
CYBER
SECURITY

INTRODUCTION

- **Cyber crime** is committed using a computer and the internet to steal a person's identity or illegal imports or malicious programs
- **Definition: Cyber security** or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.
- The objective of cyber security is to establish rules and measures to use against attacks over the internet

RECENT SECURITY BREACHES

- **Hanna Andersson [January 20, 2020]**
- Children's clothing retailer, Hanna Andersson, had sensitive payment information exposed.
- This breach is the latest in a string of Magecart attacks, where hackers install malicious malware in Point of Sale (POS) systems to skim credit card information.
- Customers who made online purchases from September 16, 2019, to November 11, 2019, had their names, shipping addresses, billing addresses, payment card numbers, CVV codes, and expiration dates skimmed and put for sale on the Dark Web.

- **Microsoft [January 22, 2020]**
- A customer support database holding over 280 million Microsoft customer records was left unprotected on the web.
- Microsoft's exposed database disclosed email addresses, IP addresses, and support case details.

- **Slickwraps [February 21, 2020]**
- Slickwraps, a company that makes vinyl skins for phones, tablets and laptops, suffered a significant data breach affecting the personal information of over 330,000 customers.
- Worryingly, the hackers sent out an email blast to all affected users, mentioning their name, home address and an indictment of Slickwraps security measures.

IMPORTANCE OF CYBER SECURITY

1. The rising cost of breaches

- The fact is that cyberattacks can be extremely expensive for businesses to endure. Recent statistics have suggested that the average cost of a data breach at a larger firm is 25,807.20 United States Dollar.
- It is not just the financial damage suffered by the business or the cost of remediation; a data breach can also inflict untold reputational damage.
- Suffering a cyberattack can cause customers to lose trust in a business and spend their money elsewhere. Additionally, having a reputation for poor security can also lead to a failure to win new contracts.

2. Increasingly sophisticated hackers

- Almost every business has a website and externally exposed systems that could provide criminals with entry points into internal networks.
- Hackers have a lot to gain from successful data breaches, and there are countless examples of well-funded and coordinated cyber-attacks against some of the largest companies in the UK.
- Ironically, even Deloitte, the globe's largest cybersecurity consultant, was itself rocked by an attack in October last year

3. Widely available hacking tools

- wide availability of hacking tools and programmes on the internet also means there is also a growing threat from less skilled individuals.

4. A proliferation of IoT devices

- IOT devices can simplify and speed up tasks, as well as offer greater levels of control and accessibility. There proliferation, however, presents a problem.
- If not managed properly, each IoT device that is connected to the internet could provide cyber criminals with a way into a business.
- IT services giant Cisco estimates there will be 27.1 billion connected devices globally by 2021 – so this problem will only worsen with time.

5. Tighter regulations

- The introduction of regulations such as the GDPR means that organisations need to take security more seriously than ever, or face heavy fines.
- The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals.
- The GDPR has been introduced by the EU to force organisations into to taking better care of the personal data they hold.
- Among the requirements of the GDPR is the need for organisations to implement appropriate technical and organisational measures to protect personal data, regularly review controls, plus detect, investigate and report breaches.

ELEMENTS OF CYBER SECURITY

1. APPLICATION SECURITY:

It protecting websites and web based application from different cyber security threats that exploit vulnerabilities in an application's code.

CATEGORIES OF APPLICATION THREATS:

- Input validation
- Authorization
- Session management
- Parameter tampering

2. INFORMATION SECURITY

Information security (IS) or Info Sec refers to the process and methodology to preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

There are three main principle of Information Security commonly known as **CIA – Confidentiality, Integrity, and Availability.**

3. NETWORK SECURITY

Network security is another **elements of IT security** which process of preventing and protecting against unauthorized access into computer networks.

