PII
Pakistan Insurance Institute
Since 1951

CYBER INSURANCE

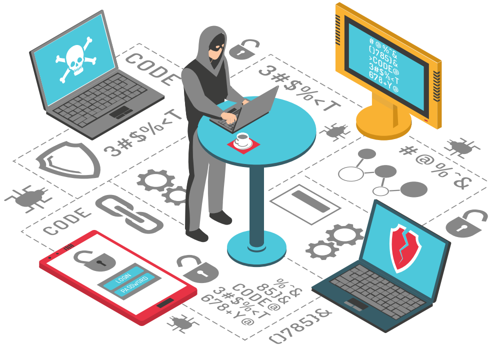
Farrukh Khan
MBA (Finance), PGD (Insurance)
Cert. CII (UK)

“There are only two types of companies: those that have been hacked and those that will be.”

Robert Mueller

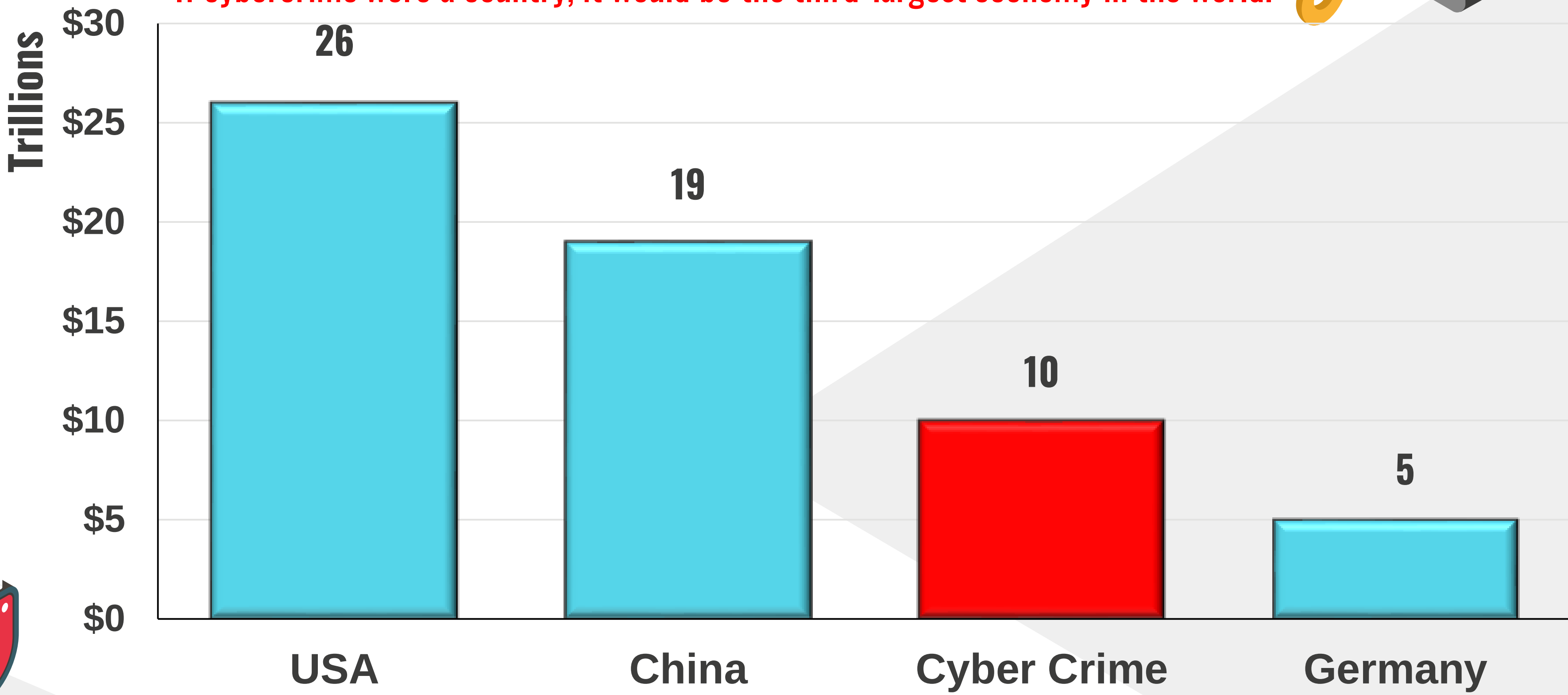
FBI Director, 2012

"By 2025, cybercrime will cost the world **$10 trillion annually**—more than all natural disasters combined."



Top Economies by 2025

"If cybercrime were a country, it would be the third-largest economy in the world."



Learning Objectives

What is Cyber Insurance?

How is Cyber Insurance different from Traditional Insurance?

Types of Cyber Events, Attacks & Threats?

Coverage under Cyber Insurance?

Exclusions under Cyber Insurance?

Analyzing IT Security & Assessing its Vulnerabilities while offering Cyber Insurance

Quick Exercise To Test our Learnings

Cyber Insurance Claims Allocation by Industry

Cyber Breach Incidents

1.

What is Cyber Insurance?

Cyber Insurance?

Specialized type of insurance designed to protect businesses and individuals from financial losses caused by CYBER EVENT/THREAT, such as:

- Data Breaches
- Ransomware Attacks
- System Failures

It typically covers costs related to data recovery, legal expenses, regulatory fines, business interruption, and reputational damage.

2.

How is Cyber Insurance different from Traditional Insurance?

