


Impact of Cybersecurity in Electricity Sector

Eng. Marwa Mohamed Sayed Ahmed
General Manager of Cyber Security
EEHC



1

InfoSec VS Cybersecurity



2

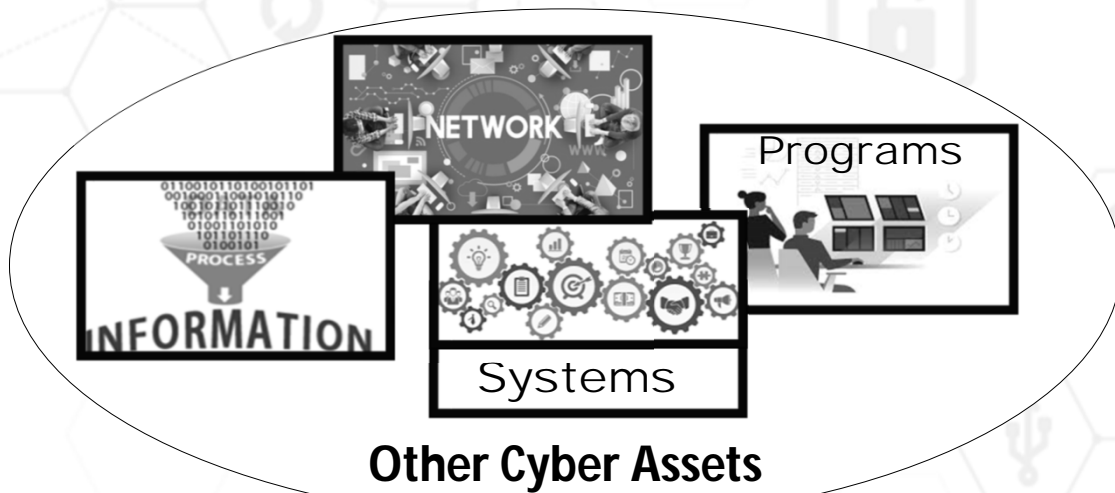
Cyber

- The word “Cyber” stand for a relationship with information technologies (IT)
- Including:
 - Storing data
 - Protecting data
 - Accessing data
 - Processing data
 - Transmitting data
 - Linking data



3

Cyber Assets



4

What is Information

Information is an asset which is essential to an organization's business and consequently needs to be suitably protected.



An information system is any set of components that is used to handle information SUCH AS applications, services, or any other assets that handle information.

transmitted
by post /
by using electronic means



Printed / written on paper
(notes/documents)

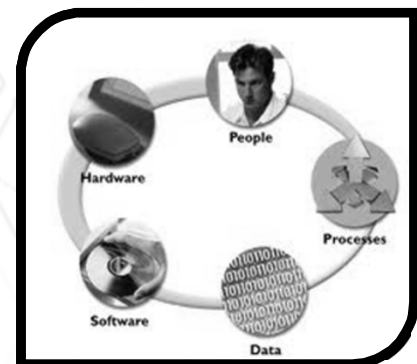


Stored on
electronic devices

5

InfoSec Systems

- **information system security consists of technologies, processes and controls which used to protect organization and people from cyber crimes by protecting:**
People, Process and Technologies.



6

People " Who we are "

- **People who use or interact with the Information include:**
 - **Share Holders / Owners**
 - **Management**
 - **Employees**
 - **Business Partners**
 - **Service providers**
 - **Contractors**
 - **Customers / Clients**
 - **Regulators**

7

Process " What we do "

- **Processes are the repeatable steps to accomplish business objectives. Typical process in our IT Infrastructure could include:**
 - **Helpdesk / Service management**
 - **Incident Reporting and Management**
 - **Change Requests process**
 - **Request fulfillment**
 - **Access management**
 - **Identity management**
 - **Service Level / Third-party Services Management**
 - **IT procurement process**

8

Technology "What we use"

- **The Network Infrastructure:**
 - **Cabling, Data/Voice Networks and equipment**
 - **Server computers and associated storage and communication devices**
 - **VPNs and Virtual environments / Remote access services and Wireless connectivity**
- **The Application software:**
 - **Finance and assets systems, including Accounting, Inventory, HR systems,...**
 - **Software as a service (Sass) - software as a packaged or custom-made product.**
- **Physical Security components:**
 - **CCTV Cameras / Clock in systems / Biometrics**
 - **Environmental management Systems: Air Conditioning, Fire Control systems....**
- **The Access devices:**
 - **Desktop computers / Laptops, ultra-mobile laptops / Thin client computing.**
 - **Digital cameras, Printers, Scanners, Photocopier**

