uses to view the web page- for example, Internet Explorer). File sharing and instant messaging services are also able to be exploited in the same way.

This form of attack is referred to as a drive-by download.

drive-by download – the unintended receiving of malicious software on to a device through an internet page, electronic service or link. Malicious software that is subject to frequent adaption to more effectively evade anti-malware is known as polymorphic malware.

polymorphic malware –malicious software that can change its attributes to help avoid detection by anti-malware. This mutation process can be automated so that the function of the software continues but the method of operation, location and other attributes may change.

It should also be considered that zones with very high security can be created to add substantially more protection to the most sensitive data. Just like a high security site, it can be a requirement for this area to either be a closed system, or for all inbound and outbound traffic to be fully decrypted and inspected.

closed system – a collection of applications, systems and devices that only have the ability to communicate with each other. No connection to any component outside the known and trusted group is permitted.
Closed systems are frequently used, for example, in manufacturing lines and in aircraft control.

To summarize, it is possible to form highly effective defenses against attacks.

- The most critical item is to have executive (board level) support for the correct investment into security. That requires presenting the executive with a clear understanding of the size and scale of the organizations risk exposure.
- Reduce the attack surface to the minimum appropriate size to meet the business needs.
- Use a security architect to help simplify your range of cyber defense points.
- Classify your information to know what sets of data require the greatest amount of security control.
- Zone your attack surface into discrete segments that reflect the value and sensitivity of the information they transact. Apply the greatest security to the highest value zones.
- Remove or destroy data that has insignificant or low value.
- Use up to date anti-malware across all devices that carry, store or transact your information.
- Ensure that you have strong user access controls that work on the basis of providing people with the lowest amount of privilege they require to perform their role.
- Patch all devices and operating systems promptly with the latest security updates from their manufacturers.
- Deploy other, key, technical countermeasures such as advanced firewalls with strong policies to critical locations.
- Make sure the security settings on all applications, systems and physical devices are set to an appropriately high level and remove all default accounts.

But most importantly – remember that defense in depth requires a holistic view of security. Physical security, procedural controls and cultural conditions are key contributors to the most significant and successful attacks. Only organizations with an informed view of the full picture will be able to prevent substantial attacks. The primary challenge to create effective defense is achieving sufficient investment in securing electronic devices. Creating investment requires building an effective business case (justification for the expense) and with the number of successful attacks making headlines and enormous losses, the value of improved security over electronic devices and their data will be relatively easy to demonstrate. Effective security over electronic devices and their information requires an expensive and extensive approach that is championed at the board level.

Ineffective security is even more expensive. Under investment in security is now frequently leading to the dismissal of key board members who were poorly informed about the cyber risks they were allowing their organization to take.

1. How do security frameworks contribute to the overall resilience of a business against cyber threats?
2. In what ways can businesses tailor security frameworks to address industry-specific challenges?
3. What role does employee awareness and training play in the success of a security framework?
4. How do regulations and compliance standards shape the development and implementation of security frameworks?
5. What are some challenges businesses might face when adopting and maintaining a security framework?

Activities:

1. Develop a mock cybersecurity framework tailored to a specific business scenario.
2. Create a presentation or infographic summarizing the key elements of a successful security Background:

UNIT 30
CASE STUDY. SONY COMPANY

1. What are the potential motivations behind cyberattacks on major organizations like Sony Pictures Entertainment?
2. How might the sophistication of a cyberattack impact the organization's ability to defend against it?
3. Why is the theft of sensitive data and internal communications particularly concerning for a company like Sony Pictures Entertainment?
4. What are the potential consequences of a cyberattack on a major film studio, not only in terms of data loss but also in terms of reputation and business continuity?
5. How can organizations prepare and protect themselves against sophisticated cyber threats?

Pre-Reading Tasks:

1. Research the "Guardians of Peace" (GOP) cyberattack on Sony Pictures Entertainment and gather information on the attackers' methods and motives.
2. Explore the impact of the Sony Pictures cyberattack on the entertainment industry and cybersecurity practices.
3. Investigate how the incident affected Sony Pictures' response and communication strategies during and after the attack.

4. Look into the cybersecurity measures and policies that were in place at Sony Pictures before the attack.
5. Identify any legal or regulatory implications for organizations that experience a significant cyber breach.

During Reading Tasks:

1. Take detailed notes on the timeline of events during the Sony Pictures cyberattack.
2. Analyze the methods and tactics used by the "Guardians of Peace" to breach Sony Pictures' systems.
3. Explore the immediate and long-term consequences of the cyberattack on Sony Pictures' operations and reputation.
4. Identify the key weaknesses or vulnerabilities that the attackers exploited during the breach.
5. Examine the response strategies employed by Sony Pictures to contain the cyberattack and recover from the incident.

Background:

In November 2014, Sony Pictures Entertainment, a major film studio, became the target of a highly sophisticated cyberattack. The attackers, who identified themselves as the "Guardians of Peace" (GOP), claimed responsibility for the breach. The incident resulted in the theft of sensitive data, internal communications, unreleased films, and the defacement of Sony Pictures' computer systems.

Key Events:

1. Data Theft and Leakage:
   - Hackers stole a vast amount of sensitive and confidential information, including executive emails, employee data, unreleased films, and business contracts.
   - The stolen data was gradually leaked online, exposing internal communications, financial details, and unreleased films.

2. Attribution and Motivation:
   - The U.S. government later attributed the cyberattack to North Korea, alleging that it was in retaliation for Sony's upcoming film, "The Interview," a comedy that depicted the fictional assassination of North Korea's leader.
   - The motive was believed to be an attempt to suppress the release of the film, which North Korea considered offensive.

3. Denial of Service and System Disruption:
   - The attackers used destructive malware to compromise and disrupt Sony Pictures' computer systems.
   - The malware rendered many systems inoperable, leading to significant disruptions in the company's day-to-day operations.

4. Impact on Sony Pictures:
   - The cyberattack had severe consequences for Sony Pictures, resulting in financial losses, reputational damage, and legal challenges.
   - It prompted a reevaluation of cybersecurity practices within the entertainment industry and highlighted the potential geopolitical implications of cyber incidents.

Lessons Learned:

1. Importance of Cybersecurity Preparedness:
   - The Sony Pictures breach underscored the critical importance of having robust cybersecurity measures in place to safeguard sensitive information.

2. Geopolitical Implications:
   - The incident highlighted the potential for cyberattacks to have geopolitical consequences, with nation-states using cyber tools to achieve political objectives.

3. Need for Incident Response Plans:
   - Sony's response to the incident was criticized for being slow and uncoordinated. The case emphasized the importance of having well-defined incident response plans in place.

4. Supply Chain Security:
   - The breach also raised concerns about the cybersecurity of third-party vendors and the need for companies to assess the security posture of their entire supply chain.

The Sony Pictures cyberattack serves as a prominent case study in cybersecurity, illustrating the evolving nature of cyber threats, the potential impact on organizations, and the importance of proactive cybersecurity measures.

Post-Reading Questions:

1. How did the cyberattack on Sony Pictures impact its relationships with stakeholders, including employees, partners, and customers?
2. What lessons can other organizations learn from the Sony Pictures cyberattack regarding cybersecurity preparedness and response?
3. How did the incident highlight the importance of collaboration between private entities and government agencies in responding to cyber threats?
4. What changes or improvements in cybersecurity measures were implemented by Sony Pictures in the aftermath of the attack?
5. How has the Sony Pictures cyberattack influenced the development of cybersecurity policies and practices in the entertainment industry?

Post-Reading Activities:

1. Develop a cybersecurity incident response plan for a fictional film studio based on the lessons learned from the Sony Pictures cyberattack.
2. Create a timeline or infographic illustrating the key events, actions, and consequences of the Sony Pictures cyberattack.
3. Write a report on the potential economic and financial impacts of a cyberattack on a major film studio.

UNIT 31

THE OVERVIEW OF NEW TECHNOLOGY

1. What do you understand about the term "new technologies in cybersecurity"?
2. Can you name some traditional cybersecurity measures and technologies, and how effective do you think they are in the current digital landscape?
3. Why is it important for cybersecurity professionals to stay updated on emerging technologies?

4. What are some common challenges and threats that modern cybersecurity technologies aim to address?
5. Have you heard of any recent cybersecurity incidents that might have prompted the development of new technologies?

Pre-Reading Tasks:

1. Research and create a list of traditional cybersecurity technologies and practices.
2. Explore recent cybersecurity trends and incidents that highlight the need for innovative solutions.
3. Investigate the role of artificial intelligence and machine learning in modern cybersecurity.
4. Look into the concept of zero trust security and its relevance in contemporary cybersecurity strategies.
5. Familiarize yourself with new encryption technologies used to secure data and communications.

During Reading Tasks:

1. Take notes on key advancements in cybersecurity technologies mentioned in the overview.
2. Identify specific examples of how artificial intelligence is being applied to enhance cybersecurity measures.
3. Look for information on the integration of blockchain technology in cybersecurity.
4. Explore the use of automation and orchestration in incident response and threat detection.
5. Investigate how cloud computing is influencing the landscape of cybersecurity.

The most amazing thing about technology is that we no longer need to consider if something is possible. Almost anything is now possible to create. Instead of easibility, the only real question now is – 'Will it make money?'

The lure of profits, earnings and power will continue to be the main driving force for the advancement of technology.

There are certain easy predictions that we can begin with:

- The amount of electronic information we use and store will also continue to grow.
- The costs for storing and processing electronic data will continue to drop.
- The amount of processing power will continue to grow in line with Moore's Law.
- Displays will get larger, more flexible and more immersive.
- The number of devices we use that can connect to each other will grow.
- Power sources (batteries included) will get physically smaller and faster to charge.

Moore's Law –created in 1965 by Gordon E. Moore, states that over the history of computing, the processing power doubles approximately every two years. There is also a very important, underlying trend to consider. The change in the way companies earn profit. Instead of selling one-off products or services, everybody is looking at how to create invaluable streams of services that attract repeating and regular income. Items that were once one-off product purchases are increasingly becoming
subscription services.

The closer any organization can get to their customers, the better they can learn and extend those service sales into new areas. This means 2 things:

1) Organizations want to increase the amount of information they store and analyze about their customers.

2) There is an incentive to turn items that are currently physical products into subscription services.

Putting electronics into anything that we possibly can is now referred to as the **Internet of Things (IoT).**

Internet of Things – the inclusion of electronics and software in any device not usually considered computerized in nature, to enable it to achieve greater value and service by giving it the ability to network and communicate with other devices.