NETWORK SECURITY METHODS:

1. Antivirus software
2. Data loss prevention
3. web security
4. wireless security
5. firewalls

4. DISASTER RECOVERY PLAN

A Disaster Recovery Plan (DRP) is a business continuity plan and managed procedures that describe how work can be resumed quickly and effectively after a disaster.There are 12 steps to help you to prepare a disaster recovery plan which are as follows:

1. **Define scope of the organization assets**
2. **Take back up regularly**
3. **Identifying the possible threats and vulnerabilities**
4. **Ensure Data Protection**
5. **Create a Disaster Recovery Team**
6. **Provide training to team members**
7. **Establish team members accountability**
8. **Create a data recovery plan**
9. **Test your data recovery plan**
10. **Review regularly**
11. **Update and Revise Your Plan and**
12. **Possible to implement Cloud Backup**

5. OPERATIONAL SECURITY:

Operational security (OPSEC) is an analytical and risk management process that identifies the organization's critical information and developing a protection mechanism to ensure the security of sensitive information.There are five steps to process the operational security program, which are as follows:

1. **Define the organization sensitive information.**
2. **Identify the categories of threat**
3. **Analyze the security holes**
4. **Assessment of risk**
5. **Implementation of appropriate**

It is also known as procedural security which encourages manager to view operations in order to protect sensitive information from falling.

6. END USER EDUCATION

End user education is most important element of Computer security. End users are becoming the largest security risk in organizations because it can happen anytime.The end user threats can be created according to following ways:

- **Using of Social Media**
- **Text Messaging**
- **Apps Download**
- **Use of Email**
- **Password creation and usages**

USERS NEED TO BE TRAINED AND INFORMED ABOUT THE FOLLOWING:

- **Phishing and Social Engineering**
- **Access, Passwords and Connection**
- **Device Security**
- **Physical Security**
- **Password creation and usages**

SOUNDS FAMILIAR?

PHISHING

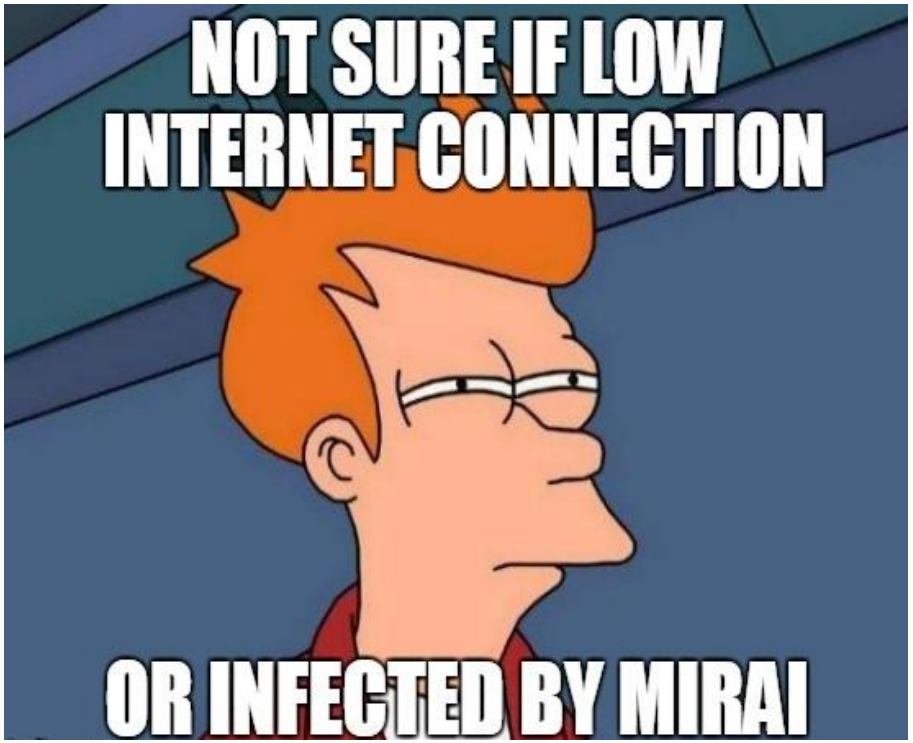
- Lures the victim into a fake website via email.
- Fake website looks and feels exactly like the authentic one.
- The victim is then induced to reveal sensitive information.