PII
Pakistan Insurance Institute
Since 1951

Cyber Insurance v/s Traditional Insurance

ASPECT	Cyber Insurance	Traditional Insurance
Risk Type	Digital risks (cyberattacks, data breaches)	Physical risks (fire, theft, accidents)
Assets Covered	Intangible (data, IT systems, reputation)	Tangible (buildings, vehicles, equipment)
First-Party Losses	Data recovery, business interruption, ransomware payments	Property damage, medical bills
Third-Party Liabilities	Legal claims for leaked customer data	Lawsuits for physical injuries or damage
Risk Nature	Dynamic, ever-changing cyber threats	Stable and predictable risks
Regulatory Impact	Covers fines and legal costs	Covers legal claims unrelated to cyber laws
Incident Response	Includes cybersecurity audits, forensic teams	Typically no active risk prevention
Business Impact	Ensures business continuity (post-cyberattack)	Restores physical assets after damage

3.

Types of Cyber Events, Attacks & Threats?

TYPES OF CYBER ATTACKS

Pakistan Insurance Institute
Since 1951

PHISHING ATTACK

Deceptive email messages or websites to obtain sensitive information

MAN IN THE MIDDLE

Intercepting and manipulating communication between two parties without their knowledge

DENIAL-OF-SERVICE (DOS)

Overloading a system or network to disrupt normal functioning

MALWARE/ RANSOMWARE

Software designed to encrypt files and demand payment for their release

TYPES OF CYBER ATTACKS – Contd.

STRUCTURED QUERY LANGUAGE (SQL) INJECTION

Exploiting vulnerabilities in database queries to gain unauthorized access

ZERO DAY EXPLOITS

Attackers exploiting unknown vulnerabilities before developers can address them

CROSS SITE SCRIPTING (XSS)

Injecting malicious scripts into websites viewed by other users

DNS SPOOFING

Redirecting DNS queries to malicious sites for unauthorized access

TYPES OF CYBER ATTACKS – Contd.

CREDENTIAL STUFFING

Using stolen usernames and passwords from one breach to access accounts on multiple platforms (due to password reuse).

INSIDER THREATS

Employees or insiders misuse their access to steal data, sabotage systems, or assist cybercriminals

ADVANCED PERSISTENT THREATS

Long-term cyberattacks where hackers infiltrate networks undetected, often for espionage or large-scale data theft.

BUSINESS EMAIL COMPROMISE

Attackers impersonate executives or trusted partners to trick employees into transferring money or sharing sensitive data.

4.

Coverage under Cyber Insurance?

Cyber Insurance Coverage Events & Costs

CYBER EVENTS	First Party	Third Party Liability
Data Breach	• Emergency Response Costs • Event Management Costs • Notification Costs • Monitoring Costs • Recovery Costs • Bricking Costs	• Damages • Regulatory Fines and Penalties • Defence Costs • Investigation Costs
Cyber Attack	• Emergency Response Costs • Event Management Costs • Recovery Costs • Bricking Costs	• Damages • Defence Costs • Investigation Costs
Human Error	• Emergency Response Costs • Event Management Costs • Recovery Costs	• Damages • Defence Costs • Investigation Costs

Cyber Insurance Coverage Events & Costs

CYBER EVENTS	First Party	Third Party Liability
Insured's or Outsourced Systems Disruption	- Direct Business Interruption (ISD) - Contingent Business Interruption (OSD)	- Not Applicable
Electronic Media Claim	- Emergency Response Costs - Event Management Costs	- Damages - Defence Costs
E-Threat	- E-threat Response Costs	- Damages - Defence Costs

Cyber Events – Explained

1 DATA BREACH

Confidential, Sensitive, or Protected Information is Accessed, Stolen, Exposed, or used by Unauthorized Individuals

2 CYBER ATTACK

Deliberate Attempt by Hackers or Malicious Actors to Gain Unauthorized Access to, Damage, Or Disrupt Computer Systems, Networks, Or Data

3 HUMAN ERROR

Negligent Acts or Errors in the Active Maintenance, Operation, Programming or Update of Insured's Systems

4 SYSTEM'S DISRUPTION

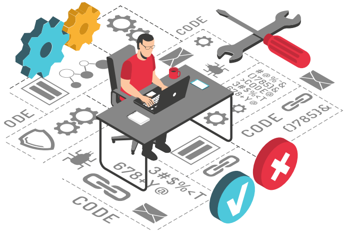
Unavoidable Interruption Unavailability or Disruption of the Insured's Systems as a result of Cyber Attack or Human Error

5 ELECTRONIC MEDIA CLAIM

Libel, Slander or Reputational Damage including Breach of Unlawful Disclosure of Personal or Confidential Information through Online Platforms following Cyber Attack or Data Breach

6 E-THREAT

Verifiable Threat Including Ransomware to cause or have caused the Cyber Attack or Data Breach



First Party Costs – Explained

Emergency Response Costs

Cost of Legal, IT & PR Response Team incurred within 72 hours from Reporting of a Cyber Event

Monitoring Costs

Cost of Professional Credit and Identity Theft Monitoring Services

Business Interruption

Losses suffered & costs incurred as a result of Insured's System Disruption or an Outsourced Systems Disruption

Event Management Costs

Cost of Forensic, Legal & PR Response Team incurred after Reporting of a Cyber Event

Recovery Costs

Cost of IT Response Team in restoring or recollecting any part or contents of the Insured's Systems impaired, lost or destroyed to its original state

