Clearbridge Webinars

*Helping You Do Your **Best** Work*

Cybersecurity 201 - Types of Cyberattacks

On average, *30,000 websites* are hacked *every day*. That’s a business falling victim to a cyberattack every *39 seconds*!

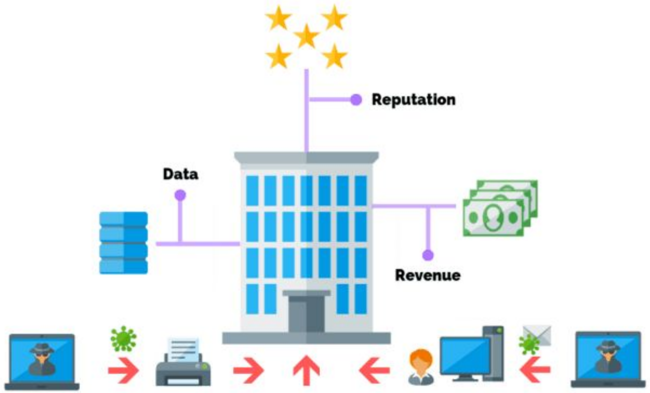
It cost businesses *globally* *$6 trillion* to fix breaches in 2021

This is why *cybersecurity* is so *critical* to you and your business!

So, let’s revisit a basic definition of cybersecurity

- Cybersecurity is **how** you **protect** your data and information systems from cyberthreats and attacks.

- Over time, cyberattacks affect your business’ **data**, which impacts your **revenue** and **reputation**.



Common *myths* (and *truths*) about cybersecurity

MYTH 1

MYTH Big companies and wealthy people are more likely to be targeted.

TRUTH It's not about who you are, it's about whether or not your information is valuable.

MYTH 2

MYTH Your security software will always protect you.

TRUTH Your security software is not an invincible shield between your data and hackers.

*In 2019, a Russian hacking collective breached three top US antivirus companies, profiting over $1M USD from the cyberattack.

MYTH 3

MYTH Cyber threats are always external.

TRUTH According to the Verizon 2021 Data Breach Investigations Report, insiders are responsible for around 22% of security incidents.

MYTH 4

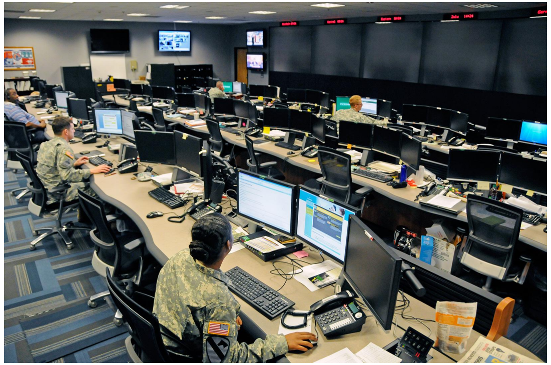
MYTH Your password will never be cracked

TRUTH Hackers use programs to run billions of password combinations and use sophisticated methods to identify the passwords you create.

MYTH 5

MYTH Cybersecurity is expensive to deploy and maintain.

TRUTH It will be cheaper than rebuilding an infected system and replacing lost information.



Lack of *awareness*, *training* and *persistent misinformation* put businesses at *risk*

At Clearbridge, we’re here to *help educate you*, so you can *better protect* yourself and business

Understanding the types of cyberattacks is *essential* to keep your data and systems safe.

TYPES OF CYBERATTACKS

5

Man In the Middle Attacks

1

Malware

4

Internal Threats

3

Phishing/ Social Engineering

2

Ransomware

1. What is it?
2. How does it happen?
3. Statistic about the attack
4. Example of the attack

1 - Malware

WHAT IS IT?

- A file or code that **disrupts**, **damages**, or **gives access** to your system.

HOW DOES IT HAPPEN?

- Downloading programs
- Opening or downloading attachments
- Clicking on links in emails or text messages

STAT

- In 2019, **93.6%** of malware observed was polymorphic, meaning it has the ability to constantly change its code to evade detection (2020 Webroot Threat Report)

EXAMPLE

- In May 2021, Canada Post was the victim of a malware attack through a third-party vendor. It affected **950,000 parcels**. Postal addresses, emails and phone numbers were exposed.

2 - Ransomware

WHAT IS IT?

