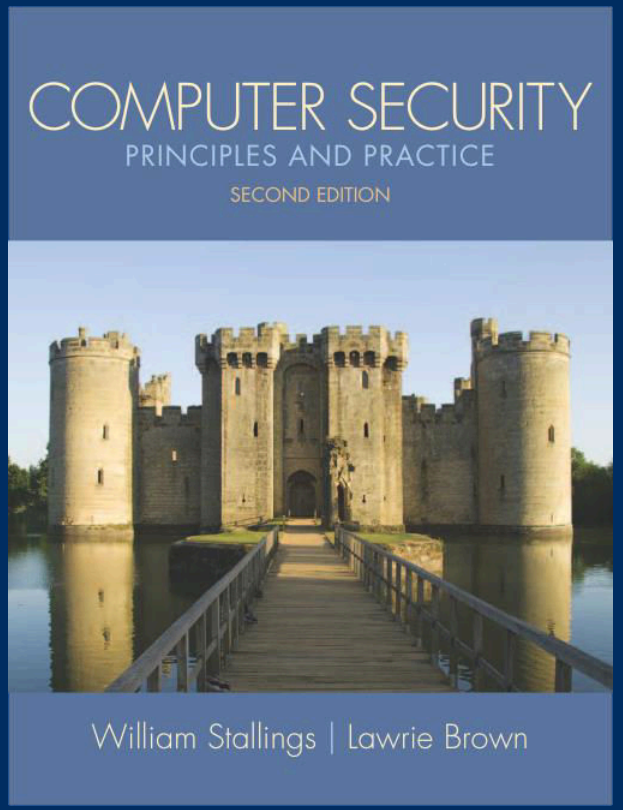
Lecture 1: Overview



modified from slides of Lawrie Brown

Outline

- Context: Cyber attack in Bangladesh
- Cyber Threat in Numbers
- Key Security Concepts
- Cyber Security
- Web Security
- Security Target
- Security Services
- Global Cyber Attack
- Potential Threats
- Cyber Attack Attributes

Do you have experienced with Cyber Attack

Bangladesh has become one of the most vulnerable countries in cyber space

- BGD e-GOV CIRT

Context: Cyber Attack in Bangladesh

- Recently, Bangladesh suffered a major and coordinated cyber attack (Feb, 2021)
  - A total of 147 banks and non-bank financial institutions
    - Bangladesh Bank (BB), Lanka Bangla Finance, Trust Bank, Bank Asia, Dhaka Bank
    - Hacker group called Hafnium known as threat actor
  - Tactic: a malware is inserted through Microsoft Exchange Server(MES)
    - Microsoft detected multiple zero day exploitations
    - What are the consequences?
    - How to mitigate?
      - Microsoft's Test-ProxyLogon.ps1 script
      - Scanner "MSERT

https://thefinancialexpress.com.bd/national/latest-cyber-attack-hit-at-least-147-bangladeshi-entities-1617416432

Context: Cyber Attack in Bangladesh

- In Nov 2017, SWIFT warned banks around the world
  - What : A hacker stole $81 million from Bangladesh Bank in February 2016.
  - How: Customized malware attack that compromised SWIFT software so that threat actor can infiltrate the system and transfer funds
- DBBL cyber attack
  - What : losing $3 million between May 1 and 3 from cash machines in Cyprus, Russia and Ukraine.
  - How: A malware in the bank's card management system around three months ago and duplicate switch, which the bank could not detect.
  - It is undetected: Visa asked it to settle payments for transactions made by the bank's "clients" in Cyprus
  - Why DBBL?
    - It has the highest number of ATM booths across the country

Context: Cyber Attack in Bangladesh

Bangladesh Bank Warned to all banks of a fresh cyber attack from North Korea based hacker group during the Pandemic

Banks limits online activities which is already boosted during the pandemic

The monthly transactions increased to Tk7,421 crore by June this year.

Background-Cyber Security

- Today, cyber security requires a new line of defence
  - Traditional security defence such as signature based detection is not sufficient
  - Every year there are new threats , breaches and unknown vulnerabilities
- Severity of cyber security risk is very high
  - Attacks are well funded and well organized
  - The stakes at cyber security risk become larger every year
  - half of business organizations suffer at least one security incident per year

norm rather than an exception

- We need
  - Proactive defence
  - Shorten the window between compromise and detection
  - Predicate future risk
    - Effectiveness of existing controls

Cyber Threats Numbers

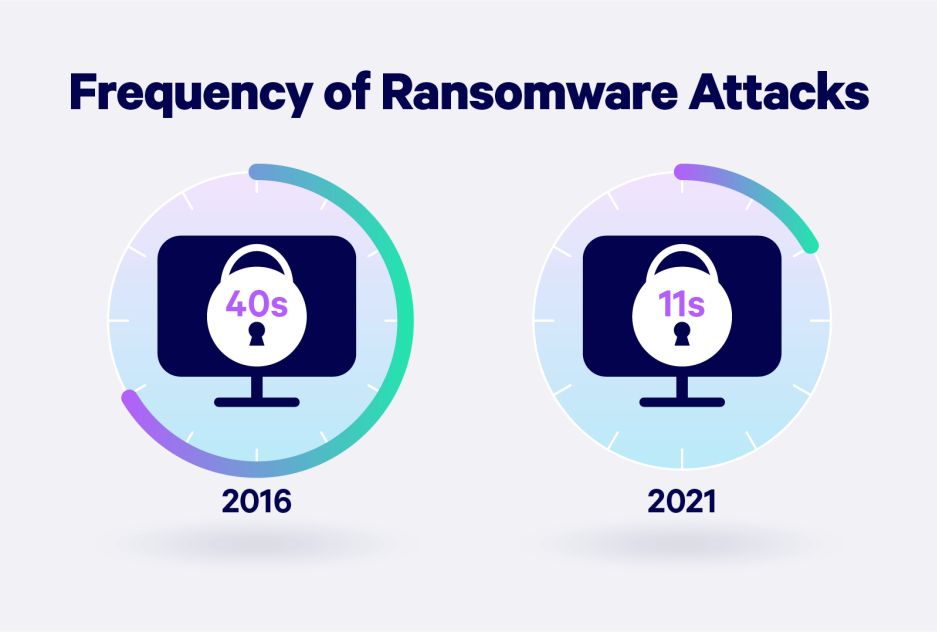
- How many cyber attack / day?
  - 30,000 website hacked per day
  - 4.3 million phishing attempts / hour
  - Every 39 seconds, there is a new attack somewhere on the web.
- There were 20M breached records in March 2021.
- It only takes 82 seconds to become the first victim of malware spam
- Companies 500 employees or more the average cost of the most severe breach is now between £1.46 million and £3.14 million
- 88% of organizations worldwide experienced spear phishing attempts in 2019.
- An estimated 300 billion passwords are used by humans and machines worldwide.

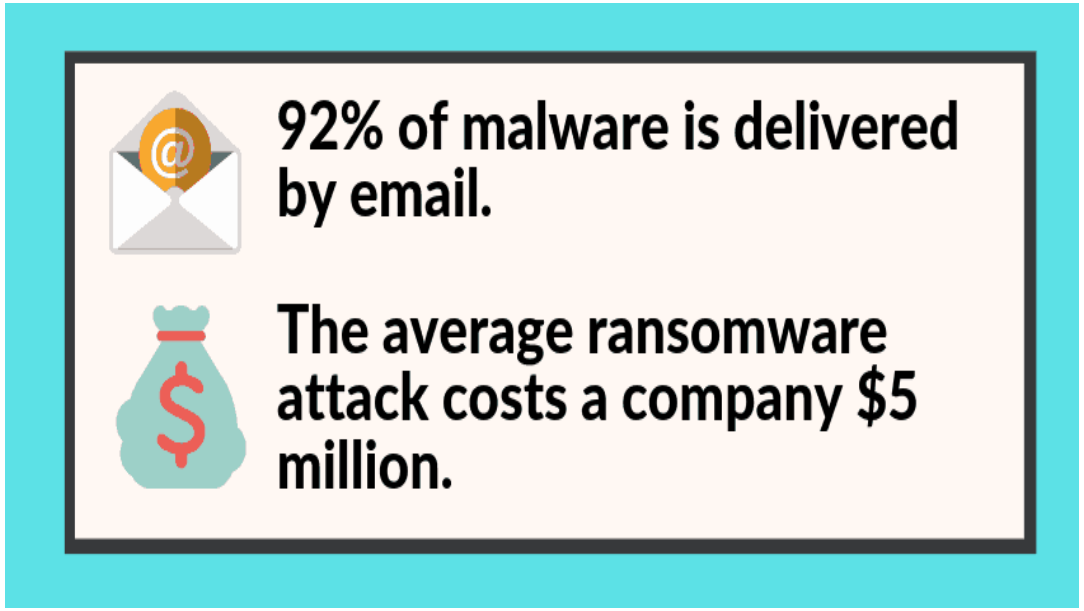
It difficult for computer users to stay safe online

Source: EU, McAfee, UK Gov,Deloitte

Attack Trends

- There are side effects of the global pandemic
- .zip and .jar are the most popular malicious e-mail attachments
- 48% of malicious email attachments are office files.
- About 20% of malicious domains are very new and used around one week after they are registered.