9

What is Security

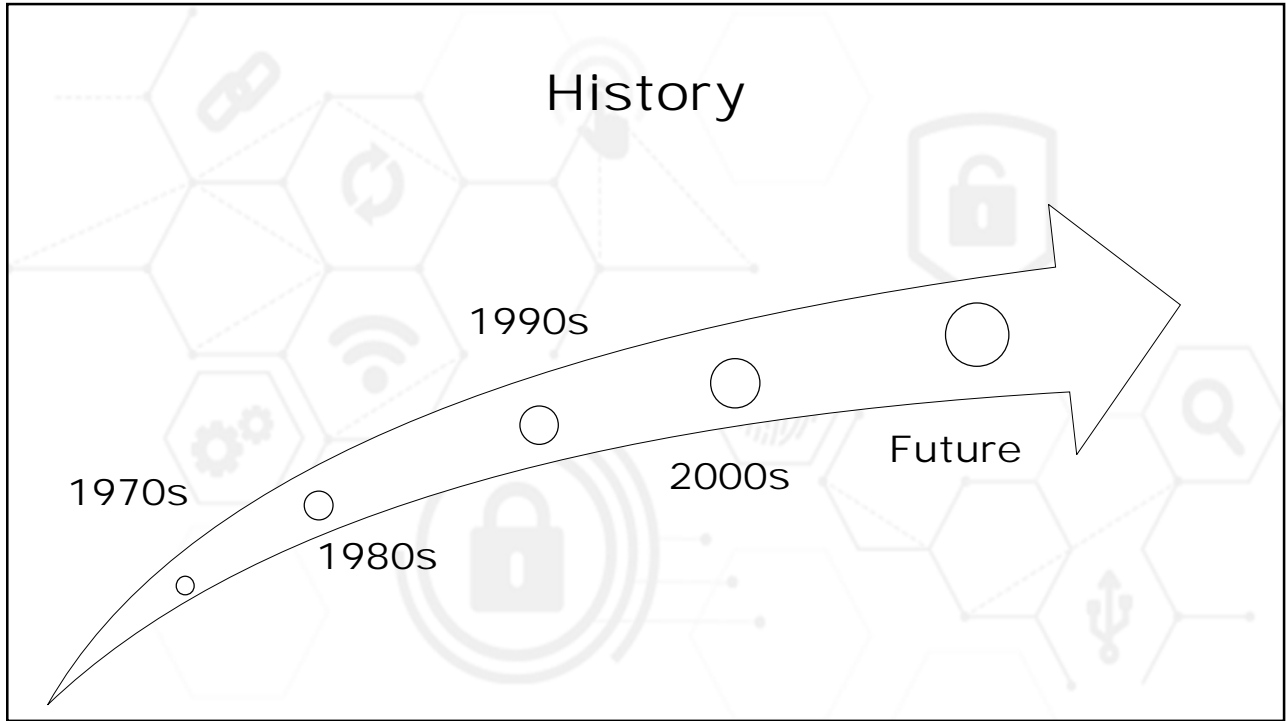
Information security is the protection of information which achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions.

- **is a set of tools and practices that use to protect your information including infrastructure and network security, auditing, and testing.**

Such as controls that need to be established, implemented, monitored, reviewed and improved to ensure that the specific security and business objectives of the organization are met and prevent harms related to information theft, modification, or loss.



