Chambre de Commerce et d'Industrie Franco-Arménienne

Cybersecurity for SMEs

Protecting your business, reputation, and future in a digital world.

Presenter - Milind BHAWSAR

NOTICE & DISCLAIMER

This presentation, provided in collaboration with the **Chambre de Commerce et d'Industrie Franco-Arménienne (CCIFA)**, is for **informational and educational purposes only**.

By reviewing these materials, you acknowledge and agree to the following terms –

1. Consolidatory Nature of Information

The information contained herein has been consolidated from various international cybersecurity frameworks, industry white papers, and historical threat intelligence. It represents a "snapshot" of the current cyber landscape and is not exhaustive.

2. No Professional Recommendation

Any mention of specific products, vendors, or services (e.g., Microsoft, CrowdStrike, ESET, etc.) is intended **solely for illustrative purposes** to help SMEs understand market categories.

- **No Endorsement:** CCIFA does not endorse, recommend, or favor any specific commercial product or vendor.
- **Neutrality:** The selection of examples is arbitrary and does not imply that these are the only or the best solutions for your specific business.

3. No "One-Size-Fits-All" Solution

Cybersecurity is highly dependent on a **company's unique digital architecture, local infrastructure, and risk appetite.**

Strategies discussed during the webinar are general frameworks.

You are strongly advised to consult with a certified **Managed Service Provider (MSP)** or a dedicated Cybersecurity Consultant to perform a professional audit before implementing any solution.

4. Limitation of Liability

While every effort has been made to ensure the accuracy of the information provided, CCIFA, the presenter, and its partners:

Make no warranties or guarantees regarding the effectiveness of the strategies discussed.

Shall not be held liable for any direct, indirect, or consequential damages (including data loss or financial loss) resulting from the use or misuse of the information presented.

5. "Live" Nature of Threats

Cyber threats evolve daily. Information provided today may become obsolete or incomplete within a short timeframe. The responsibility for maintaining up-to-date security remains solely with the business owner.

