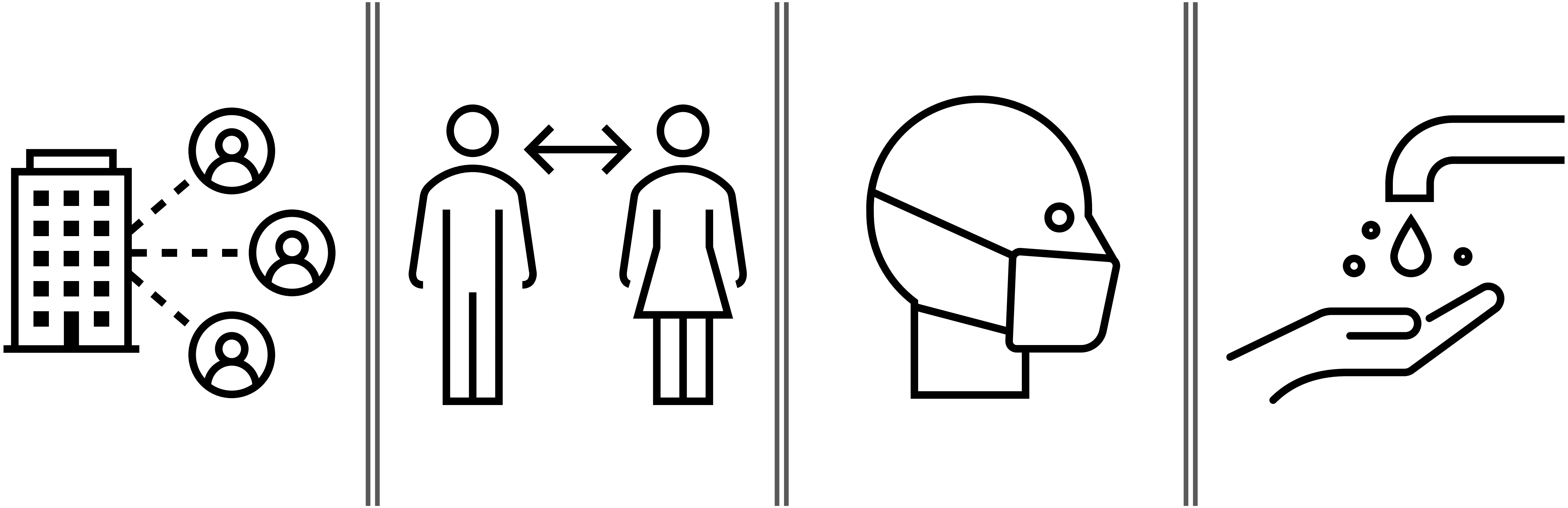
Surviving the Cyber Threat Landscape in the COVID-19 Era & Beyond

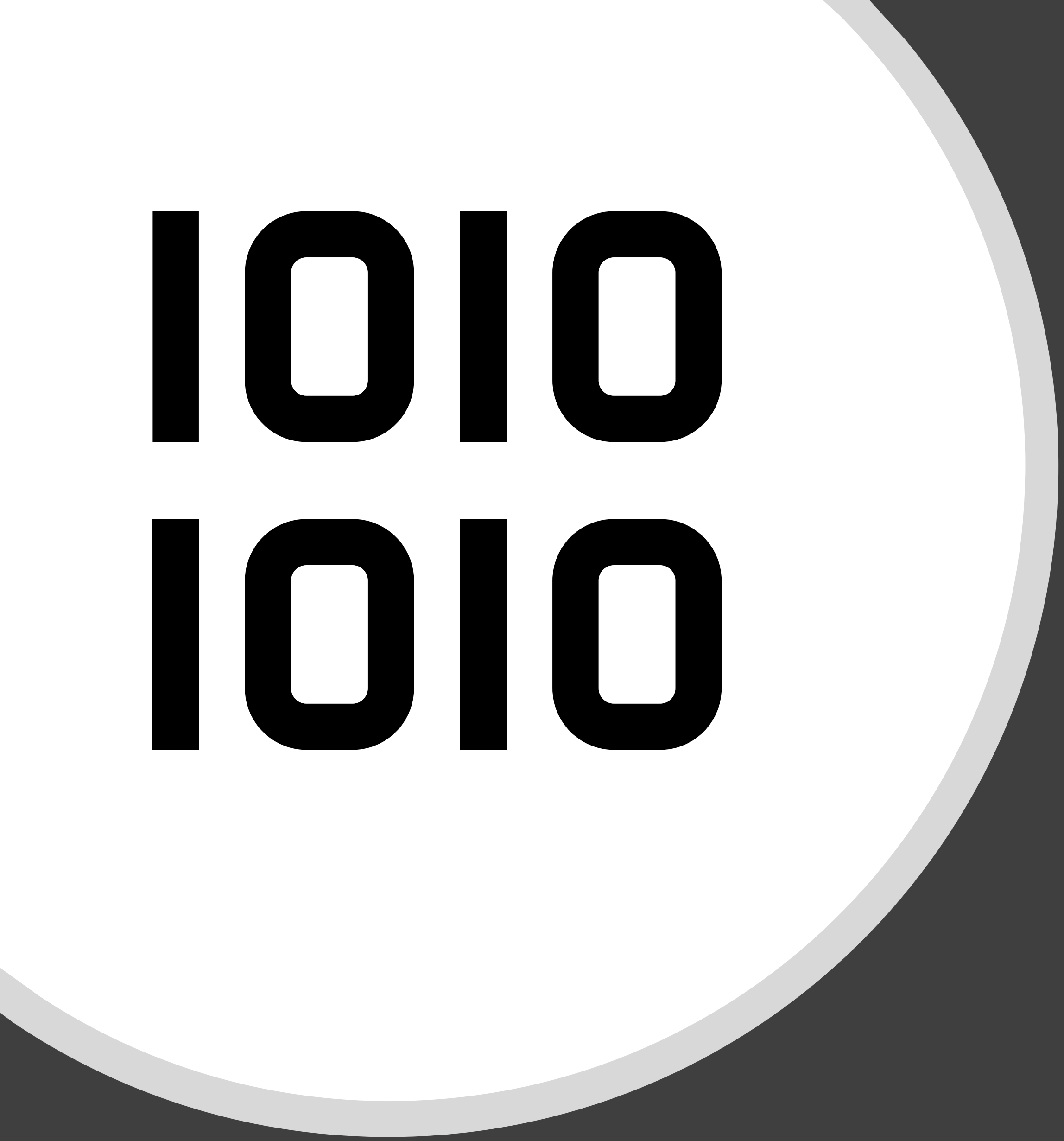
Balancing Security & Flexibility

Presented by: Umar Sa’ad



We live in interesting times!!