Put simply, the internet of things is the idea that there is probably some value in anything electronic being able to connect to each other and to the internet. As things change, there will be early adopters, late adopters and frequent attempts at new technologies that are ridiculous and never succeed. Every year at the Consumer Electronics Show (CES) in Las Vegas, there are literally tens of thousands of new gadgets on display. Only a small number become successful. With the price of technology power continuing to fall, more and more devices will be connected to the internet. As we begin to carry, wear and house more connected devices we can expect that those devices will be targeted by all kinds of organizations and people good and bad.

Wearable technology is also set to progress. Why put a computer in a jacket? Well, it could be useful if you can scan and change the fabric color whenever you want and use the sleeve as a display for any messages that your phone receives. One of the new gadgets just being launched includes a 3D food printer for your home. Put in some small ingredients cartridges, select your desert and the food printer will instantly make it for you. Simply print and serve. Having this device on the internet of things has the potential to allow it to download new recipes and also to monitor what you like most and suggest other things you might like. We already have Smart televisions that are close to fully functioning computers in their own right, in fact in some ways more advanced. As I was writing the first edition of this book, one manufacturer issued a warning that conversations in front of their smart televisions can be recorded, automatically changed to text and sent to the manufacturer to help with product improvement of their voice command services! If you think that seeing targeted ads on your computer or tablet is disturbing, wait until those advertising display screens start displaying ads specifically for you as you walk past them. Imagine moving up the escalator on the subway and the ads in front of you promoting that holiday you have been researching.

Self-driving cars are set to revolutionize how we use transport. Most of us are not using our cars 95% of the time. Why have your own cars if you could order one immediately to your door? Get it to drop you off exactly where you want and no need to worry about parking, maintenance costs. You can also enjoy a drink if you choose. Rather than paying for an entire car, you will literally be able to use one by the minute, hour and mile. Without the cost of a driver, this type of service, still reliant on technology, will probably be so cheap to use that it will soon cost little more than just the fuel you currently pay for. However, that also means that whatever car service you subscribe to will know where you go, when, who you travel with, what you travel with and more. Almost certainly, it will aim to show you targeted ads, or offer you sponsored opportunities (stop here for 50% off your meal) during your journey.

And then there is **nanotechnology.**

nanotechnology – incredibly small products and devices manufactured through the manipulation of items as small as atoms and molecules. From delivering non-invasive surgery, to enhancing battery performance or even enhancing human strength and durability, the ability to manufacture, deliver and control technology at such extremely small sizes creates even more possibilities.

Forget corrective eye surgery, in the not too distant future, you may be able to splash the right collection of nanotechnology on your eyes to get not only perfect vision, but the ability to zoom in on distant objects, record what you see or even overlay a computer display.

All of these advances also mean that far more electronic data about all of us will be created and accessible. Over the past 40 years, the progress in reducing cost of storing information electronically, the physical size of storage and increasing the speed of access have been unbelievable. To put this into perspective, if you wanted to put the entire works of Shakespeare (text only) on to an electronic storage device, the electronic storage required (about 4 megabytes) would have cost around $4,000 in 1978. Today, you could store that for less than 20 cents. In ten years time, the cost will probably be less than one cent. The entire scanned content of an average print library can already be stored on a few 2 Terabyte SD cards, no larger than your thumbnail.

More data means there will be an increase in the surface area that needs to be protected and more types of data also opens up new potential threats and exploits. These changes mean we can expect attempts at data theft to become faster and more frequent. Attacks will no longer need to be over a period of hours or days to be significant.

The speed that technology is evolving also has certain other affects on how quickly or slowly we choose to adopt it. Although televisions are evolving rapidly, few of us want to take on the cost of changing up to the latest features every 3 years. This is a similar situation with cars and even most other household fixtures. The technologies we adopt most quickly tend to be those that are consumable, cheap or offer substantial value beyond their cost. If someone offered me a free smart refrigerator for a subscription, I might sign up, but if they want $500 for it, I will probably stick with what I have until it goes wrong.

That means that we can expect wearable, consumable items to continue to evolve rapidly and higher value items to evolve at a slower pace. All these changes will affect the available jobs also. Even quite highly skilled jobs, such as general doctors, will be decreased as technologies become increasingly able to deliver faster, more effective and lower cost alternatives. It will not be the case that there are no doctors; it will just be that your medical condition will need to have reached a certain point in the diagnosis and treatment before a person may need to be involved.

If we think about the near term impact that changes in technology will create,there are going to be new and expanding challenges for cybersecurity. As a species, we evolve by trying out lots of options. Most fail, some succeed.

One thing that will change in the coming years is that organizational security will become strengthened through this attrition process. Organizations that are repeatedly compromised will lose customers and organizations that don’t will gain them.

Gradually, it is likely that cyber attacks will move more toward targeting homes and private people (where the security is the weakest) and that will also create new cybersecurity markets.

To summarize the next decade, expect to be dealing with new technologies and devices all the time. Expect the amount of data and locations of the data to continue to increase. Looking further into the future, many people wonder about artificial intelligence and a point in time known as the singularity.

singularity (the) – the predicted point in time when artificial intelligence exceeds human intelligence.

There are still a lot of unsolved problems that need to be solved before artificial intelligence can become a reality. Before that time, what is likely to happen is a greater degree of convergence between people and technology.

Post-Reading Questions:

1. How do emerging technologies address the limitations of traditional cybersecurity measures?
2. What role does artificial intelligence play in detecting and preventing cyber threats?
3. How might blockchain technology contribute to improving the security of digital transactions and data storage?
4. In what ways can automation and orchestration streamline cybersecurity processes and response times?
5. How does the adoption of cloud computing impact the design and implementation of cybersecurity strategies?

Activities:

1. Create a presentation or infographic summarizing the key technologies discussed in the overview of cybersecurity.
2. Collaborate with peers to design a hypothetical cybersecurity strategy incorporating the latest technologies.
3. Write a blog post or opinion piece reflecting on the ethical considerations of using advanced technologies in cybersecurity.

UNIT 32
NEW TRENDS IN CYBERSECURITY

1. What are the current challenges and threats facing cybersecurity?
2. How has the landscape of cybersecurity evolved in recent years?
3. Can you name some emerging technologies that impact the field of cybersecurity?
4. What role does artificial intelligence play in enhancing or challenging cybersecurity efforts?
5. How do global events and trends, such as remote work or IoT (Internet of Things), influence cybersecurity concerns?

Pre-Reading Tasks:

1. Research the recent major cybersecurity breaches and their implications.
2. Explore the concept of "zero trust" security models and their implementation in organizations.
3. Investigate the impact of artificial intelligence and machine learning on the detection and prevention of cyber threats.
4. Look into the significance of securing IoT devices and their vulnerabilities.
5. Read about the role of blockchain in enhancing cybersecurity measures.

During Reading Tasks:

1. Take notes on the key trends shaping the future of cybersecurity.
2. Identify specific technologies or methodologies mentioned for improving cybersecurity.
3. Explore case studies or examples illustrating the application of new cybersecurity trends.
4. Investigate the challenges and criticisms associated with implementing certain cybersecurity trends.
5. Pay attention to any predictions or forecasts regarding the future of cybersecurity.

1. Increase of zero-day vulnerabilities in extortion attacks

Attackers could more often use zero-day vulnerabilities to target multiple organizations, said Dick O'Brien, principal intelligence analyst at Symantec, part of Broadcom, an enterprise tech vendor. As evidenced in the MoveIt Transfer attacks, malware groups can use a single vulnerability to target multiple organizations that use the affected tool or technology.

"This is quite effective in that you get multiple victims for a single attack or campaign," O'Brien said. "The damage is done before awareness of the TTPs [tactics, techniques and procedures] become common knowledge."

To combat this social engineering attack, Tavakoli recommended organizations conduct employee awareness training, regularly determine their overall security postureand ensure their downstream security measures can handle an employee falling for a phishing attack.

"You don't want to be overly reliant on any one particular defense mechanism," he said.

2. Generative AI impacts email security

The release of generative AI dominated the tech industry in 2023, so no trend list would be complete without looking at how it could affect organizations from a threat perspective. While attackers already use generative AI to improve phishing emails and reduce the likelihood of spelling and grammar mistakes, they will further integrate generative AI into their social engineering campaigns by using large language models to impersonate high-level decision-makers and publicly visible executives.

"People are super active on LinkedIn or Twitter where they produce lots of information and posts. It's easy to take all this data and dump it into something like ChatGPT and tell it to write something using this specific person's style," said Oliver Tavakoli, CTO at Vectra AI, a cybersecurity vendor. "The attacker can send an email claiming to be from the CEO, CFO or similar role to an employee. Receiving an email that sounds like it's coming from your boss certainly feels far more real than a general email asking for Amazon gift cards."

To combat this social engineering attack, Tavakoli recommended organizations conduct employee awareness training, regularly determine their overall security postureand ensure their downstream security measures can handle an employee falling for a phishing attack.

3. Widespread adoption of passwordless

It's been said for many years, but 2024 could finally be the year passwordless takes off in the enterprise.

"This coming year we're going to truly go passwordless, with biometrics being the winning modality," said Blair Cohen, founder and president of AuthenticID, an identity and access management (IAM) vendor. "It's finally going to happen."

Biometrics makes sense as the common authentication option since people have used fingerprint and facial scanning on consumer devices for years, he said. It can also stand up to attack and fraud better than SMS or email one-time passcodes or other methods.

What industry standard wins out, however, is up for debate. FIDO2 is a contender, but not the winner, Cohen said. "I applaud it and think it's great for everyday consumer use, but don't think FIDO2 will be the choice of enterprises, large-scale banks, etc. There are just too many vulnerabilities," he said, specifically highlighting its vulnerability to first-party fraud.

4. CSOs, CISOs and CEOs work more closely together

Continued economic uncertainty has led to tightened budgets. In 2024, CEOs will likely be working more closely with CSOs and CISOs to determine where to best spend budget security-wise, said Chuck Randolph, CSO, and Marisa Randazzo, executive director of threat management, at security vendor Ontic. This requires CSOs and CISOs to determine where their organizations' risk exists and how to keep data and employees safe, both in-office and remote, they added.

"If I'm a C-suite individual, I'm thinking about risk prioritization, budget optimization and proactive investment in security, whether physical or digital," Randolph said. Organizations should conduct a risk assessment and ensure stakeholders have a say in the security budget, he advised.

Randolph and Randazzo said there could be a convergence of IT security with physical or corporate security, such as identifying and monitoring potential insider threats and disgruntled employees. CISOs can offer input on IT security, they added, while CSOs consider workplace violence issues.