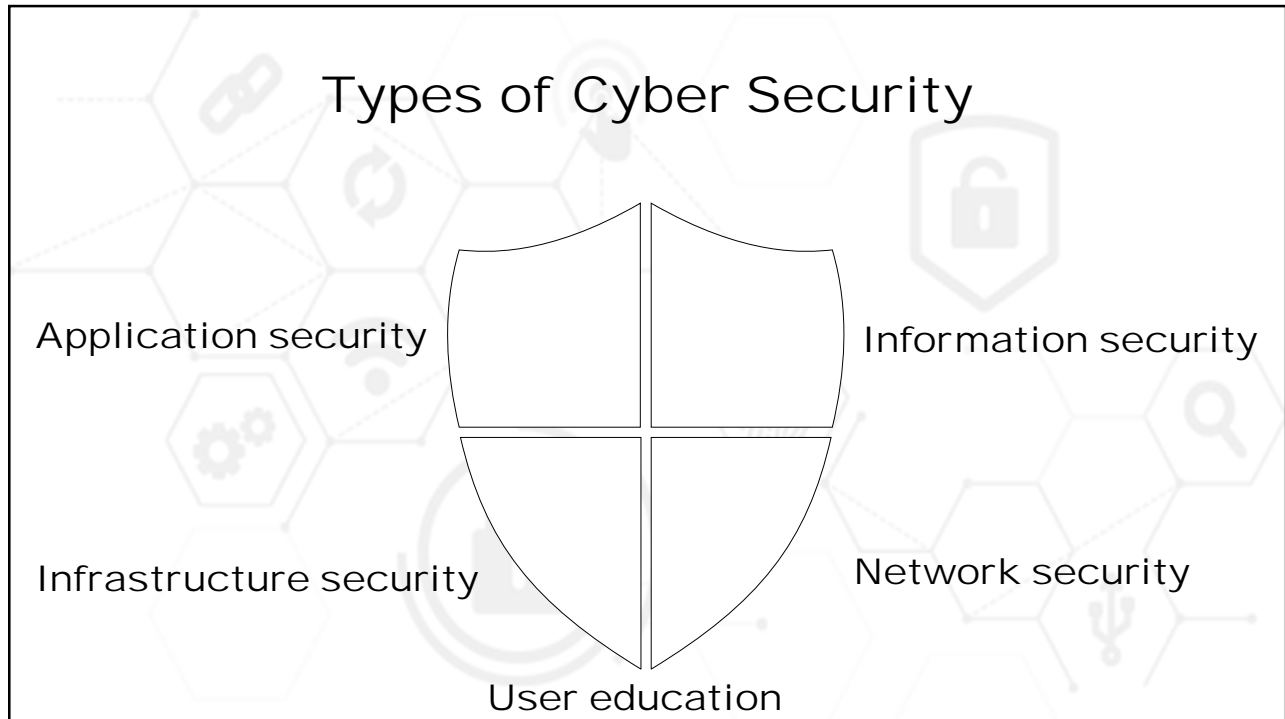
10



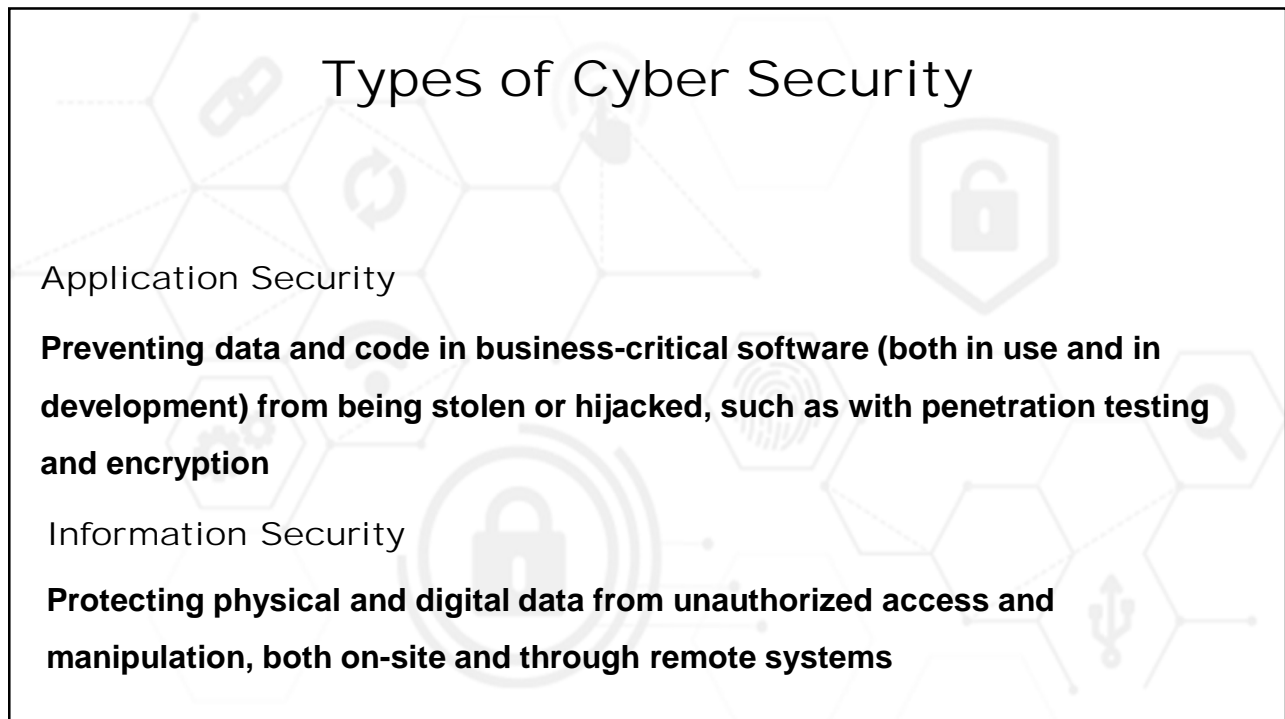
11



12



13



14

Types of Cyber Security Cont.

Infrastructure Security

Ensuring that the structures and facilities you rely on, such as electrical grids and data centers, are access-controlled and guarded against physical harm or disruption

Network Security

Securing internal networks against unauthorized access, with tools like remote access management and two-factor authentication (2FA)

User Education

Teaching employees and customers best practices for recognizing and avoiding cyber threats, such as malware and phishing attacks

15

Goal of Security



Prevent



Detect



Correct



Lorem
Ipsum

is to prevent and detect the attacks and correct the damage done by attacks and continue to function even if attack succeeds

16

Information Security Controls

- **Security controls** are safeguards to avoid, detect, counteract, or minimize **security** risks to physical property, **information**, computer **systems**, or other assets.
- The **Three Types of Security Controls** are:
 - Preventative
 - Detective
 - Responsive.
- **Controls** and countermeasures must be implemented as one or more of these previous **types**, or the **controls** are not there for the purposes of **security**.

17

Controls

Preventive Controls

- Two-Factor Authentication
- Firewalls
- Encryption
- Antivirus

Detective Controls

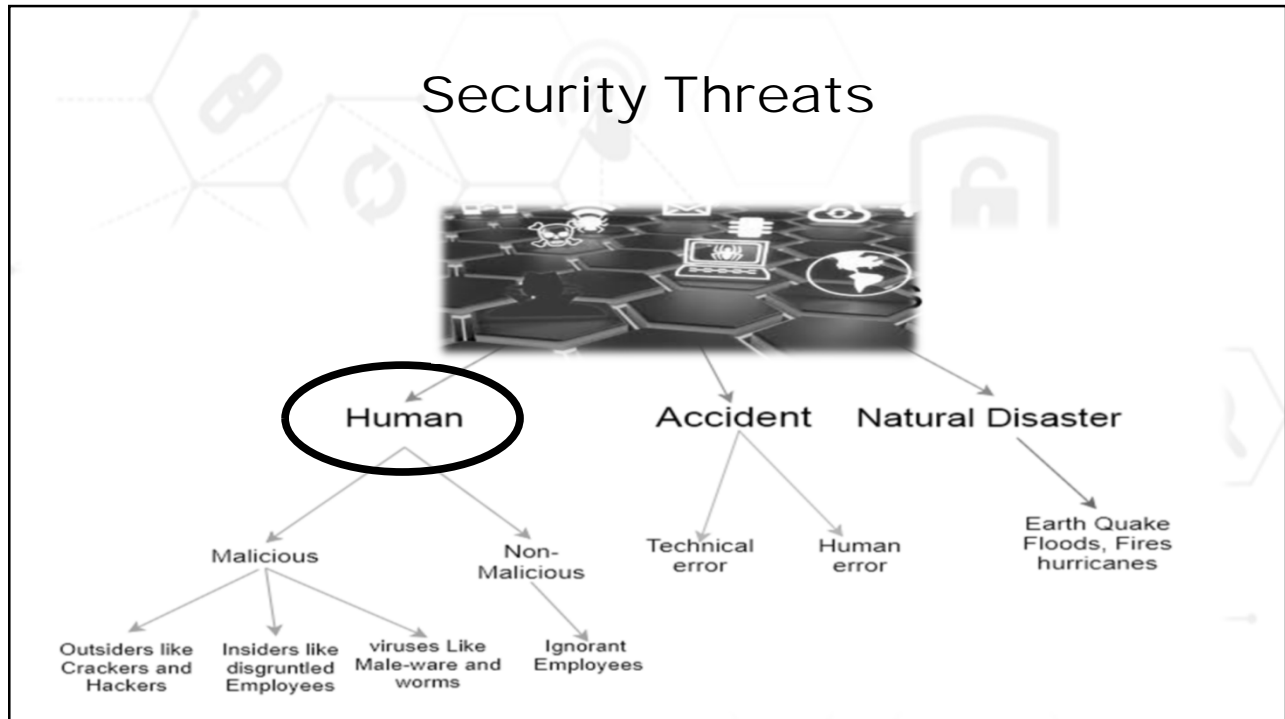
- CAPTCHA
- Antivirus Protection
- System Monitoring & Logging

Responsive Controls

- Block IP addresses of suspected threat actors based upon detected activities.
- Lock accounts suspected of unauthorized access. (Administrators – Users ...)



