OVERVIEW

What is Information Security?

Information security focuses on the value of the information being protected rather than how it is being protected. It encompasses physical security and cybersecurity.

Cybersecurity tends to focus on the security of digital systems, but it should not be limited to digital elements as most attacks have human and physical factors as well.

OFFENSE : Threat Actor Groups

# Cybersecurity professionals must know different types of threat actor groups, varying in motivation, resources, and techniques.

# The five main types of cyber attacker groups are Script Kiddie, Hacktivist, Criminal Gang, Nation State Hacker, and Malicious Insider.

What are Threat Actor Groups

# Cybersecurity professionals must know different types of threat actor groups, varying in motivation, resources, and techniques.

# The five main types of cyber attacker groups are Script Kiddie, Hacktivist, Criminal Gang, Nation State Hacker, and Malicious Insider.

Group 1: Script Kiddie

# Least advanced, relies on off-the-shelf penetration testing tools, publicly available exploits.

# Main motivations are reputation, status in the eyes of the hacking community, entertainment, or settling grudges.

Group 1: Script Kiddie (cont)

# Self-taught via forums, videos, and experimentation, typically teenagers or young adults.

# Little funding, little or no technical expertise and assistance, may use free tools written by others.

# Defenses should ensure patching schedule is effective and basic perimeter defenses are up to date.

Group 2: Hacktivist

# Driven by ideological reasons, uses hacking to achieve political or economic change.

# Range from impressionable amateurs to experienced members within the security community.

# Motivations vary greatly, involve supporting one cause the individuals believe in.

# Operate at scale with varying tools and biggest attribute is size.

# Defenses should cope with an extended disruptive attack.

Group 3: Criminal Gang

# Fastest growing group, running ransomware attacks, committing extortion, theft of customer data or intellectual property, and so on.

# Cyber-based criminal is a full-time and quite lucrative proposition.

# Gangs range from few individuals to multinationals with hundreds of members.

# Gangs frequently develop and deploy their malware, access substantial infrastructure such as servers and domains.

# International laws make securing a prosecution near impossible.

Group 3: Criminal Gang (cont)

# Defenses should be comprehensive and detect, respond, and recover from attacks.

Group 4: Nation State Hacker

# Operates on behalf of a government, military, or intelligence agency.

# Targets range from national security interests to commercial enterprises to personal data.

# Uses advanced and sophisticated tools and techniques.

# Uses large resources, such as funding, personnel, infrastructure, and expertise.

# Attacks can be difficult to detect and attribute, and may use false flag operations.

# Defenses require intelligence and expertise, including identifying potential targets and advanced threat hunting capabilities.

Group 5: Malicious Insider

# Insider threat actors with authorized access to an organization's systems or data.

# Can be current or former employees, contractors, or third-party vendors.

# Can be motivated by financial gain, ideology, revenge, or other reasons.

# Can use their access to steal, leak, or damage data, install malware or backdoors, or conduct espionage.

# Defenses require access control, monitoring, and insider threat detection capabilities, as well as comprehensive security awareness and training programs.

OFFENSE : Types of Cyber Attacks

Denial of Service (DoS) Attack:

Any attack that causes a complete or partial system outage.

Can range from causing a system to crash to making it unreachable or incapable of continuing work due to abnormal levels of forwarded network traffic.

Example: sending a maliciously formatted file to a server that causes it to overload.

Distributed Denial of Service (DDoS) Attack:

A DoS attack that comes from more than one source at the same time.

Machines used in such attacks are collectively known as "botnets" and will have previously been infected with malicious software.

Example: sending a large number of page requests to a web server in a short space of time, overloading it.

Phishing Attack:

The practice of sending messages that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something.

Combines social engineering and technical trickery.

Example: sending an email with a file attachment or a link to a fake website that loads malware onto a target's computer.

Spear Phishing Attack:

A very targeted type of phishing activity.

Attackers take the time to conduct research into targets and create messages that are personal and relevant.

Example: an attacker collects a target's details from social media and calls the target pretending to be a representative from the bank.

Structured Query Language (SQL) Injection:

SQL allows users to query databases.

SQL injection is the placement of malicious code in SQL queries, usually via web page input.

Example: in the UK, two teenagers managed to target TalkTalk's website in 2015 to steal hundreds of thousands of customer records from a database that was remotely accessible.

Malware:

A catch-all term for malicious software.

Any software designed to perform in a detrimental manner to a targeted user without the user's informed consent.

Example: ransomware, which holds a victim's files captive in exchange for a ransom payment.

Man in the Middle (MitM) Attack:

Occurs when hackers insert themselves in the communications between a client and a server.

