Welcome To The 10th Annual Hacking Conference

Dungeons and Dragons™

InfoSec Master Edition

The Institute of Internal Auditors Chicago

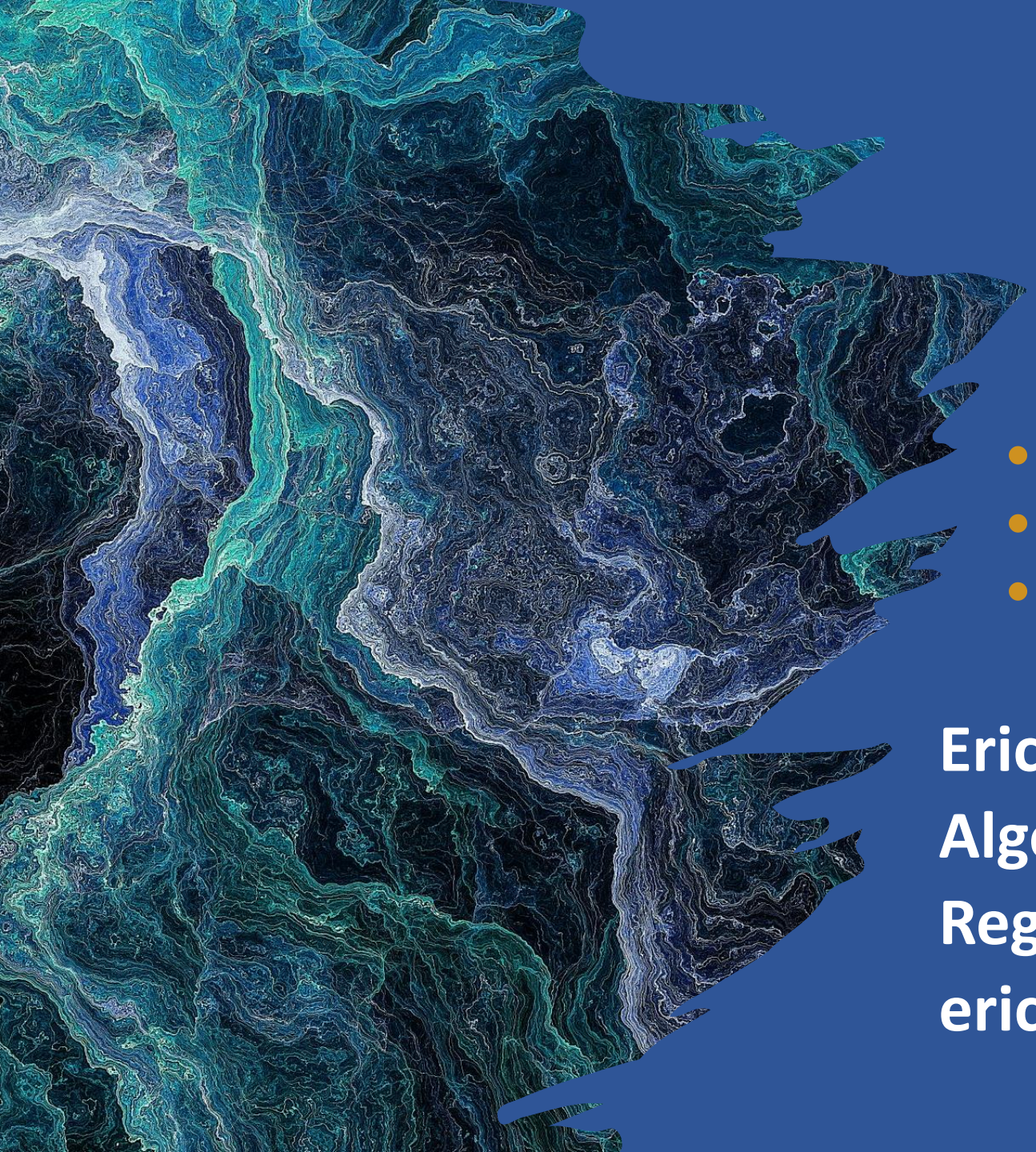
ISACA Chicago Chapter

Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter



Business Leadership and Cybersecurity Integration

- 10th Annual IIA/ISACA IT Hacking Conference
- Chicago, IL
- November 6, 2023

Eric Jeffery, TOGAF Master Architect
AlgoSec
Regional Solutions Engineer
eric.Jeffery@algosec.com