5. Identity verification to see wider adoption

Expect to see more organizations embrace identity verification in 2024 to ensure employees, partners and customers are who they say they are during account onboarding, especially as AI improves.

"If I've never met you before, even if you're appearing on Zoom, how do I know it's really you and not an imposter with access to your computer?" ESG's Poller said. "From an enterprise perspective, how do I authenticate you correctly against a government document?"

Organizations will increasingly use identity verification to onboard and secure account access or reset requests. The technology can also compare employee photographs and information to government documents, as well as provide liveness detection to ensure someone isn't using an AI-generated image or video.

6. Increased adoption of proactive security tools and technology

Organizations should invest more in proactive security tools and technology in 2024 to better detect vulnerabilities and security gaps, said Maxine Holt, senior director of research and content at analyst firm Omdia. With proactive security, she said, organizations can learn where to best spend their budget for their specific use cases.

Holt recommended organizations research proactive security technologies to decide which could most help them. She said to consider the following:

- Risk-based vulnerability management.
- Attack surface management, including cyber asset ASM and external surface ASM.
- Security posture tools for applications, cloud and data.

- Attack path management and security control validation, including penetration testing, red teaming, and breach and attack simulation.

7. More regulations for connected and embedded devices

IoT adoption continues strong, and so does the lack of appropriate security measures on embedded devices. In 2024, we could see more regulatory scrutiny, especially as the threat of AI grows and malicious actors look for additional attack vectors.

"The regulatory outlook for connected devices will continue to evolve as governments and regulatory bodies develop more comprehensive frameworks to address the increased use and development of connected devices and the increased sophistication of attackers," said Veronica Lim, U.S. product security leader at consulting firm Deloitte. "We'll see organizations adhere more closely to cybersecurity-by-design standards."

How organizations will handle increased regulations remains to be seen. Lim explained that organizations already struggle with patch management, which opens opportunities for attackers to exploit. "Connected devices are a frequent target for attackers because they often contain outdated and vulnerable software," she said.

8. Third-party security struggles continue

Breaching a third party, such as a vendor or partner organization, can net attackers more lucrative outcomes. Third parties have their own security strategies and infrastructure, which might not stack up to those of their customers, opening further vectors for attackers.

"The bad guys have gotten really good at identifying these third parties that help them get past the big security apparatus of bigger organizations, such as a bank," said Alex Cox, director of threat intel at LastPass, a password manager vendor. "A big bank spends a ton of money on security, but the vendors they use don't. If you get access to that vendor, it gets you access to a bunch of other companies."

There's no easy answer for organizations worried about third-party security, either. Cox said while it's difficult to enforce a certain level of security with third parties, organizations should consider creating a security checklist their vendors must follow or require third-party security evaluations before doing business with any vendor.

9. Vendors could affect cyber insurance policies

Organizations obtain cyber insurance policies to ease the aftermath of ransomware attacks. At the same time, cyber insurance carriers are tweaking underwriting procedures. Certain vendors could be identified as red flags and affecting an organization's ability to get a policy in 2024. For example, if an organization uses a vendor the insurance carrier deems risky, such as Progress Software, which supplied the MoveIt Transfer application, the carrier could increase premiums or deny coverage.

"There is going to be more scrutiny under your hood when it comes to security posture and technology vendors," said Jess Burn, analyst at advisory firm Forrester. "Product security is going to become something insurance carriers get more involved in. They're going to ask organizations who provides the product and not just if you have it."

Organizations might have to spend time vetting their current and potential vendor partners if cyber insurance providers want more say in their clients' security posture, she said.

Some infosec professionals already think cyber insurance carriers have too much influence when it comes to incident response decisions. Forrester predicted this will continue in the coming year.

Post-Reading Questions:

1. How do the new trends in cybersecurity address the evolving nature of cyber threats?
2. What are the potential benefits and drawbacks of implementing a "zero trust" security model?
3. In what ways does artificial intelligence contribute to both offense and defense in cybersecurity?
4. How can organizations adapt their cybersecurity strategies to accommodate the rise of remote work?
5. What ethical considerations should be taken into account when adopting new cybersecurity technologies?

Activities:

1. Create a presentation outlining the key takeaways from the reading on new trends in cybersecurity.
2. Collaborate with peers to discuss and propose solutions to the challenges associated with implementing new cybersecurity trends.
3. Write a reflective essay on the ethical implications of using advanced technologies in cybersecurity.

CASE STUDY 1

These questions, tasks, and activities are designed to enhance understanding and critical thinking about the considerations involved in hiring a web host, as presented in the case study.

Pre-Reading Questions:

1. What factors should be considered when choosing a web host for a website?
2. How does the type and purpose of a website influence the choice of a web hosting provider?
3. What are the common challenges or issues people face when selecting a web hosting service?
4. Have you ever had experience with choosing a web host, and if so, what were the key considerations you had in mind?
5. What security measures and features should be a priority when evaluating web hosting options?

Pre-Reading Tasks:

1. Research different types of web hosting services (shared hosting, VPS, dedicated hosting) and their respective advantages and disadvantages.
2. Explore customer reviews and testimonials for various web hosting providers to understand user experiences.
3. Investigate the security features offered by different web hosts and how they protect against common threats.
4. Familiarize yourself with the technical requirements of a website and how they align with different hosting options.
5. Look into industry standards and best practices for web hosting to set a benchmark for evaluation.

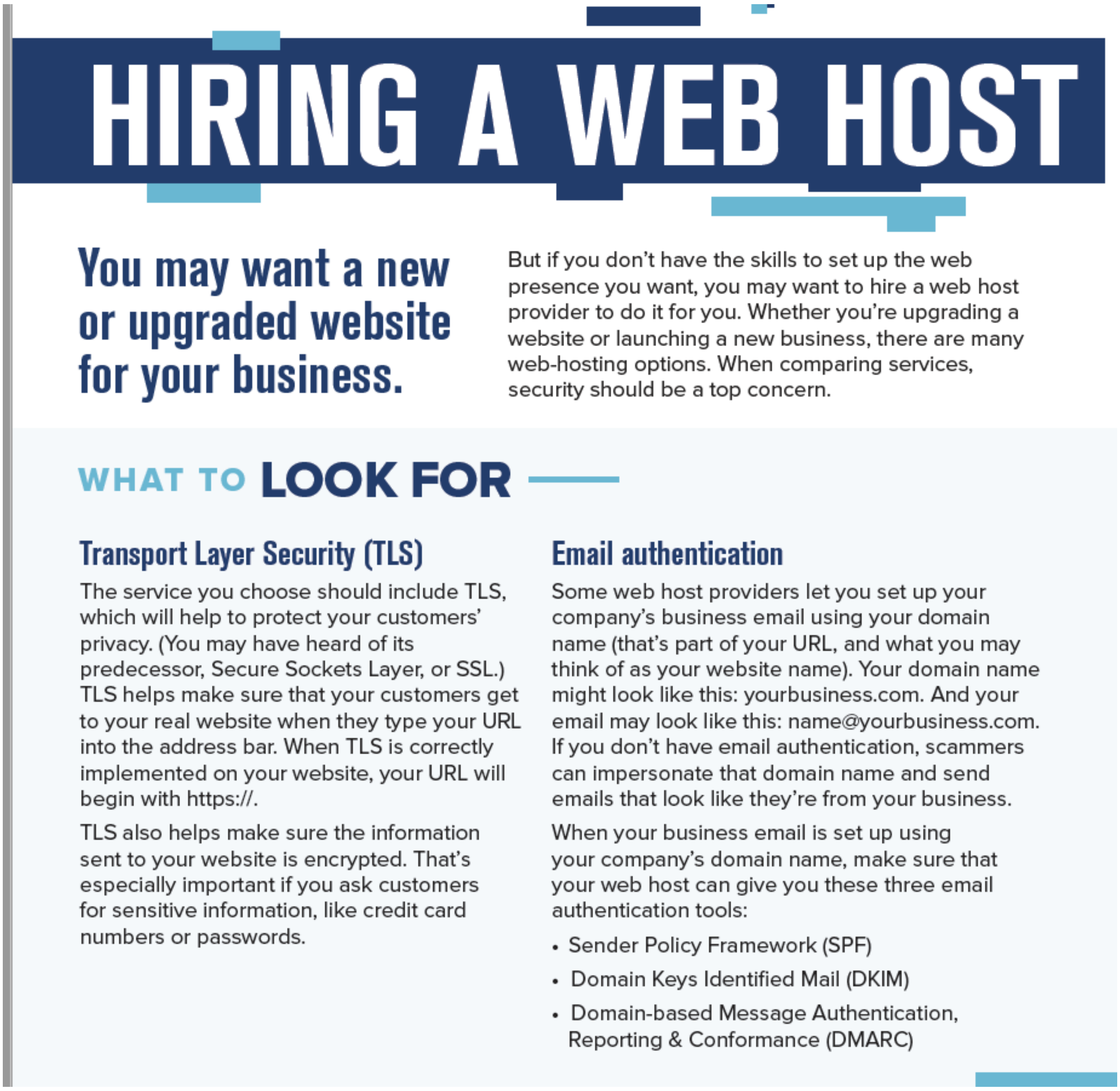
During Reading Tasks:

1. Take notes on the key criteria discussed in the case study for selecting a web host.
2. Identify the specific needs and requirements mentioned in the case study that influence the web hosting decision.
3. Analyze any challenges or constraints faced by the website owner in the case study.
4. Pay attention to the decision-making process and the rationale behind choosing a particular web host.
5. Look for information on how the case study evaluates the scalability and flexibility of potential web hosts.

Post-Reading Questions:

1. What were the main factors influencing the choice of a web host in the case study, and how do they align with your own considerations?
2. What challenges did the website owner face during the decision-making process, and how were they addressed?
3. How did the case study emphasize the importance of scalability and flexibility in web hosting decisions?

4. In retrospect, were there any additional criteria you think should have been considered in the case study?
5. How might the web hosting landscape change in the future, and how can businesses prepare for these changes?



HIRING A WEB HOST

You may want a new or upgraded website for your business.

But if you don't have the skills to set up the web presence you want, you may want to hire a web host provider to do it for you. Whether you're upgrading a website or launching a new business, there are many web-hosting options. When comparing services, security should be a top concern.

WHAT TO LOOK FOR

Transport Layer Security (TLS)

The service you choose should include TLS, which will help to protect your customers' privacy. (You may have heard of its predecessor, Secure Sockets Layer, or SSL.) TLS helps make sure that your customers get to your real website when they type your URL into the address bar. When TLS is correctly implemented on your website, your URL will begin with https://.