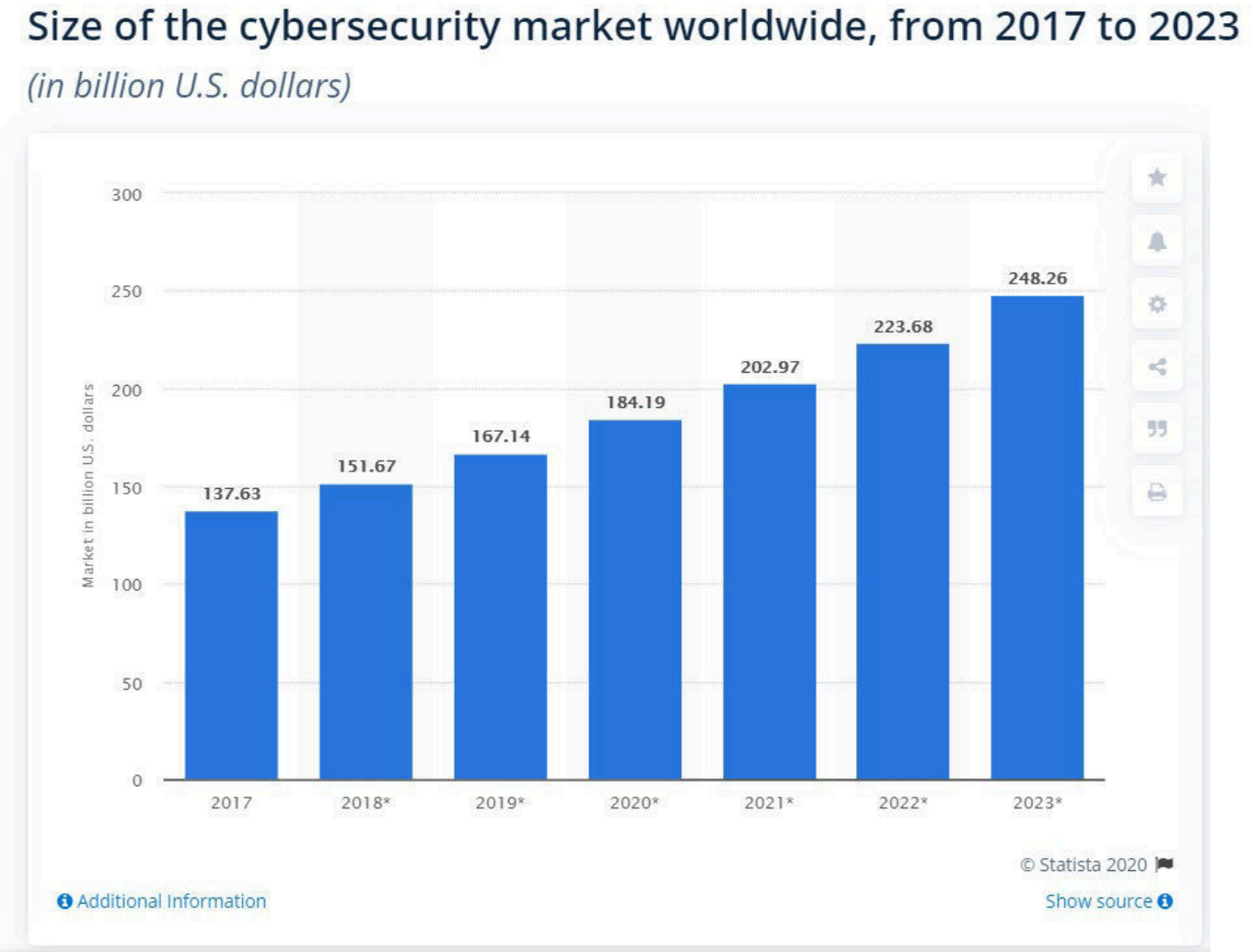


Cyber Security Market

- IT investment
  - Cybersecurity has the most significant budget

Worldwide information security market is forecast to reach $170.4 billion in 2022

-Gartner



A context is given

let’s move on

Key Security Concepts

- **Access** - a subject or object's ability to use, manipulate, modify, or affect another subject or object.
- **Asset** – anything that has value to an individual, an organization or a government
- **Cyber Space-** interconnected digital environment of networks, services, systems, and processes
- **Threat**: potential cause of an unwanted incident, which may result in harm to a system, individual or organization
- **Vulnerability**: weakness of an asset or control that can be exploited by a threat
- **Exploit** - to take advantage of weaknesses or vulnerability in a system.
- **Cyber incident-** cyber event that involves a loss of information security or impacts business operations

Key Security Concepts

- **Attack** - an act that is an intentional or unintentional attempt to cause damage or compromise to the information and/or the systems that support it.
  - Can be classified into:
    - Web-based attacks: attacks on a website or web application
    - System-based attacks: attacks that are intended to compromise a computer or computer network

- **Control countermeasure-** means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature
- **Exposure** - a single instance of being open to damage.

Key Security Concepts

- **Malicious contents-** applications, documents, files, data or other resources that have malicious features or capabilities embedded, disguised or hidden in them
- **Risk** - the probability that something can happen.
- **Cyber insurance**: insurance that covers or reduces financial loss to the insured caused by a cyber incident
- **Cyber-Physical Systems (CPS):** are systems composed of physical systems (hardware), software systems and potentially other types of systems (e.g., human systems). These are closely integrated and networked to deliver some global behaviour.