Agenda

- introduction
- leadership matters
- disparity requires variety
- true stories
- statistics
- engage and understand
- level up cyber security
- conclusion: solutions that make a difference

introduction

Disparate Entities Experience Unique Challenges

people training
locations technology
regulations
industry skills size
priorities revenue
networks geography

Distinct Enterprises Require Varying Solutions

true stories – beware & be aware

Third (4th, 5th, Etc.) Party Devastation

“The Biggest Hack of 2023 Keeps Getting Bigger” – Wired Magazine

Progress MOVEit

$100 Million

$100 Million

Major Brand Demolished

$100 Million

$100 Million

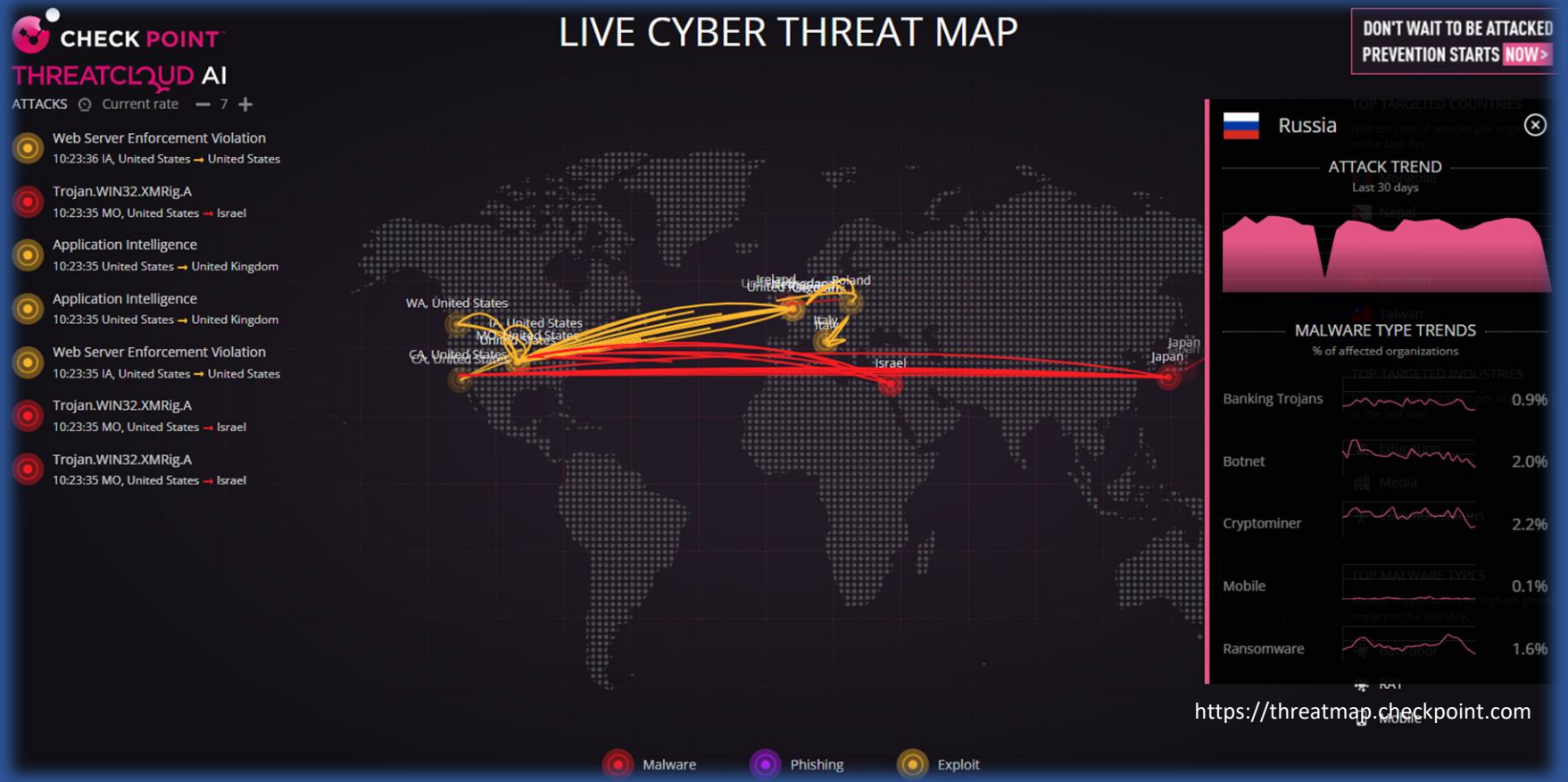
MGM GRAND

Children Impacted

bad guy statistics

Bad Guys are Everywhere and Have Completely Different Goals

WHO	WHAT
Nation states	Data theft
Organized crime	Extortion
Hacktivists	Damage
Petty thieves	Embarrass
Vandals	Punish
Insider threats	Signaling
	Shaping
	Coercion