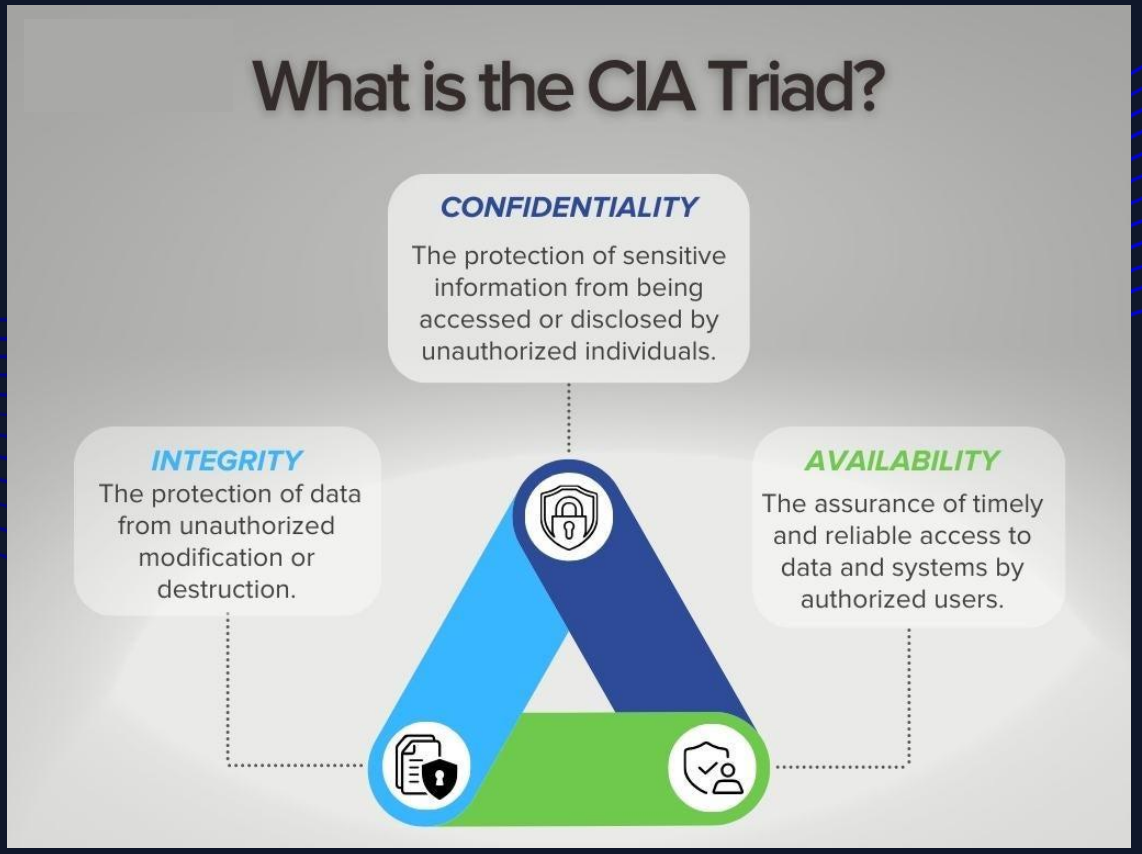
What is Cyber Security

Protecting Data & Assets in a connected world

Cyber Security is the practice of protecting systems, networks, and programs from digital attacks

The Cyber attacks are usually aimed at –

- Accessing sensitive information.
- Changing or destroying data.
- Extorting money from users (Ransomware).
- Interrupting normal business processes.



The Digital Context

A Digital Paradox

While Yerevan’s tech sector is booming, 60% of Armenian SMEs still operate without modern digital tools. The offline mentality often creates a false sense of security.

The Global Reality

As you adopt digital tools (banking, email, tax reporting) to compete, you become part of the global attack surface. Cybercriminals use automated bots that scan for vulnerabilities, not specific company names.