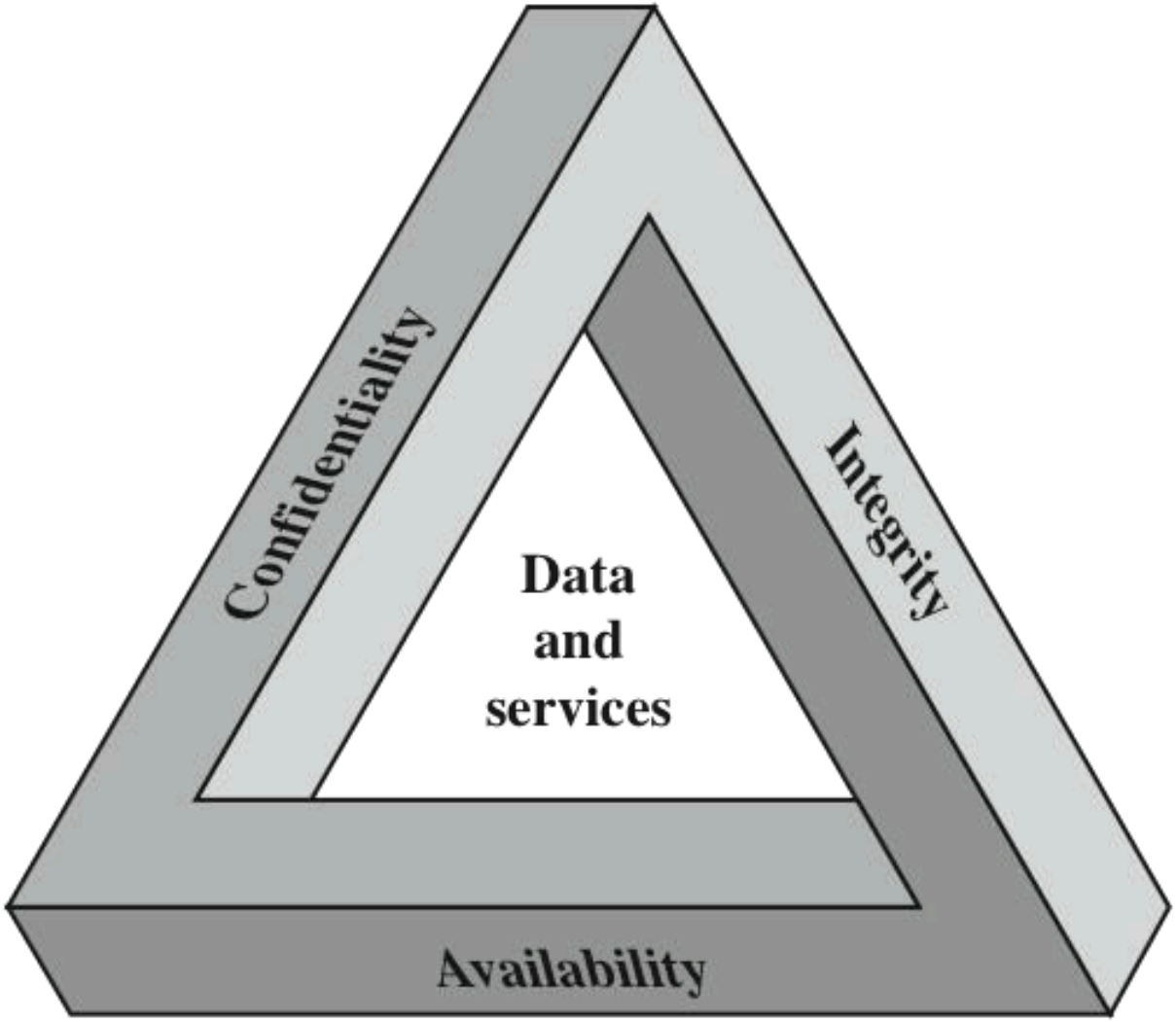
Cyber Security

Cybersecurity = security of information systems and networks in the face of attacks, accidents and failures with the goal of protecting operations and assets

availability, integrity and secrecy

- Protection of internet-connected systems such as hardware, software and data from cyberthreats

The CIA Triad



Key Security Concepts

- preserving authorized restrictions on information access and disclosure.
- including means for protecting personal privacy and proprietary information

- guarding against improper information modification or destruction,
- including ensuring information nonrepudiation and authenticity

- ensuring timely and reliable access to and use of information

Is this all?

Computer Security Challenges

- computer security is not as simple as it might first appear to the novice
- potential attacks on the security features must be considered
- procedures used to provide particular services are often counterintuitive
- physical and logical placement needs to be determined
- multiple algorithms or protocols may be involved

Computer Security Challenges

- attackers only need to find a **single** weakness, the developer needs to find **all** weaknesses
- users and system managers tend to not see the benefits of security until a failure occurs
- security requires regular and constant monitoring
- is often an afterthought to be incorporated into a system after the design is complete
- thought of as an impediment to efficient and user-friendly operation

Computer Security Terminology

- **Adversary** (threat agent) - An entity that attacks, or is a threat to, a system.
- **Attack** - An assault on system security that derives from an intelligent threat; a deliberate attempt to evade security services and violate security policy of a system.
- **Countermeasure** - An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

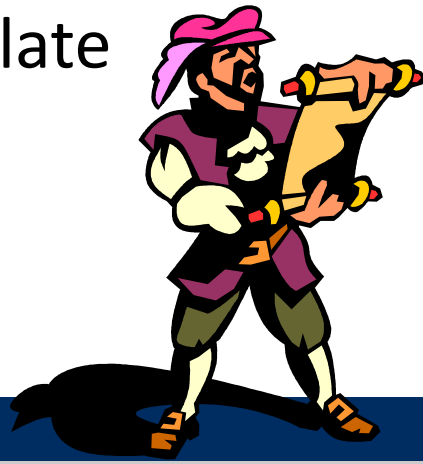
Computer Security Terminology

- **Risk** - An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
- **Security Policy** - A set of rules and practices that specify how a system or org provides security services to protect sensitive and critical system resources.
- **System Resource (Asset)** - Data; a service provided by a system; a system capability; an item of system equipment; a facility that houses system operations and equipment.

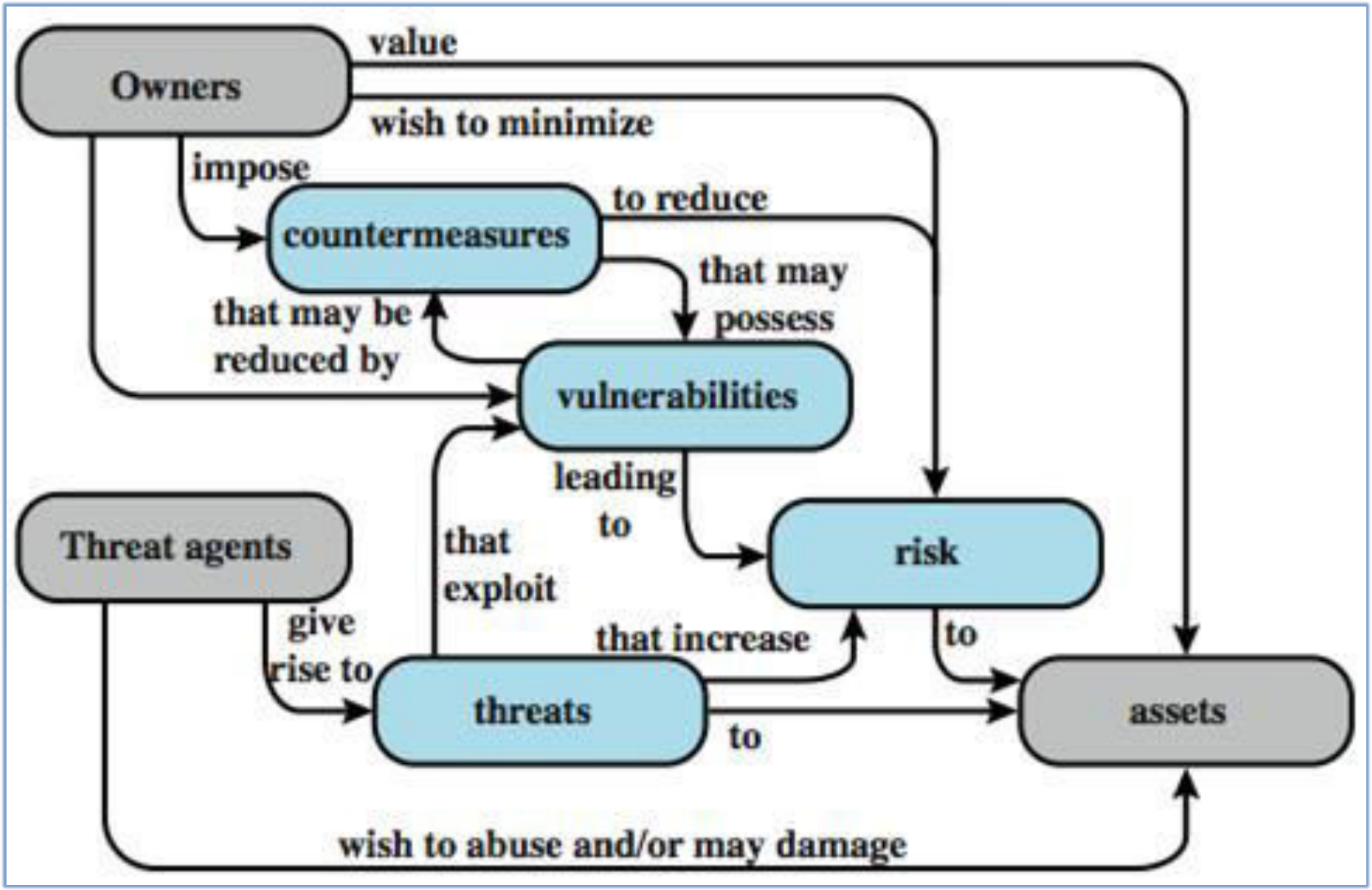
Computer Security Terminology

- **Threat** - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

- **Vulnerability** - Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.