E-Threat Response Costs

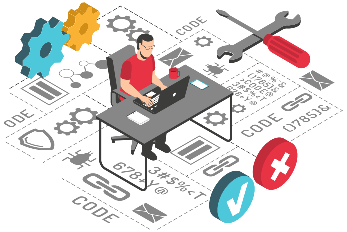
Cost of Investigation, Resolution or Mitigation of Cyber Event including Legal, IT and PR Response Team including payment to E-Threat Perpetrator

Notification Costs

Cost legally necessitating notification to victims of Data Breach and/or competent regulatory body

Bricking Costs

Repurchasing cost of any part or contents of Insured's Systems impaired, lost or destroyed where it is technically impossible to restore it or more cost effective than actual restoration



Liability Costs – Explained

Damages

Amount of Final Judgements, Arbitral Awards and Compensation which the Insured is Legally Obliged to Pay

Regulatory Fines & Penalties

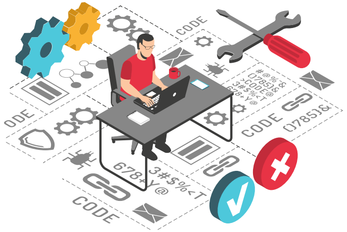
Civil or Administrative Fines & Penalties Awarded by Regulatory Body

Investigation Costs

Professional Legal Cost in Response to an Investigation

Defence Costs

Professional Legal Cost to Defend, Investigate and Settle Claim

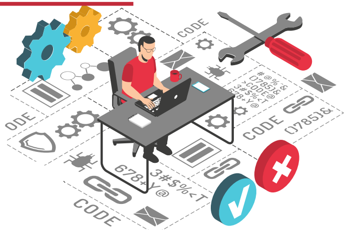


5.

Exclusions under Cyber Insurance?

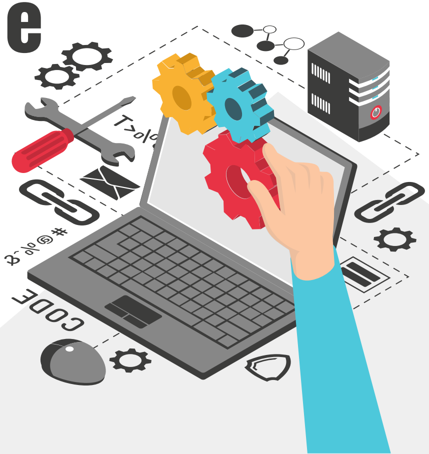
GENERAL EXCLUSIONS

- Bodily Injury & Property Damage
- Fraudulent & Malicious Acts
- Government Mandated Shutdowns
- Physical Event
- Theft of Funds
- War or Cyber Operations
- Betterment Costs
- Infrastructure Failure
- Undersize Security (CVSS)
- Criminal Reward Fund
- Loss Prevention Services

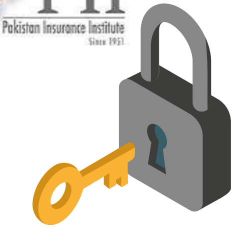


6.

Analyzing IT Security in Place & Assessing its Vulnerabilities while offering Cyber Insurance



MINIMUM CONTROL REQUIREMENTS



1. **Multifactor Authentication (MFA)** for all email, privileged accounts, and remote connections (including vendor access and remote desktop protocol) – **high priority item**.

2. An Endpoint Detection and Response Solution rolled out across the IT environment / simple EDR solution / managed EDR solution in place

3. Secure offline backups which are tested for integrity, subject to MFA / encryption / segmentation / Privileged Access Management (PAM) etc.

4. Incident Response Plan specific to cyber incidents which is updated and tested periodically

5. Business Continuity Plan and Disaster Recovery Plan addressing network outages, off-line communications and data recovery protocols, tested periodically

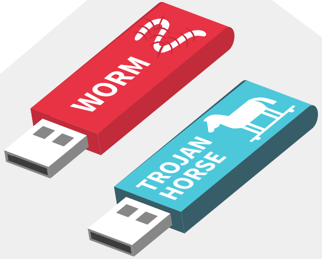
6. Updated software and patching protocols (i.e. critical patches to be carried out immediately or within 2-3 days of their release, subject to testing) - **CVSS**