Dispelling the "Too Small" Myth

43%

of cyber attacks target Small Businesses

Why you?

Small businesses are often seen as “low hanging fruit”. You have money, date, and typically weaker defenses than a bank or large corporation. Hackers use automated bots to find open doors; they are not choosing you personally, their software is.

Unique Local Risks

Pirated Software

Using unlicensed or "cracked" software is common but risky. These often contain pre-installed malware that silently steals data.

Public WiFi

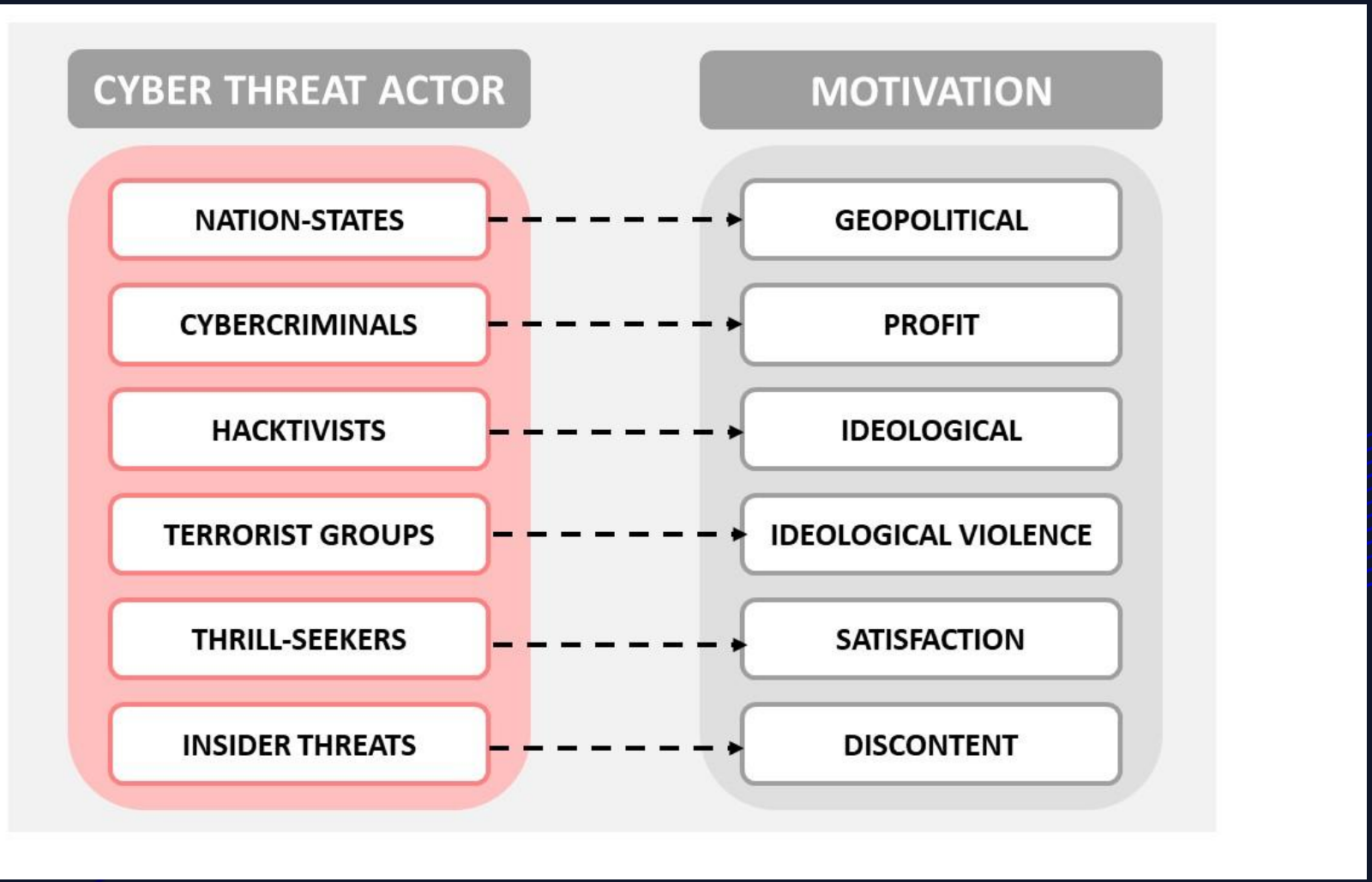
Conducting business in cafes without a VPN exposes your passwords to anyone on the same network using simple sniffing tools.