- Software that attackers use to **hold your system ransom** until a **sum of money is paid**.

HOW DOES IT HAPPEN?

- By encrypting files and demanding a ransom payment for a decryption key, attackers **force organizations to pay the ransom** to regain access to their files.

STAT

- The average ransomware attack only takes **3 seconds** to begin encrypting your network and lock your business files.

- 82% of attacks that took place in 2021 impacted organizations with **less than 1000 employees.**

EXAMPLE

- Cybercriminals attacked a small business with only 8 computers! Their insurance company paid the **$150,000 ransom** because the alternative was to shut down the business.

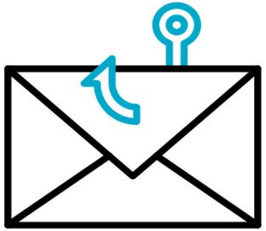
3 - Phishing/Social Engineering

WHAT IS IT?

- A scam where attackers impersonate a **legitimate company** or **person** asking for **sensitive information**.

HOW DOES IT HAPPEN?

- Say they've noticed some suspicious activity or log-in attempts
- Claim there's a problem with your payment information
- Say you must confirm some personal information
- Include a fake invoice
- Want you to click on a link to make a payment
- Say you're eligible to register for a government refund
- Offer a coupon for free stuff



STAT

- Phishing emails sent globally have increased by **667%**! A whopping **70% to 90%** of all data infiltration is due to phishing and social engineering attacks.

EXAMPLE

- Posing as the CEO, an attacker emails a manager using a **subject line that looks legitimate**. The manager clicks on a link that redirects to a **spoofed version of an invoice**, and the attacker steals his credentials **gaining full access** to their network.

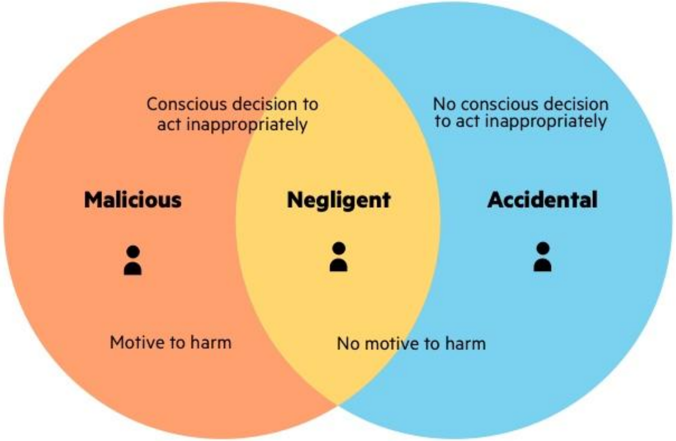
4 - Internal Threats

WHAT IS IT?

- An insider who uses their **authorized access**, willingly or unwillingly, to do harm to a company's system.

HOW DOES IT HAPPEN?

- **Activity at unusual times**—signing in to the network at 3 am
- **The volume of traffic**—transferring too much data via the network
- **The type of activity**—accessing unusual resources


Conscious decision to act inappropriately
No conscious decision to act inappropriately
Malicious
Negligent
Accidental
Motive to harm
No motive to harm

STAT

- Companies from North America suffer the most from insider attacks and their consequences with an average cost of **$13.3M**. Further to that, **98%** of organizations feel vulnerable to insider attacks.

EXAMPLE

- In 2021, a Pfizer employee uploaded **12,000 confidential files** to her Google Drive account from her corporate laptop. She shared confidential documents including drug development data and trade secrets related to the COVID-19 vaccine and its studies.