https://threatmap.checkpoint.com

Cost of a Data Breach

Total cost of a data breach

USD 4.45M

Global average total cost of a data breach

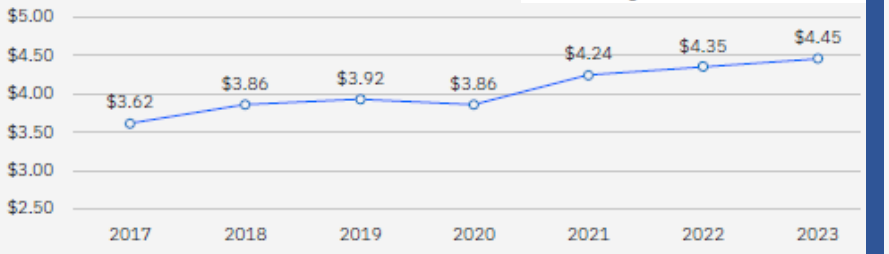


Figure 1. Measured in USD millions

Time to identify and contain the breach

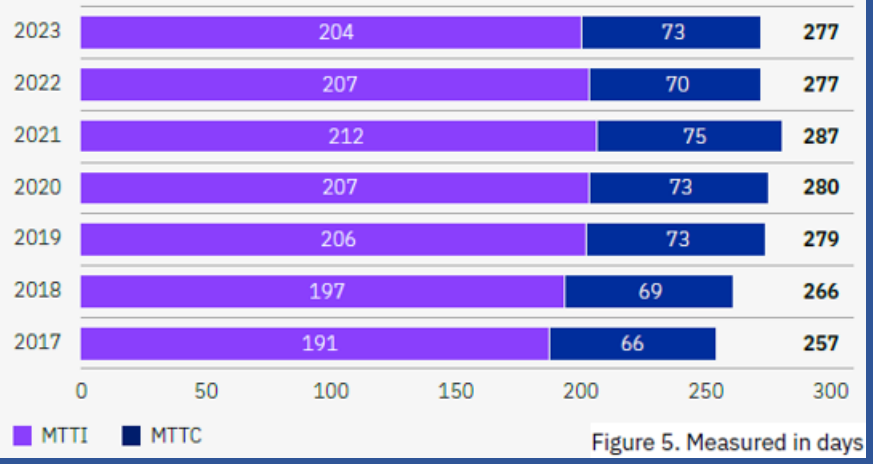


Figure 5. Measured in days

Cost of a data breach by industry

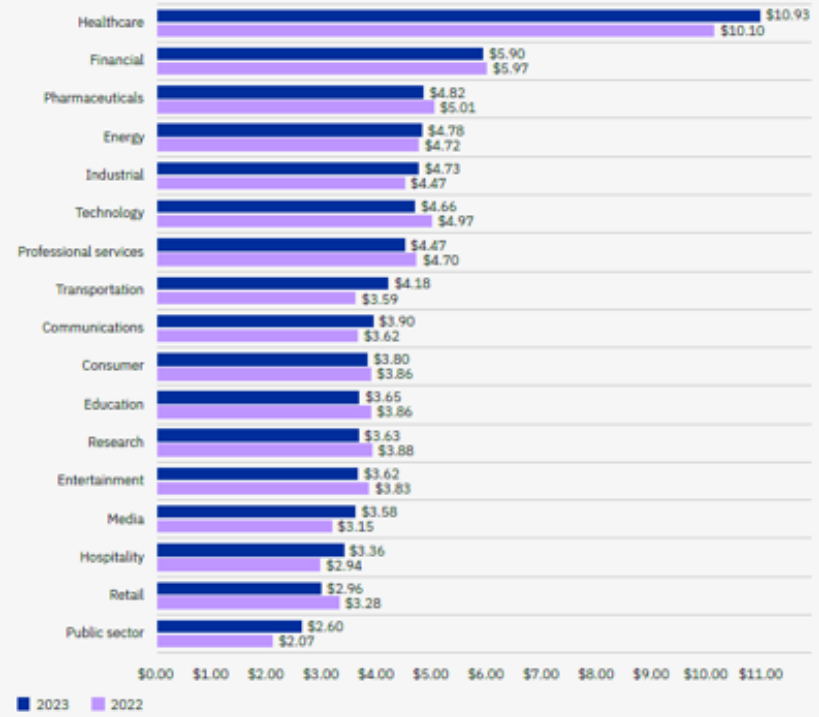


Figure 4. Measured in USD millions

12%

Share of data breaches originated from a software supply chain attack

33%

Only one-third of breaches were identified by the organizations' internal security teams and tools

		2023	2022
1	↑	United States USD 9.48 million	United States USD 9.44 million
2	↑	Middle East USD 8.07 million	Middle East USD 7.46 million
3	↓	Canada USD 5.13 million	Canada USD 5.64 million
4	↓	Germany USD 4.67 million	United Kingdom USD 5.05 million
5	↓	Japan USD 4.52 million	Germany USD 4.85 million

Type of data compromised

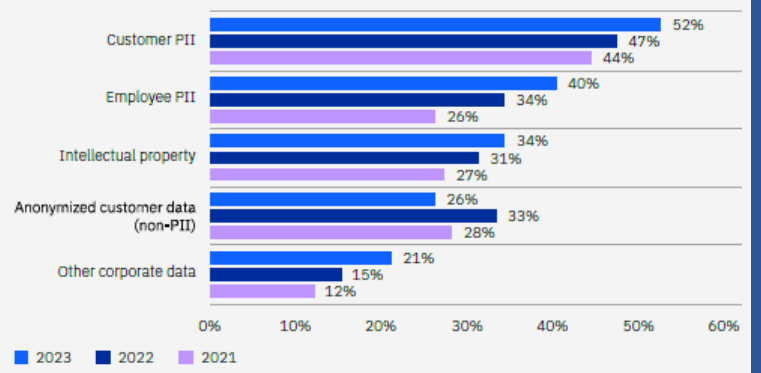


Figure 9a. More than one response permitted

USD 250,000