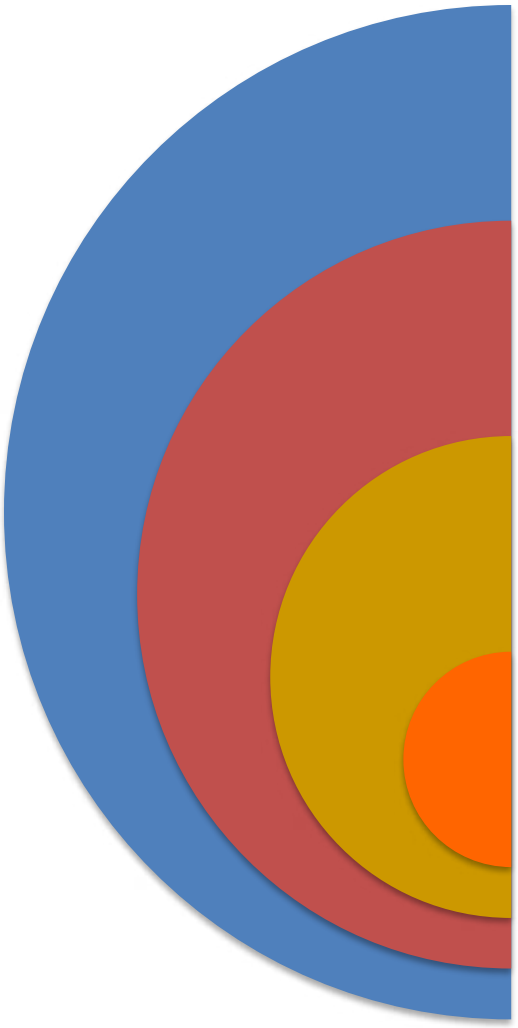
Security Concepts and Relationships



Vulnerabilities, Threats and Attacks

- vulnerabilities
  - corrupted (loss of integrity)
  - leaky (loss of confidentiality)
  - unavailable or very slow (loss of availability)
- threats
  - capable of exploiting vulnerabilities
  - represent potential security harm
- attacks (threats carried out)
  - passive or active attempt to alter/affect system resources
  - insider or outsider

Countermeasures



means used to deal with security attacks

- **prevent**
- **detect**
- **recover**

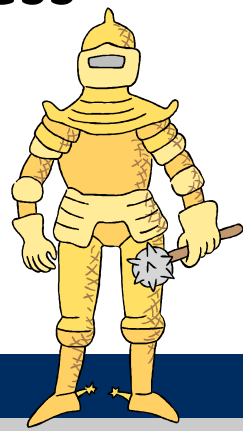
may introduce new vulnerabilities

Residual vulnerabilities may remain

goal is to minimize residual level of risk to the assets

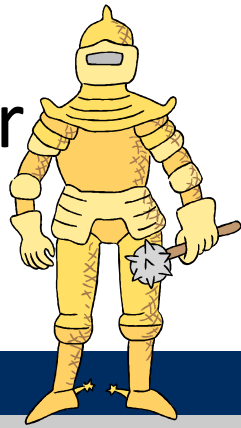
Threat Consequences

- Unauthorized disclosure is a threat to **confidentiality**
- **Exposure**: This can be deliberate or be the result of a human, hardware, or software error
- **Interception**: unauthorized access to data
- **Inference**: e.g., traffic analysis, use of limited access to get detailed information
- **Intrusion**: unauthorized access to sensitive data



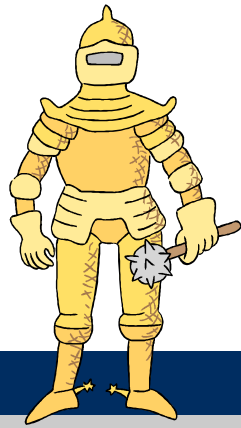
Threat Consequences

- **Deception** is a threat to either system or data integrity
- **Masquerade**: e.g., an attempt by an unauthorized user to gain access to a system by posing as an authorized user; Trojan horse.
- **Falsification**: altering or replacing of valid data or the introduction of false data
- **Repudiation**: denial of sending, receiving or possessing the data.



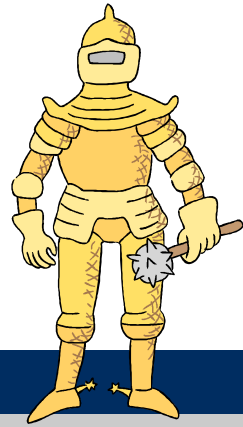
Threat Consequences

- **Disruption** is a threat to availability or system integrity
- **Incapacitation**: a result of physical destruction of or damage to system hardware
- **Corruption**: system resources or services function in an unintended manner; unauthorized modification
- **Obstruction**: e.g. overload the system or interfere with communications



Threat Consequences

- **Usurpation** is a threat to system integrity.
- **Misappropriation**: e.g., theft of service, distributed denial of service attack
- **Misuse**: security functions can be disabled or thwarted

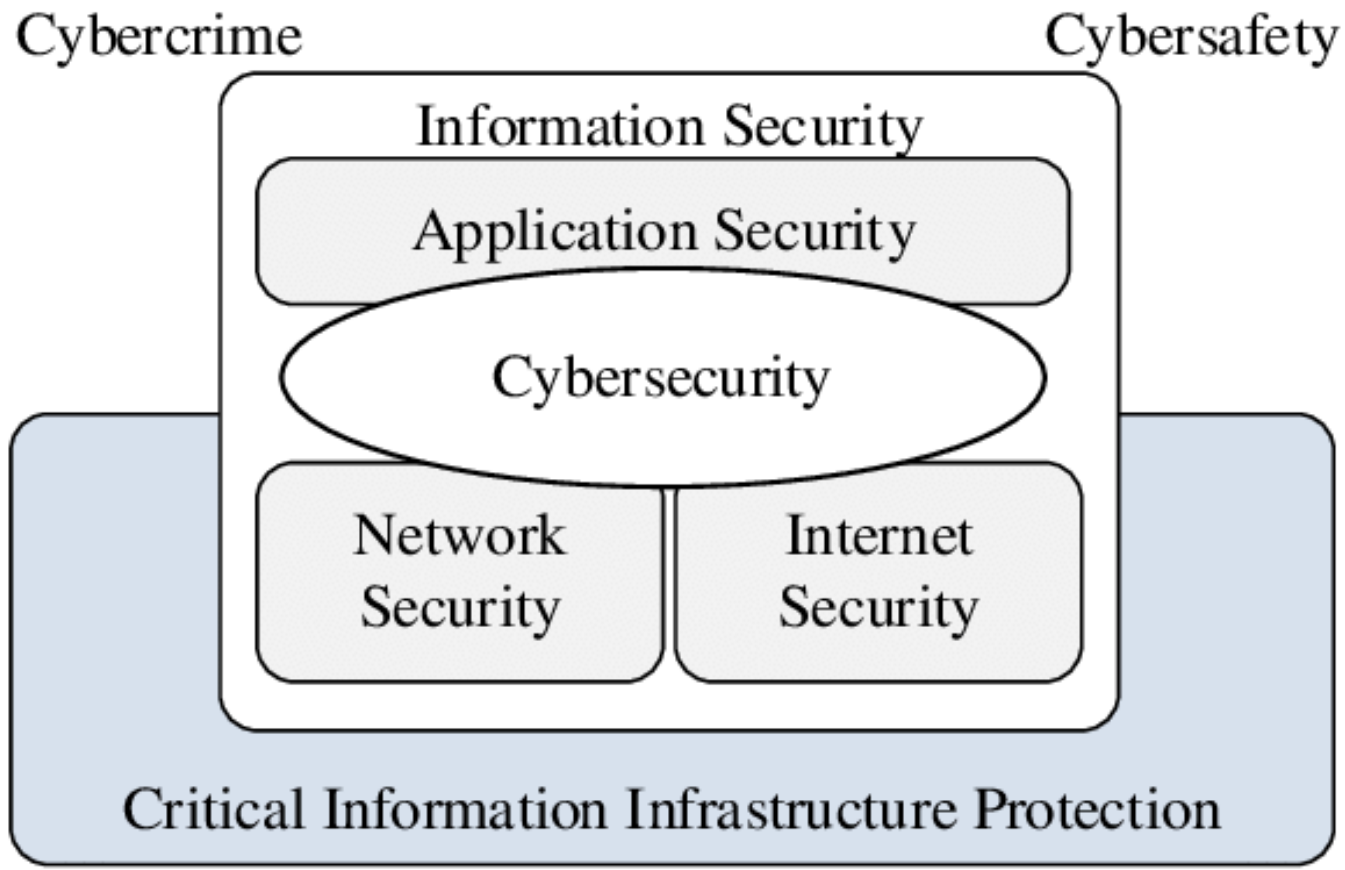


Cyber Security

- **Corporate cybersecurity** = availability, integrity and secrecy of information systems and networks in the face of attacks, accidents and failures with the goal of protecting a corporation's operations and assets
- **National cybersecurity** = availability, integrity and secrecy of the information systems and networks in the face of attacks, accidents and failures with the goal of protecting a nation's operations and assets

Information Security Vs. Cyber Security

- Information security
  - Protecting information and information systems from unauthorized use, assess, modification or removal.
  - Two sub-categories
    - Physical environment by ensuring the premises is secure
    - No one can access information electronically
  - Concerned with making sure data in any form is kept secure and is a bit more broad than cybersecurity
- Cyber Security
  - How individuals and organisations reduce the risk of cyber attack.
  - Cyber security is the practice of protecting information and data from outside sources on the Internet.
  - cyber security focuses on digital information but also, it deals with other things as well: Cyber crimes, cyber attacks, cyber frauds, law enforcement.