Social Engineering

Attackers exploit our trust-based culture, posing as known partners or suppliers to request urgent fraudulent payments.

Etc....

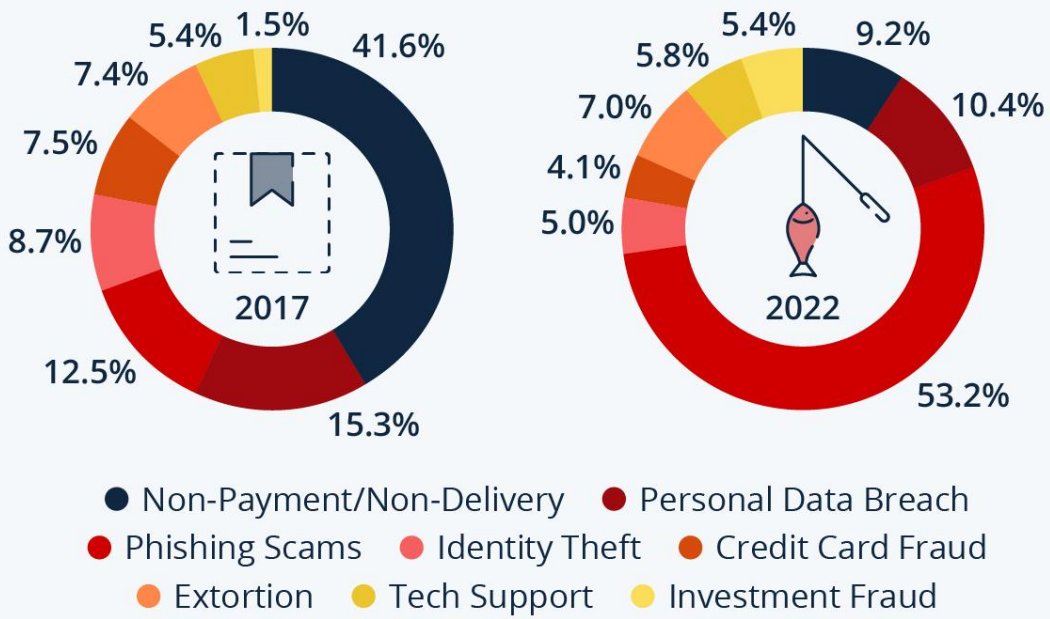
Cyber Threat Actors



Overview of Cyber Crime

The Most Prevalent Forms of Cyber Crime

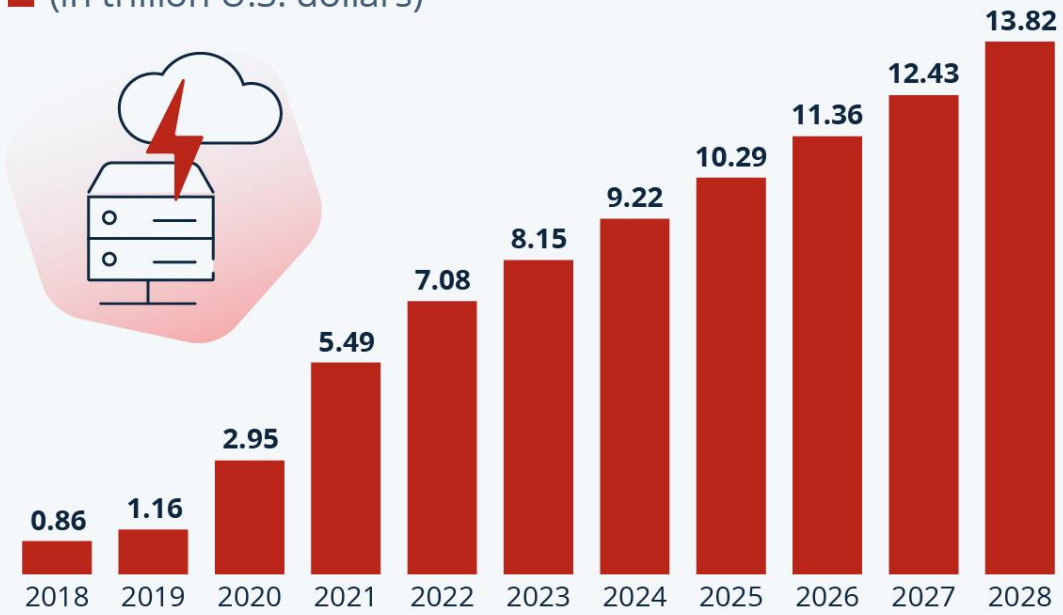
Share of worldwide cyber attacks by type



Sources: Statista Market Insights, National Cyber Security Organisations, FBI, IMF

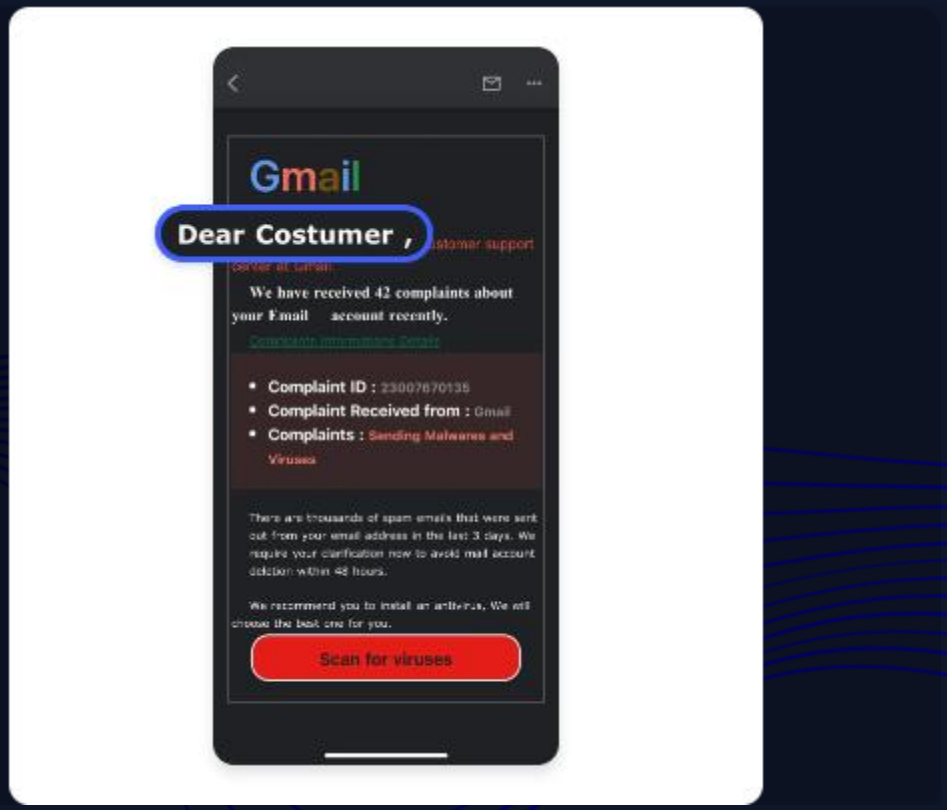
Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide (in trillion U.S. dollars)



As of Sep. 2023. Data shown is using current exchange rates.
Source: Statista Market Insights

The #1 Threat: Phishing



Deception by Email

Phishing is the entry point for 90% of cyber attacks. It rarely looks like a scam anymore. It looks like:

- An urgent invoice from a supplier.
- A password reset request from "Google".
- A tax document from the government.