PHARMING

- A means to point you to a malicious and illegitimate website by redirecting the legitimate URL.
- Involves modifying the DNS entries.
- Even if the URL is entered correctly, it can still be redirected to a fake website.

BOTNETS

- A collection of software robots, or 'bots', that creates an army of infected computers (known as ‘zombies') that are remotely controlled by the originator.
- Yours may be one of them and you may not even know it.
- Send spam emails with viruses attached.
- Spread all types of malware.
- Can use your computer as part of a DoS attack against other systems.



Mirai is a malware that turns network devices running Linux into remotely controlled bots.

HACKING

- Gaining unauthorized access to a computer.
- Find weaknesses (or pre-existing bugs) in your security settings and exploit them in order to access your information.
- Install a Trojan horse, providing a backdoor for hackers to enter and search for your information.

DENIAL OF SERVICE (DoS) OR DISTRIBUTED DENIAL OF SERVICE(DDoS)

- Disruption of computing services of the victim.
- Advanced DoS slows down the web server to prevent alarm.
- A distributed denial-of-service (DDoS) attack is when a malicious user gets a network of zombie computers to sabotage a specific website or server.
- The attacks are "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attacks.

MALWARE

- Malicious software that infects your computer, such as computer viruses, worms, Trojan horses, spyware, and adware.
- Intimidate you with scareware, which is usually a pop-up message that tells you your computer has a security problem or other false information.
- Alter or delete files.
- Steal sensitive information.
- Send emails on your behalf.
- Take control of your computer and all the software running on it.

VIRUSES

- Malicious computer programs that are often sent as an email attachment or a download with the intent of infecting your computer
- Send spam.
- Provide criminals with access to your computer and contact lists.
- Scan and find personal information like passwords on your computer.
- Hijack your web browser.

WORMS

- A worm, unlike a virus, goes to work on its own without attaching itself to files or programs. It lives in your computer memory, doesn't damage or alter the hard drive and propagates by sending itself to other computers in a network – whether within a company or the Internet itself.
- Spread to everyone in your contact list.
- Cause a tremendous amount of damage by shutting down parts of the Internet, wreaking havoc on an internal network and costing companies enormous amounts of lost revenue.

TROJAN HORSE

- A malicious program that is disguised as, or embedded within, legitimate software. It is an executable file that will install itself and run automatically once it's downloaded.
- Delete your files.
- Use your computer to hack other computers.
- Watch you through your web cam.
- Log your keystrokes (such as a credit card number you entered in an online purchase).

SPYWARE AND ADWARE

- Spyware and adware are often used by third parties to infiltrate your computer.
- Software that collects personal information about you without you knowing.
- They often come in the form of a ‘free' download and are installed automatically with or without your consent.
- These are difficult to remove.
- Change the way your computer runs without your knowledge.
- Take you to unwanted sites or inundate you with uncontrollable pop-up ads.

Wi-Fi EAVESDROPPING

- WiFi eavesdropping is another method used by cyber criminals to capture personal information.
- Virtual “listening in” on information that's shared over an unsecure (not encrypted) WiFi network.
- Potentially access your computer with the right equipment.
- Steal your personal information including logins and passwords.

RANSOMWARE

- Ransomware is a type of malware that restricts access to your computer or your files and displays a message that demands payment.
- There are two common types of ransomware:
  - Lockscreen ransomware: displays an image that prevents you from accessing your computer
  - Encryption ransomware: encrypts files on your system's hard drive, shared network drives, USB drives and cloud storage drives, preventing you from opening them

WPA2 HANDSHAKE VULNERABILITIES

- The Key reinstallation attack (or Krack) vulnerability allows a malicious actor to read encrypted network traffic on a Wi-Fi Protected Access II (WPA2) router and send traffic back to the network.
- Krack can affect both personal and enterprise networks. Any devices that are connected to the network can be read by the attacker.
- A malicious actor could use this vulnerability to steal sensitive information, and also insert malware or ransomware.