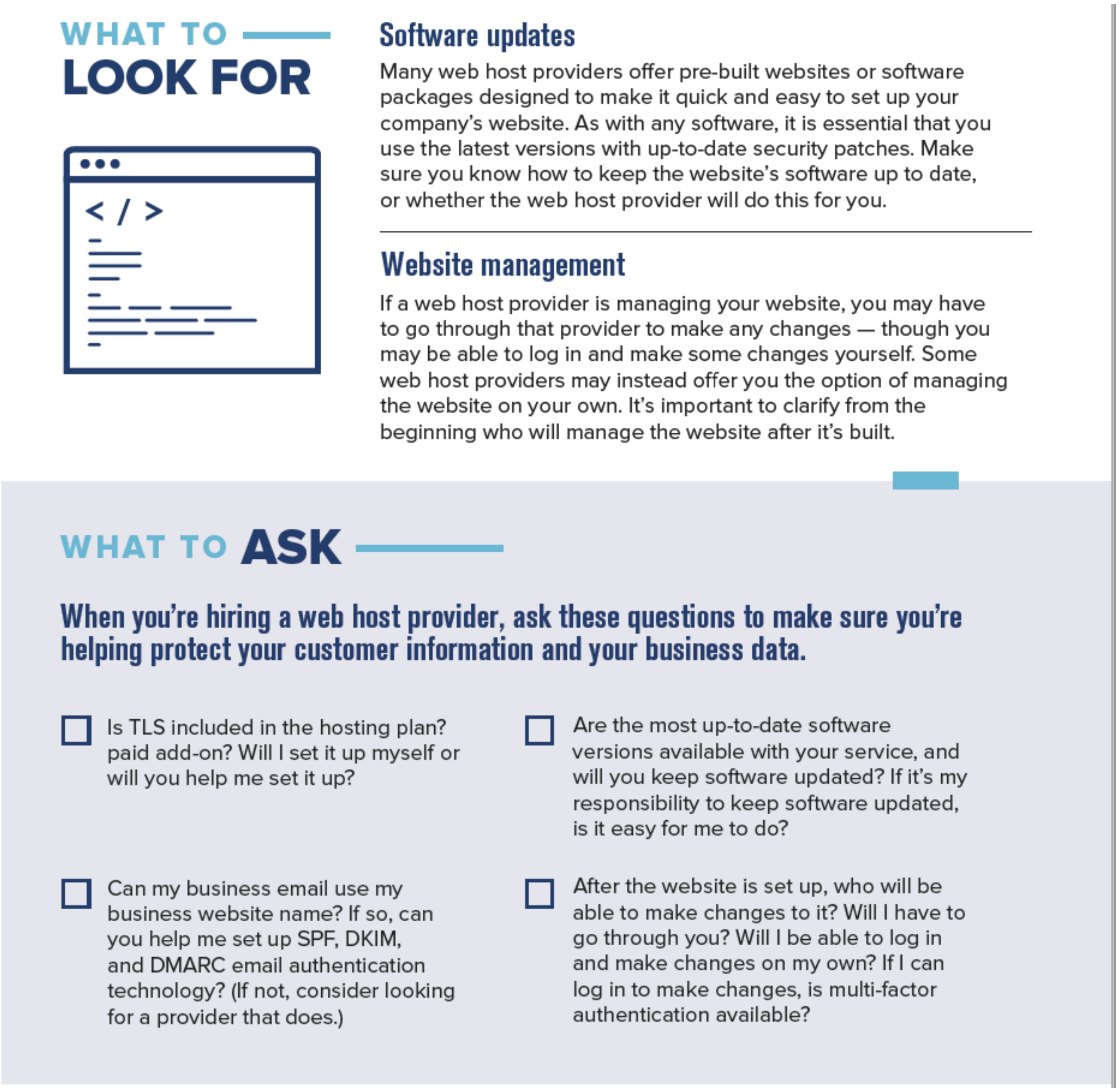
TLS also helps make sure the information sent to your website is encrypted. That's especially important if you ask customers for sensitive information, like credit card numbers or passwords.

Email authentication

Some web host providers let you set up your company's business email using your domain name (that's part of your URL, and what you may think of as your website name). Your domain name might look like this: yourbusiness.com. And your email may look like this: name@yourbusiness.com. If you don't have email authentication, scammers can impersonate that domain name and send emails that look like they're from your business.

When your business email is set up using your company's domain name, make sure that your web host can give you these three email authentication tools:

- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting & Conformance (DMARC)



WHAT TO LOOK FOR

Software updates

Many web host providers offer pre-built websites or software packages designed to make it quick and easy to set up your company's website. As with any software, it is essential that you use the latest versions with up-to-date security patches. Make sure you know how to keep the website's software up to date, or whether the web host provider will do this for you.

Website management

If a web host provider is managing your website, you may have to go through that provider to make any changes — though you may be able to log in and make some changes yourself. Some web host providers may instead offer you the option of managing the website on your own. It's important to clarify from the beginning who will manage the website after it's built.

WHAT TO ASK

When you're hiring a web host provider, ask these questions to make sure you're helping protect your customer information and your business data.

□ Is TLS included in the hosting plan? paid add-on? Will I set it up myself or will you help me set it up?

□ Can my business email use my business website name? If so, can you help me set up SPF, DKIM, and DMARC email authentication technology? (If not, consider looking for a provider that does.)

□ Are the most up-to-date software versions available with your service, and will you keep software updated? If it's my responsibility to keep software updated, is it easy for me to do?

□ After the website is set up, who will be able to make changes to it? Will I have to go through you? Will I be able to log in and make changes on my own? If I can log in to make changes, is multi-factor authentication available?

Post-Reading Activities:

1. Create a checklist or decision matrix for selecting a web host based on the insights from the case study.
2. Role-play scenarios where different stakeholders discuss and debate the choice of a web host, considering varying perspectives and priorities.
3. Develop a comparative analysis chart showcasing different web hosting providers and their features.
4. Write a blog post or article offering advice to others based on the lessons learned from the case study.
5. Organize a group discussion to share personal experiences related to web hosting decisions and learn from each other's insights.

CASE STUDY 2

1.What are the key considerations for ensuring secure remote access to a corporate network?
2.How has the landscape of remote work changed the importance of secure access to organizational resources?
3.Can you list potential security challenges associated with remote access to corporate networks?
4.What technologies and protocols are commonly used for secure remote access?
5.How do businesses balance the need for accessibility with the imperative to maintain security in a remote work environment?

Pre-Reading Tasks:

1.Research common remote access technologies such as VPNs (Virtual Private Networks) and multi-factor authentication (MFA).
2.Investigate recent case studies or examples of security breaches related to insecure remote access.
3.Explore best practices for securing remote access in various industries.
4.Look into the role of cloud-based solutions in providing secure remote access.
5.Familiarize yourself with compliance requirements related to remote access in specific sectors (e.g., healthcare, finance).

During Reading Tasks:

1.Take notes on the specific challenges and solutions presented in the case study.
2.Identify the technologies and strategies employed for securing remote access in the case study.
3.Analyze any incidents or problems encountered and how they were addressed.
4.Evaluate the impact of remote access security measures on user experience and productivity.
5.Pay attention to the role of user training and awareness in the case study.

Post-Reading Questions:

1. What were the key security concerns addressed in the case study, and how were they mitigated?
2. How did the organization balance the need for secure remote access with providing a user-friendly experience?
3. What lessons can be learned from the case study regarding the implementation of multi-factor authentication for remote access?
4. In what ways did the organization ensure compliance with relevant regulations in the case study?
5. What are the potential future challenges or developments that the case study suggests for remote access security?

Post-Reading Activities:

1.Develop a security awareness training module for employees focusing on best practices for secure remote access.
2.Create a flowchart or infographic illustrating the secure remote access architecture mentioned in the case study.

3.Role-play scenarios involving potential security incidents related to remote access and discuss appropriate responses.
4.Write a report or presentation comparing the remote access security measures in the case study with industry best practices.
5.Organize a panel discussion with peers to share insights and experiences related to securing remote access in different organizational contexts.
6.These questions, tasks, and activities aim to enhance your understanding of secure remote access through the exploration of a case study, fostering critical thinking and practical application of knowledge.

TEACHER’S NOTES

UNIT 17

These tasks and activities will help students deepen their understanding of browser requirements and their implications.

1. **Browser Security Discussion:** Engage students in a discussion about browser security and the importance of keeping browsers up to date. They can research and share examples of browser vulnerabilities and the consequences of using outdated browsers. Students can also discuss the different security features offered by various browsers and how they can protect themselves while browsing the internet.

2. **User Reviews and Ratings:** Have students explore user reviews and ratings of different web browsers. They can visit websites or forums where users share their experiences and opinions about different browsers. Students can compile a list of pros and cons for each browser based on these reviews and ratings.

3. **Browser Evolution Timeline:** Ask students to create a timeline showcasing the evolution of web browsers over the years. They can research and include significant milestones, such as the release of major browsers, important updates, and technological advancements that have shaped the development of browsers.

4. **Browser Performance Test:** Have students conduct a performance test comparing different browsers. They can measure factors like page load times, memory usage, and CPU usage while accessing the same website on different browsers. Students can then analyze the results and draw conclusions about the performance of each browser.

UNIT 18

1. Research and create a list of the top five antivirus software programs to protect against online threats.
2. Create a poster or infographic highlighting the dos and don'ts of safe browsing.
3. Role-play different scenarios where someone encounters a potential online threat and discuss the appropriate actions to take.
4. Conduct a group discussion on the importance of password security and ways to create strong passwords.
5. Assign students to find and analyze real-life examples of online scams or phishing attempts, and present their findings to the class.

UNIT 19

1. Set up a small wireless LAN network at home or in a classroom, and document the steps and challenges encountered during the setup process.
2. Create a poster or infographic illustrating the key components and working principles of a wireless LAN.

UNIT 20

1. Role-play scenarios where users encounter security threats on their home Wi-Fi networks and discuss how to handle them.
2. Engage in a group discussion about the ethical implications of using open Wi-Fi networks and potential risks involved.

UNIT 21

1. Conduct a self-audit of your social media accounts, adjusting privacy settings and security features.
2. Develop a set of guidelines for safe social media usage and share them with your peers.
3. Create an infographic or poster highlighting the dos and don'ts of safe browsing on social networking sites.
4. Organize a group discussion or workshop on online safety, focusing on practical tips for social media users.
5. Write a short guide for parents on how to educate their children about safe browsing and social media use.

UNIT 22

1. Develop a checklist for configuring email clients with security best practices.
2. Organize a workshop or webinar on email security for your community or workplace.