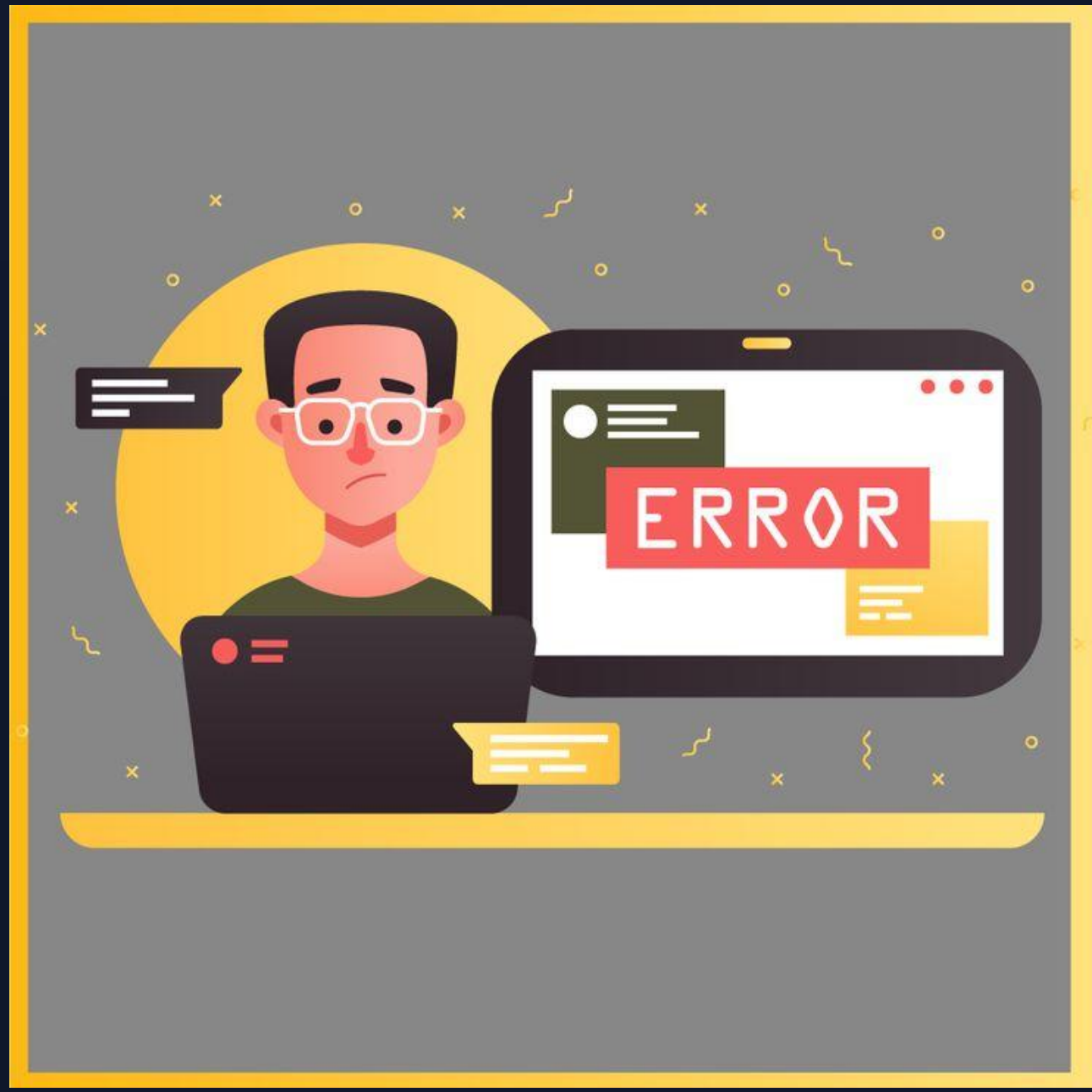
Goal: To steal credentials or install ransomware.

Business Impact

Beyond the Computer

A cyber attack is not just an IT inconvenience; it is a business crisis. Ransomware can lock your files, halting operations for weeks.

Reputation is Key: In a close-knit market, losing client trust due to a data leak can be more damaging than the financial cost of the attack itself.



Defense 1/4: The Human Firewall

DO: Strong Password

Remind and train your staff to use Strong Passwords.

Do not use same passwords everywhere.

DO: Verify First

Train staff to use the **STOP - LOOK - THINK** method.