Cybercrime
Cybersafety
Information Security
Application Security
Cybersecurity
Network Security
Internet Security
Critical Information Infrastructure Protection

Web security

- Process, technology or method for protecting
  - Web servers, web applications, and web services against different security threats that exploit vulnerabilities in an application's code.
  - Critical to the business continuity

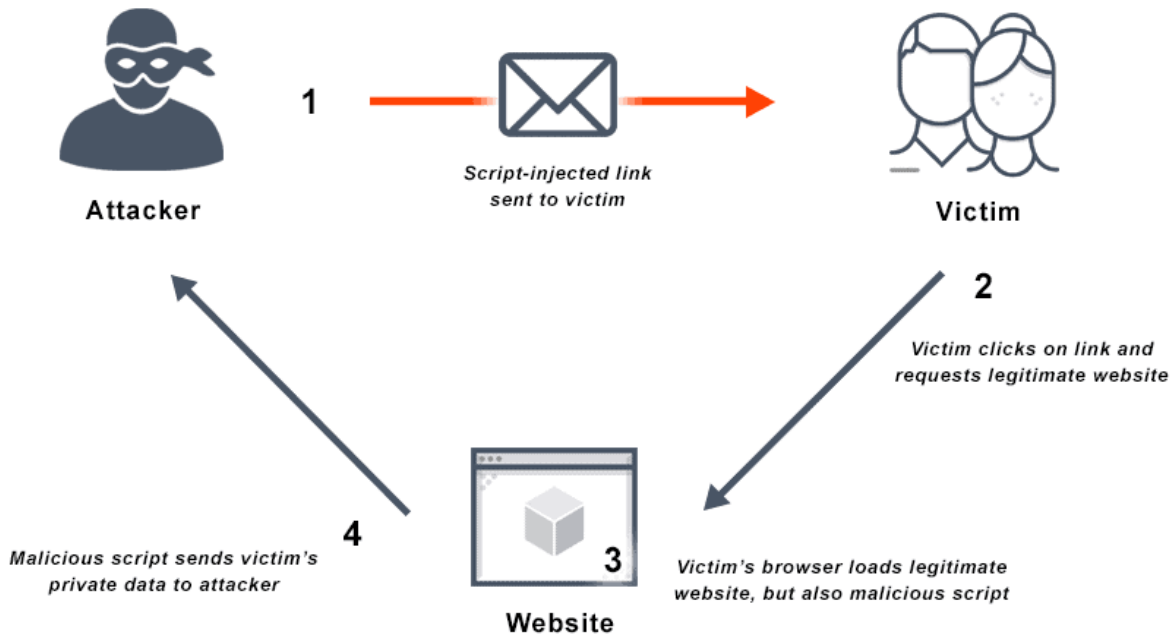
The web and the use of DNS services specifically are part of 91% of all malware attacks

Email and web together are a key part for 99% of successful breaches.

- Commonly, prime target by the threat actors
  - High value rewards, including sensitive private data collected from successful source code manipulation.
  - Ease of execution
  - Apps are now in every where from financial institutions, service delivery , personal entertainment and e-commerce
    - A simple bug in the code can pose for any information leak.

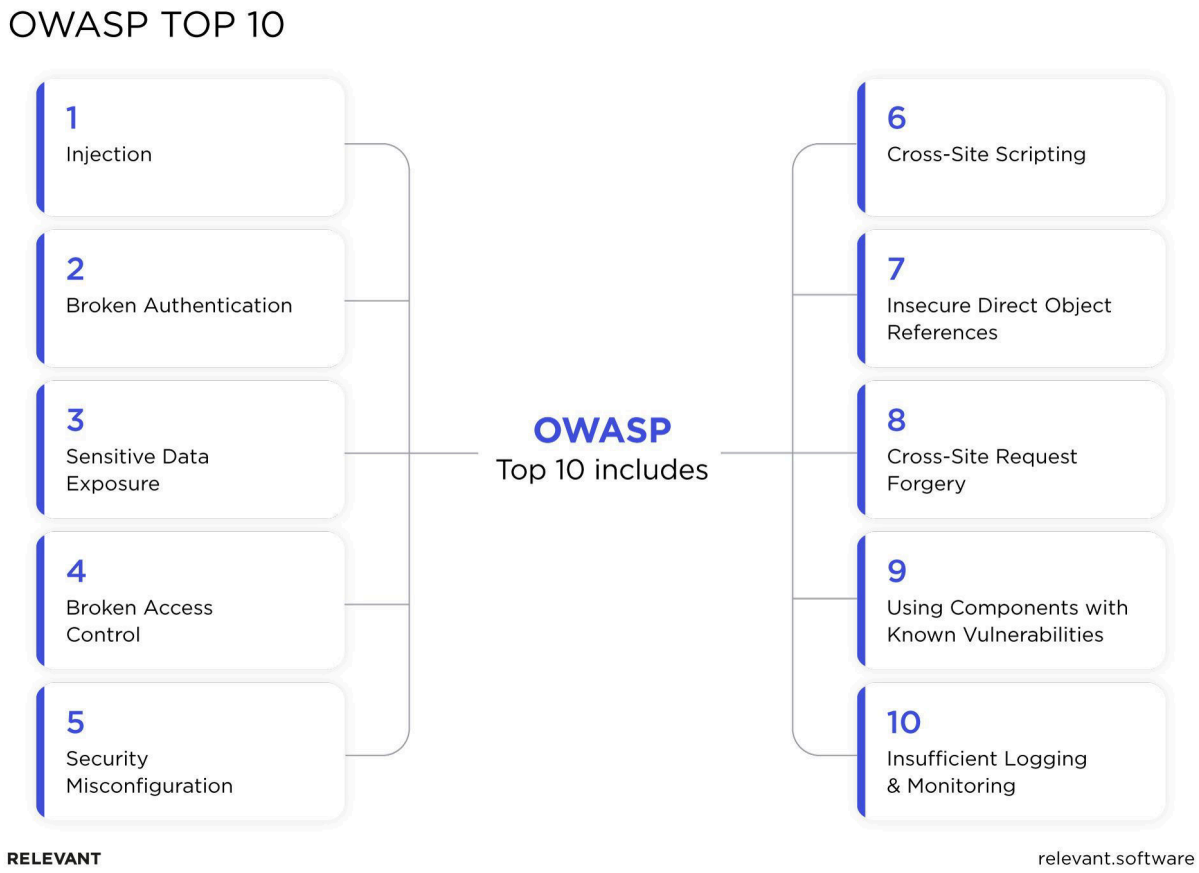
Web security: Vulnerabilities

- Web security threat exploits the vulnerabilities within the websites and applications
- Cross-site scripting(XSS)
  - Attacker attaches code onto a legitimate website that will execute when the victim loads the website
  - How can malicious code inserted?
    - Added to the end of a URL
    - Posted directly onto a page that displays user-generated content.