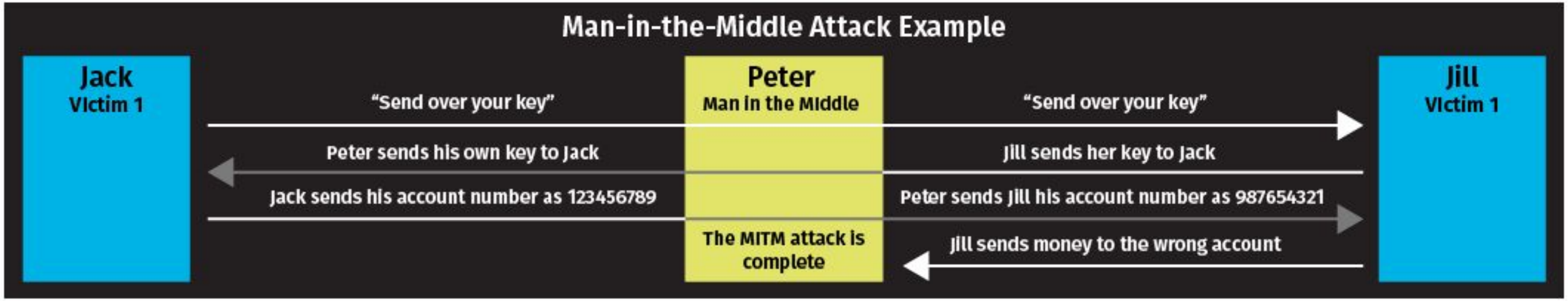
5 - Man-in-the-Middle Attacks

WHAT IS IT?

- An eavesdropping attack where cybercriminals **intercept** and **relay messages** between two parties to **steal data**.

HOW DOES IT HAPPEN?

- The hacker sets up a **false Wi-Fi network**. Meanwhile, the hacker can note down **passwords**, **usernames**, and any **private data** users enter while on their network.



Man-in-the-Middle Attack Example

Jack
Victim 1

Peter
Man in the Middle

Jill
Victim 1

"Send over your key"

"Send over your key"

Peter sends his own key to Jack

Jill sends her key to Jack

Jack sends his account number as 123456789

Peter sends Jill his account number as 987654321

The MITM attack is complete

Jill sends money to the wrong account

STAT

- Attackers sent over **30 emails** to disrupt a financial transaction worth **$1M**. By impersonating users and modifying banking details, funds were transferred to the attackers’ account.

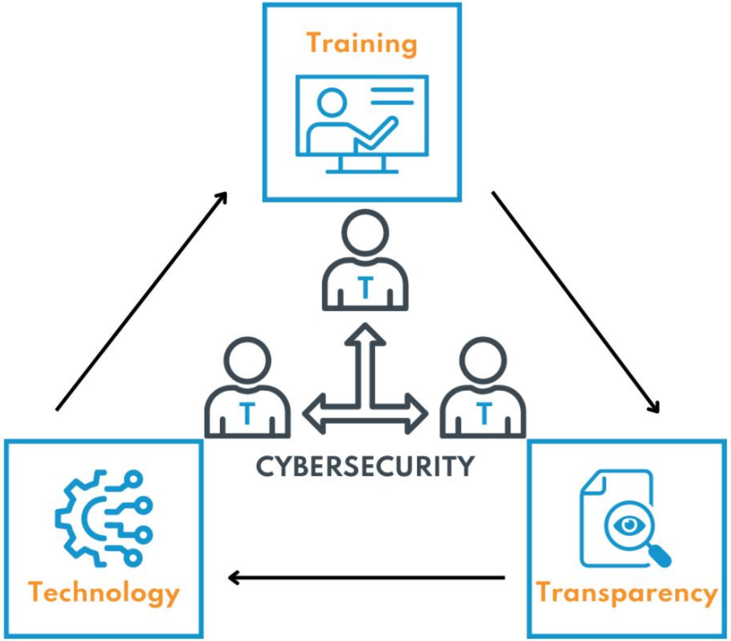
EXAMPLE

- In a wire-transfer heist, an attacker used unique tactics—including **communicating through email** and even **cancelling a critical in-person meeting**–to fool both parties on either end of the transfer.

How can you protect *yourself* and your *business*?

Follow the three *Ts*!

Employees should understand and be trained on company policies about software use, and data ownership.



Technology should support **employees and employers** in detecting, investigating and responding to data breaches.

Employers should be transparent about what activities the company is monitoring on work-issued laptops.

Top tips

1. Be SENSIBLE - *Never* click on links, download files or open attachments in emails (or on social media) that aren't from a **known, trusted source**.

2. Be PROACTIVE - **Learn** as much as possible about *cybersecurity*, **get certified**, and **ask for training** at the workplace.

3. Be VIGILANT - *Every* **situation** you come across *could* be a **potential scam**. It's better to be safe than sorry.

Q + A

support@clearbridge.ca

clearbridge.ca/lifewithclearbridge

Clearbridge Webinars

*Helping You Do Your **Best** Work*

Thank you!