If an email demands urgent action, call the sender on a known number to verify it before clicking any links.

DON'T: Shadow IT

Prohibit the use of personal accounts (Gmail, personal WhatsApp) for sensitive company business. Keep data within secured, company-monitored channels.

Defense 2/4: EDR

EDR is a cybersecurity technology that continuously monitors endpoints for evidence of threats and performs automatic actions to help mitigate them.

For example - Xcitium EDR, Microsoft Defender for Endpoint, CrowdStrike Falcon, etc.

Feature	Traditional Antivirus	EDR (Endpoint Detection & Response)
Strategy	Passive: Blocks known "bad" files.	Active: Watches behaviour in real-time.
Analogy	A Wanted Poster at the door.	A Security Guard walking the halls.
Reaction	Alerts you after a virus is found.	Detects a thief while they are trying to break in.
Superpower	Stops common, old viruses.	Can stop "Zero-Day" (brand new) attacks.

Defense 3/4: Multi-Factor Authentication

The Digital Lock

MFA (2FA) is an effective security measure. It requires a second proof of identity (e.g. a code on your phone) in addition to your password.

Even if a hacker steals your password, they cannot access your account without your phone. Enable this on email, banking, and social media immediately.

Example – Google or Microsoft Authenticator

Defense 4/4: The 3-2-1 Backup Rule

Your Insurance Policy

Ransomware relies on you having no other copy of your data.

If you have backups, you don't need to pay the ransom.

- **3** copies of your data.
- **2** different media types (e.g., Laptop + External Drive).
- **1** copy offsite (Cloud Storage).

Adopting European Standards

Leveraging the guidelines from ANSSI (France) to build a robust defense strategy.

Questions?

Let's secure the future of your business.

Q1. Why hackers are hard to "trace" after a payment?

Even if you use a credit card, professional cybercriminals are masters of digital camouflage. Here is why the trail usually goes cold –

- ***Money Laundering*** - Hackers rarely use their own bank accounts. They use "money mules" often innocent people recruited via fake job ads, who receive the stolen funds and then transfer them via untraceable methods like cryptocurrency.

- ***The Shell Game*** - Stolen funds are bounced through dozens of accounts across multiple countries (often in jurisdictions that don't cooperate with Western police) in seconds.

- ***Infrastructure Shifting*** - Hackers use VPNs, Tor, and "bulletproof" hosting services. When a payment is made, the IP address associated with the transaction usually points to a server in a country like North Korea, not the hacker's living room.

Q2. Emergency Response: What to do first?

If you've been hacked, speed is your best friend.

Do not panic, but act methodically.

Immediate Steps

1.Disconnect: If a device is compromised, take it off the Wi-Fi/Ethernet immediately. Do not turn it off (forensic evidence is often stored in the RAM), just isolate it.

2.Change Credentials: From a clean device, change passwords for your most sensitive accounts (Email, Bank, Social Media etc).

Q3. Who to contact in France?

In France, there is a specific hierarchy for reporting -

The Hub - Go to Cybermalveillance.gouv.fr

This is the government's primary platform. It provides a diagnostic tool and connects you with certified local professionals.

The Police/Gendarmerie - Yes, you should file a complaint. You can now do this online via THESEE (for scams, phishing, and ransomware) on the Service-Public.fr website.

The Bank - If money is involved, call your bank's fraud department immediately to freeze cards or stop transfers.

Q4. Does AI pose a new threat / challenege for Cyber?

Yes, AI is a major shift. In the past, you could spot a phishing email because the English was poor. Today, a hacker in another country can use AI to write a perfect, professional email in any language. The 'spelling mistake' clue is gone.

The "Voice/Video" Threat (Deepfakes) -

"We are entering an era where you can't even trust your ears. There have already been cases globally where an accountant received a 'Zoom' call from their CEO, it looked and sounded like him, asking for an urgent transfer. This is why we need **Process**. You never move money because of a 'call'; you move money because the secondary verification process was followed."

The "Human" Advantage -

"But here is the good news: AI is also what powers the EDR solutions we discussed. While an AI bot is trying to break in, your AI security guard is watching. It’s an 'AI vs. AI' war in the background. Your job as a business owner isn't to outsmart the AI, it’s to make sure you have the right defense AI (through an MSP, for example) on your side."

"AI makes the 'Human Firewall' (your employees) even more important. They need to be more skeptical than ever. If something feels 'too fast' or 'too urgent,' it probably is, even if it looks like it's coming from a 'smart' source."