18



19



20




21


Cyber / Computer Crimes

Cybercrime is any criminal activity that involves a computer, a network or a networked device.

Hacker
someone who identifies the flaws in the security systems and work to improve and patch
Called "White Hatter"



Cracker
someone who unethically exploits highly sensitive information and uses the flaws in the security systems to his advantage
Called "Black Hatter"



22

Types of Attacks

Cybercrimes can generally be divided into two categories:

**Crimes that target networks
or devices**

**Crimes using devices to participate in
criminal activities**

Viruses

Phishing Emails

Malware

Cyberstalking

DoS Attacks

Identity Theft

23

Computer crime cont.

Viruses: is a malicious software when executed, replicates itself by modifying other computer programs and inserting its own code to serve a purpose.



worms



Ransomware



Spyware
(Key Loggers)



Adware



Trojan horses



Rootkits

24

Computer Crimes Cont.

Spyware: Software that monitors the activity on a computer, such as the websites visible or even the key-strokes of the user (such as Keylogger)

Cookies: Are files that are saved on pc from browsers that contain important information about the user such as credit card number.

Spam: is bulk e-mail sent to large numbers of people, few of which would have interest in it, often attempting to sell products or distribute malware.

25

Computer Crime

Social Engineering : using lies and manipulation to trick people into revealing their personal information.

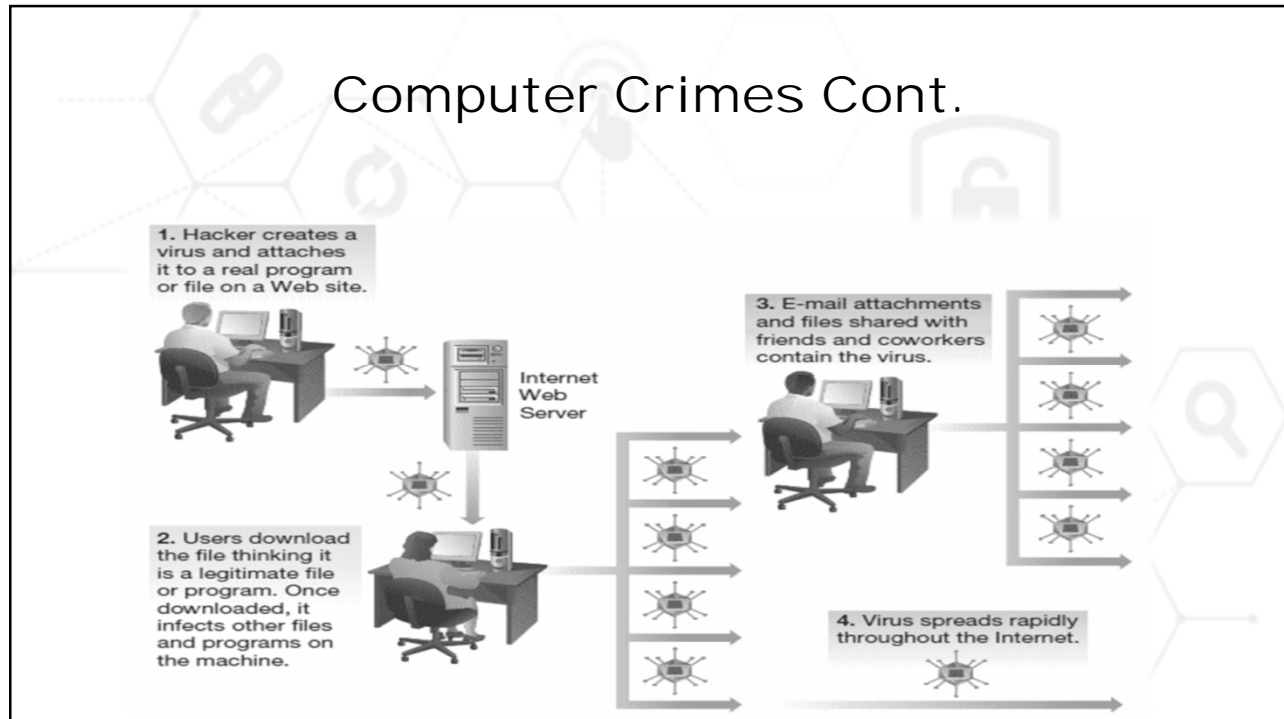
Phishing: sending emails faking to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Identity Theft: is one of the fastest growing information crimes such as Stealing Social Security, credit card, bank account numbers.



26

Computer Crimes Cont.



27

Impact of Attacks

- **Interception**
- **Modification**
- **Fabrication**
- **Interruption (DoS)**
- **Replay Attack**
- **Traffic Analysis**



28

Strategies of Security

- A plan of actions designed to improve the security and resilience of national infrastructures and services.
- It is a high-level top-down approach to cybersecurity that establishes a range of national objectives and priorities that should be achieved in a specific timeframe.



29

Strategies of Security

Cont.