UNIT 23

1. Organize a workshop or presentation on smartphone security for a local community or organization.
2. Role-play scenarios where individuals practice securing their smartphones in various public settings.

UNIT 24

1. Conduct a comparative analysis of different encryption algorithms and their suitability for specific communication needs.
2. Engage in a group discussion about the ethical considerations surrounding privacy and secure communication in the digital era.

UNIT 25

1. Conduct a mock debate on the legality and morality of hacktivist actions.
2. Develop a cybersecurity strategy for an organization to mitigate the risks associated with hacktivist threats.
3. Collaborate on a group project to analyze a recent hacktivist incident, including its causes and consequences.

UNIT 26

1. Design a simple IoT project or prototype and outline its functionalities.
2. Engage in a group discussion about potential regulations and standards needed to ensure the responsible development and use of IoT technology.

UNIT 27

1. Organize a mock cybersecurity incident response drill to practice handling a security breach scenario.

2. Participate in a group discussion or debate on the ethical considerations of cybersecurity practices and policies.

UNIT 28

1. Engage in a group discussion on emerging cyber threats and how organizations can adapt their Cyber Risk Registers to address these new challenges.

UNIT 29

1. Conduct a workshop or training session on the importance of security frameworks for business stakeholders.
2. Analyze a recent cybersecurity incident in the business world and discuss how a robust framework might have mitigated the risk.
3. Formulate a set of guidelines for businesses to assess and select an appropriate security framework based on their needs.

UNIT 30

1. Organize a simulated tabletop exercise where participants respond to a fictional cyberattack scenario based on the Sony Pictures incident.
2. Conduct a group discussion on the ethical considerations surrounding cyberattacks and the protection of sensitive information in the entertainment industry.

UNIT 31

1. Develop a case study illustrating the application of artificial intelligence in a real-world cybersecurity scenario.
2. Role-play a discussion between cybersecurity professionals evaluating the adoption of new technologies in a corporate setting.

UNIT 32

1. Develop a scenario-based exercise where participants have to apply the principles of a "zero trust" security model.
2. Design a cybersecurity awareness campaign highlighting the importance of securing IoT devices.

GLOSSARY

A

access control — The means and mechanisms of managing access to and use of resources by users. There are three primary forms of access control: DAC, MAC, and RBAC. DAC (Discretionary Access Control) manages access through the use of on-object ACLs (Access Control Lists), which indicate which users have been granted (or denied) specific privileges or permissions on that object. MAC (Mandatory Access Control) restricts access by assigning each subject and object a classification or clearance level label; resource use is then controlled by limiting access to those subjects with equal or superior labels to that of the object. RBAC (Role Base Access Control) controls access through the use of job labels, which have been assigned the permissions and privilege needed to accomplish the related job tasks. (Also known as authorization.)

anti-virus (anti-malware) — A security program designed to monitor a system for malicious software. Once malware is detected, the AV program will attempt to remove the offending item from the system or may simply quarantine the file for further analysis by an administrator. It is important to keep AV software detection databases current in order to have the best chance of detecting known forms of malware.

antivirus software — A software program that monitors a computer system or network communications for known examples of malicious code and then attempts to remove or quarantine the offending items. (Also known as Malware Scanner.) Most anti-virus (AV) products use a pattern recognition or signature matching system to detect the presence of known malicious code. Some AV products have adopted technologies to potentially detect new and unknown malware. These technologies include anomaly detection (i.e. watch for programs which violate specific rules), behavioral detection (i.e. watch for programs that have behaviors that are different from the normal baseline of behavior of the system), and heuristic detection (i.e. watch for programs that exhibit actions which are known to be those of confirmed malware; it is a type of technological profiling).

APT (Advanced Persistent Threat) — A security breach that enables an attacker to gain access or control over a system for an extended period of time usually without the owner of the system being aware of the violation. Often an APT takes advantage of numerous unknown vulnerabilities or zero day attacks, which allow the attacker to maintain access to the target even as some attack vectors are blocked.

asset — Anything that is used in and is necessary to the completion of a business task. Assets include both tangible and intangible items such as equipment, software code, data, facilities, personnel, market value and public opinion.

authentication — The process of proving an individual is a claimed identity. Authentication is the first element of the AAA services concept, which includes Authentication, Authorization, and Accounting. Authentication occurs after the initial step of identification (i.e. claiming an identity). Authentication is accomplished by providing one or more authentication factors—Type 1: something you know (e.g. password, PIN, or combination), Type 2: something you have (e.g. smart card, RSA SecureID FOB, or USB drive), and Type 3: something you are (e.g. biometrics—fingerprint, iris scan, retina scan, hand geometry, signature verification, voice recognition, and keystroke dynamics).

authorization — The security mechanism determining and enforcing what authenticated users are authorized to do within a computer system. The dominant forms of authorization are DAC, MAC and RBAC. DAC (Discretionary Access Control) manages access using ACL (Access Control Lists) on each resource object where users are listed along with the permissions or privileges granted or denied them. MAC (Mandatory Access Control) manages access using labels of classification or clearance on both subjects and objects, and only those subjects with equal or superior clearance are allowed to access resources. RBAC (Role Based Access Control) manages access using labels of a job role that has been granted the permissions and privileges needed to accomplish a specific job or role.

B

backing up — Creating a duplicate copy of data onto a separate physical storage device or online/cloud storage solution. A backup is the only insurance against data loss. With a backup, damaged or lost data files can be restored. Backups should be created on a regular, periodic basis such as daily. A common strategy is based on the 3-2-1 rule: you should have three copies of your data - the original and 2 backups; you should use 2 different types of media (such as a physical media (such as a hard drive or tape) and a cloud storage solution); and do not store the three copies of data in 1 plane (i.e. backups should be stored offsite). It is important to store backups for disaster recovery at an offsite location in order to insure they are not damaged by the same event that would damage the primary production location. However, additional onsite backups can be retained for resolving minor issues such as accidental file deletion or hard drive failure.

BCP (Business Continuity Planning) — A business management plan used to resolve issues that threaten core business tasks. (Also known as Business Continuity Management.) The goal of BCP is to prevent the failure of mission critical processes when they have be harmed by a breach or accident. Once core business tasks have been stabilized, BCP dictates the procedure to return the environment back to normal conditions. BCP is used when the normal security policy has failed to prevent harm from occurring, but before the harm has reached the level of fully interrupting mission critical processes, which would trigger the Disaster Recovery Process (DRP).

behavior monitoring — Recording the events and activities of a system and its users. The recorded events are compared against security policy and behavioral baselines to evaluate compliance and/or discover violations. Behavioral monitoring can include the tracking of trends, setting of thresholds and defining responses. Trend tracking can reveal when errors are increasing requiring technical support services, when abnormal load levels occur indicating the presence of malicious code, or when production work levels increase indicating a need to expand capacity. Thresholds are used to define the levels of activity or events above which are of concern and require a response. The levels below the threshold are recorded but do not trigger a response. Responses can be to resolve conflicts, handle violations, prevent downtime or improve capabilities.

blacklist — A security mechanism prohibiting the execution of those programs on a known malicious or undesired list of software. The blacklist is a list of specific files known to be malicious or otherwise are unwanted. Any program on the list is prohibited from executing while any other program, whether benign or malicious, is allowed to execute by default. (See whitelist.)

block cipher — A type of symmetric encryption algorithm that divides data into fixed length sections and then performs the encryption or decryption operation on each block. The action of dividing a data set into blocks enables the algorithm to encrypt data of any size.

botnet — A collection of innocent computers which have been compromised by malicious code in order to run a remote control agent granting an attacker the ability to remotely take advantage of the system's resources in order to perform illicit or criminal actions. These actions include DoS flooding attacks, hosting false Web services, spoofing DNS, transmitting SPAM, eavesdropping on network communications, recording VOIP communications and attempting to crack encryption or password hashes. Botnets can be comprised of dozens to over a million individual computers. The term botnet is a shortened form of robotic network.

bug — An error or mistake in software coding or hardware design or construction. A bug represents a flaw or vulnerability in a system discoverable by attackers and used as point of compromise. Attacks often use fuzzing technique (i.e. randomize testing tools) to locate previously unknown bugs in order to craft new exploits.

BYOD (Bring Your Own Device) — A company’s security policy dictating whether or not workers can bring in their own devices into the work environment, whether or not such devices can be connected to the company network and to what extent that connection allows interaction with company resources. A BYOD policy can range from complete prohibition of personal devices being brought into the facility to allowing any device to be connected to the company network with full access to all company resources. Generally, a BYOD policy puts reasonable security limitations on which devices can be used on company property and severely limits access to sensitive company network resources. BYOD should address concerns such as data ownership, asset tracking, geo location, patching and upgrades, security applications (such as malware scanners, firewalls and IDS), storage segmentation, appropriate vs inappropriate applications, on-boarding, off-boarding, repair/replacement due to damage, legal concerns, internal investigations and law enforcement investigations and forensics.

C

ciphertext — The unintelligible and seeming random form of data that is produced by the cryptographic function of encryption. Ciphertext is produced by a symmetric algorithm when a data set is transformed by the encryption process using a selected key. Ciphertext can converted back into its original form (i.e. plain text) by performing the decryption process using the same symmetric encryption algorithm and the key used during the encryption process. (Also known as cryptogram.)

clickjacking — A malicious technique by which a victim is tricked into clicking on a URL, button or other screen object other than that intended by or perceived by the user. Clickjacking can be performed in many ways; one of which is to load a web page transparently behind another visible page in such a way that the obvious links and objects to click are facades, so clicking on an obvious link actually causes the hidden page's link to be selected.

cloud computing — A means to offer computing services to the public or for internal use through remote services. Most cloud computing systems are based on remote virtualization where the application or operating environment offered to customers is hosted on the cloud provider's computer hardware. There are a wide range of cloud solutions including software applications (examples include e-mail and document editing), custom code hosting (namely execution platforms and web services) as well as full system replacements (such as remote virtual services to host databases or file storage). (See SaaS, PaaS, and IaaS.) Most forms of cloud computing are considered public cloud as they are provided by a third party. However, private cloud (internally hosted), community cloud (a group of companies' privately hosted cloud), a hosted private cloud (the cloud servers are owned and managed by a third party but hosted in the facility of the customer) and hybrid cloud (a mixture of public and private) are also options.