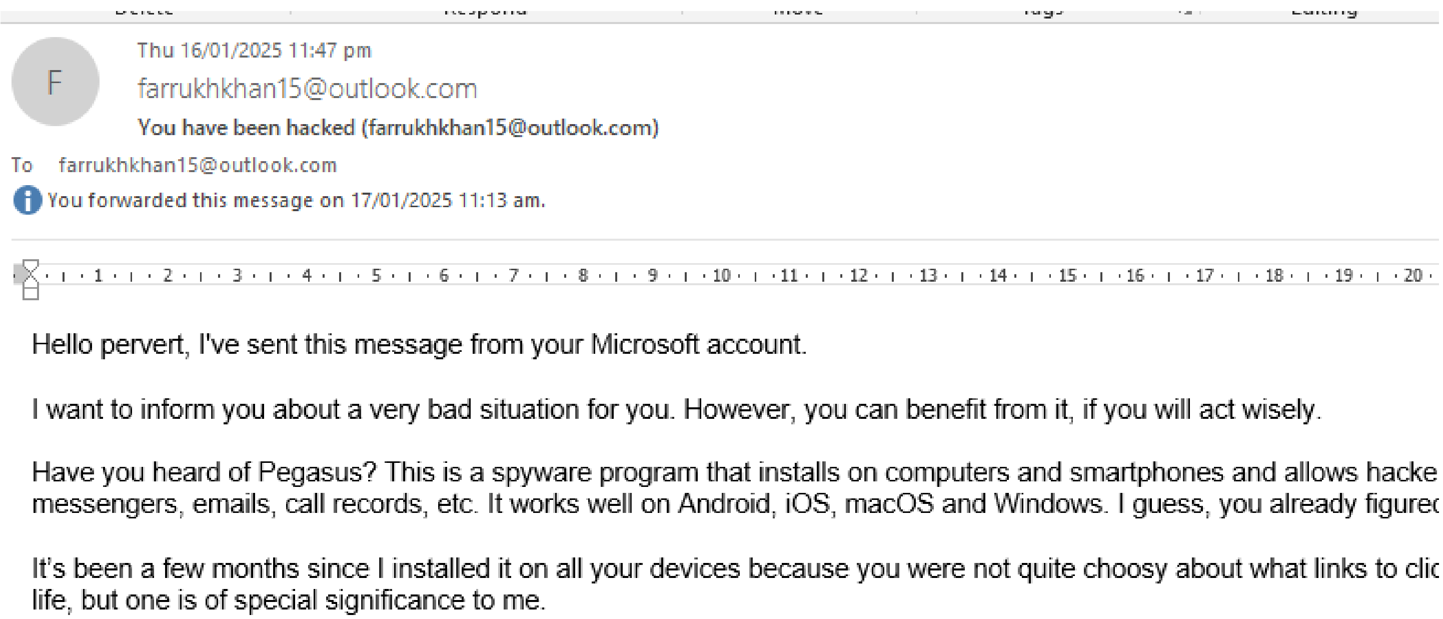
7. Privileged Access Controls / Privileged Access Management Solution

8. Periodic Employee Awareness training involving phishing campaigns

9. Annual vulnerability assessments

10. **Network Segmentation**





Thu 16/01/2025 11:47 pm

farrukhkhan15@outlook.com

You have been hacked (farrukhkhan15@outlook.com)

To farrukhkhan15@outlook.com

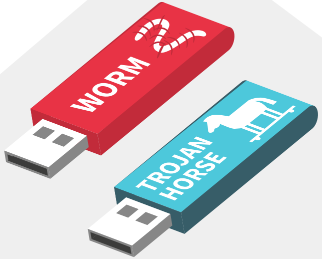
You forwarded this message on 17/01/2025 11:13 am.

Hello pervert, I've sent this message from your Microsoft account.

I want to inform you about a very bad situation for you. However, you can benefit from it, if you will act wisely.

Have you heard of Pegasus? This is a spyware program that installs on computers and smartphones and allows hacke messengers, emails, call records, etc. It works well on Android, iOS, macOS and Windows. I guess, you already figurec

It's been a few months since I installed it on all your devices because you were not quite choosy about what links to clic life, but one is of special significance to me.



What is Multi Factor Authentication (MFA)?

Imagine your house has a **lock** on the front door. If someone **steals your key**, they can easily enter.

Now, what if you also had a fingerprint scanner? Even with the stolen key, they **still** couldn't get in!

That's exactly how **Multi-Factor Authentication (MFA)** works—it adds an **extra layer of security** beyond just a password.

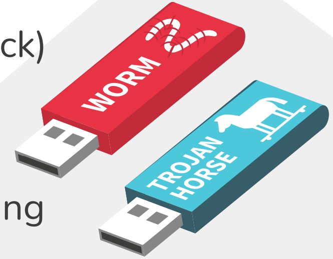
How MFA Works (In Everyday Terms)

To access an account, you need **two or more** of these factors:

- **Something You Know** → Password or PIN (like your house key)
- **Something You Have** → Phone, security token, or card (like an access badge)
- **Something You Are** → Fingerprint, face scan, or voice recognition (like a biometric lock)

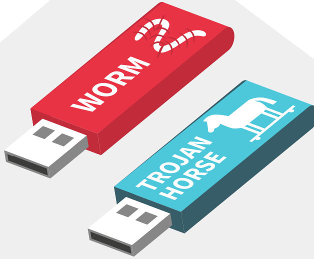
Why is MFA Important?

- **Without MFA:** If a hacker steals your password, they can access your account.
- **With MFA:** Even if they have your password, they **still need the second factor**, making it **much harder** to break in.



Example Scenario of MFA

- Hackers **steals your password** through phishing or a data breach.
- They **try to log in** to your bank account.
- The system **prompts for an extra security step** (e.g., a **one-time code** sent to your phone).
- The hacker **doesn't have your phone**, so they **can't enter the code**.
- **Access is denied** to the hacker!
- You **receive an alert** about an unauthorized login attempt.
- **Your account stays safe because of MFA!** ✓



What is Common Vulnerability Scoring System (CVSS)?

Imagine you live in a neighborhood, and you want to assess how dangerous different threats are—like burglars, storms, or gas leaks. **CVSS is like a risk rating system for cybersecurity threats**, helping companies decide which issues need urgent attention.

How CVSS Works (In Everyday Terms)

CVSS scores range from **0 to 10**, just like a **danger meter**:

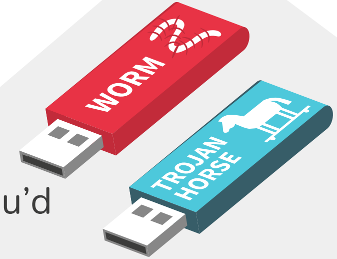
- **0.0 (No Risk):** Like a harmless prank—no real danger.
- **1.0 - 3.9 (Low):** A small crack in your window—not ideal, but not urgent.
- **4.0 - 6.9 (Medium):** A weak lock on your front door—could be a problem if ignored.
- **7.0 - 8.9 (High):** A door left wide open at night—risky and needs fixing soon.
- **9.0 - 10.0 (Critical):** A gas leak in your house—**drop everything and fix it immediately!**

Why Does CVSS Matter?