COVID-19



According to McKinsey:

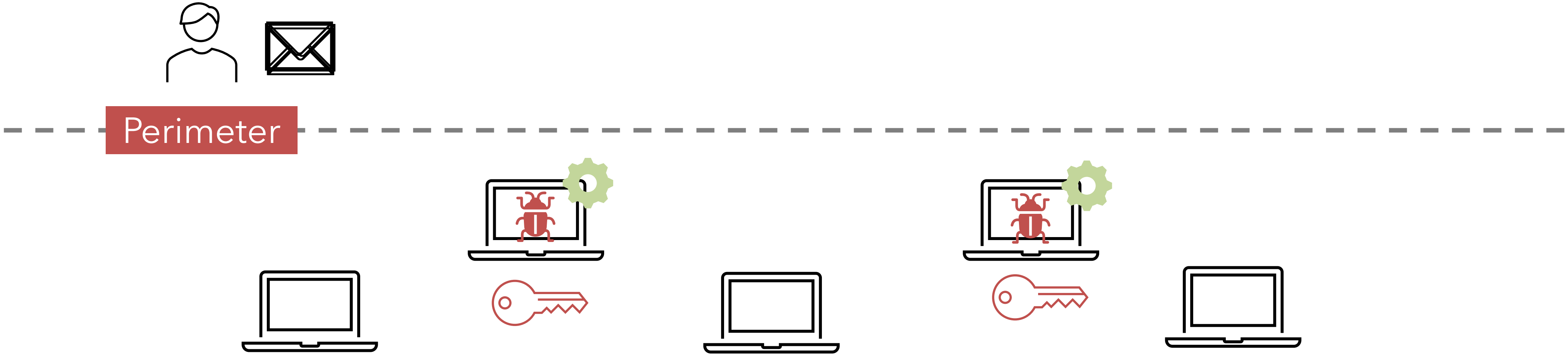
Responses to COVID-19 have accelerated the adoption of digital technologies by several years – and many of these changes are here to stay.

February 2016

- Bangladesh Central Bank was hacked
- $81 million was embezzled by cybercriminals