CND (Computer Network Defense) — The establishment of a security perimeter and of internal security requirements with the goal of defending a network against cyberattacks, intrusions and other violations. A CND is defined by a security policy and can be stress tested using vulnerability assessment and penetration testing measures.

cracker — The proper term to refer to an unauthorized attacker of computers, networks and technology instead of the misused term "hacker." However, this term is not as widely used in the media; thus, the term hacker has become more prominent in-spite of the terms misuse. (See hacker.)

critical infrastructure — The physical or virtual systems and assets that are vital to an organization or country. If these systems are compromised, the result would be catastrophic. If an organization's mission critical processes are interrupted, this could result in the organization ceasing to exist. If a country's critical infrastructure is destroyed, it will have severe negative impact on national security, economic stability, citizen safety and health, transportation and communications.

CVE (Common Vulnerabilities and Exposures) — An online database of attacks, exploits and compromises operated by the MITRE organization for the benefit of the public. It includes any and all attacks and abuses known for any type of computer system or software product. Often new attacks and exploits are documented in a CVE long before a vendor admits to the issue or releases an update or patch to resolve the concern.

cryptography — The application of mathematical processes on data-at-rest and data-in-transit to provide the security benefits of confidentiality, authentication, integrity and non-repudiation. Cryptography includes three primary components: symmetric encryption, asymmetric encryption and hashing. Symmetric encryption is used to provide confidentiality. Asymmetric encryption is used to provide secure symmetric key generation, secure symmetric key exchange (via digital envelopes created through the use of the recipient's public key) verification of source, verification/control of recipient, digital signature (a combination of hashing and use of the sender's private key) and digital certificates (which provides third-party authentication services). Hashing is the cryptographic operation that produces a representational value from an input data set. A before and after hash can be compared in order to detect protection of or violation of integrity.

cyberattack — Any attempt to violate the security perimeter of a logical environment. An attack can focus on gathering information, damaging business processes, exploiting flaws, monitoring targets, interrupting business tasks, extracting value, causing damage to logical or physical assets or using system resources to support attacks against other targets. Cyberattacks can be initiated through exploitation of a vulnerability in a publicly exposed service, through tricking a user into opening an infectious attachment, or even causing automated installation of exploitation tools through innocent website visits. (Also known as drive-by download.)

cyber ecosystem — The collection of computers, networks, communication pathways, software, data and users that comprise either a local private network or the world-wide Internet. It is the digital environment within which software operates and data is manipulated and exchanged.

cyberespionage — The unethical act of violating the privacy and security of an organization in order to leak data or disclose internal/private/confidential information. Cyberespionage can be performed by individuals, organization or governments for the direct purpose of causing harm to the violated entity to benefit individuals, organizations or governments.

cybersecurity — The efforts to design, implement, and maintain security for an organization's network, which is connected to the Internet. It is a combination of logical/technical-, physical- and personnel-focused countermeasures, safeguards and security controls. An organization's cybersecurity should be defined in a security policy, verified through evaluation techniques (such as vulnerability assessment and penetration testing) and revised, updated and improved over time as the organization evolves and as new threats are discovered.

cyber teams — Groups of professional or amateur penetration testing specialists who are tasked with evaluating and potentially improving the security stance of an organization. Common cyber teams include the red, blue and purple/white teams. A red team is often used as part of a multi-team penetration test (i.e. security evaluation), which is responsible for attacking the target which is being defended by the blue team. A purple team or white team is either used as a reference between the attack/red and defense/blue teams; or this team can be used as an interpreter of the results and activities of the red and blue teams in order to maximize their effectiveness in the final results.

D

data breach — The occurrence of disclosure of confidential information, access to confidential information, destruction of data assets or abusive use of a private IT environment. Generally, a data breach results in internal data being made accessible to external entities without authorization.

data integrity — A security benefit that verifies data is unmodified and therefore original, complete and intact. Integrity is verified through the use of cryptographic hashing. A hashing algorithm generates a fixed length output known as a hash value, fingerprint or MAC (Message Authenticating Code), which is derived from the input data but which does not contain the input data. This makes hashing a one-way operation. A hash is calculated before an event, and another hash is calculated after the event (an event can be a time frame of storage (i.e. data-at-rest) or an occurrence of transmission (i.e. data-in-transit); the two hashes are then compared using an XOR Boolean operation. If the two hashes exactly match (i.e. the XOR result is zero), then the data has retained its integrity.

However, if the two hashes do not match exactly (i.e. the XOR result is a non-zero value), then something about the data changed during the event.

data mining — The activity of analyzing and/or searching through data in order to find items of relevance, significance or value. The results of data mining are known as meta-data. Data mining can be a discovery of individual important data items, a summary or overview of numerous data items or a consolidation or clarification of a collection of data items.

data theft — The act of intentionally stealing data. Data theft can occur via data loss (physical theft) or data leakage (logical theft) event. Data loss occurs when a storage device is lost or stolen. Data leakage occurs when copies of data is possessed by unauthorized entities.

DDoS (Distributed Denial of Service) Attack — An attack which attempts to block access to and use of a resource. It is a violation of availability. DDOS (or DDoS) is a variation of the DoS attack (see DOS) and can include flooding attacks, connection exhaustion, and resource demand. The distinction of DDOS from DOS is that the attack traffic may originate from numerous sources or is reflected or bounced off of numerous intermediary systems. The purpose of a DDoS attack is to significantly amplify the level of the attack beyond that which can be generated by a single attack system in order to overload larger and more protected victims. DDoS attacks are often waged using botnets. (See botnet.)

decrypt — The act which transforms ciphertext (i.e. the unintelligible and seeming random form of data that is produced by the cryptographic function of encryption) back into its original plaintext or cleartext form. Ciphertext is produced by a symmetric encryption algorithm when a data set is transformed by the encryption process using a selected key. Ciphertext can converted back into its original form (i.e. plaintext) by performing the decryption process using the same symmetric encryption algorithm and the same key used during the encryption process.

digital certificate — A means by which to prove identity or provide authentication commonly by means of a trusted third-party entity known as a certificate authority. A digital certificate is based on the x.509 v3 standard. It is the public key of a subject signed by the private key of a certificate authority with clarifying text information such as issuer, subject identity, date of creation, date of expiration, algorithms, serial number and thumbprint (i.e. hash value).

digital forensics — The means of gathering digital information to be used as evidence in a legal procedure. Digital forensics focuses on gathering, preserving and analyzing the fragile and volatile data from a computer system and/or network. Computer data that is relevant to a security breach and/or criminal action is often intermixed with standard benign data from business functions and personal activities. Thus, digital forensics can be challenging to properly collect relevant evidence while complying with the rules of evidence in order to ensure that such collected evidence is admissible in court.

DLP (Data Loss Prevention) — A collection of security mechanisms which aim at preventing the occurrence of data loss and/or data leakage. Data loss occurs when a storage device is lost or stolen while data leakage occurs when copies of data is possessed by unauthorized entities. In both cases, data is accessible to those who should not have access. DLP aims at preventing such occurrences through various techniques such as strict access controls on resources, blocking the use of email attachments, preventing network file exchange to external systems, blocking cut-and-paste, disabling use of social networks and encrypting stored data.

DMZ (Demilitarized Zone) — A segment or subnet of a private network where resources are hosted and accessed by the general public from the Internet. The DMZ is isolated from the private network using a firewall and is protected from obvious abuses and attacks from the Internet using a firewall. A DMZ can be deployed in two main configurations. One method is the screened subnet configuration, which has the structure of I-F-DMZ-F-LAN (i.e. internet, then firewall, then the DMZ, then another firewall, then the private LAN). A second method is the multi-homed firewall configuration, which has the structure of a single firewall with three interfaces, one connecting to the Internet, a second to the DMZ, and a third to the private LAN.

DOS (Denial of Service) — An attack that attempts to block access to and use of a resource. It is a violation of availability. DOS (or DoS) attacks include flooding attacks, connection exhaustion and resource demand. A flooding attack sends massive amounts of network traffic to the target overloading the ability of network devices and servers to handle the raw load. Connection exhaustion repeatedly makes connection requests to a target to consume all system resources related to connections, which prevents any other connections from being established or maintained. A resource demand DoS repeatedly requests a resource from a server in order to keep it too busy to respond to other requests.

drive-by download — A type of web-based attack that automatically occurs based on the simple act of visiting a malicious or compromised/poisoned Web site. A drive-by download is accomplished by taking advantage of the default nature of a Web browser to execute mobile code, most often JavaScript, with little to no security restrictions. A drive-by download can install tracking tools, remote access backdoors, botnet agents, keystroke loggers or other forms of malicious utilities. In most cases, the occurrence of the infection based on the drive-by download is unnoticed by the user/victim.

E

eavesdropping — The act of listening in on a transaction, communication, data transfer or conversation. Eavesdropping can be used to refer to both data packet capture on a network link (also known as sniffing or packet capture) and to audio recording using a microphone (or listening with ears).

encode — The act which transforms plaintext or cleartext (i.e. the original form of normal standard data) into ciphertext (i.e. the unintelligible and seeming random form of data that is produced by the cryptographic function of encryption). Ciphertext is produced by a symmetric encryption algorithm when a data set is transformed by the encryption process using a selected key (i.e. to encrypt or encode). Ciphertext can converted back into its original form (i.e. plaintext) by performing the decryption process using the same symmetric encryption algorithm and the same key used during the encryption process (i.e. decrypt or decode).

encryption key — The secret number value used by a symmetric encryption algorithm to control the encryption and decryption process. A key is a number defined by its length in binary digits. Generally, the longer the key length, the more security (i.e. defense against confidentiality breaches) it provides. The length of the key also determines the key space, which is the range of values between the binary digits being all zeros and all ones from which the key can be selected.

F

firewall — A security tool, which may be a hardware or software solution that is used to filter network traffic. A firewall is based on an implicit deny stance where all traffic is blocked by default. Rules, filters or ACLs can be defined to indicate which traffic is allowed to cross the firewall. Advanced firewalls can make allow/deny decisions based on user authentication, protocol, header values and even payload contents.

H

hacker — A person who has knowledge and skill in analyzing program code or a computer system, modifying its functions or operations and altering its abilities and capabilities. A hacker may be ethical and authorized (the original definition) or may be malicious and unauthorized (the altered but current use of the term). Hackers can range from professionals who are skilled programmers to those who have little to no knowledge of the specifics of a system or exploit but who can follow directions; in this instance, they are called script kiddies.

hacktivism — Attackers who hack for a cause or belief rather than some form of personal gain. Hacktivism is often viewed by attackers as a form of protest or fighting for their perceived “right” or “justice.” However, it is still an illegal action in most cases when the victim’s technology or data is abused, harmed or destroyed.

honeypot — A trap or decoy for attackers. A honeypot is used to distract attackers in order to prevent them from attacking actual production systems. It is a false system that is configured to look and function as a production system and is positioned where it would be encountered by an unauthorized entity who is seeking out a connection or attack point. A honeypot may contain false data in order to trick attackers into spending considerable time and effort attacking and exploiting the false system. A honeypot may also be able to discover new attacks or the identity of the attackers.