20% of organizations that experienced a data breach paid this much or more in fines

82%

Share of breaches that involved data stored in cloud environments—public cloud, private cloud or across multiple environments

51%

Percentage of organizations increasing security investments after a breach

16%

Percentage of breaches in which phishing was the initial attack vector

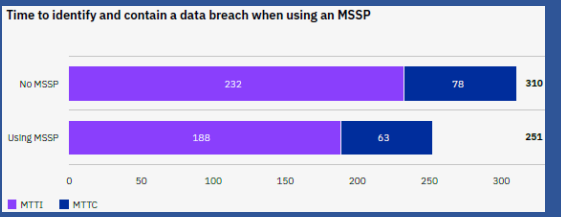
USD 3.98M

Cost of a data breach for organizations that deployed robust risk-based analysis

277 days

Time to identify and contain a data breach

Time to identify and contain a data breach when using an MSSP



engage and understand

Cyber Security Encompasses Everyone: The C-Suite Must Engage and Stay Involved

Board

CEO

CRO

CPO

CIO

COO

CFO

CISO

CMO

Understand Risk Management and Risk Quantification Inside the Enterprise

People, Property, Information

*An **Asset** is what we're trying to protect.*

Threat – Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

*A **Threat** is what we're trying to protect against.*

Vulnerability – Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.