CYBER SECURITY TACTICS

OWASP

Open Web Application Security Project

What is OWASP?

OWASP stands for the Open Web Application Security Project, an online community that produces articles, methodologies, documentation, tools, and technologies in the field of web application security.

What is the OWASP Top 10?

OWASP Top 10 is the list of the 10 most common application vulnerabilities. It also shows their risks, impacts, and countermeasures

The Top 10 OWASP vulnerabilities in 2020 are:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access control
- Security misconfigurations
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Insufficient logging and monitoring

Security Vulnerabilities in E-Commerce Systems

The success of e-commerce websites relies heavily on the value and service to customers and the reputation and trust that customers, in turn, give them back. If a website has vulnerabilities or poor encryption it is less likely to be used by consumers, regardless of how good the products are, as people are becoming a lot more security aware and do not want their details compromised or stolen so will not trust the website with their card details.

Common Threats Include:

Malicious code, hacking, credit card fraud/theft, spoofing, Dos attacks

1. SQL Injection:

•SQL injection refers to an injection attack were an attacker can **execute malicious code (a SQL statement)** that can control a web applications **database server.**

•Many e-commerce systems rely on a database to store **critical information** such as stock details, stock levels and customer details.

•Attacking the database will allow the criminal to potentially be able to read sensitive data**, modify database data** (Insert/ update/ delete)

Vulnerability:

•SQL injections attacks allow criminal to **manipulate existing data** such as coding transactions and changing balances, disclose the data on the system or make it unavailable e.g. destroy.

2. Priced Manipulation

Price Manipulation is an **attack completely unique to online shopping systems**, as e-commerce systems are completely automated. Some e-commerce software may have a vulnerability that allows a criminal to **enter a lower price than what is set**, bringing the total cost of items down which can cause a very high financial losses for the company.

Vulnerability:

The most common occurrence of the vulnerability is when the total payable goods price is stored in **HTML format**. An attacker can use a web proxy or developer tools to modify the amount that is shown and when the information is passed on to the payment gateway. If a fraud detection system isn't in place then the system will not pick up that the price has changed.

The Appearance of the Attack/ How to test

Which means 2 items costing 24$ and the item no 1000 and 1003 . We can manipulate the cost price 24$ to 0$ and buy the items for free

```
1444628668:2:24:1000:1003
```

3. Unsecured Authentication

•Many systems require some type of authentication, log in.

•These authentication sessions should pass **through SSL encryption**, an attacker could obtain potentially sensitive user information over the web.

Vulnerability

•Malicious users can **register as admin** and gain all privileges over the website. This results in complete compromise of the system. Users could also log in as a different user, which may have different user privileges to themselves, allowing them to execute tasks that they wouldn't normally have access to. If a users card details are stored on the website, then an attacker could potentially purchase items through their name without their consent or knowledge. This is also apparent as the e-commerce systems cannot fully authenticate a user as the genuine account holder and credit verification systems cannot check to see if the card details match the user logged into the account.

Appearance of Attack:

•If the web site uses HTTP Basic Authentication or does not pass session IDs over SSL (Secure Sockets Layer), an attacker can sniff the traffic to discover user's authentication and/or authorization credentials. Since HTTP is a stateless protocol, web applications commonly maintain state using session IDs or transaction IDs stored in a cookie on the user's system. Thus this session ID becomes the only way that the web application can determine the online identity of the user.

4. Discovery

•If a **website captures and stores sensitive data**, they need to have a **SSL certificate** in order to properly transmit sensitive data to their server.