How did it happen

Step 1: Perimeter Compromise



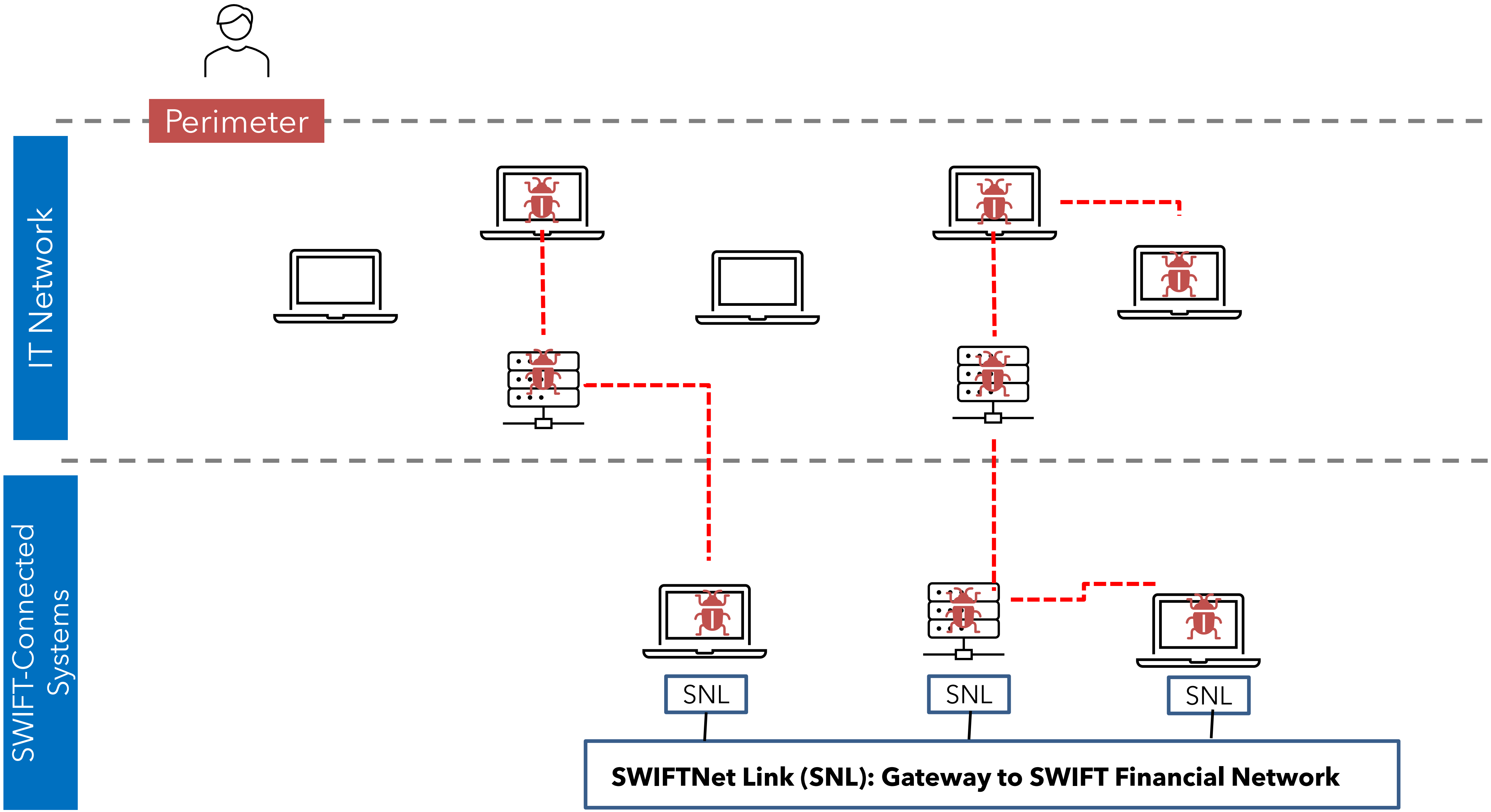
Spear-phishing campaign

Endpoints infected

Attackers gained access

Attackers steal credentials

Step 2: Lateral Movement & Privilege Escalation



Step 3: Launch of High Coordinated Attack

Compromised Local admin accounts

Installed monitoring software

Captured SWIFT credentials

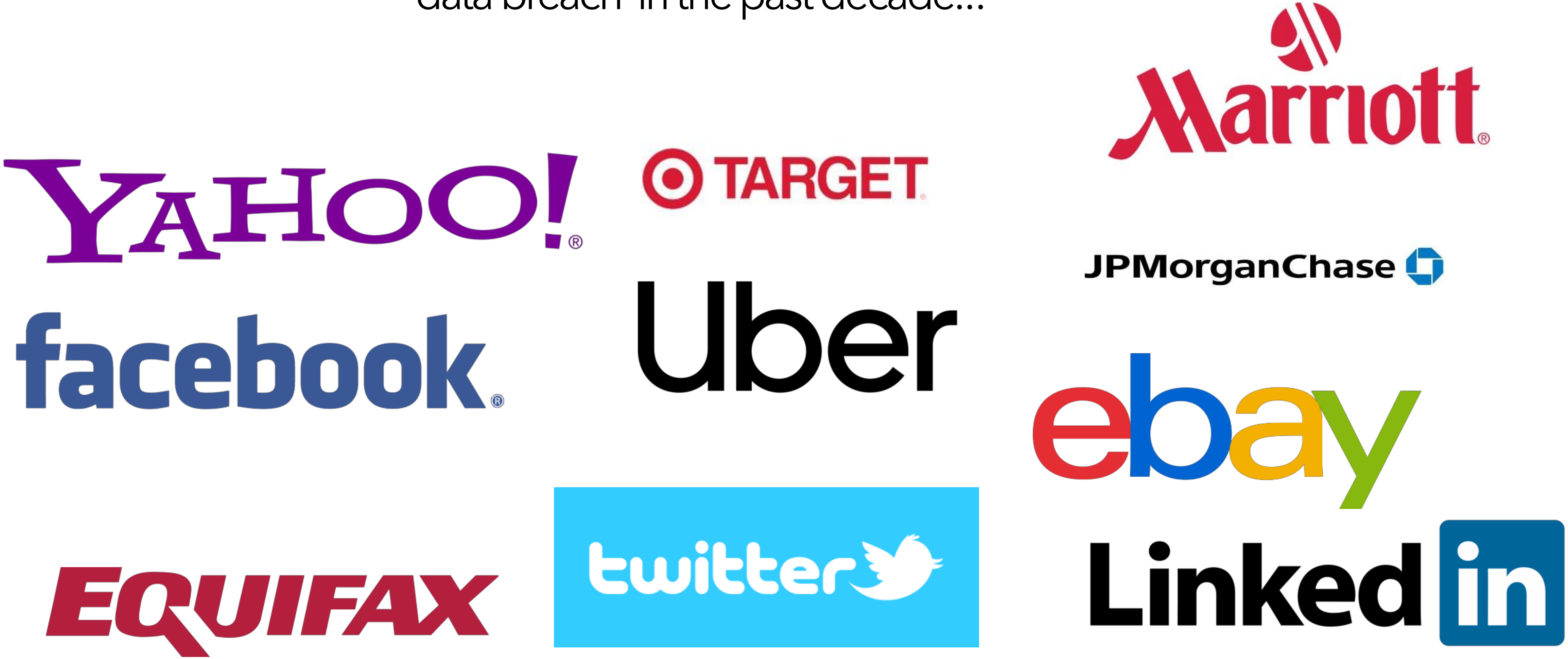
Initiated 35 transactions worth $951 million

Attack was foiled when banker noticed a spelling error “Shalika Fandation”

$81 million was unrecovered

What do these companies have in common?

They have all suffered from a major
data breach in the past decade...



According to Data Breach Level Index of 2018

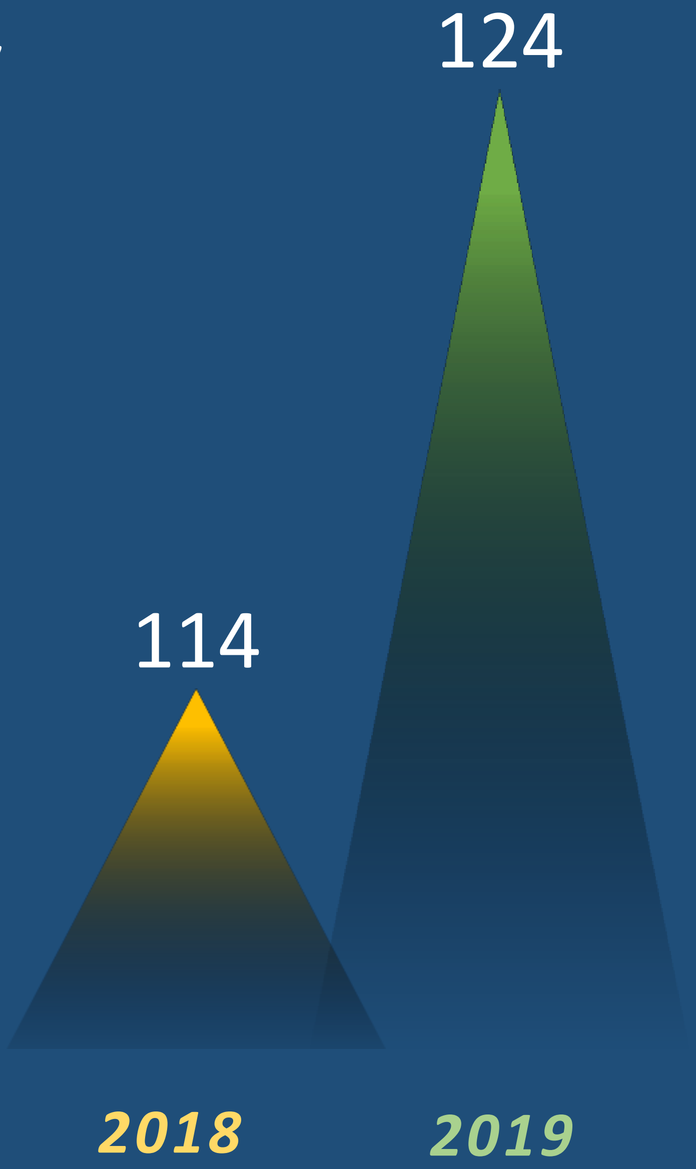
14.7 Billion

No. of lost/stolen records
2013 - 2018

4%

Were considered
“secure breaches”

Global Cyber Security Spending (in $ billion)



Source: *Gartner, Aug 2018*

Agenda

Defining Cyber Security

Why You Should be Concerned

COVID-19 Threat Landscape

Measuring Security Level

Cyber Defense Strategies

Defining Cyber Security

Security is two things…..

Feeling

Refers to how we feel about the risk of an activity

Reality

Refers to what we objectively know about the risk of an activity

The Decision Matrix of Security…

		Reality	
		👍	👎
Feeling	👍	*Appropriate*	*Delusional*
	👎	*Paranoid*	*Appropriate*

What Cyber Security ISN'T!!!

- Cyber Security is not a commodity.
- It is more than just technical measures such as installing an antivirus, firewall, or password protection.
- It isn't meant for only IT Professionals.
- It is more than protection against hackers.

What is Cyber Security?