Allows hackers to see what’s being sent and received by both sides.

Example: setting up a "free" WiFi hot spot in a popular public location.

Domain Name System (DNS) Attack:

DNS is one of the core protocols used on the internet.

Attack vectors directly target DNS, including DNS spoofing, domain hijacking, and cache poisoning.

Example: in 2016, the DNS service provided by a company called Dyn was attacked.

OFFENSE : Structure of a Cyber Attack

What is the Structure of a Cyber Attack?

Computer systems evolve over time, making it necessary for cyber attacks to adapt accordingly. While specific techniques may change, the overall structure of a cyber attack can be studied. This section aims to provide a basic understanding of this structure.

Lockheed Martin Cyber Kill Chain® framework

Developed by researchers at Lockheed Martin to examine the typical sequence of a cyber attack Consists of seven steps: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), Actions on Objectives Each step is dependent on the previous one's completion

Reconnaissance: Information gathering

Weaponization: Arming the deliverable payload

Delivery: Delivering the payload via email, web, USB, etc.

Exploitation: Exploiting a vulnerability to execute code on victim's system

Installation: Installing malware on the victim's system

Command & Control (C2): A command channel for remote manipulation of victim

Lockheed Martin Cyber Kill Chain® framework (cont)

Actions on Objectives: With 'Hand on Keyboard' access, intruders accomplish their original goal

Each step is dependent on the previous one's completion

MITRE ATT&CK matrix

# Developed by the American non-profit organization MITRE to collect and present a set of tactics, techniques, and procedures (TTP) used by cyber attackers

# Presented in a matrix to help organizations examine cyber attacks in a simplified form

# The matrix consists of a list of tactics and techniques used by cyber attackers

# The ATT&CK matrix is open and available to any person or organization for use at no charge

# https://attack.mitre.org/

MITRE ATT&CK Example

An attacker's objective may be to gain credentialed access to a system

If poor logging and no account lockouts are in use, the attacker may use the Brute Force technique, which involves trying millions of username and password combinations until a successful one is identified

If this technique fails, the attacker can switch to another approach and continue trying

Offense : Funding and profitability of cyber crime

OFFENSE : Funding and profitability of cyber crime

What are the drivers of cyber crime?

Activism	National Interest	Profitability

In this section we will understand the cyber crime ecosystem.

Marketplace:

# Thriving international marketplace made up of hundreds of forums, platforms, and systems

# Criminals buy and sell data, identities, and tools to make a profit

# Specialism drives efficiencies and allows criminals to focus on what they each do best

Initial Cash Injection:

# Stolen from victim: done through compromising banking systems or compromising accounts, most common manner is through fraud or deception

# Criminal for hire: offer services to carry out illegal tasks to regular people and organizations; gets paid by the organization or individual

# Extorted from victim: criminal gains the ability to disrupt a victim by disabling key systems or threatening to divulge sensitive data

Cryptocurrency:

# Rapid increase in cryptocurrencies, such as Bitcoin, proposed a new method for monetary exchange based on a shared ledger called a Blockchain

Cryptocurrency: (cont)

# Designed to be near impossible to regulate or block, making them unbelievably useful for money laundering or for other criminal marketplace activities

# Rapid growth of ransomware due to cryptocurrencies; easier for victims to make concealed payments

Ecosystem in Action

Step 1. Malware designed to record keystrokes and screen shots

Step 2. Criminals buy a list of known email addresses and send out malware as an email attachment

Step 3. Malware authors have a list of passwords and banking logins

Step 4. Criminal gang attempts to login and make transfers to money mules

Step 5. Money mules buy and transfer cryptocurrencies to accounts controlled by the gang

Step 6. Trail often ends with only the money mule being traceable

OFFENSE : Social Engineering

What is Social Engineering?

# Social Engineering is the art of making someone do what you want them to do.

# It involves psychology, biology, and mathematics.

# In cybersecurity, it's the use of deception to manipulate individuals into divulging confidential or personal information.

# Social engineering attacks are the dark art of using social interactions to trick someone into making a security mistake.

Examples of Social Engineering Tactics:

# Scams and confidence tricks that defraud vulnerable individuals of their savings.

# Tailgating, or closely following, individuals in order to gain access to secure areas.

# Persuading young adults to act as money launderers for gangs.

# Get-rich-quick schemes online.

# Within certain organizations, employees might skip a long business process like verifying caller identities or getting the right levels of approvals to grant access rights.

# Attackers use time restrictions, impersonate a trusted authority figure, or pretend to be a potential love interest.

Why Does Social Engineering Work?