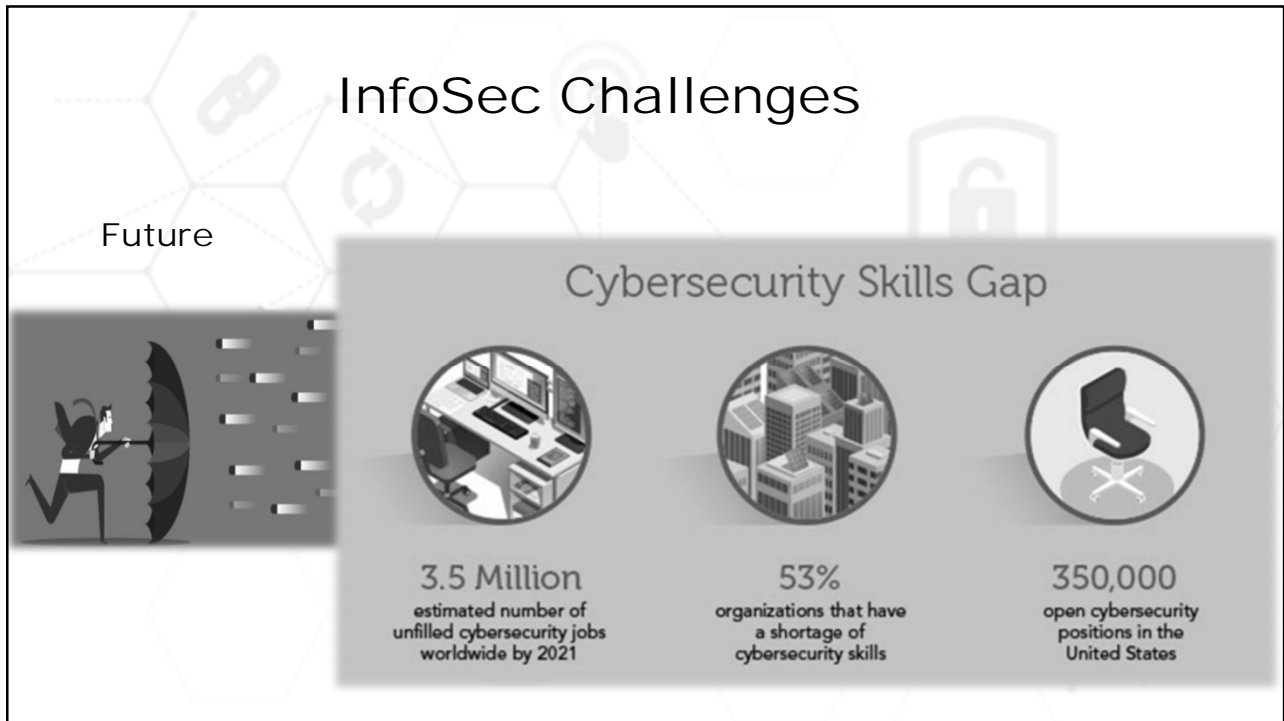
- Risk Assessment
- Digital Forensics Investigations
- Disaster Recovery Plans
- Information Security Awareness Program
- Digital Solutions Acquisition Assessment
- Penetration Testing
- Vulnerability Management
- Monitoring Activities
- Design Validation



30



31



32

InfoSec Challenges

System Complexity / Addressing new method of attack

Attackers Target Data



3 Billion
number of accounts with PII and passwords compromised in an online data breach







500 Million
guest records compromised in massive attack on major hotel chain



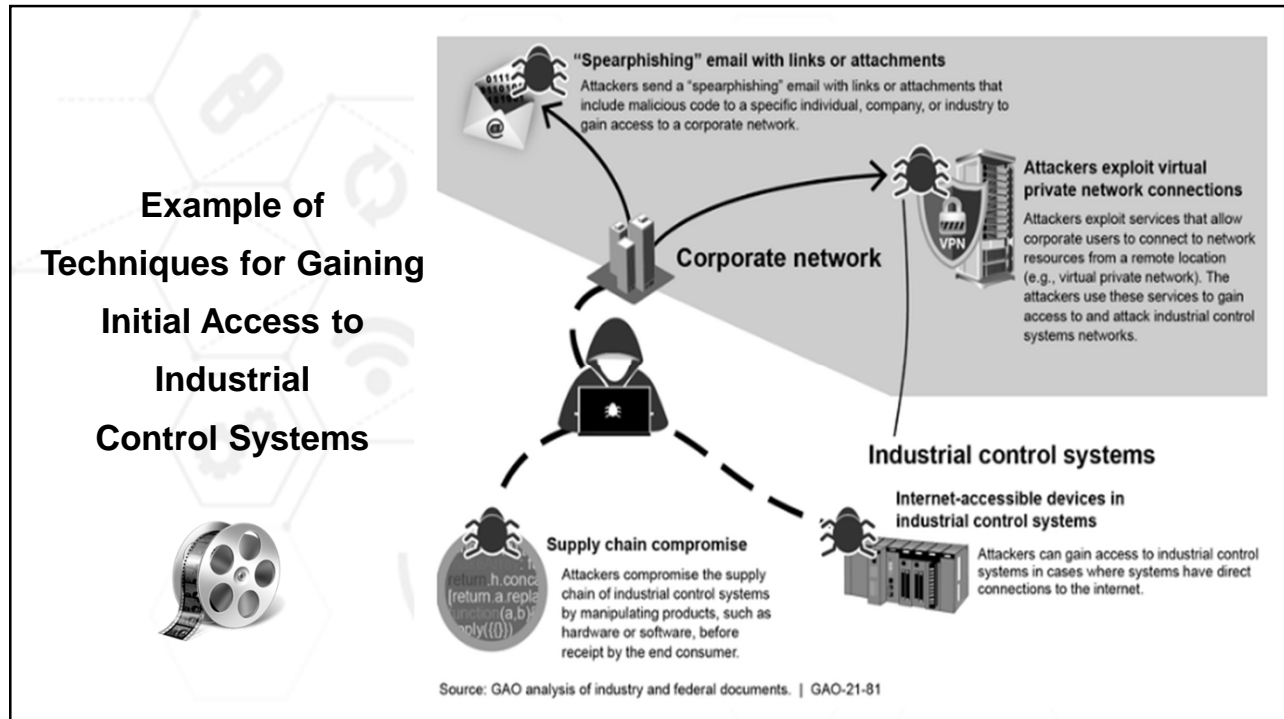
21.5 Million
data records lost after attackers targeted central databases in a government agency