> “ Cyber security is the deliberate synergy of technologies, processes, and practices to protect information and the networks, computer systems and appliances, and programs used to collect, process, store, and transport that information from attack, damage, and unauthorized access. ”

- Gregory J. Touhill and C. Joseph Touhill

In a nutshell

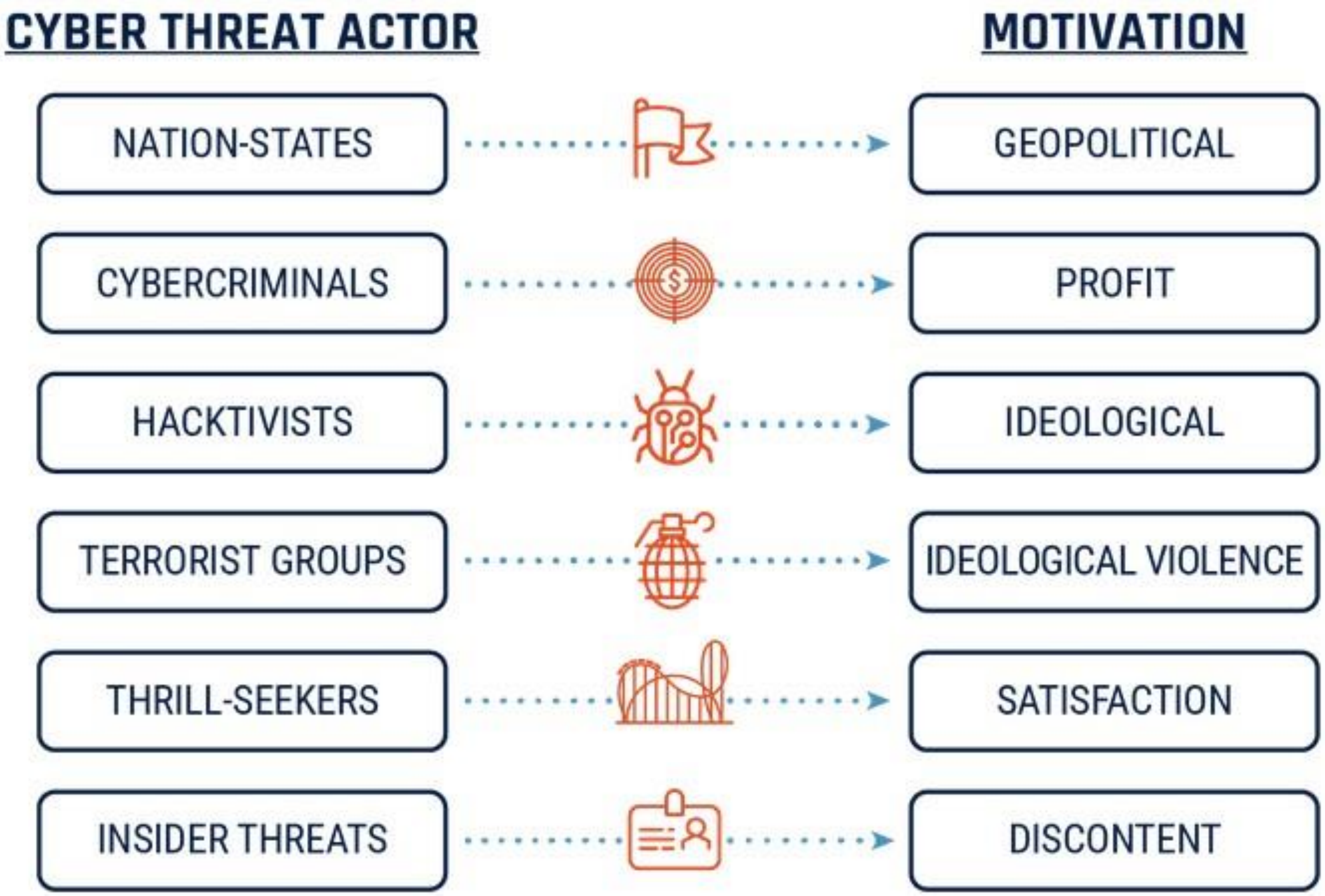
Cyber Security is a holistic set of activities aimed at protecting an organization’s vital information and systems.

Why you should be concerned

> “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

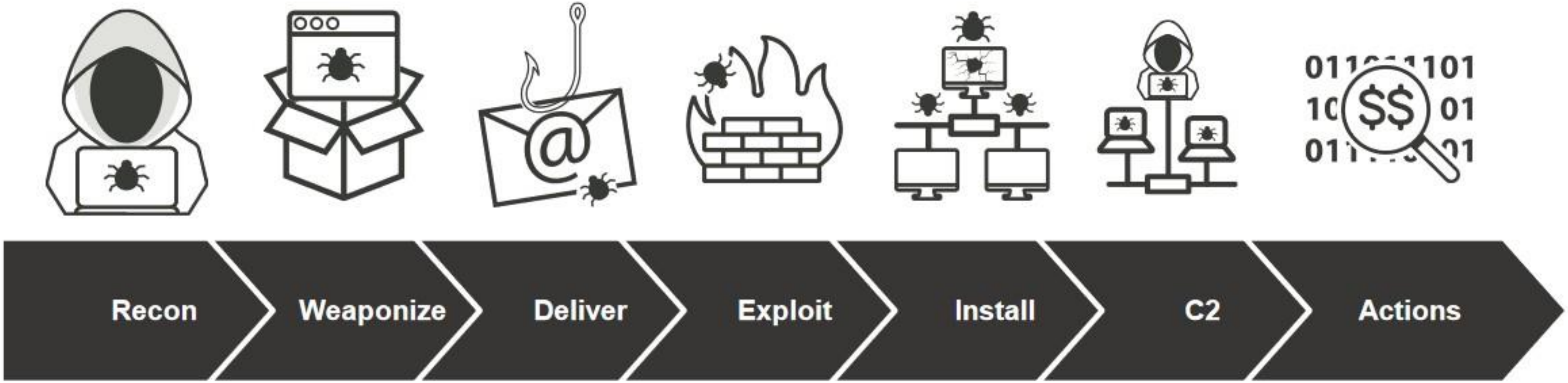
- Sun Tzu, The Art of War

Cyber Threat Actors



CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

How they operate a.k.a. Cyber Kill Chain



Recon

Weaponize

Deliver

Exploit

Install

C2

Actions

Gather data and intelligence on target organization

Craft malicious payload, use exploits for vulnerabilities

Payload sent to target (phishing)

Compromise system

Install malware, obtain credentials and establish backdoors.

Navigate internal network and setup command and control

Ultimate goals achieved

COVID-19 Cyber Threat Landscape

COVID-19 Threat Landscape

Employees	Organizations
Working remotely with access to enterprise apps at any time	Increased reliance on service providers and third parties to assist transition to remote work
Increased use of personal devices that are not "company-issued"	Increased uncertainty leading to lack of visibility on emerging cyber risks
Connecting via home Wi-Fi systems without advanced security capabilities	Cyber criminals exploiting the COVID-19 panic to launch new phishing campaigns
Inability to perform security tasks, creating challenges with real-time monitoring & SOC services	Fake social media profiles/users disseminating false information.