# Humans are imperfect. Our decisions are irrational and flawed. Human decision making varies greatly throughout the day and depends on changing circumstances.

# Short term gratification or greed can be utilized to manipulate a target. Attackers benefit from affecting a target's decision--making process to achieve a result.

All these factors impact a target's ability to make a good decision or even identify they are being manipulated in the first place.

What Makes a Good Social Engineering Attack?

# It is well researched.

# It is delivered confidently.

# The attack feels plausible and realistic.

How Can You Defend Against Social Engineering?

# Be aware and guard against common social engineering attacks.

# If something seems too good to be true, it probably is.

# Don't be afraid to challenge others who make unusual requests or appear out of place.

# Verify unexpected emails or requests.

# Check the sender's email address.

# Be cautious of phishing emails.

OFFENSE : OSINT

What is Open Source Intelligence (OSINT)

# Intelligence operations using publicly available information

# All information that can be easily collected without active collection methods (hacking, wiretaps)

Benefits of OSINT

# Virtually free and considerably easy to acquire compared to traditional forms of information gathering

# Undetectable to the target

Sources of Open Information

1. Company website: can reveal helpful information, use "Google hacking" and Wayback Machine to find more advanced information

2. Media and news: good journalists are skilled at processing open information, may provide help for further investigations

3. Social media: people share information widely, even small pieces of information can add credibility to social engineering attacks

Sources of Open Information (cont)

4. Government or public records: many countries keep detailed records of both citizens and companies

Good rules for gathering open information

1. Get lots of information: quantity is valuable, analyst tools operate better with more information

2. Get a range: do not rely on a single source, not everything online is true

3. Be ethical: do not use illegal methods or violate privacy laws

4. Verify information: confirm information from multiple sources, use critical thinking and skepticism

5. Keep a low profile: avoid drawing attention to the investigation, take measures to maintain privacy and security.

OFFENSE : Technical Scanning

What is Technical Scanning?

They are techniques used by attackers to collect information about computers and networks during the reconnaissance stage of an attack.

Ping Test:

# Sends an Internet Control Message Protocol (ICMP) packet to target machine’s IP address.

# If target machine responds with an echo reply packet, scanning machine knows target machine is active and switched on.

# Provides a basic test to identify machine status and how far into network machine is located by using packet's "time to live" (TTL).

Ping Test: (cont)

# Can be used to tell attackers and defenders if machine is responsive and, when repeated in a sweep, how many devices are on a network.

# Can be started using the command ‘ping target_name’ on Windows machines.

Traceroute:

# Calculates traceroute between two computers by sending out packets with increasing or decreasing "times to live" (TTL).

# Used to map out network and determine how many switches and routers exist between you and your destination.

# A complete list of the network nodes between scanner and target can be produced.

# Can be started using the command ‘tracert target_name’ on Windows machines.

Port Scanning:

# Based on the idea of attempting to open a connection with a certain number of ports on target machine.

# Scans the most common 1,000 ports for a given protocol.

# Can work out what machine is being used for by working through the list of "well known" ports on target device.

# Can identify "open" and "closed" ports.

# Can be performed using Network Mapper (Nmap). It is a free and open-source network scanner.

Network Vulnerability Scanning:

# Certain actions are done to exploit vulnerability in real time to determine if it exists on target system (dynamic scanning).

# Version numbers of software are compared against a database to find vulnerabilities.

OFFENSE : Case Studies

Stuxnet

Advanced and targeted malware collection that targeted Iranian uranium processing

Used four previously unidentified vulnerabilities and a pair of compromised digital certificates

Spread through infected USB drives

The definitive example of a cyber weapon deployed for military and political objectives

Equifax

Large-scale data breach due to the organization's failure to apply a security patch

Attackers stole at least 147 million names and dates of birth, 145.5 million Social Security numbers, and 209,000 payment card numbers and expiration dates

Basic mistakes in the organization made the breach possible

Placed the idea of data breaches into US attention

National Security Agency

Malicious insider, Edward Snowden, released a significant amount of classified information

Leaked files included technical capability overviews, guidance on operations, and other highly sensitive material

National Security Agency (cont)

Several business arrangements between the NSA and US companies were brought under a high degree of scrutiny as a result

Considered the most damaging set of leaks the US had ever suffered

SolarWinds

Large-scale supply chain attack affecting thousands of organizations

Attacker compromised SolarWinds' update process, spreading malware to thousands of SolarWinds' customers

Highlighted how trusted relationships within supply chains can be used by attackers

Patches for software are still recommended as a routine step, despite supplier compromises.