33

Threats Impact on Electric Power System

 <p>Generation Disruption of service and ransomware attacks against power plants and clean-energy generators Root cause: Legacy generation systems and clean-energy infrastructure designed without security in mind</p>	 <p>Transmission Large-scale disruption of power to customers through remotely disconnecting services Root cause: Physical security weaknesses allow access to grid control systems</p>	 <p>Distribution Disruption of substations that leads to regional loss of service and disruption of service to customers Root cause: Distributed power systems and limited security built into SCADA¹ systems</p>	 <p>Network Theft of customer information, fraud, and disruption of services Root cause: Large attack surface of IoT devices, including smart meters and electric vehicles</p>
---	--	---	---

34



35



36

Hardware Authentication

- Dedicating a portion of the chipset for security functions to make a device part of the authentication process
- Hardware authentication can be particularly important for the Internet of Things (IoT)



37

User-behavior Analytics

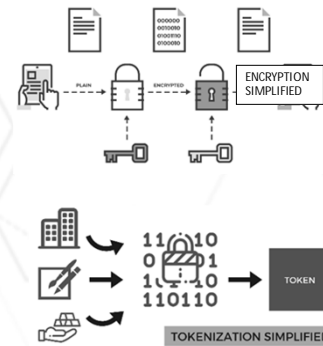
- Differentiate between a legitimate user's activity and an attacker who has gained entry.
- **Peer Analysis:** compares how someone is behaving compared to people with the same manager or same department.



38

Data loss prevention

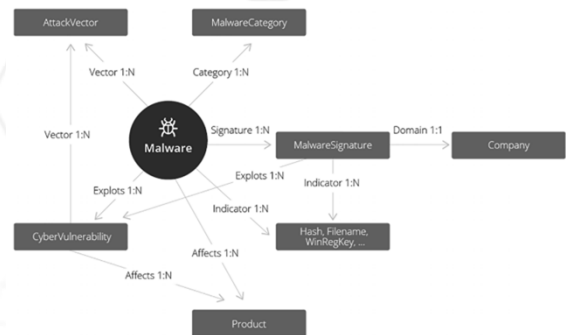
- **Techniques:**
 - Encryption
 - Tokenization
- **Protection of**
 - Payment card information (PCI)
 - Personally identifiable information (PII)
 - Protected health information (PHI)



39

Deep learning


- Encompasses number of technologies like Artificial Intelligence
- Focuses on Anomaly Detection
- Instead of looking for users, it looks for entities, persistent threats



40

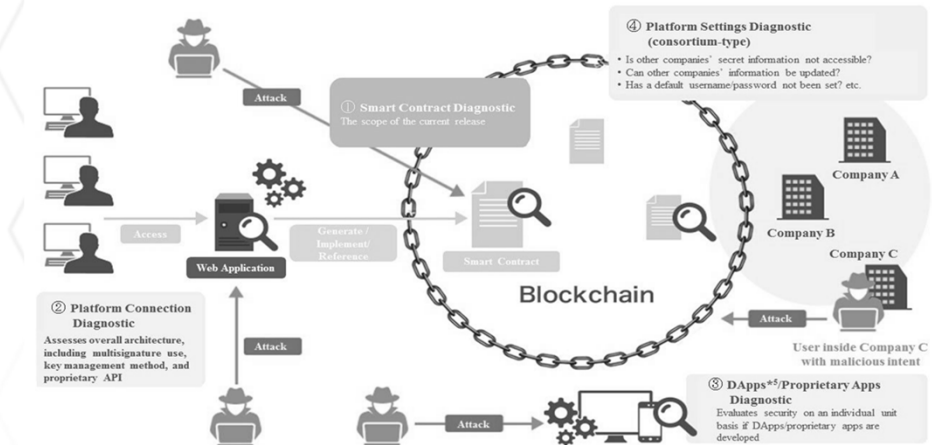
The cloud

- Virtualized security hardware
- Virtualized firewalls
- Virtualized intrusion detection and prevention systems