Common Cyber Threats

Malware

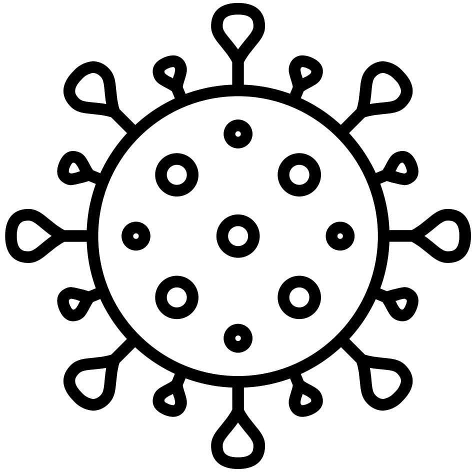
Denial of service attack

Phishing & Social Engineering

Man in the middle attack

Identity Theft

Common Cyber Threats



Malware

Malware stands for **Mal**icious Soft**ware.**

Virus

Worm

Trojan

Spyware

Ransomware

Bot/Botnet

Common Cyber Threats

Denial of service attack

A DoS is an **attack** meant to shut down a machine or network, making it inaccessible to its intended users.

This is accomplished by flooding the target with bogus traffic or sending it information that triggers a crash.

Another type of DoS is the Distributed Denial of Service (DDoS) attack that occurs when multiple systems orchestrate a synchronized DoS attack to a single target.

Common Cyber Threats

Phishing & Social Engineering

Social engineering is a set of mostly psychological phenomena, applied predominantly in the context of computer and information security. E.g.

- **Phishing**
- **Dumpster Diving**
- **Shoulder Surfing**
- **Baiting**
- **Piggy-backing**
- **Pretexting**

Common Cyber Threats

Man in the middle attack

This is when an attacker intercepts communications between two parties either to secretly eavesdrop or modify traffic traveling between the two. E.g.

Evil Twin

SSL Stripping

Common Cyber Threats

Identity Theft

This refers to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. E.g.

Account Takeover

Credit/Debit Card Fraud

Identity Cloning

Measuring Security Levels

Measuring Security Level

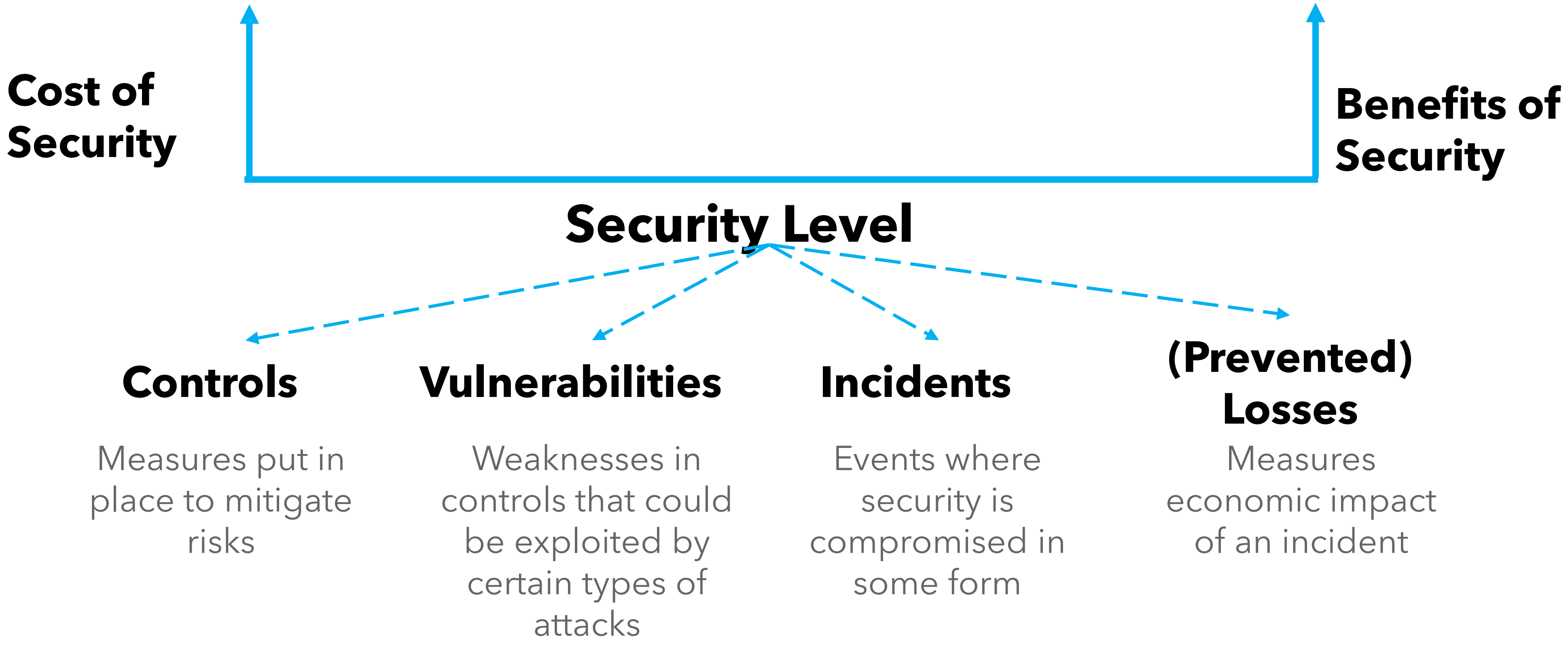
Security level is a “latent construct”, i.e., it can’t be observed or measured directly.

A latent construct can only be measured through indicators or metrics that reflect aspects of it.

For example, human intelligence, also a latent construct is measured through indicators like IQ tests.

Together, these indicators give us an estimate of the security level.

Security Indicators/Metrics



Cost of Security

Benefits of Security

Security Level

Controls

Measures put in place to mitigate risks

Vulnerabilities

Weaknesses in controls that could be exploited by certain types of attacks

Incidents

Events where security is compromised in some form

(Prevented) Losses

Measures economic impact of an incident

Security Indicators/Metrics

Controls

Physical

e.g., Door locks, CCTV cameras etc.

Organizational

e.g., incident response team

Procedural

e.g., password policy, BYOD policy etc.

Technical

e.g., encryption, firewall, antispyware etc.

Security Indicators/Metrics

Vulnerabilities

Known

Finding known vulnerabilities through vulnerability scanners, CERT alerts etc.

Unknown

Finding unknown vulnerabilities through penetration testing, red teaming etc.

Incidents

- This is where controls meet actual attacks, instead of potential attacks.
- Some incidents are easy to detect while others are hard.
- Automated tools for event monitoring (e.g., SIEMs) can be helpful, however, they tend to generate a lot of false positives.
- More sophisticated attacks e.g., APT could go undetected for months or even years.

Prevented Losses

- Mapping incidents to losses is hard.
- Mapping prevented incidents to prevented losses is even harder.
- For example, how do we measure events that didn’t happen?
- Did number of incidents fall because of failed attacks or fewer attacks?