I

IaaS (Infrastructure-as-a-Service) — A type of cloud computing service where the provider offers the customer the ability to craft virtual networks within their computing environment. An IaaS solution enables a customer to select which operating systems to install into virtual machines/nodes as well as the structure of the network including use of virtual switches, routers and firewalls. It also provides complete freedom as to the software or custom code run on the virtual machines. An IaaS solution is the most flexible of all the cloud computing services; it allows for significant reduction in hardware by the customer in their own local facility. It is the most expensive form of cloud computing service.

identity cloning — A form of identity theft in which the attacker takes on the identity of a victim and then attempts to live and act as the stolen identity. Identity cloning is often performed in order to hide the birth country or a criminal record of the attacker in order to obtain a job, credit or other secured financial instrument.

identity fraud — A form of identity theft in which a transaction, typically financial, is performed using the stolen identity of another individual. The fraud is due to the attacker impersonating someone else.

IDS (Intrusion Detection System) — A security tool that attempts to detect the presence of intruders or the occurrence of security violations in order to notify administrators, enable more detailed or focused logging or even trigger a response such as disconnecting a session or blocking an IP address. An IDS is considered a more passive security tool as it detects compromises after they are already occurring rather than preventing them from becoming successful.

information security policy — A written account of the security strategy and goals of an organization. A security policy is usually comprised of standards, policies (or SOPs – Standard Operating Procedures) and guidelines. All hardware, software, facilities and personnel must abide by the terms of the security policy of an organization. (Also known as security policy.)

insider threat — The likelihood or potential that an employee or another form of internal personnel may pose a risk to the stability or security of an organization. An insider has both physical access and logical access (through their network logon credentials). These are the two types of access that an outside attacker must first gain before launching malicious attacks whereas an insider already has both of these forms of access. Thus, an insider is potentially a bigger risk than an outsider if that insider goes rogue or is tricked into causing harm.

IPS (Intrusion Prevention System) — A security tool that attempts to detect the attempt to compromise the security of a target and then prevent that attack from becoming successful. An IPS is considered a more active security tool as it attempts to proactively respond to potential threats. An IPS can block IP addresses, turn off services, block ports and disconnect sessions as well as notify administrators.

ISP (Internet Service Provider) — The organization that provides connectivity to the Internet for individuals or companies. Some ISPs offer additional services above that of just connectivity such as e-mail, web hosting and domain registration.

J

JBOH (JavaScript-Binding-Over-HTTP) — A form of Android-focused mobile device attack that enables an attacker to be able to initiate the execution of arbitrary code on a compromised device. A JBOH attack often takes place or is facilitated through compromised or malicious apps.

K

keylogger — Any means by which the keystrokes of a victim are recorded as they are typed into the physical keyboard. A keylogger can be a software solution or a hardware device used to capture anything that a user might type in including passwords, answers to secret questions or details and information form e-mails, chats and documents.

L

LAN (Local Area Network) — An interconnection of devices (i.e. a network) that is contained within a limited geographic area (typically a single building). For a typical LAN, all of the network cables or interconnection media is owned and controlled by the organization unlike a WAN (Wide Area Network) where the interconnection media is owned by a third party.

link jacking — A potentially unethical practice of redirecting a link to a middle-man or aggregator site or location rather than the original site the link seemed to indicate it was directed towards. For example, a news aggregation service may publish links that seem as if they point to the original source of their posted articles, but when a user discovers those links via search or through social networks, the links redirect back to the aggregation site and not the original source of the article.

M

malware (malicious software) — Any code written for the specific purpose of causing harm, disclosing information or otherwise violating the security or stability of a system. Malware includes a wide range of types of malicious programs including: virus, worm, Trojan horse, logic bomb, backdoor, Remote Access Trojan (RAT), rootkit, ransomware and spyware/adware.

O

outsider threat — The likelihood or potential that an outside entity, such as an ex-employee, competitor or even an unhappy customer, may pose a risk to the stability or security of an organization. An outsider must often gain logical or physical access to the target before launching malicious attacks.

outsourcing — The action of obtaining services from an external entity. Rather than performing certain tasks and internal functions, outsourcing enables an organization to take advantages of external entities that can provide services for a fee. Outsourcing is often used to obtain best-of-breed level service rather than settling for good-enough internal operations. It can be expensive and increases an organization's security risk due to the exposure of internal information and data to outsiders.

OWASP (Open Web Application Security Project) — An Internet community focused on understanding web technologies and exploitations. Their goal is to help anyone with a website improve the security of their site through defensive programming, design and configuration. Their approach includes understanding attacks in order to know how to defend against them. OWASP offers numerous tools and utilities related to website vulnerability evaluation and discovery as well as a significant amount of training and reference material related to all things web security.

P

PaaS (Platform-as-a-Service) — A type of cloud computing service where the provider offers the customer the ability to operate custom code or applications. A PaaS operator determines which operating systems or execution environments are offered. A PaaS system does not allow the customer to change operating systems, patch the OS or alter the virtual network space. A PaaS system allows the customer to reduce hardware deployment in their own local facility and to take advantage of on-demand computing (also known as pay as you go).

packet sniffing — The act of collecting frames or packets off of a data network communication. This activity allows the evaluation of the header contents as well as the payload of network communications. Packet sniffing requires that the network interface card be placed into promiscuous mode in order to disable the MAC (Media Access Control) address filter which would otherwise discard any network communications not intended for the specific local network interface. (Also known as sniffing or eavesdropping.)

patch — An update or change or an operating system or application. A patch is often used to repair flaws or bugs in deployed code as well as introduce new features and capabilities. It is good security practice to test all updates and patches before implementation and attempt to stay current on patches in order to have the latest version of code that has the fewest known flaws and vulnerabilities.

patch management — The management activity related to researching, testing, approving and installing updates and patches to computer systems, which includes firmware, operating systems and applications. A patch is an update, correction, improvement or expansion of an existing software product through the application of new code issued by the vendor. Patch management is an essential part of security management in order to prevent downtime, minimize vulnerabilities and prevent new untested updates from interfering with productivity.

payment card skimmers — A malicious device used to read the contents of an ATM, debit or credit card when inserted into a POS (Point of Sale) payment system. A skimmer may be an internal component or an external addition. An attacker will attempt to use whatever means to imbed their skimmer into a payment system that will have the highest likelihood of not being detected and thus gather the most amount of financial information from victims. (See POS intrusions.)

pen testing — A means of security evaluation where automated tools and manual exploitations are performed by security and attack experts. This is an advanced form of security assessment that should only be used by environments with a mature security infrastructure. A penetration test will use the same tools, techniques and methodologies as criminal hackers, and thus, it can cause downtime and system damage. However, such evaluations can assist with securing a network by discovering flaws that are not visible to automated tools based on human (i.e. social engineering) or physical attack concepts. (Also known as penetration testing or ethical hacking.)

phishing — A social engineering attack that attempts to collect information from victims. Phishing attacks can take place over e-mail, text messages, through social networks or via smart phone apps. The goal of a phishing attack may be to learn logon credentials, credit card information, system configuration details or other company, network, computer or personal identity information. Phishing attacks are often successful because they mimic legitimate communications from trusted entities or groups such as false emails from a bank or a retail website.

PKI (Public Key Infrastructure) — A security framework (i.e. a recipe) for using cryptographic concepts in support of secure communications, storage and job tasks. A PKI solution is a combination of symmetric encryption, asymmetric encryption, hashing and digital certificate-based authentication.

POS (Point of Sale) intrusions — An attack that gains access to the POS (Point of Sale) devices at a retail outlet enabling an attacker to learn payment card information as well as other customer details. POS intrusions can occur against a traditional brick-and-mortar retail location as well as any online retail websites. (See payment card skimmers.)

R

ransomware — A form of malware that holds a victim's data hostage on their computer typically through robust encryption. This is followed by a demand for payment in the form of Bitcoin (an untraceable digital currency) in order to release control of the captured data back to the user.

restore — The process of returning a system back to a state of normalcy. A restore or restoration process may involve formatting the main storage device before re-installing the operating system and applications as well as copying data from backups onto the reconstituted system.

risk assessment — The process of evaluating the state of risk of an organization. Risk assessment is often initiated through taking an inventory of all assets, assigning each asset a value, and then considering any potential threats against each asset. Threats are evaluated for their exposure factor (EF) (i.e. the amount of loss that would be caused by the threat causing harm) and frequency of occurrence (i.e. ARO—Annualized Rate of Occurrence) in order to calculate a relative risk value known as the ALE (Annualized Loss Expectancy). The largest ALE indicates the biggest concern or risk for the organization.

risk management — The process of performing a risk assessment and evaluating the responses to risk in order to mitigate or otherwise handle the identified risks. Countermeasures, safeguards or security controls are to be selected that may eliminate or reduce risk, assign or transfer risk to others (i.e. outsourcing or buying insurance) or avoid and deter risk. The goal is to reduce risk down to an acceptable or tolerable level.

S

SaaS (Software-as-a-Service) — A type of cloud computing service where the provider offers the customer the ability to use a provided application. Examples of a SaaS include online e-mail services or online document editing systems. A user of a SaaS solution is only able to use the offered application and make minor configuration tweaks. The SaaS provider is responsible for maintaining the application.

sandboxing — A means of isolating applications, code or entire operating systems in order to perform testing or evaluation. The sandbox limits the actions and resources available to the constrained item. This allows for the isolated item to be used for evaluation while preventing any harm or damage to be caused to the host system or related data or storage devices.

SCADA (Supervisory Control and Data Acquisition) — A complex mechanism used to gather data and physical world metrics as well as perform measurement or management actions of the monitored systems for the purposes of automatic large complex real-world processes such as oil refining, nuclear power generation or water filtration. SCADA can provide automated control over very large complex systems whether concentrated in a single physical location or spread across long distances.

security control — Anything used as part of a security response strategy which addresses a threat in order to reduce risk. (Also known as countermeasure or safeguard.)

security perimeter — The boundary of a network or private environment where specific security policies and rules are enforced. The systems and users within the security boundary are forced into compliance with local security rules while anything outside is not under such restrictions. The security perimeter prevents any interactions between outside entities and internal entities that might violate or threaten the security of the internal systems.