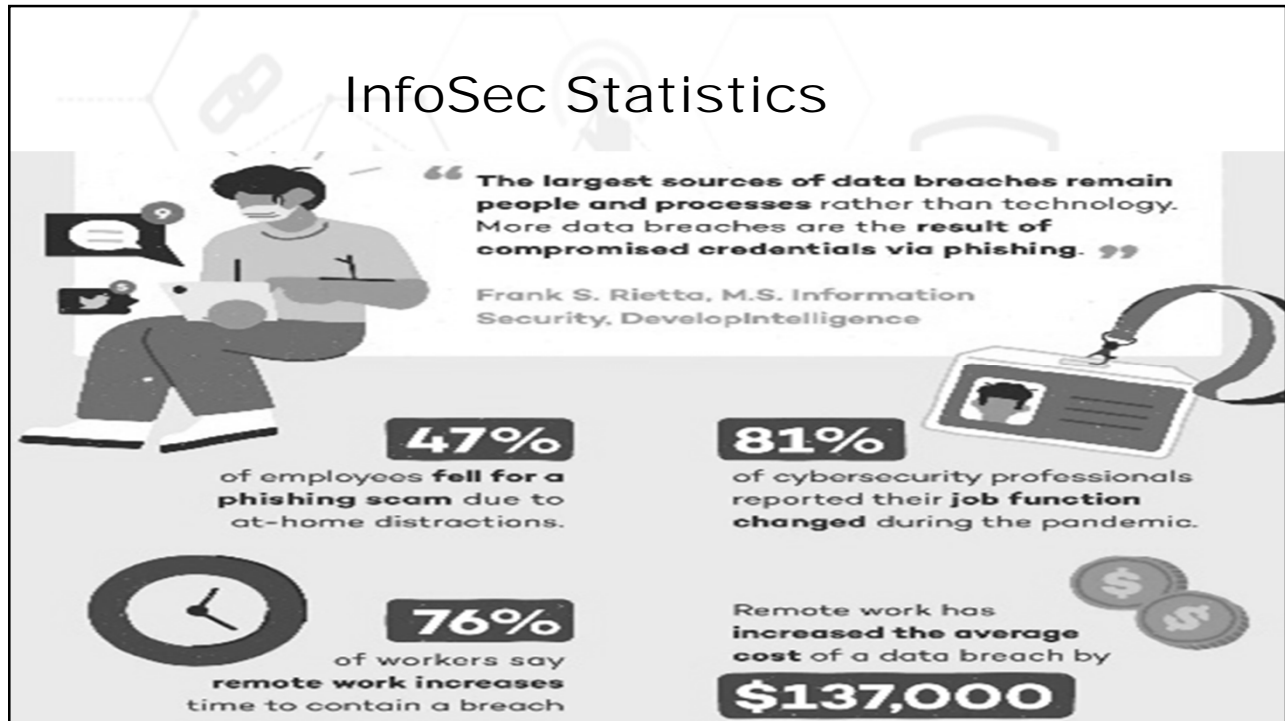
41

Blockchain

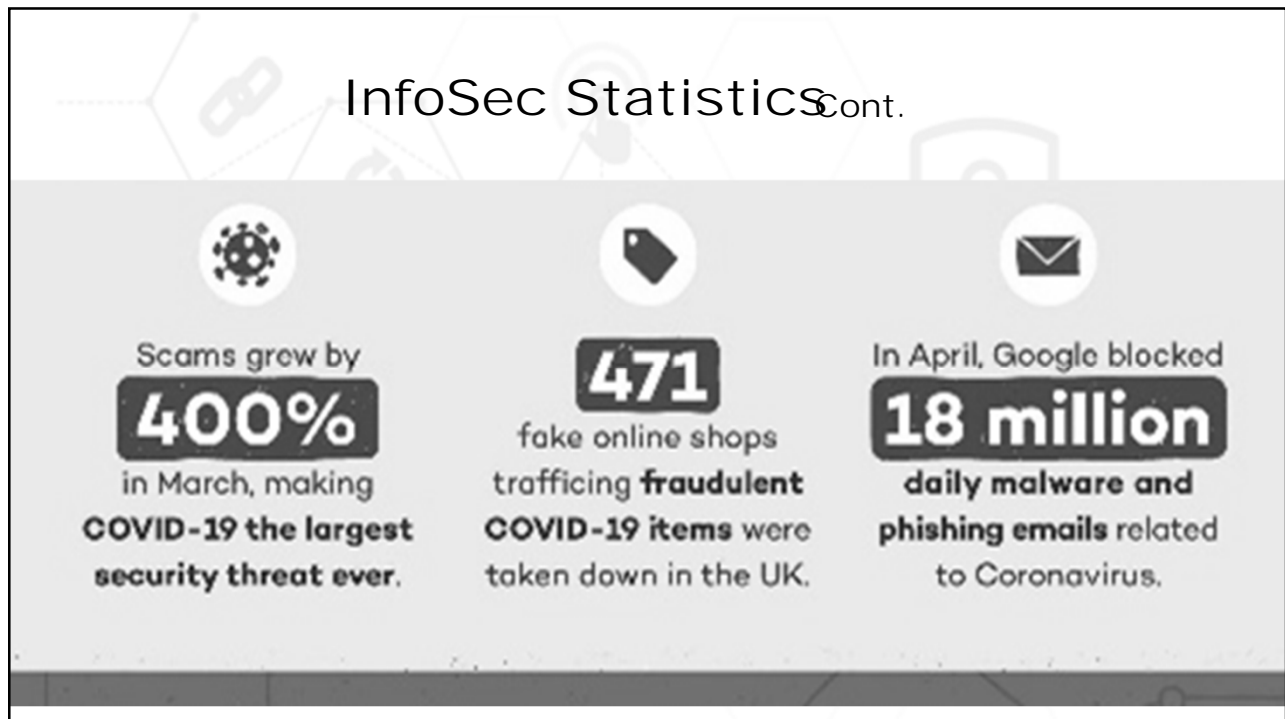


Eliminates the problem of a single point of failure

42



43



44

InfoSec Statistics Cont.