Cyber Defense Strategies

Cyber Defense Strategies

Defense In-Depth

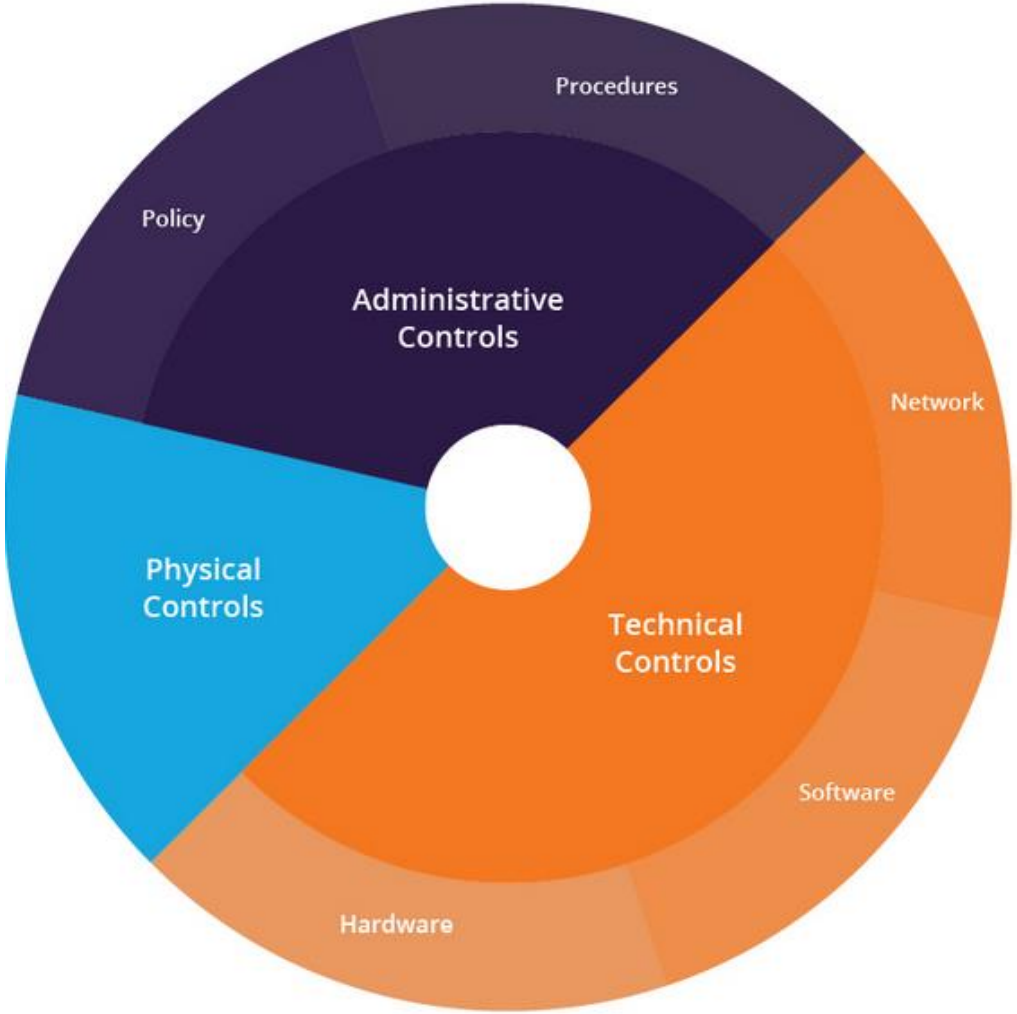
Assume Breach

Cyber Defense Strategies

Defense In-Depth

What is it?
It is a cyber defense strategy that provides multiple, redundant layers of protection in case a security control fails, or a vulnerability is exploited.

Focus..
A "multi-layered" security approach to PREVENT cyber attacks.



Physical controls – These controls include security measures that prevent physical access to IT systems, such as security guards or locked doors.

Technical controls – These include security measures that protect network systems or resources using specialized hardware or software, such as a firewall appliance or antivirus program**.**

Administrative controls – These are security measures consisting of policies or procedures directed at an organization’s employees, e.g., instructing users to label sensitive information as “confidential”.

Cyber Defense Strategies

Assume Breach

What is it?

In today’s cyberspace, it’s not a question of if but **WHEN** you will be breached. An assume breach strategy is about accepting this as a fact and building cyber resilience to withstand a cyberattack.

Focus..

RESILIENCE to cyber attacks through rapid DETECTION and CONTAINMENT of cyber attacks.

What is Cyber Resilience?

- This is the ability to prepare for, respond to and recover from cyber attacks.
- It helps an organization protect against cyber risks, defend against and limit the severity of attacks, and ensure its continued survival despite an attack.
- Cyber resilience has emerged over the past few years because traditional cyber security measures are no longer enough.