Web security: OWASP

- The Open Web Application Security Project(OWASP) foundation
  - Source for developers and technologists to secure the web.
  - OWASP Top Ten Web security risk is the most widely used

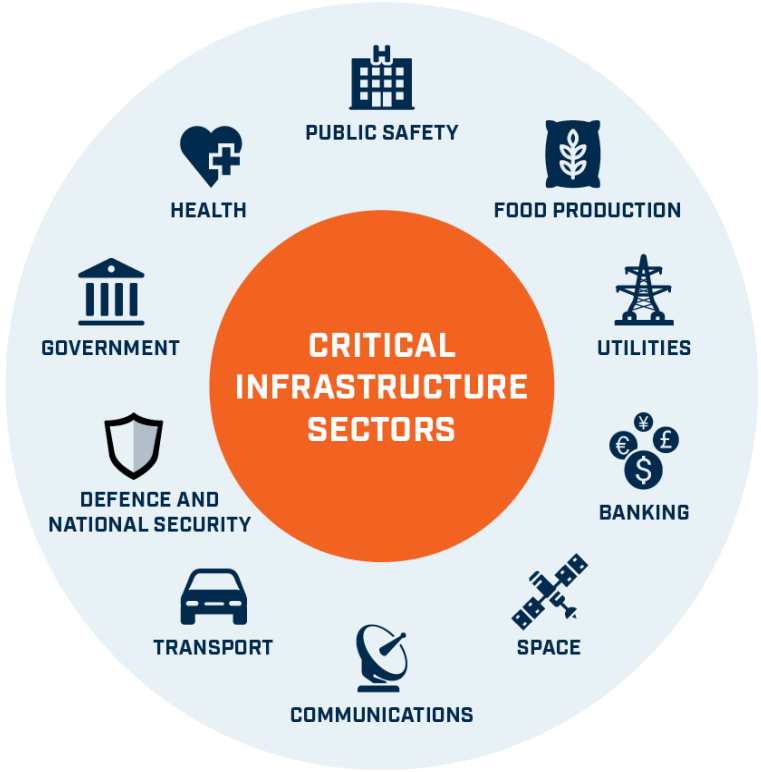


Web security: Control

- Secure website design using creating and renewing passwords, client side code
- Up-to-date Encryption
- Connection Security
  - Transport Layer Security : enabling two networked applications or devices to exchange information privately and robustly
  - HTTPS (HyperText Transfer Protocol Secure): Encrypted version HTTP protocol
    - SSL or TLS to encrypt all communication between a client and a server
- Data Security
  - HTTP cookie: Server sends to the user's web browser for session management, personalization, tracking
  - Restrict access to cookies :sent securely and are not accessed by unintended parties or scripts
- Web Application Firewall
  - protect a web application against malicious HTTP traffic.
  - protect against attacks like cross site forgery, cross site scripting and SQL injection

Critical infrastructure

Facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends.



Security Target

- The desired levels of security and assurance varies between organization, industries, even departments

  There is not single approach applies to every one

- Three main security goals
  - Confidentiality(C)
  - Integrity(I)
  - Availability(A)
- Three security services necessary to support the CIA
  - Identification
  - Authentication
  - Authorization

Confidentiality

- Ensuring that information is accessible only to those authorised to have access.
- Variation of confidentiality
  - Data protection/Personal data privacy – Fair collection and use of personal data, in Europe a set of legal requirements
  - Anonymity/Untraceability – Ability to use a resource without disclosing identity/location.
  - Unlinkability – Ability to use a resource multiple times without others being able to link these uses together HTTP “cookies” and the Global Unique Document Identifier (GUID) in Microsoft Word documents were both introduced to provide linkability.
  - Pseudonymity – Anonymity with accountability for actions.
  - Unobservability – Ability to use a resource without revealing this activity to third parties low probability of intercept radio, steganography, information hiding
  - Copy protection, information flow control – Ability to control the use and flow of information

Confidentiality(cont..)

- Variety of techniques are used to protect information:
  - Access control mechanisms: Prevent unauthorized individuals from accessing the system;
  - File system security controls: Prevent individuals authorized to use a system from exceeding their authority and reading confidential information they shouldn’t be able to access;
  - Cryptography: Can be used to encrypt the contents of sensitive files and protect them from prying eyes, even when access control and file system security mechanisms fail.

Integrity

- Integrity mechanisms protect data against unauthorized modification.
- Some common integrity mechanisms include:
  - Access control mechanisms: Prevent unauthorized individuals from accessing the system and modifying data.
  - – File system security controls: Control the rights of data users. They might grant a large number of users permission to read data but prevent all except a select handful from modifying the data
  - -Cryptography: The system of using digital signatures to confirm that a message wasn't altered in transit.
- The main threat on Integrity is known as:
  - – Alteration: malicious individual might attempt to alter data for a
- variety of reasons, like financial and deception
- When data integrity is preserved, the data is called *reliable*

Availability

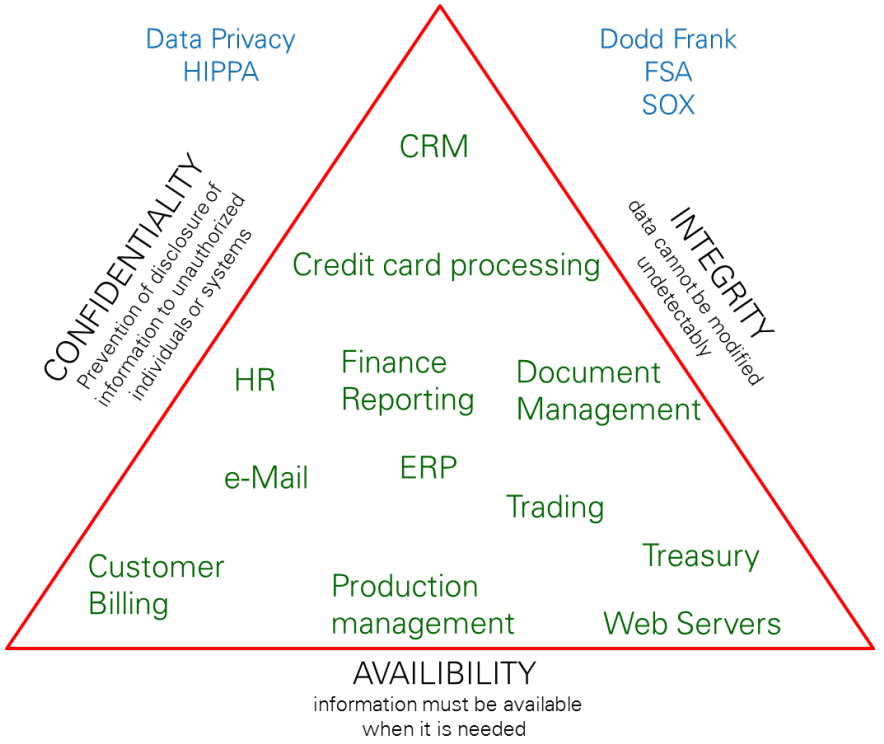
- To ensure that information or service is available as per the specification without any interference or obstruction
- It's perhaps more obvious that the confidentiality and integrity of data is extremely important.
- Only for the authorized user should able to access the information or service
- Depend on confidentiality and integrity
- Denial of service is a common attack to violate availability
- Security mechanism, i.e., back up and recover, monitor

CIA

Ability to control or restrict access so that only authorized individuals can view sensitive information. Classification's may include

- Secret
- Confidential
- Internal &
- Public

Typical risks: Loss of privacy, unauthorised access to information, Identity theft, etc.



Information is accurate and reliable and has not been tampered or changed in an unauthorized way. Integrity controls ensure that the information is authentic, accurate and reliable.

Typical risks: Fraudulent activities, manufacturing defects, inaccurate financial reporting, etc.

Data is available to the users when needed

Typical risks: Business disruption, loss of customer confidence, loss of revenue, etc.

Computer and Network Assets

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Security services

- To provide the security services necessary to support the three legs of the CIA triad, security professionals must have systems in place that perform three main functions:
  - Allow users to identify themselves to the protected resource
  - Provide a means for the resource to objectively confirm the identity of the user
  - Provide the administrator of the resource with mechanisms to specify which users might access the resource and the actions those users might perform
- This can be achieved by the following three-steps:
  - Identification
  - Authentication
  - Authorization

Identification

- Identification specifies the extent to which a system shall identify its users (e.g., human actors and external applications) before interacting with them.

  Allow users to identify themselves to a resource

- Typically necessary prerequisites for authentication requirements.
- Minimum percentage to time an identified external in a specified situation shall occur

Systems must have a means of identifying individual users to achieve accountability

Authentication

- Verifies the identity of the users (e.g., human actors and external applications) before interacting with them.

  Allows a user to prove his identity to the satisfaction of the resource.

- Ensures that externals are actually who or what they claim to be and to avoid compromising security to an impostor.
- Depends on identification. If identity is important enough to specify, then so is authentication

Authorization

- After a user has identified herself and has satisfied any applicable authentication mechanisms, the system must have some means of deciding what level of access to grant her.
- Deals with the access and usage privileges of users.
- Identification and authentication establishes the basis for accountability and is the prerequisite for authorization
- Ensures that authenticated users have access specific application or data up to the agreed level
- Can be granted to: Individual persons or applications or groups of related persons or applications.