IT teams use CVSS to **prioritize security fixes** just like you prioritize home repairs.

- A **CVSS 9.8 vulnerability** means hackers can break in **easily**—so fixing it ASAP is crucial.
- A **CVSS 4.5 issue** might not be an emergency, but it's worth keeping an eye on.

In short, **CVSS helps organizations focus on the biggest cyber threats first**, just like you'd fix a gas leak before worrying about a loose fence!



Example Scenario of CVSS

A Company Discovers a Software Vulnerability

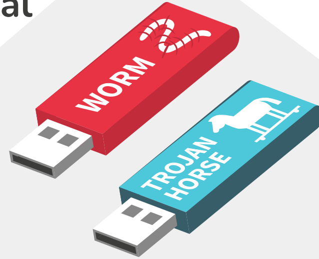
A security researcher finds a **bug in a company’s web application** that allows hackers to steal customer data. The IT team uses **CVSS to assess the severity** of this vulnerability.

<u>Breaking it Down Using CVSS Metrics:</u>

- Attack Vector - Can be exploited **remotely** over the internet
- Attack Complexity - Easy to exploit, requiring no special conditions
- Privileges Required - No login required—**anyone can attack**
- User Interaction - No user action needed—attacks happen automatically
- Impact on Data - Exposes **sensitive customer information**

Based on these factors, the CVSS system **calculates a score** e.g., **9.1/10**, which is **Critical**

- The IT team **prioritizes fixing this issue immediately** before hackers exploit it.
- A **patch is released**, and customers are advised to update their software.



What is Network Segmentation?

Imagine you live in a **huge apartment building**. If **everyone had access to every room**, a thief could easily move from one apartment to another, stealing from multiple places without restriction.

Now, what if:

- Each **floor had locked doors** so only residents of that floor could enter?
- The **main vault** was in a special, **high-security area** with extra protections?

This is exactly how **Network Segmentation** works in cybersecurity! Instead of having **one big open network**, we **divide it into smaller, secured sections** to prevent cyber threats from spreading.

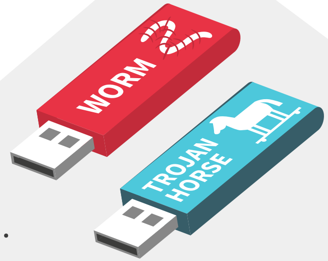
How Network Segmentation Works (Real-Life Comparisons)

Flat Network (No Segmentation) → Like an Open Mall

- A hacker who enters can **move freely** and attack any system.

Segmented Network → Like a Secure Office Building

- Different floors (departments) have **controlled access**.
- Even if a hacker gets in, they are **trapped in one section** and **can't access everything**.



Example Scenario of Network Segmentation

A **hospital** has a large network that connects:

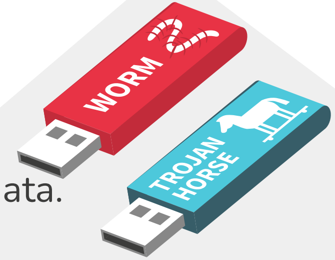
- **Patient records & billing systems** 📄
- **Medical devices (MRI, ventilators, etc.)** ⛨
- **Public Wi-Fi for visitors** 📶

What Happens If There's No Network Segmentation?

- A **hacker gains access** through the **public Wi-Fi** by exploiting weak security.
- Since there's **no separation** between networks, the hacker moves to **medical devices** and patient records.
- They **steal sensitive data** and could **disrupt life-saving equipment**!

What Happens WITH Network Segmentation?

- The hospital **divides** its network into **separate zones**:
  - **Public Wi-Fi** (Isolated from other networks)
  - **Medical Devices** (Highly secured, restricted access)
  - **Patient Records & Billing** (Accessible only by authorized staff)
- A hacker **gets into public Wi-Fi** but **CANNOT access** medical devices or patient data.
- The **attack is contained**, and security teams **detect & block** the threat.
- **Patient safety and critical data remain protected!**



What is Endpoint Detection & Response Solution (EDR)?

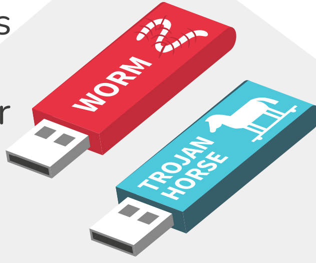
Imagine your home has **multiple entry points**—doors, windows, and even a garage.
If a burglar tries to break in, wouldn't you want an **intelligent security system** that:

- **Monitors every entry point** in real-time
- **Detects suspicious activity** (like forced entry)
- **Sounds an alarm** and **alerts security** if something is wrong
- **Records evidence** of the break-in for further investigation

That's exactly what **Endpoint Detection and Response (EDR) solutions** do—but for **computers, laptops, and servers** instead of houses!