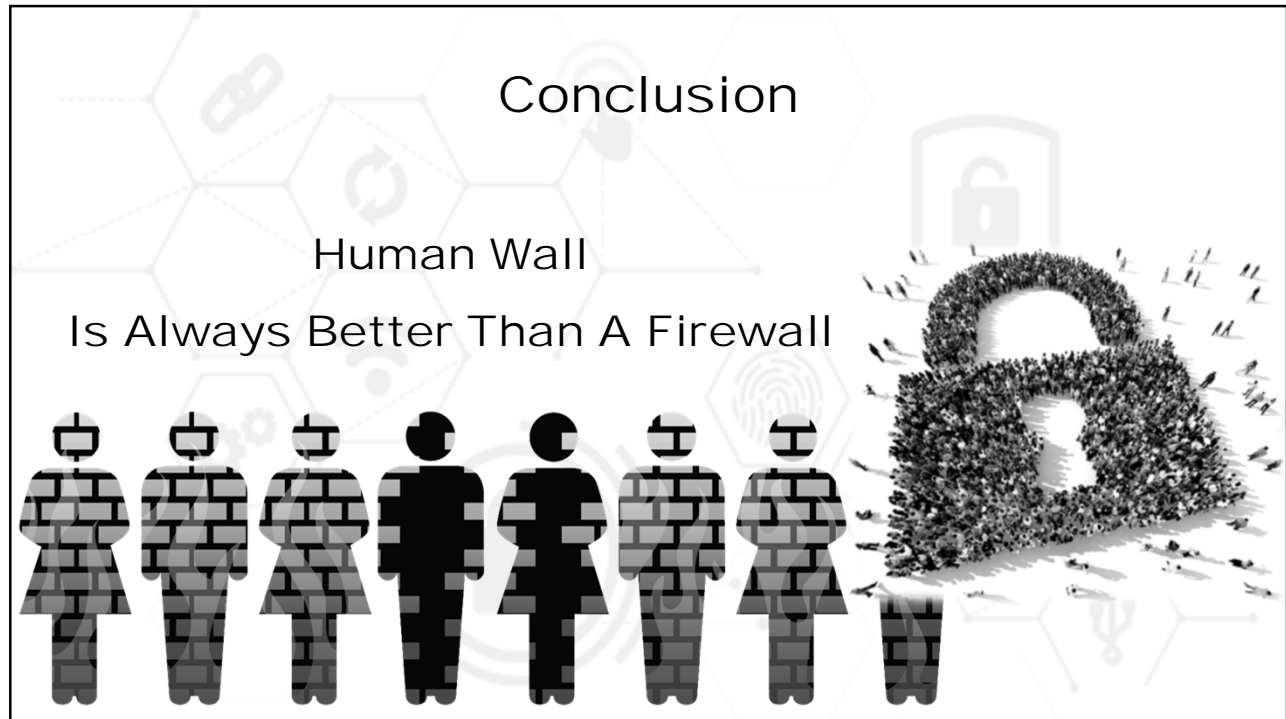


45

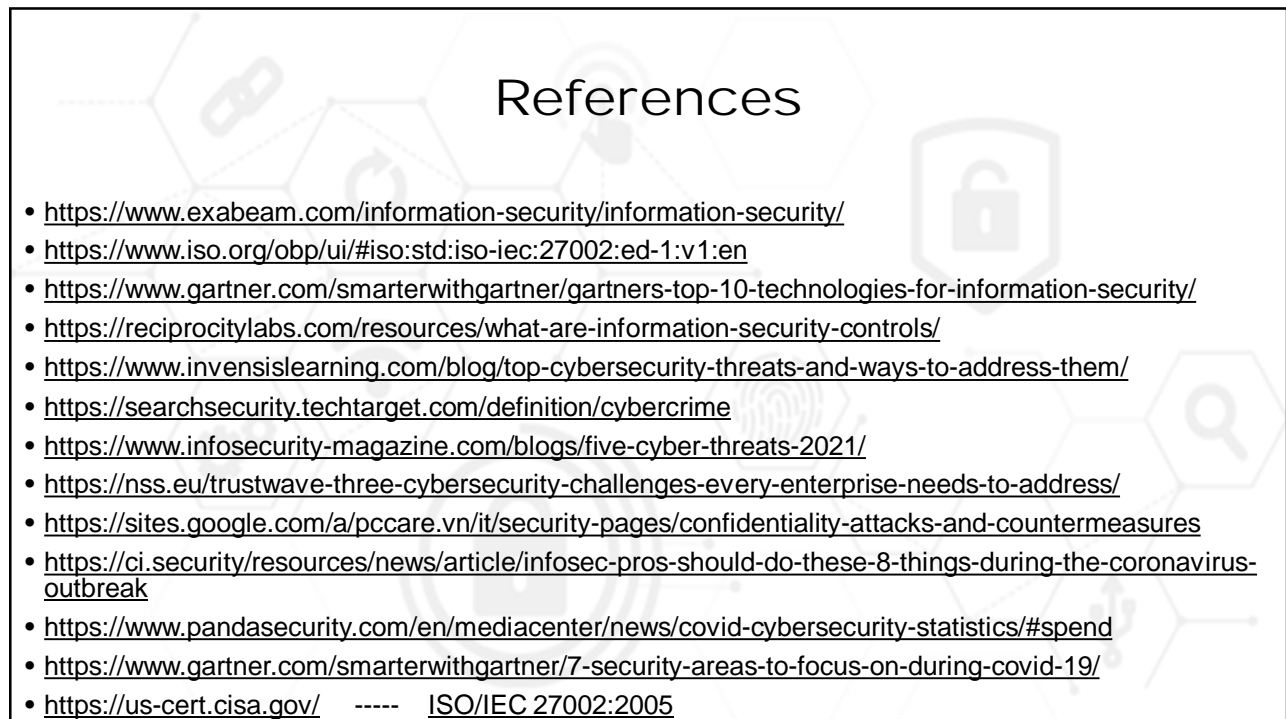
2020 VS 2021

Market	2020	2021	Growth
Application security	3,333	3,738	12.2%
Cloud security	595	841	41.2%
Data security	2,981	3,505	17.5%
Identity access management	12,036	13,917	15.6%
Infrastructure protection	20,462	23,903	16.8%
Integrated risk management	4,859	5,473	12.6%
Network security equipment	15,626	17,020	8.9%
Other security software	2,306	2,527	9.6%
Security services	65,070	72,497	11.4%
Consumer security software	6,507	6,990	7.4%
Total	133,776	150,409	12.4%

46



47



48