Let’s talk about the global cyber attack

Global Cyberattack: Game Publisher Electronic Arts (EA)

- A very recent attack on 10/06/2021
- One of the largest game companies in the works
  - Battlefield, Star Wars: Jedi Fallen Order, The Sims
- Hackers have stolen valuable information
  - Consequence: 780GB of data was stolen which is source code of the game
  - Consequence: intrusion into the network
  - But, no player data had been stolen in the breach
- Does not impact on the games or our business

Global Cyberattack: JBS

- World's largest meat supplier targeted by a sophisticated cyber-attack on May 31, 2021
  - Consequence: Temporarily shutting down some operations in Australia, Canada and the US, with thousands of workers affected.
  - Consequence: Forced the shutdown of all its U.S. beef plants
  - Consequence: Delay certain transactions with customers and suppliers.
  - Threat actor: Criminal group from Russia
  - Threat: Ransomware attack
    - Hackers get into a computer network and threaten to cause disruption or delete files unless a ransom is paid.
    - Suspended all affected IT systems as soon as the attack was detected

What Security goal is affected?

https://www.bloomberg.com/news/articles/2021-05-31/meat-is-latest-cyber-victim-as-hackers-hit-top-supplier-jbs

Global Cyberattack : British Airways

- BA website diverted to a fraudulent site disclose

380,000 customer data in 2018.

Login detailed, bank detailed

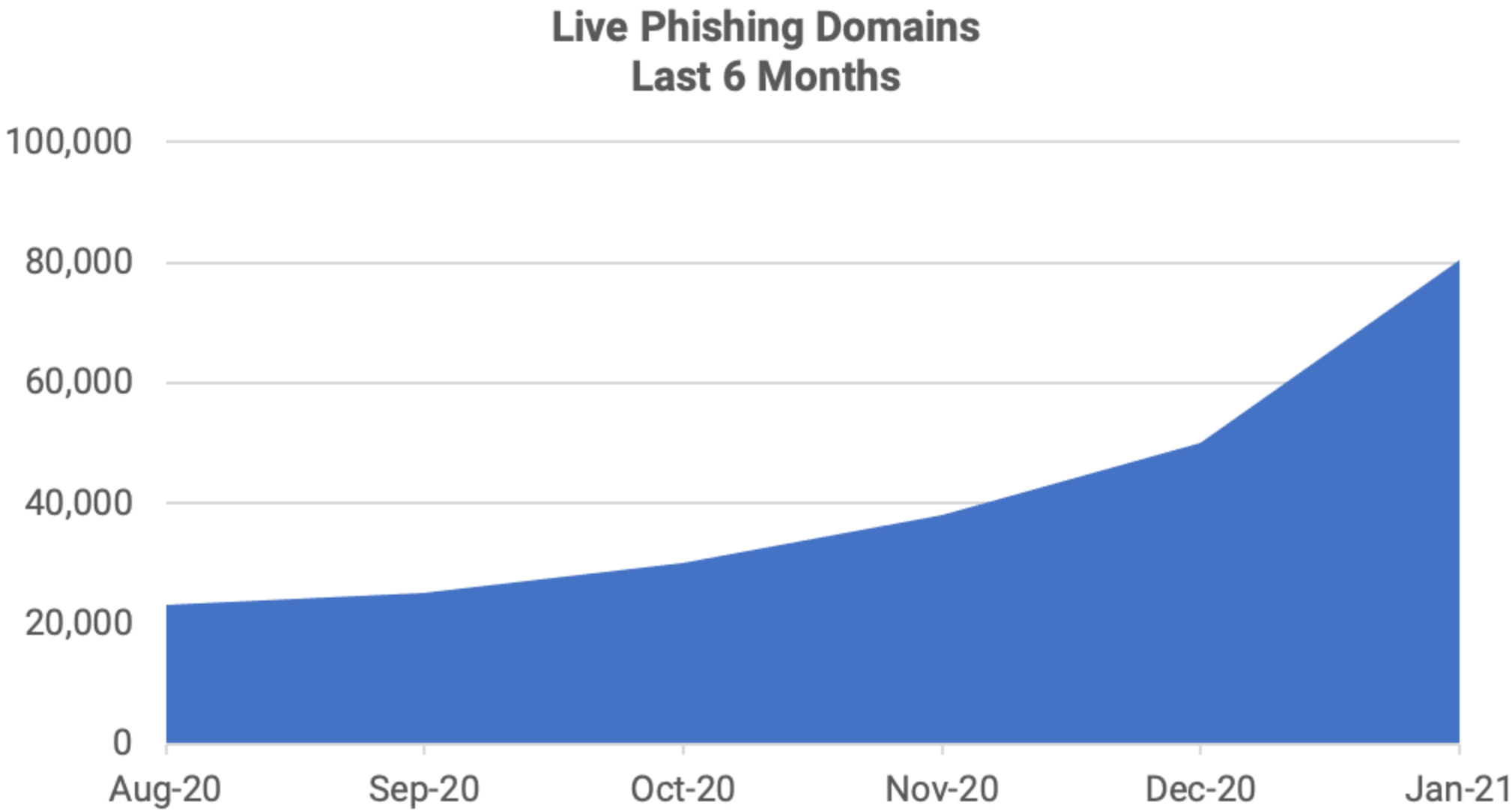
- Stolen data did not include travel or passport details.
- Magecart a financially-motivated threat group used malicious piece of code
  - Monitored for certain mouse-up and touch-up interactions, extracted data entered in the checkout page payment form, and sent it to a remote server

First penalty after imposing GDPR law £183m

This is the biggest shake-up to data privacy in 20 years.

Potential Threat: Phishing

- A common type of social engineering attack often used to steal user data, including login credentials and credit card numbers
- An attacker disguises as a trusted individual and tricks the victim into clicking a link in a spoofed email.
    - Pretend to come from trusted organization such as banks, credit card companies etc.
    - Malware hidden inside invoices
    - Steganography – code hidden in photos
- **Spear phishing** is a type of phishing attack that has an intended target user, organization or business.
- **Whaling** even more targeted type of phishing as it goes after the whales, the really BIG fish
    - These attacks target the CEO, CFO within an industry or a specific business.


Live Phishing Domains
Last 6 Months
100,000
80,000
60,000
40,000
20,000
0
Aug-20
Sep-20
Oct-20
Nov-20
Dec-20
Jan-21

Phishing: Tactics

- **Email:** appears in inbox. usually with a request to follow a link, send a payment, reply with private info, or open an attachment.
- **Domain spoofing:** mimic valid email addresses. These scams take a real company's domain (ex: @iit.du.ac.bd) and modify it.
- **Social media phishing:** Threat actor uses posts or direct messages to persuade victim into a trap.
- **Clone phishing:** duplicates a real message that was sent previously, with legitimate attachments and links replaced with malicious ones.
- Examples of common phishing scams
  - The tax refund/rebate
  - Contest winner/Inheritance email.
  - Office 365 deletion alerts

Potential Threat: Malware

- A Malware is a set of instructions that run on your computer and make your system do something that an attacker wants it to do.
- The purpose is often to steal, damage or manipulate sensitive information relating to an individual

Malware = Malicious Software

- Set of instructions that cause a site's security policy to be violated
- Often leveraging an inadvertent flaw or vulnerability (design or implementation)
  - –To propagate/install on target
  - –To cause harm on target