DEFENSE : Financial Impacts

Financial Impact

# Average global total cost of a data breach is $4.35M

# Cost of data breaches has increased by 14.8% since 2015

# Lost business is the biggest contributor to these costs

# Regulatory fines and remediation costs may impact an organization

Hiscox Cyber Readiness Report 2021

# Proportion of firms reporting attacks is on the rise

# Hackers' favorite targets are TMT, financial services, and energy sectors

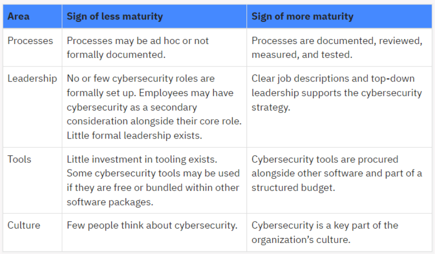
# Average firm devotes more than 21% of its IT budget to cybersecurity

# 16% of firms reporting cyber attacks had to deal with a ransomware demand

# Cyber attacks are an unavoidable cost of doing business today

DEFENSE : Security Strategy

Metrics to Assess Security Maturity



Area	Sign of less maturity	Sign of more maturity
Processes	Processes may be ad hoc or not formally documented.	Processes are documented, reviewed, measured, and tested.
Leadership	No or few cybersecurity roles are formally set up. Employees may have cybersecurity as a secondary consideration alongside their core role. Little formal leadership exists.	Clear job descriptions and top-down leadership supports the cybersecurity strategy.
Tools	Little investment in tooling exists. Some cybersecurity tools may be used if they are free or bundled within other software packages.	Cybersecurity tools are procured alongside other software and part of a structured budget.
Culture	Few people think about cybersecurity.	Cybersecurity is a key part of the organization's culture.

Cybersecurity maturity is a scale, and an organization may show development in one area while not being mature in another area.

Security Maturity Levels (PRISMA)

Level 1: Policies - Documented policies exist and are readily available. Policies establish a cycle of assessing risk, implementing security controls, and monitoring effectiveness.

Level 2: Procedures - Formal, documented procedures exist to implement security controls. Procedures define IT security responsibilities and expected behaviors, and document implementation and rigor.

Level 3: Implementation - Procedures are communicated to individuals who need to follow them, and security controls are implemented consistently and reinforced through training.

Level 4: Test - Tests are routinely conducted to evaluate the adequacy and effectiveness of security controls, and corrective actions are taken to address weaknesses. Information from potential and actual security incidents is used as test results.

Level 5: Integration - IT security is fully integrated into the culture and decision--making processes. A comprehensive IT security program is in place, and costs and benefits are measured precisely. Threats are continually reevaluated, and controls are adapted as needed.

10 Steps to Cyber Security offered by NISC UK

1. Risk management

2. Engagement and training

3. Asset management

4. Architecture and configuration

5. Vulnerability management

6. Identity and access management

7. Data security

8. Logging and monitoring

10 Steps to Cyber Security offered by NISC UK (cont)

9. Incident management

10. Supply chain security

Marketplace for the security industry

# Large organizations typically have products from various cybersecurity vendors.

# These cybersecurity vendors contribute to a vibrant ecosystem supported by various standard authorities, charities, and government entities.

DEFENSE : Protection

Goal of Cybersecurity

Goal: Aim to make cyber attacks frustratingly difficult. The emphasis is on reducing operational risk to an acceptable level.

Preventive Strategy 1 - Perimeter Security

Attack surface: the sum total of an organization's infrastructure and software environment that is exposed where an attacker could choose to attack.

Protecting the attack surface: keeping the attack surface as small as possible by limiting which services are externally accessible and what devices can be connected.

Perimeter: a defined boundary that neatly separated an organization's assets from the outside world.

Preventive Strategy 2 - Network Segregation

Demilitarized zone (DMZ) : a middle ground area on the network which is partly controlled and managed, used to refer to servers that may be used by both internal and external applications.

An attacker who compromises a server in the DMZ would need a second successful attack to move further into the organization.

Preventive Strategy 3 - Least Privilege

Granting the fewest permissions to enable a role to be completed, which means that the consequences of a successful attack are reduced when compared to a less restricted system.

Preventive Strategy 4 - Patch Management

Patch management: the process of updating software to reduce the risk of them being successfully attacked.

Vulnerability management: the process of identifying flaws within software.

Vulnerability scanner: a piece of software that assesses if there are any vulnerabilities within a server or application.

Compensating controls: a temporary solution if a vulnerability is identified for which a patch is not available.