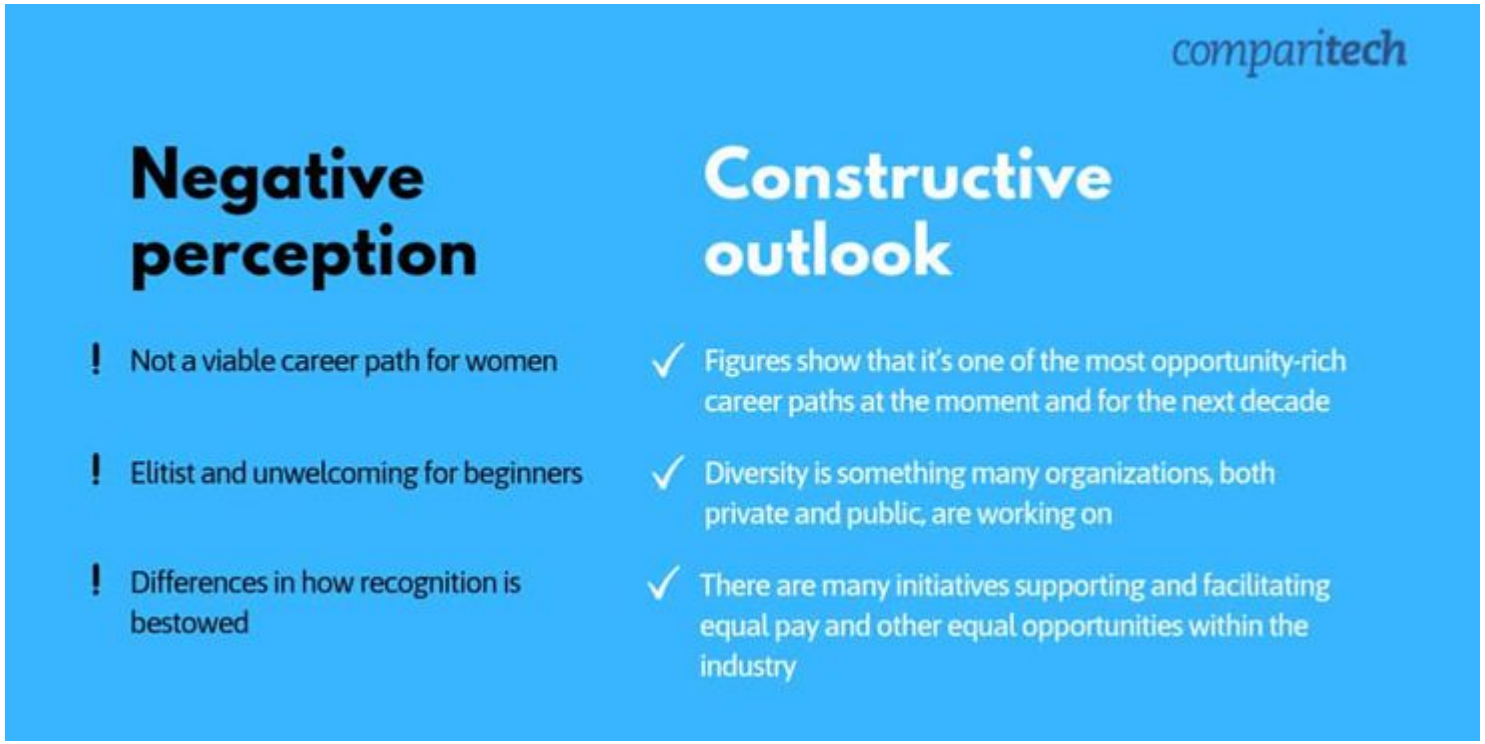
•A user can manually check to see whether a website has SSL certificates by checking to see if the website has ‘https://’ at the beginning of the URL, checking to see if a padlock icon is displayed at the top of the page by the address bar and viewing ‘Page info’ or ‘Properties’ and look for a connection or security tab which will contain the security status (secure, unsure, not secure) and the certificate and encryption used, if in place. It is also possible to check whether a server has SSL installed by using simple Linux commands and tools.