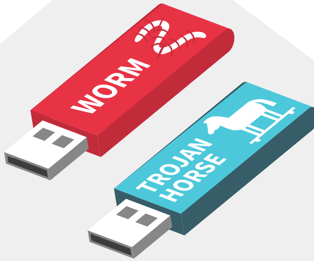
<u>How EDR Works (Real-Life Comparison)</u>

- **Continuous Monitoring** → Like **security cameras** watching 24/7 for unusual behavior
- **Real-Time Threat Detection** → Like an **alarm system** that alerts security if a break-in is attempted
- **Automatic Response & Containment** → Like **locking down an area** to stop the intruder from moving further
- **Investigation & Reporting** → Like **collecting CCTV footage** to analyze what happened and prevent future attacks



Example Scenario of EDR

- An employee **accidentally downloads malware** on their laptop.
- The EDR system **detects** unusual activity, like data being stolen.
- EDR **isolates** the laptop from the network to stop the attack.
- IT teams use **EDR reports** to analyze and improve security.



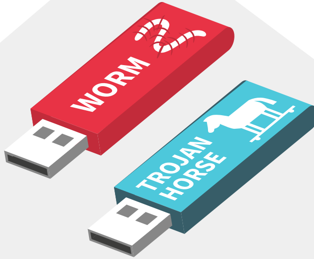
What is Incident Response Plan?

Imagine a **fire drill** in a building. Everyone knows **what to do**, where the **emergency exits** are, and who is in charge.

An **Incident Response Plan (IRP)** works the same way—but for **cybersecurity incidents** instead of fires!

An **IRP is a structured plan** that helps organizations **detect, respond to, and recover from cyber incidents** (like hacking, malware, or data breaches).

It ensures **quick action** to **minimize damage** and **restore normal operations**.



Example Scenario of Incident Response Plan

A company's IT team receives **an alert** that ransomware has locked employees' computers.

Step 1: Preparation ▯

- The IT team has **trained staff** and **security tools** in place before an attack happens.

Step 2: Detection & Analysis 🔍

- Security software **detects the ransomware**, and IT confirms **which systems are affected**.

Step 3: Containment 🛑

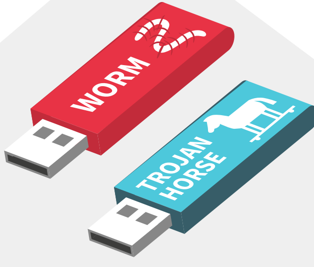
- The **infected computers** are **disconnected from the network** to stop the ransomware from spreading.

Step 4: Eradication & Recovery 🔄

- IT **removes the malware**, restores data from **backups**, and strengthens security.

Step 5: Lessons Learned 📝

- The company **reviews** what went wrong, **updates security** policies, and **improves training** to prevent future attacks.



7.

Quick Exercise To Test our Learnings

The Unbreakable Password?

🔐 **Question:**
A hacker wants to break into an insurance company's database. They try the following passwords:

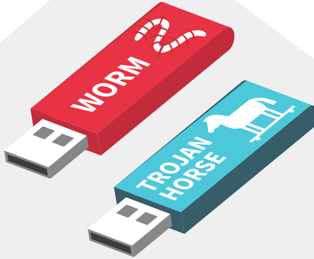
A. **"Insurance123“**
B. **"P@ssw0rd“**
C. **"ZxQ!7pL$9vT"**

How is the Access Best Protected!!?

❗ Answer: None of them!

➡□ Even complex passwords can be hacked if **password reuse** or **social engineering** is involved.

The best approach? **Multi-Factor Authentication (MFA).**



Spot the Weakest Link?

🔗 **Question:**

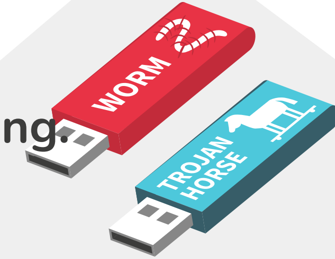
A company invests millions in cybersecurity, firewalls, and encrypted backups. Despite this, hackers breach their system in minutes.

How?

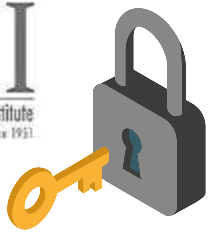
💡 **Answer: The Human Factor!**

➡□ A single **employee clicking on a phishing email** or **using a weak password** can bypass even the best security measures.

Cybersecurity isn't just about tech—it's about **awareness and training.**



The "CEO’s" Urgent Request?



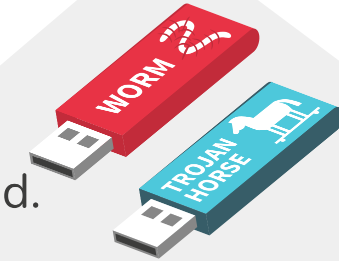
Your company’s CEO sends a **WhatsApp message**:
"Hey, I’m in a meeting. Can you urgently transfer PKR 50,000 to xxx Account?"

💡 **Options:**
A) Do it—it’s your boss!
B) Call the CEO directly to verify.
C) Reply asking for more details.

💡 **Answer: B – Call to verify!**

→□ This is a **social engineering scam** called **"Executive Impersonation."**

Always confirm unusual financial requests through a trusted method.



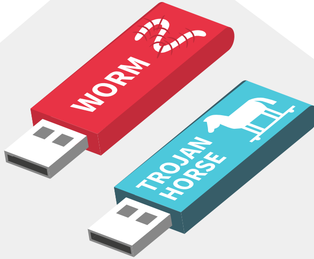
The Impossible Login?

▯ **Scenario:**
You receive a security alert: **“Your account was accessed from another country at 3 AM.”** You’re certain you didn’t log in. What’s your next move?

💡 **Options:**
A) Ignore it—maybe it’s a glitch.
B) Change your password immediately.
C) Report it and enable Multi-Factor Authentication (MFA).

