What is cyber security?

- How individuals and organisations reduce the risk of cyber attacks.
- The core function is to protect the devices we all use. And the services we access - both online and work - from theft and damage. Preventing unauthorised access to vast amounts of personal info.

Why is cyber security important? It is important because smartphones , computers and the internet are now such a fundamental part of modern life. Information for families , employment , banking and a dozen more are all stored online.

https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

---

https://www.itgovernance.co.uk/what-is-cybersecurity

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber attacks.

Why is cyber security important?

- The costs of security breaches are rising
- Organisations that suffer cyber security may face significant fines. Also non financial costs and negatives like reputational damage , bad publicity and loss of customers.
- It is a board level issue.

- Cyber attacks are increasingly sophisticated , attackers are using an ever expanding variety of attacks.
- Such as SOCIAL ENGINEERING, MALWARE and RANSOMWARE.

Cyber Crime is a big business

- According to a study by McAfee and the CSIS, based on data collected by Vanson Bourne , the world economy loses more than $1 TRILLION each year due to cybercrime.

https://www.mcafee.com/el-gr/consumer-corporate/newsroom/press-releases/press-release.html?news_id=6859bd8c-9304-4147-bdab-32b35457e629&virus_k=98318

More info from the McAfee report:

- ⅔ of surveyed companies reported some kind of cyber incident in 2019
- Average cost was $500,000 per incident
- IP theft and financial crime account for at least 75% of cyber losses and pose the greatest threat to companies.
- Damage to companies also includes downtime, brand reputation and reduced efficiency.
- 56% of surveyed organisations said they do not have a plan to both prevent and respond to a cyber incident.

- Political,ethical and social incentives can also drive attackers.

Example: The Bangladesh Bank Robbery.
https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery

The **Bangladesh Bank robbery**, also known colloquially as the **Bangladesh Bank cyber heist**,[1] was a theft that took place in February 2016. Thirty-five fraudulent instructions were issued by security hackers via the SWIFT network to illegally transfer close to US$1 billion from the Federal Reserve Bank of New York account belonging to Bangladesh Bank, the central bank of Bangladesh. Five of the thirty-five fraudulent instructions were successful in transferring US$101 million, with US$81 million traced to the Philippines and US$20 million to Sri Lanka. The Federal Reserve Bank of New York blocked the remaining thirty transactions, amounting to US$850 million, due to suspicions raised by a misspelt instruction.

McAfee Report continued: the hidden costs of cybercrime

- Survey revealed 92 percent of businesses felt there were other negative effects on their business beyond financial costs and lost work hours.
- For example
- System downtime - the average costs to organisations from their longest amount of downtime in 2019 was roughly $700,000.
- 33% of respondents stated IT security incidents resulting in system downtime cost them between $100,000 and $500,000.
- Incident response costs - according to the report, it took an average of 19 hours for most organisations to move from the discovery of an incident to remediation.
- Brand and reputation damage - cost of rehabilitating the external image of the brand , working with outside agencies to mitigate brand damage or hiring new employees is a huge part of the HIDDEN costs of cybercrime.

Methodology of the McAfee Report:

McAfee commissioned independent technology market research specialist Vanson Bourne to undertake the research that this report is based on.

Between April and June 2020, the quantitative study was carried out, interviewing 1,500 IT and line of business decision makers. Respondents came from the US (300), Canada (200), the UK (200), France (200), Germany (200), Australia (200) and Japan (200). Respondents' organizations have 1,000 or more employees and were from all sectors except construction and property. However, only IT decision makers were interviewed in the Government sector.

Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

Additionally, CSIS utilized a survey of open source material on losses accompanied by interviews with Government officials, and an estimate adjusted by national income levels using International Monetary Fund (IMF) income data to determine the cost of cybercrime.

Continuing: https://www.itgovernance.co.uk/what-is-cybersecurity
Types of cyber threats:

- Malware, such as ransomware, botnet software , RATs (remote access trojans) , spyware , viruses etc.
- Backdoors, which allow remote access.
- FormJacking = malicious code entered into online forms.
- Cryptojacking = steals crypto mining software.
- DDOS - floods servers and systems with huge traffic to knock them offline
- DNS - domain name system - poisoning attacks , DNS redirects traffic to harmful and malicious sites.

5 Types of cyber security.

1. Critical infrastructure cyber security - often more vulnerable to attack than others because security systems may realty on older software
2. Network Security - addressing vulnerabilities affecting OS , network architecture. Including servers , hosts , firewalls.
3. Cloud Security - securing data , apps and infrastructure in the Cloud.
4. IoT (Internet of Things) Security - involves securing smart devices and networks connected to the Iot. iot devices = include things that connect to the internet without human intervention (FIRE ALARMS , LIGHTS , SMART TECH LIKE HEATING ETC.)
5. Application Security - involves addressing vulnerabilities resulting from insecure development processes in designing , coding and publishing software.

LEGAL requirement for cyber security:

The GDPR and DPA 2018 require organisations to implement appropriate security measures to protect personal data. Otherwise, you risk substantial fines.

Approaching cyber security - a risked based approach will ensure efforts are focused where they are most needed.

- Using regular cyber security risk assessments to identify and evaluate your risks is the most effective and cost efficient way of protecting your organisation.

Why do organisations need incident response planning/reports?

- Under Article 32 of the GDPR, organisations are obligated to restore the availability of and access to personal data in the event of a physical or technical breach.

---

https://www.cisco.com/c/en_uk/products/security/what-is-cybersecurity.html#~how-cybersecurity-works
Types of CyberSecurity threats:

- Phishing - the practice of sending fraudulent emails that resemble emails from reputable sources. Aim to steal sensitive data like credit card numbers and login information. Most common type of cyber attack]

How to prevent it:
A technology solution that filters malicious emails (essentially the task for ITP Collaborative Project.

- Ransomware - a type of malicious software that is designed to extort money by blocking access to information/files/anything until the ransom is paid. Paying the ransom does not guarantee the files will be restored or safe.

- Malware - software designed to gain unauthorised access/and to cause damage to a computer

- Social Engineering - tactic that tricks you into revealing sensitive information. Can solicit a monetary payment or gain access to confidential data. Can be combined with the threats listed above.

My own example : there is a reason why banking companies and sensitive information apps will warn you to never share your password with anyone - even the so-called ‘workers' etc.

---

https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/

The different generations of cyber attacks.

- **Gen I (Virus):** In the late 1980s, virus attacks against standalone computers inspired the creation of the first antivirus solutions.
- **Gen II (Network):** As cyberattacks began to come over the Internet, the firewall was developed to identify and block them.
- **Gen III (Applications):** Exploitation of vulnerabilities within applications caused the mass adoption of intrusion prevention systems (IPS)
- **Gen IV (Payload):** As malware became more targeted and able to evade signature-based defences, anti-bot and sandboxing solutions were necessary to detect novel threats.

- **Gen V (Mega):** The latest generation of cyber threats uses large-scale, multi-vectors attacks, making advanced threat prevention solutions a priority.