Layered Cybersecurity

It means applying multiple forms of defense to an organization's infrastructure and software environment

Layered Cybersecurity (cont)

It is inspired by the military concept of defense in depth where a successful attack would have to bypass or circumvent all layers of defense, which is difficult to achieve

Defense in depth includes network defenses, device defenses, and data controls like encryption

Example of Layers of Security : Perimeter -> Network -> Host -> Application -> Data

DEFENSE : Detection

When is Detection necessary

Should an organization's defenses fail to successfully prevent a cyber attack, an organization's next priority is to detect the cyber attack. This is ideally done while the attack is in progress or in the best situation, when the breach has yet to occur at all.

Logging

Logging is the process where actions are accurately recorded in a secure location, acting as a permanent record of what has occurred within a network.

Log records should be tamper-proof and can be done on individual machines or applications.

Organizations can use a larger collection of logs to track the activities of both legitimate users and attackers.

Network Monitoring

Traffic analysis is an approach where organizations can monitor communications across their network to identify what is being done on a network, even in a passive fashion while encryption is being used.

Security information and event management (SIEM)

SIEM tools collect all the information throughout the organization's technology infrastructures and aggregate it, helping cybersecurity teams to identify events and patterns of potential attacks and analyze them.

Security operations center (SOC)

SOC is responsible for detecting attacks in progress using SIEMs and other monitoring tools, and security analysts make up the team of people responsible for assessing an organization's security in the SOC.

False alarms

False positives can occur when an alert is triggered, and the action is legitimate. Confirming if an alert is a false positive is the responsibility of a security analyst.

A balance needs to be established in adjusting the sensitivity of certain thresholds within a SOC.

Activity

An unusually high amount of activity in logging can indicate unknown or unauthorized activity.

DEFENSE : Response

Six phases of incident management

1. Preparation	2. Identification	3. Containment
4. Eradication	5. Recovery	6. Reflection

Types of tests to assess level of preparation

Paper--based Tests:	Table-top Exercises:	Live Tests:
Survey and prep	Small response exercise	Live failure and response exercise

Key terms to know

Business continuity: the ability to continue operating despite an incident

Disaster recovery: the ability to recover from a disaster

Benefit of incident response teams

Organizations with incident response capabilities saw an average cost of a breach of USD 3.26 million in 2022, compared to USD 5.92 million at organizations without incident response capabilities. This is a cost difference of USD 2.66 million, or 58%.

DEFENSE : Cryptography

What is Cryptography?

It is the art of writing and solving codes and keeping the information confidential

Secure Communications

Confidentiality: Message is private and cannot be understood by an eavesdropper.

Authenticity: Spoofing or impersonation is impossible.

Integrity: Tampering with a message can be identified by the receiver.

Encryption and its Types

Encryption converts a message into an unreadable state that can only be understood by those with a decryption key.

Two forms of encryption: Symmetric and Asymmetric.

Symmetric encryption:

Uses the same key for encryption and decryption.

Rely on both the sender and receiver having access to the same key.

Example: Rotation-based cipher like Advanced Encryption Standard (AES).

Asymmetric encryption:

Uses different keys for encryption and decryption: public and private keys.

Anyone can use the public key to encrypt a message, which can only be decrypted using the holder's private key.

Beneficial for communicating securely with unknown entities.

Example: Online shopping where an in-person meeting to create a shared, unique, symmetric key is not required.

DEFENSE : Threat Intelligence

What is Threat Intelligence?

# Intelligence has historically been used in military operations as a force multiplier, allowing commanders to use resources for their greatest impact.

What is Threat Intelligence? (cont)

# Threat Intelligence is data collected and analyzed by organizations to understand the motives and behavior of cyber attackers, focusing on attacker tactics, techniques, and procedures (TTPs) or other indicators of compromise (IOCs).

# Tactics are the "why," techniques are the “how,” and procedures are the specific implementation that the adversary uses for techniques. Indicators of compromise (IOCs) are signatures related to attacker activity.

# Organizations can benefit from threat intelligence in providing a warning, indicators of compromise, context, and learning from peers.

# Sources of threat intelligence include threat exchange platforms, conferences, articles, and news, and product vendors.

# Job roles within the world of cyber threat intelligence can be divided into two areas: production and interpretation. Production involves the collection and enrichment of information, while interpretation involves analyzing the findings and deciding the best course of action to recommend.

Key Takeaway : The use of threat intelligence enables organizations to design defenses tailored to the specific attacks they may face, rather than relying on industry or regulatory standards. This is especially beneficial for organizations that operate in complex or anomalous ways where regulations may not provide adequate guidance.