*A **Vulnerability** is a weakness or gap in our protection efforts.*

Risk – The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

***Risk** is the intersection of assets, threats, and vulnerabilities.*

TAG – Threat Analysis Group

Is This a Risk or a Threat

This is a Threat

Countless Risks Exist in Cyber Security – How to Ensure Coverage

- Insider Threat
- Data Leakage
- Phishing
- Access Management
- Ransomware
- Worms
- Trojans
- Key Loggers
- Data Breach
- Version Control
- Third Parties
- Cloud Abuse
- Insecure Software
- Man In The Middle
- Patch Management

- Denial of Service
- Passwords
- Biometric Compromise
- Threat Vectors
- Network Penetration
- Lateral Movement
- Privilege Escalation
- Impersonation
- Social Engineering
- Shoulder Surfing
- Dumpster Diving
- Tailgating
- Shadow IT Systems
- Clear Text

level up cyber security throughout the organization

Who **Owns** What, Who **Does** What, Who **Knows** What

Governance = Leadership

Engage

Listen

Decide

Delegate

Follow Up

Track

Shift as Necessary

Reward

Act and Keep Acting

Relationship Manager	Vendor Manager	Project Manager	Account Manager
Team Lead	Executives	Partner	Project Lead

Identify and Understand Those Responsible, Accountable, Supporting, Consulted and Informed (RASCI)

Phase	Task Description	Role							
		DevOps	System Integration	Deployment	MSIEM	Cloud Operations	Application Support	Hardware Support	Client
	Provision, install, and initially configure (IP address, connectivity, etc.) the SIEM SaaS System	R, A	S	C		S	C		I
	Once able to remotely connect, take over the configuration of the SIEM SaaS System and customize it based on Client requirements, including Log Source integration, Use Case implementation, Dashboard customization, Offense Manager, and reporting.	I	R, A	C, I			C, I		C, I
	Installation of licenses on the SIEM console	R, A	I	C,I			I		
	Installation of SIEM apps that require admin access to the SIEM console	I	R,A	C,I			C, I		
	Allowing app access to specific user roles	R	I	A			I		
	Installation of service token for apps	A, I	R	C, I			I		
	Download, install, and configure all Client-premise Data Gateways and/or install physical Event Collector appliances and configure as Data Gateways.	I	R, A				I		

Task	Vendor Mgmt	Executive Sponsor	Business Owner	Legal	IT & Info Sec
Identify standard terms & conditions for contract	C	-	R/A	C	C
Negociate contract	C	C	R/A	C	-
Review final draft against standars	C	C	C	R/A	C
Execute contract	I	R/A	I	I	I
Store contract in contract management system	R/A	-	I	-	-
Assig contract owner	R/A	I	I	I	I
Integrate new vendor through onboarding process	C	I	R/A	-	C

Understand Legal Requirements and Comply(ance)

California Consumer Protection Act (CCPA)

General Data Protection Regulation (GDPR)

Defense Federal Acquisition Regulation (DFARS)

Payment Card Industry Data Security Standard (PCI-DSS)

Health Insurance Portability and Accountability Act (HIPAA)

Sarbanes-Oxley (SOX)