💡 **Answer: C – Report it & enable MFA!**

➡▯ This could be a **credential stuffing attack**, where hackers use leaked passwords to access multiple accounts.



The Secure Password Paradox?

🔐 Scenario:

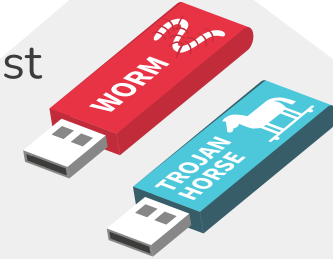
A cybersecurity expert gives the following password advice:

- It must be **long** (at least 12 characters).
- It must be **complex** (uppercase, lowercase, numbers, symbols).
- You must **never reuse** passwords.
- You must **memorize them all** without writing them down.

Question: *What’s wrong with this advice?*

💡 Answer: It’s unrealistic!

➡□ Humans can’t remember dozens of complex passwords. The best solution is to **use a password manager** and enable **Multi-Factor Authentication (MFA)** instead of relying on memory.



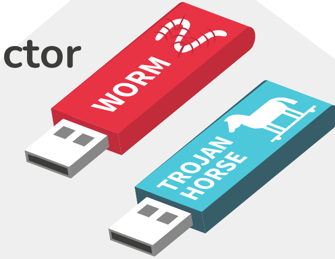
The Cyber Insurance Loophole?

📜 **Scenario:**
A company purchases **cyber insurance** to cover potential **ransomware attacks.** A year later, they suffer a ransomware attack and demand a **$5M payout.** The insurer **denies** the claim.

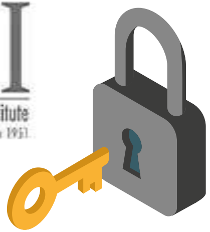
💡 **Question:** *Why did the insurer refuse to pay?*

💡 **Answer: Failure to follow cybersecurity best practices!**

➡️ Many cyber insurance policies require companies to implement **multi-factor authentication (MFA), regular security training, and strong endpoint protection.** If they don't, the insurer **can deny the claim.**



The Free USB Drive ?

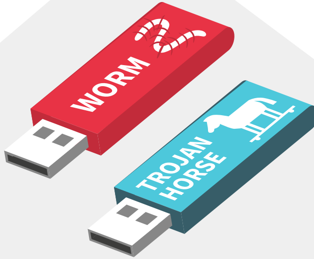


💾 Scenario:
You find a **USB flash drive** labeled "Confidential Insurance Data" in your office parking lot. You're curious and want to know what's inside.

💡 Question: *What's the safest action?*

💡 Answer: Do NOT plug it in!

➡□ Hackers use **"USB Drop Attacks"** to plant malware on company networks.
➡□ **Instead, give it to IT Security** for safe examination.



The Malvertising Trap?

🌐 **Scenario:**

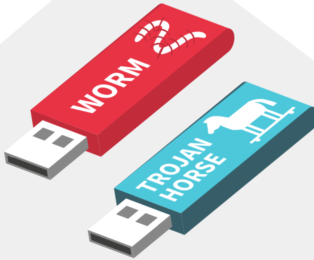
A CFO at an insurance firm searches for **"QuickBooks support"** on Google and clicks the **top ad result.** The site looks exactly like QuickBooks, but the next day, their system is infected with malware.

💡 **Question:** *What happened?*

💡 **Answer: It was a Malvertising Attack!**

➡️ Hackers **buy Google Ads to place fake websites at the top of search results.** Clicking these ads can **download malware or steal login credentials.**

✓ **Always type in official URLs instead of clicking ads.**



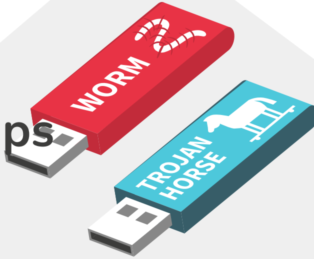
The "Infinite Loop" Ransomware Trick?

🔄 **Scenario:**
A company suffering from a **ransomware attack** refuses to pay the ransom. Instead, they **restore their systems from backups.** But hours later, **they are locked out again**, and the attackers demand even more money.