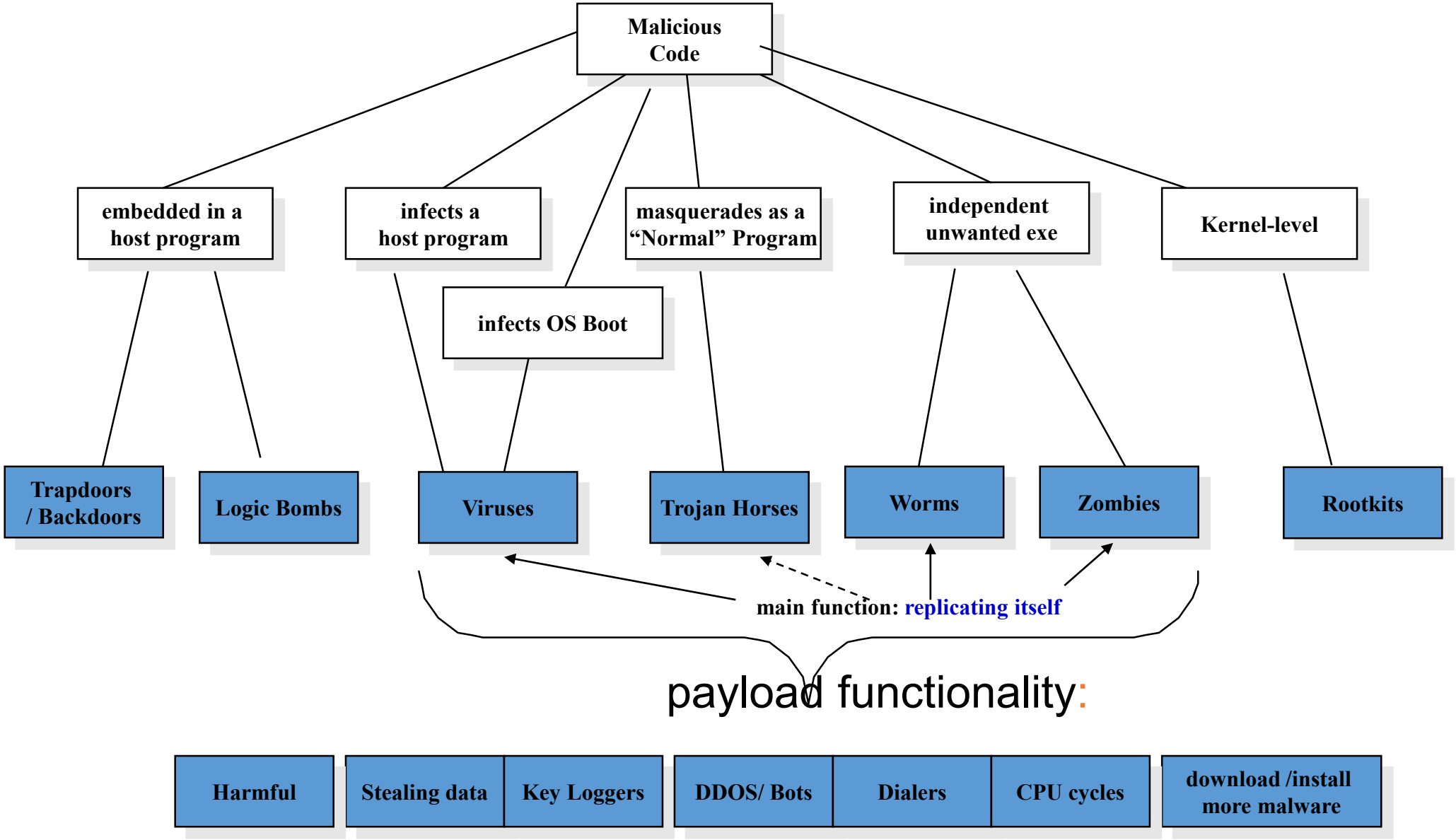
➢ Today, most malware possesses intent to destroy systems including:

- Files
- Web pages
  - Estimated that about 1 in 10 web pages contain malicious code.

Malware

- Zero day exploit
  - An exploit takes advantage of a vulnerability to attack a system and enact malicious behaviour
    - A Zero-Day exploit is based on a recently discovered vulnerability, that has no patch available yet
    - Time between exploit discovery and wide activation shrinking
    - Malware developer has trade-off
  - Big splash but faster discovery
  - Reduced attack rate but longer undiscovered

Malware Taxonomy: Pay load functionality



Payload

- The action that a threat performs, apart from its main behaviour.
- Malware that the threat actor intends to deliver
- Payloads can range from stealing personal information to deleting the contents of a hard drive.
- Example of Payload
  - Ransomware is a kind of cyber attack that involves hackers taking control of a computer system and blocking access to it until a ransom is paid.
  - Restricting the ability to carry out general activities on the system
    - Encrypting files
    - Disabling Apps

According to Symantec one in every 359 emails in existence contains a malicious payload

Payload

- Harms to the victim in many ways
  - **Data theft:** Particularly common is the theft of sensitive information such as login credentials or financial information
  - **Activity monitoring:** An executed malicious payload may serve to monitor user activity on a computer, this can be done for the purposes of spying, blackmail
  - **Displaying advertisements:** Some malicious payloads work to display persistent, unwanted ads such as pop-ups and pop-unders to the victim.
  - **Deleting or modifying files**: This is one of the most serious consequences to arise from a malicious payload. Files can be deleted or modified to either affect the behavior of a computer, or even disable the operating system and/or startup processes
  - **Downloading new files:** Some malicious payloads come in very lightweight files that are easy to distribute, but once executed they will trigger the download of a much larger piece of malicious software.

Cyber Attack Attribute

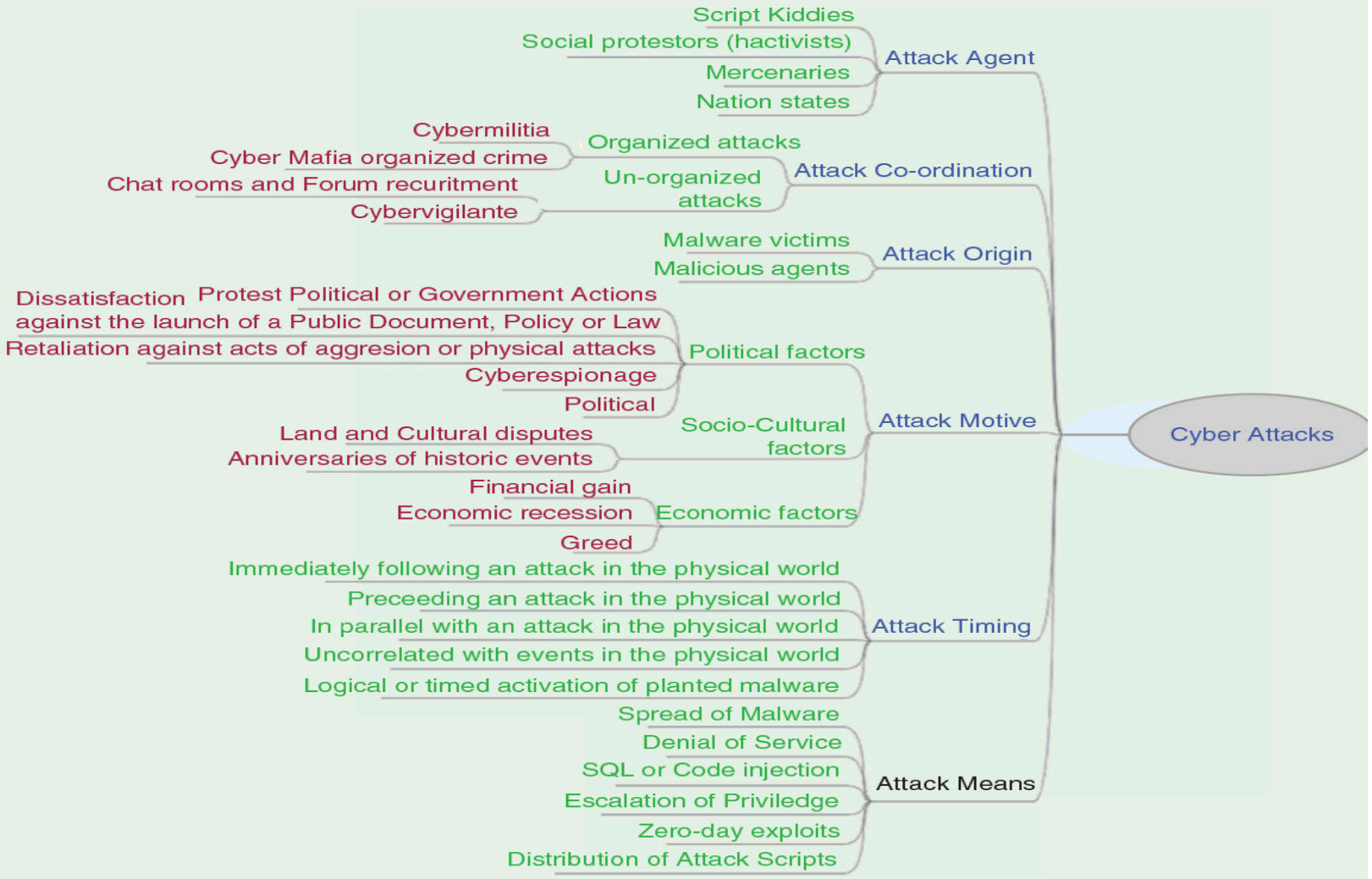


Fig. 4. Categorization of cyber-attack dimensions.

Final Note

- It is not realistic to believe that organisation can defend against every potential attack
  - Cyber attack will succeed to the infrastructure
    - May be not today but tomorrow or coming days
  - Organisations must have ability to identify and tackle the attack for the overall business continuity
- Cyber Security is a context specific
  - Need to consider defensive strategy based on the context
- What next then

Time to Think Beyond Cyber Security

Scope of Computer Security