SIEM (Security Information and Event Management) — A formal process by which the security of an organization is monitored and evaluated on a constant basis. SIEM helps to automatically identify systems that are out of compliance with the security policy as well as to notify the IRT (Incident Response Team) of any security violating events.

sniffing — See packet sniffing and eavesdropping.

social engineering — An attack focusing on people rather than technology. This type of attack is psychological and aims to either gain access to information or to a logical or physical environment. A social engineering attack may be used to gain access to a facility by tricking a worker into assisting by holding the door when making a delivery, gaining access into a network by tricking a user into revealing their account credentials to the false technical support staff or gaining copies of data files by encouraging a worker to cut-and-paste confidential materials into an e-mail or social networking post.

SPAM — A form of unwanted or unsolicited messages or communications typically received via e-mail but also occurring through text messaging, social networks or VoIP. Most SPAM is advertising, but some may include malicious code, malicious hyperlinks or malicious attachments.

spear phishing — A form of social engineering attack that is targeted to victims who have an existing digital relationship with an online entity such as a bank or retail website. A spear phishing message is often an e-mail although there are also text message and VoIP spear phishing attacks as well, which looks exactly like a legitimate communication from a trusted entity. The attack tricks the victim into clicking on a hyperlink to visit a company website only to be re-directed to a false version of the website operated by attackers. The false website will often look and operate similarly to the legitimate site and focus on having the victim provide their logon credentials and potentially other personal identity information such as answers to their security questions, an account number, their social security number, mailing address, email address and/or phone number. The goal of a spear phishing attack is to steal identity information for the purpose of account takeover or identity theft.

spoof (spoofing) — The act of falsifying the identity of the source of a communication or interaction. It is possible to spoof IP address, MAC address and email address.

spyware — A form of malware that monitors user activities and reports them to an external their party. Spyware can be legitimate in that it is operated by an advertising and marketing agency for the purpose of gathering customer demographics. However, spyware can also be operated by attackers using the data gathering tool to steal an identity or learn enough about a victim to harm them in other ways.

supply chain — The path of linked organizations involved in the process of transforming original or raw materials into a finished product that is delivered to a customer. An interruption of the supply chain can cause a termination of the production of the final product immediately or this effect might not be noticed until the materials already in transit across the supply chain are exhausted.

T

threat assessment — The process of evaluating the actions, events and behaviors that can cause harm to an asset or organization. Threat assessment is an element of risk assessment and management. (Also known as threat modeling and threat inventory.)

Trojan Horse (Trojan) — A form of malware where a malicious payload is imbedded inside of a benign host file. The victim is tricked into believing that the only file being retrieved is the viewable benign host. However, when the victim uses the host file, the malicious payload is automatically deposited onto their computer system.

two-factor authentication — The means of proving identity using two authentication factors usually considered stronger than any single factor authentication. A form of multi-factor authentication. Valid factors for authentication include Type 1: Something you know such as passwords and PINs; Type 2: Something you have such as smart cards or OTP (One Time Password) devices; and Type 3: Someone you are such as fingerprints or retina scans (aka biometrics).

two-step authentication — A means of authentication commonly employed on websites as an improvement over single factor authentication but not as robust as two-factor authentication. This form of authentication requires the visitor provide their username (i.e. claim an identity) and password (i.e. the single factor authentication) before performing an additional step. The additional step could be receiving a text message with a code, then typing that code back into the website for confirmation. Alternatives include receiving an e-mail and needing to click on a link in the message for confirmation, or viewing a pre-selected image and statement before typing in another password or PIN. Two-step is not as secure as two-factor because the system provides one of the factors to the user at the time of logon rather than requiring that the user provide both.

U

unauthorized access — Any access or use of a computer system, network or resource which is in violation of the company security policy or when the person or user was not explicitly granted authorization to access or use the resource or system

V

VPN (Virtual Private Network) — A communication link between systems or networks that is typically encrypted in order to provide a secured, private, isolate pathway of communications.

virus — A form of malware that often attaches itself to a host file or the MBR (Master Boot Record) as a parasite. When the host file or MBR is accessed, it activates the virus enabling it to infect other objects. Most viruses spread through human activity within and between computers. A virus is typically designed to damage or destroy data, but different viruses implement their attack at different rates, speeds or targets. For example, some viruses attempt to destroy files on a computer as quickly as possible while others may do so slowly over hours or days. Others might only target images or Word documents (.doc/.docx).

vishing — A form of phishing attack which takes place over VoIP. In this attack, the attacker uses VoIP systems to be able to call any phone number with no toll-charge expense. The attacker often falsifies their caller-ID in order to trick the victim into believing they are receiving a phone call from a legitimate or trustworthy source such as a bank, retail outlet, law enforcement or charity. The victims do not need to be using VoIP themselves in order to be attacked over their phone system by a vishing attack. (See phishing.)

vulnerability — Any weakness in an asset or security protection which would allow for a threat to cause harm. It may be a flaw in coding, a mistake in configuration, a limitation of scope or capability, an error in architecture, design, or logic or a clever abuse of valid systems and their functions.

W

whitelist — A security mechanism prohibiting the execution of any program that is not on a pre-approved list of software. The whitelist is often a list of the file name, path, file size and hash value of the approved software. Any code that is not on the list, whether benign or malicious, will not be able to execute on the protected system. (See blacklist.)

Wi-Fi — A means to support network communication using radio waves rather than cables. The current Wi-Fi or wireless networking technologies are based on the IEE 802.11 standard and its numerous amendments, which address speed, frequency, authentication and encryption.

worm — A form of malware that focuses on replication and distribution. A worm is a self-contained malicious program that attempts to duplicate itself and spread to other systems. Generally, the damage caused by a worm is indirect and due to the worm's replication and distribution activities consuming all system resources. A worm can be used to deposit other forms of malware on each system it encounters.

Z

zombie — A term related to the malicious concept of a botnet. The term zombie can be used to refer to the system that is host to the malware agent of the botnet or to the malware agent itself. If the former, the zombie is the system that is blinding performing tasks based on instructions from an external and remote hacker. If the latter, the zombie is the tool that is performing malicious actions such as DoS flooding, SPAM transmission, eavesdropping on VoIP calls or falsifying DNS resolutions as one member of a botnet.

REFERENCES

1.Belton, P. How the tech industry is redesigning the future workplace / P. Belton. — 1 May 2015. — URL: http://www.bbc. com/ news/business-32523448

2.Cellan-Jones, R. A computing revolution in schools / R. Cel-lan-Jones. — 1 September 2014. — URL: http://www.bbc.com/ news/technology-29010511 (a)

3.Cellan-Jones, R. The 12 tech months of 2014 / R. Cellan-Jones. — 29 December 2014. — URL: http://www.bbc.com/news/ technology-30591570 (b)

4.Cellan-Jones, R. Microsoft headset to help blind people navigate cities / R. Cellan-Jones. - 6 November 2014. - URL: http:// www.bbc.com/news/technology-29913637

5.European e-Government Action Plan 2011—2015. - URL: http://ec.europa.eu/digital-agenda/en/european-egovernment-action-plan-2011-2015

6.Evans, V. Software Engineering / V. Evans. - Express Pub-lishing, 2014. — (Career path).

7.Facebook's government user data requests up 24 %. —5 November 2014. - URL: http://www.bbc.com/news/busi-ness-29910101

8.Fitzgerald, P. English for ICT studies in Higher Education Studies / P. Fitzgerald, M. McCullagh, C. Tabor. — Garnet Educa-tion, 2011.

9. Google purpose-bui robot cars tested on public roads. -15 May 2015. - URL: http://www.bbc.com/news/technol-ogy-32750810

10.Hill, D. English for Information Technology: Level 2: Course book / D. Hill. - Pearson Education Limited, 2014.

11. ICT systems and their usage. - URL: http://www.bbc.co.uk/schools/gcsebitesize/ict/system/Oictsystemsrevl.shtml

12. Is cyber-warfare really that scary? — 6 May 2015. - URL: http://www.bbc.com/news/world-32534923

13. Jeans made that will prevent "digital pickpocketing". -17 December 2014. - URL: http://www.bbc.com/news/technol-
ogy-30513497

14. Kelion, L. "Email epidemic" is damaging UK productivity, says expert / L. Kelion. — 7 May 2015. - URL: http://www.bbc. com/news/technology-32622224 (a)

15. Kelion, L. CES 2015: The robots moving in to your house /L. Kelion. — 8 January 2015. — URL: http://www.bbc.com/news/ technology-30708953 (b)

16. Kelion, L. Moore's Law: Beyond the first law of computing /L. Kelion. — 17 April 2015. - URL: http://www.bbc.com/news/technology-32335003

17. Kellaway, L. How the computer changed the office forever /L. Kellaway. — 1 August 2013. — URL: http://www.bbc.com/ news/magazine-23509153

18. Kleinman, Z. Tech rivals join Microsoft in fight over US data demand / Z. Kleinman. – 16 December 2014. - URL: http:// www.bbc.com/news/technology-30494562

Kleinman, Z. Tech rivals join Microsoft in fight over US data demand / Z. Kleinman. -16 December 2014. - URL: http://www.bbc.com/news/technology-30494562

19. Mandebvu, S. What is ICT / S. Mandebvu. - 20 June 2014. - URL: http://www.slideshare.net/sammydhi01/what-is-ict-40492687

20.Moskvitch, K. Skype: How the online chat revolution changed lives / K. Moskvitch. — 28 August 2013. — URL: http://www.bbc. com/news/technology-23862352

21.Ricca-McCarthy, T. English for Telecoms and Information Technology (SB+MultiROM) / T. Ricca-McCarthy, M. Duck-worth. - Oxford : Oxford University Press, 2013. - (Oxford Express Series).

22. Rouse, M. Software development / M. Rouse. -April2010. — URL: http://whatis.techtarget.com/reference/Learn-IT-Software-development

23. Self-destructing virus kills off PCs. - 5 May 2015. - URL:http://www.bbc.com/news/technology-32591265 24. Shaw, K. Internet of Things 24.Shaping IT's Future / K. Shaw. -22 October 2014. — URL: http://www.webopedia.com/Blog/ internet-of-things-it-future.html

25. Shiels, M. Rise of the virtual conference / M. Shiels. —20 April 2010. — URL: http://news.bbc.co.uk/2/hi/technol-0gy/8608417.stm

26.Simmons, D. Europol kills off shape-shifting "Mystique" malware / D. Simmons. — 9 April 2015. — URL: http://www.bbc. com/news/technology-32218381 (a)

26.Simmons, D. IBM and Apple want to share how you are with others / D. Simmons. — 14 April 2015. — URL: http://www.bbc.