💡 **Question:** *Why didn't the backup save them?*

💡 **Answer: The ransomware was already hiding inside the backups!**

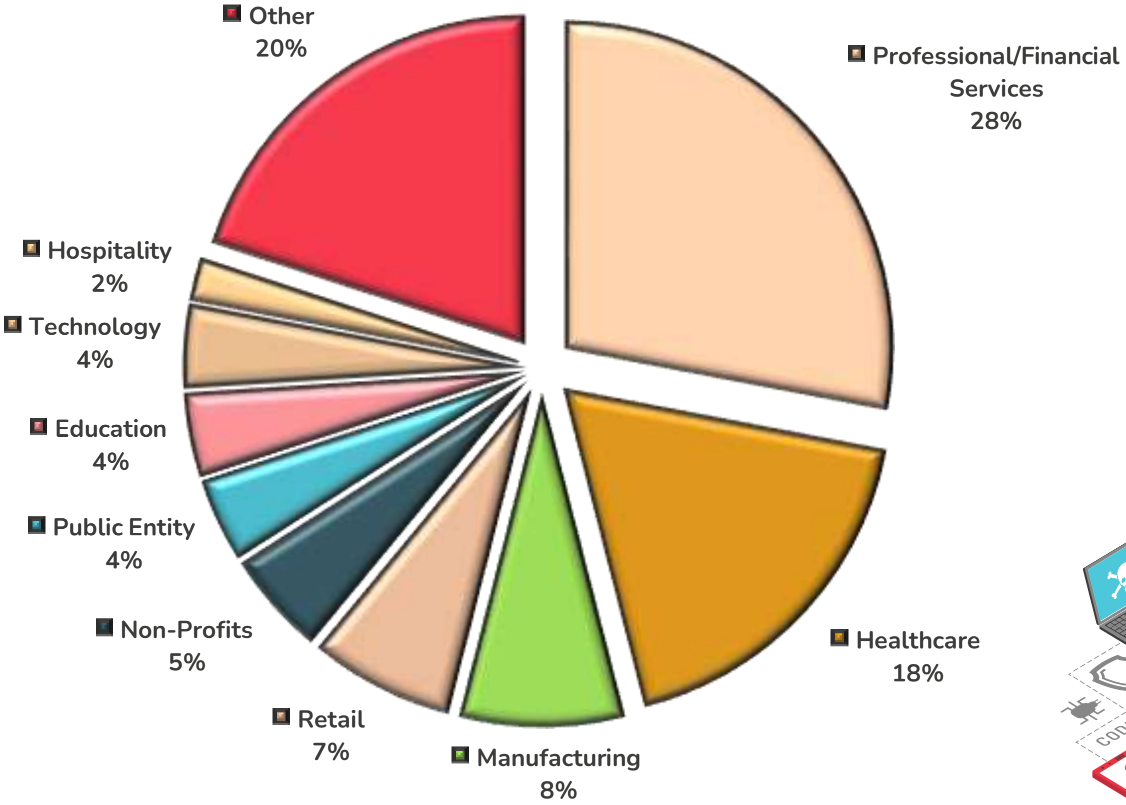
➡▯ Modern ransomware **lies dormant for weeks before activation, infecting backups along with live systems.**
✅ **Use immutable backups (that can't be changed) and scan backups for dormant malware.**



8.

Cyber Insurance Claims Allocation by Industry

Cyber Insurance Claims Allocation By Industry



9.

Cyber Breach Incidents

Cyber Breach Incidents in Pakistan

MEEZAN BANK

February 2019 - Database of bank cards was put for sale on the dark web.

BANK ISLAMI LIMITED

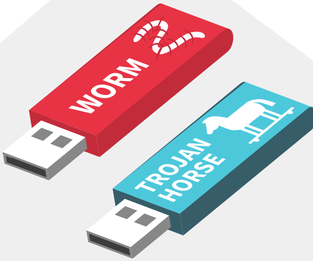
November 2018 - Data of almost all Pakistani banks was breached, affecting nearly 20,000 debit card banking customers

HABIB BANK LIMITED

2017 - 559 accounts of Habib Bank Limited were hacked through ATM cards in China. Reportedly the ATM installed at Khayaban-e-Ittehad (Karachi) has been cited as the target of the attack

FEDERAL BOARD OF REVENUE

August 2021 - Pakistan’s largest data center run by the FBR hacked bringing down all the official websites operated by the tax machinery for 72 hours.



Cyber Breach Incidents in Pakistan

K-Electric

August 2020 - Netwalker ransomware gang disrupted billing and online services

Careem

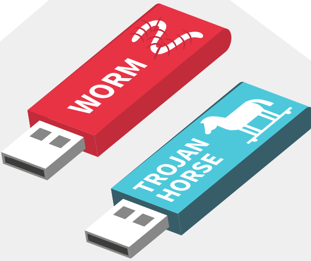
January 2018 - Major data leak following a cyber-incident involving unauthorized access of more than 14 million customers

Bykea

June 11, 2023 – Ride Hailing App Access Hacked. An inappropriate flash message was sent to all users (Reputational Loss of Income)

NIFT (Clearing Services)

June 16, 2023 – Attempted breach on NIFT’s systems (Website / Domain Servers remained down for a number of days)



Cyber Breach Incidents Globally

RESERVE BANK OF NEWZEALAND

January 2021 - Data breach as information accessed through one of the bank's third-party file sharing services

LLOYDS BANK - UK

January 2017 - Denial-of-Service (DoS) attack, more than 20 million UK accounts were blocked for payments

TESCO BANK - UK

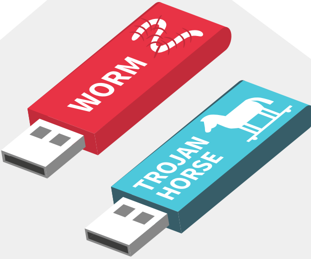
2016 - Attack on its online accounts

BANGLADESH'S CENTRAL BANK

2017 - Account maintained at US Federal Reserve hacked

MOROCCO'S CIH Bank

August 2020 - Breach customer accounts resulting in unauthorized transactions



Cyber Breach Incidents Globally

FLAGSTAR BANK - US

2021 - Hackers gained unauthorized access to customer data

CNA FINANCIAL - US INSURANCE FIRM

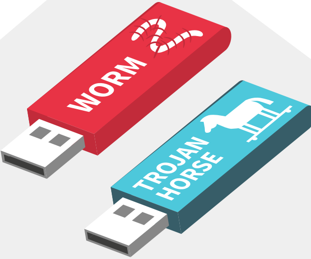
May 2021 - Ransomware attack disrupted the company’s employee and customer services for three days

UK’S MEDICAL SYSTEM - NHS

2017 – The virus named “WannaCry” was spread through email in the form of attachments, 300,000 computers were infected

COLONIAL PIPELINE GROUP - US

May 2021 - Cyber attack that involves ransomware, forcing the company to take some systems offline and disabling the pipeline



THANKS