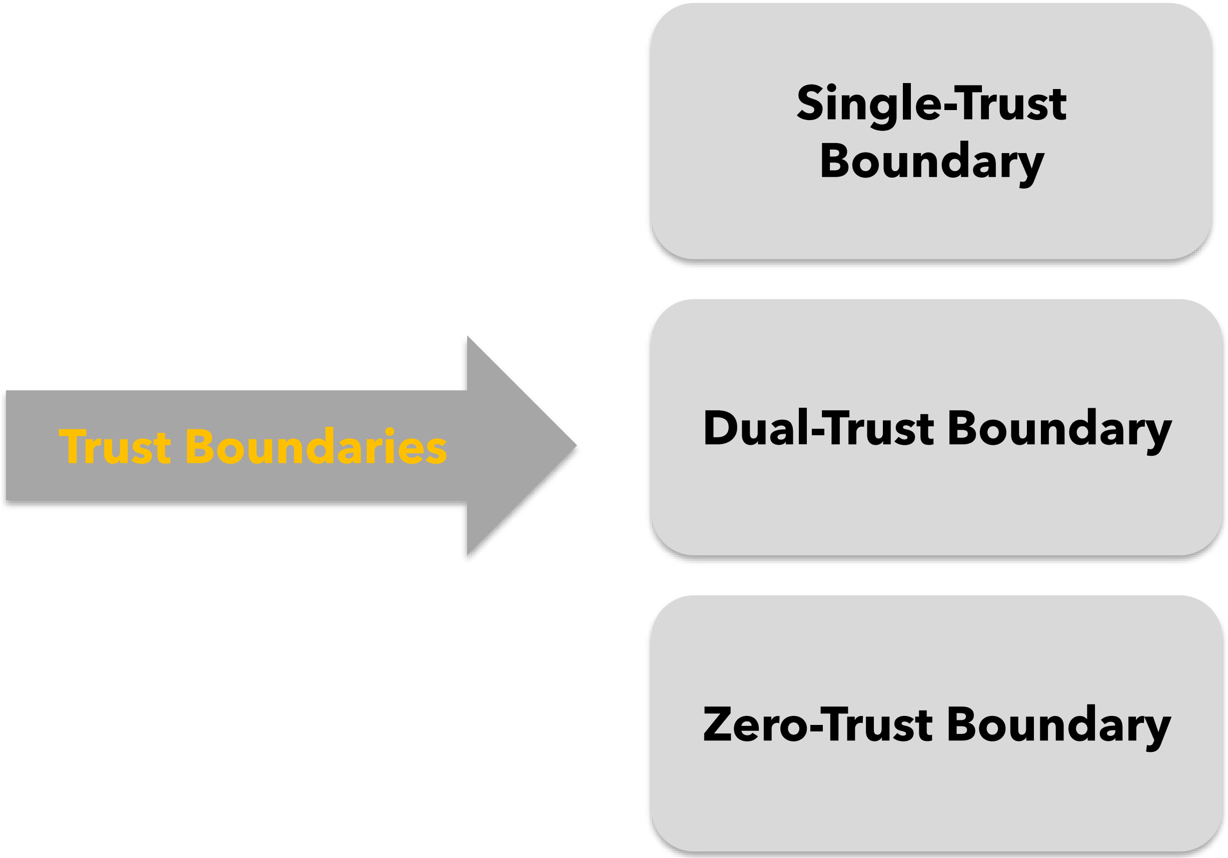
Assume Breach

Adopt an adversary mindset

Zero-Trust & Micro-segmentation

Secure The Breach

Zero-Trust & Micro-segmentation



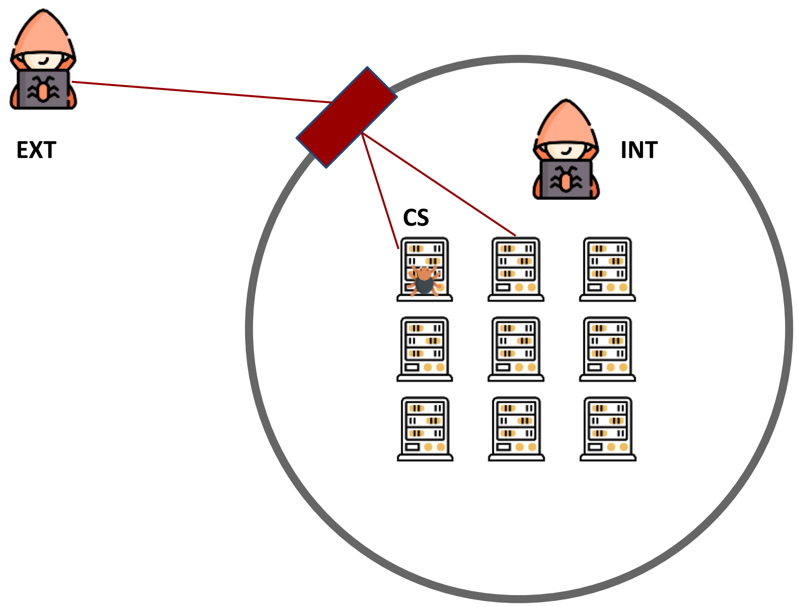
Trust Boundaries

Single-Trust Boundary

Dual-Trust Boundary

Zero-Trust Boundary

Single-Trust Boundary



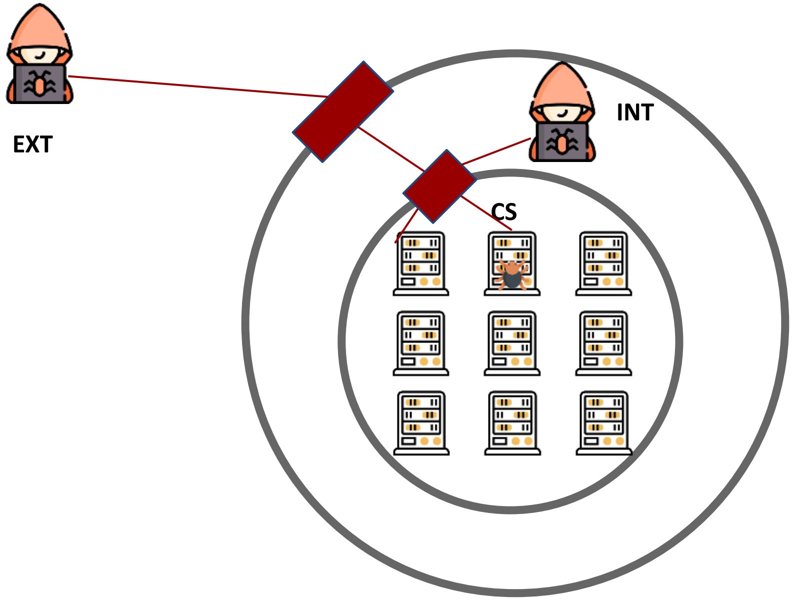
Threat Actors:

EXT: External
INT: Internal
CS: Compromised Server

Threat Exposure:

	ST
EXT	22%
INT	100%
CS	100%

Dual-Trust Boundary



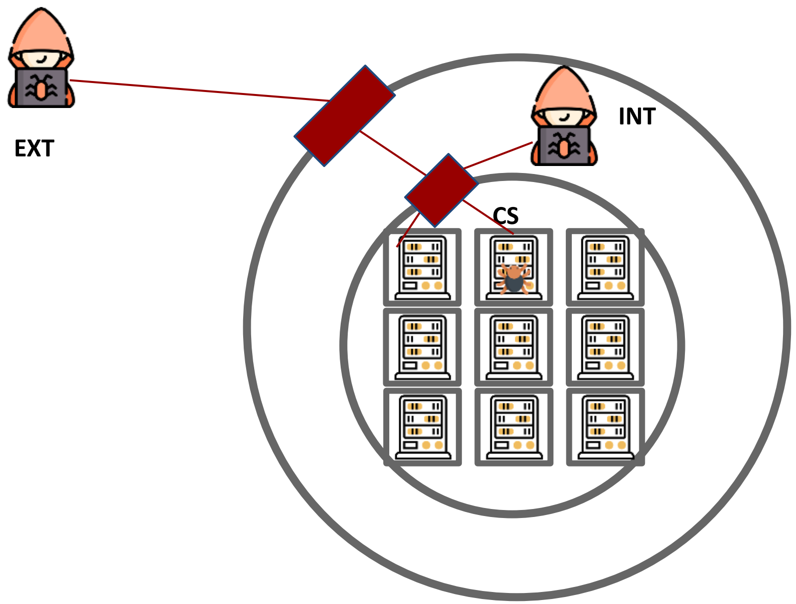
Threat Actors:

EXT: External
INT: Internal
CS: Compromised Server

Threat Exposure:

	ST	DT
EXT	22%	22%
INT	100%	22%
CS	100%	100%

Zero-Trust Boundary



Threat Actors:

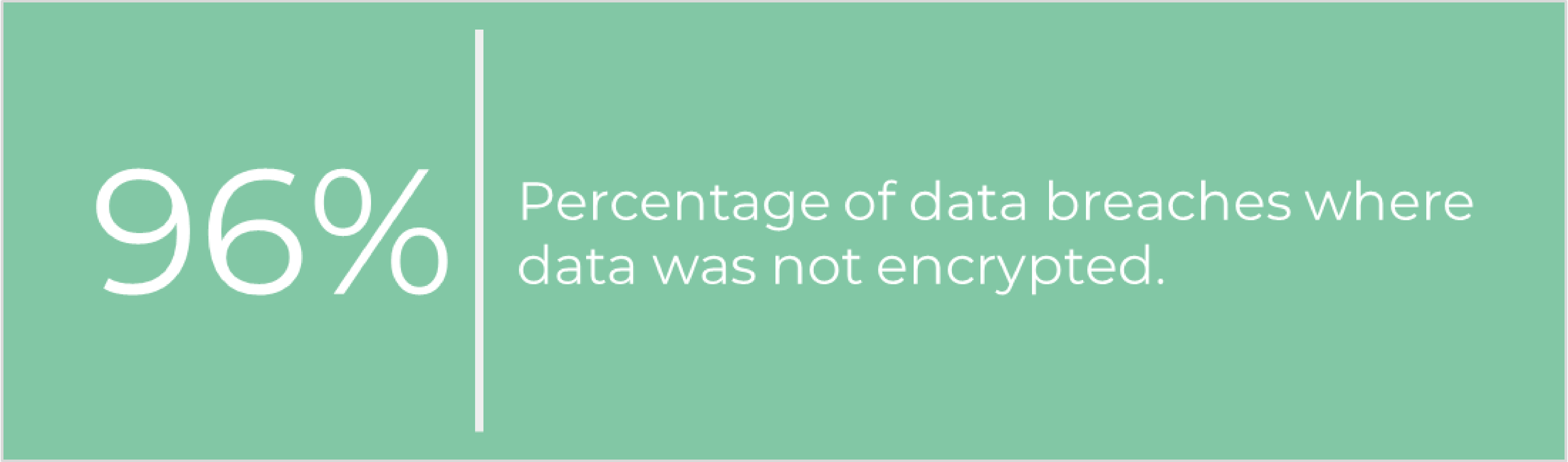
EXT: External
INT: Internal
CS: Compromised Server

Threat Exposure:

	ST	DT	ZT
EXT	22%	22%	22%
INT	100%	22%	22%
CS	100%	100%	11%

THREATS	SINGLE-TRUST BOUNDARY	DUAL-TRUST BOUNDARY	ZERO-TRUST BOUNDARY
External Threats	22%	22%	22%
Internal Threats	100%	22%	22%
Compromised Server	100%	100%	11%
Average Exposure	75%	50%	20%

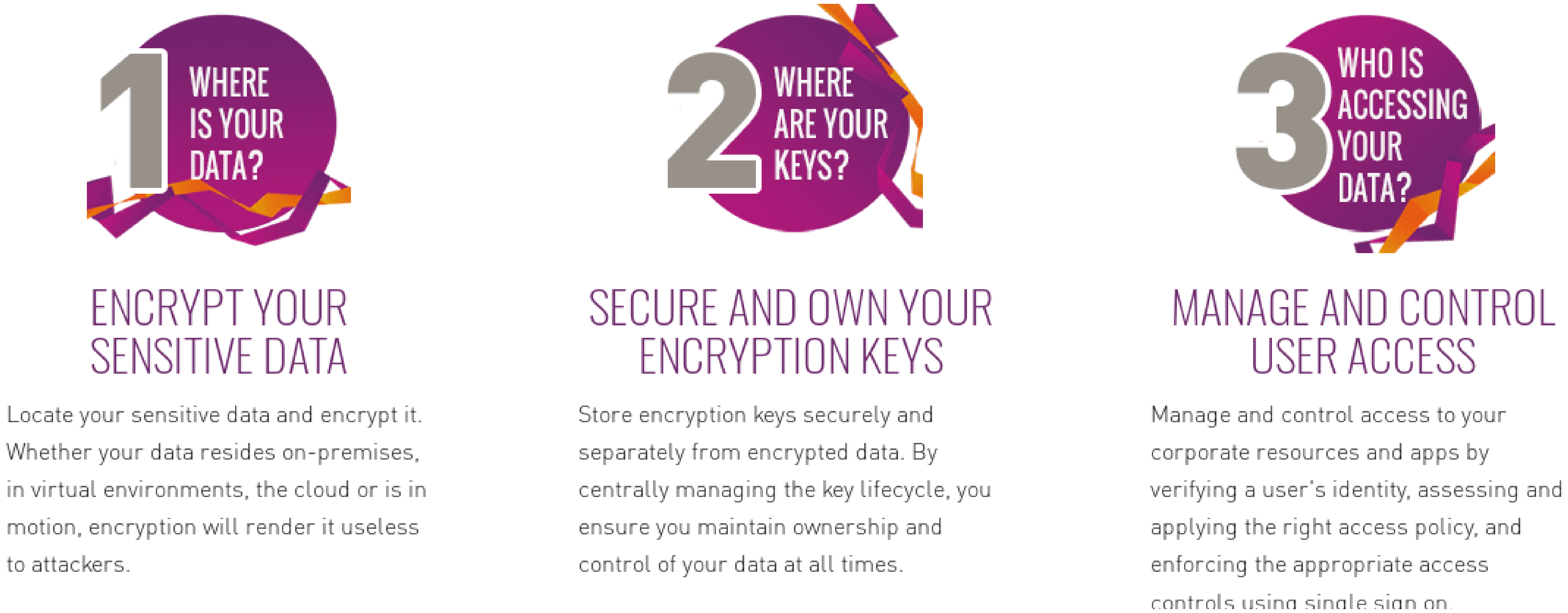
Secure The Breach



96%

Percentage of data breaches where data was not encrypted.

Secure The Breach



1 WHERE IS YOUR DATA?

ENCRYPT YOUR SENSITIVE DATA

Locate your sensitive data and encrypt it. Whether your data resides on-premises, in virtual environments, the cloud or is in motion, encryption will render it useless to attackers.

2 WHERE ARE YOUR KEYS?

SECURE AND OWN YOUR ENCRYPTION KEYS

Store encryption keys securely and separately from encrypted data. By centrally managing the key lifecycle, you ensure you maintain ownership and control of your data at all times.

3 WHO IS ACCESSING YOUR DATA?

MANAGE AND CONTROL USER ACCESS

Manage and control access to your corporate resources and apps by verifying a user's identity, assessing and applying the right access policy, and enforcing the appropriate access controls using single sign on.

In Conclusion…

Most people think that security and internal audit are two different & unrelated fields within a company.

It turns out that internal audit can play an important part in strengthening cyber security.

Internal audit can help through highlighting the privacy risks and data security, as well as identifying control and policies weaknesses.

Thank you

for Listening