Prevention

•Use SSL certificates with strong encryption for any website that captures and stores any sensitive information. A new registered user must always be given lowest privilege and then if needed, the administrator can escalate his privilege later. Multi-factor authentication can be used to stop attackers from logging in to others accounts as more than one verification method is needed.

WOMEN IN CYBER SECURITY

The cybersecurity industry is a male dominated one. But the problem isn't that there are too many men in the industry, but rather that there are not enough women.



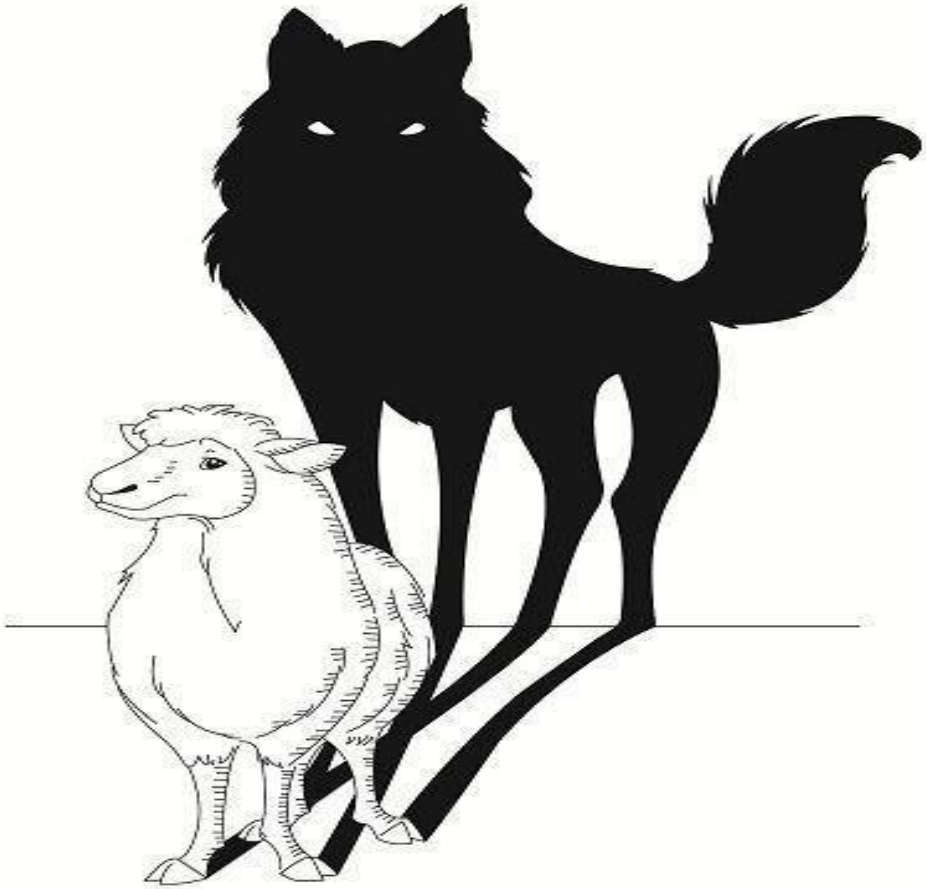
Meet the woman in charge of defending Microsoft from cyber attack

6.5 trillion: That's the astonishing number of online threats that staff at Microsoft's Cyber Defence Operations Centre see each day.

And quite a portion of those attacks are aimed at the company itself. The highest number of attempted intrusions into Microsoft's network of products and services ever detected in one 24-hour period was 1.5 billion.

Keeping these so-called "bad actors" at bay is the overall responsibility of Ann Johnson. She is the company's Corporate Vice-President, in charge of the Cybersecurity Solutions Group.

CYBERCRIME:
A WOLF IN SHEEP'S CLOTHING



Use strong passwords and ALWAYS update your computer.

DON'T BE FOOLED.

The bad guys are getting smarter.


THANK YOU
ANY QUESTIONS?