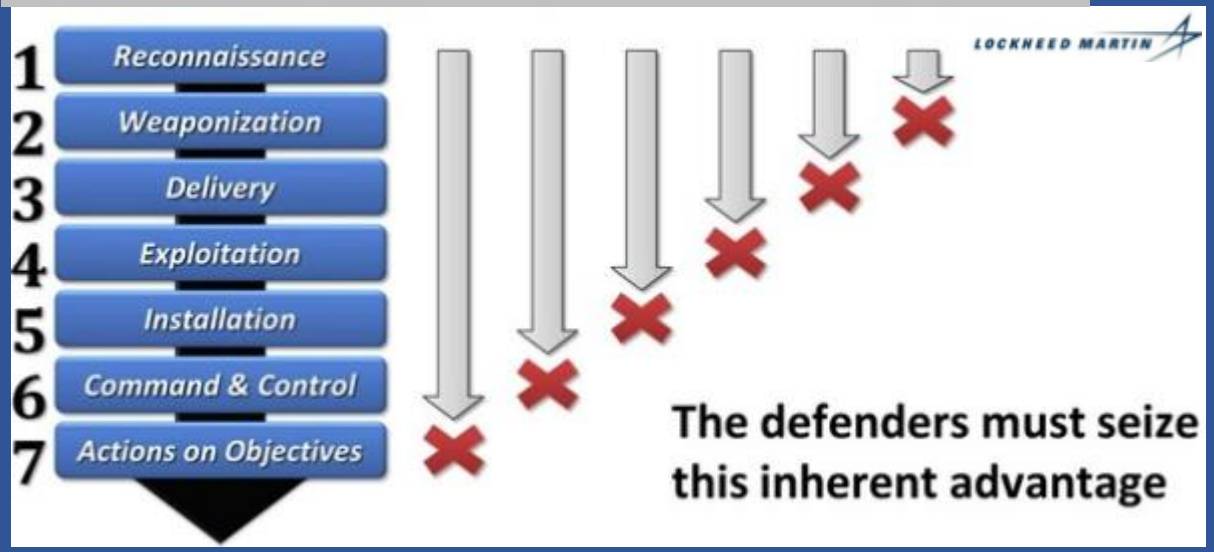
Federal Trade Commission Act §5

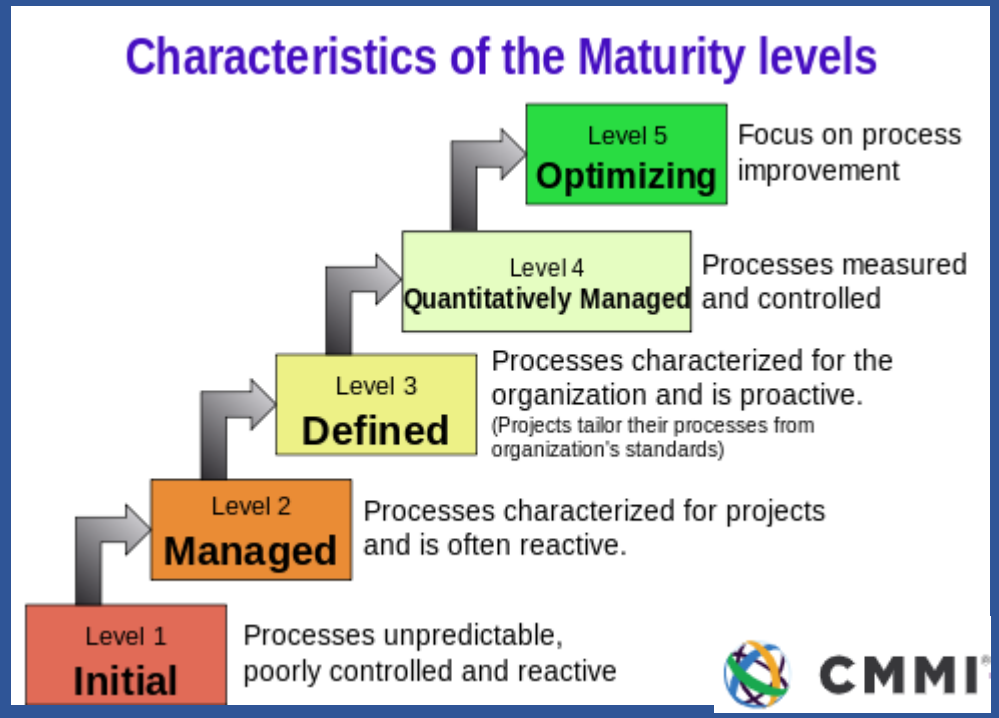
Gramm-Leach-Biley Act (GLBA)

Children's Online Privacy Protection Act (COPPA)

Standards and Frameworks to the Rescue in a Complex Arena

Just one mitigation breaks the chain





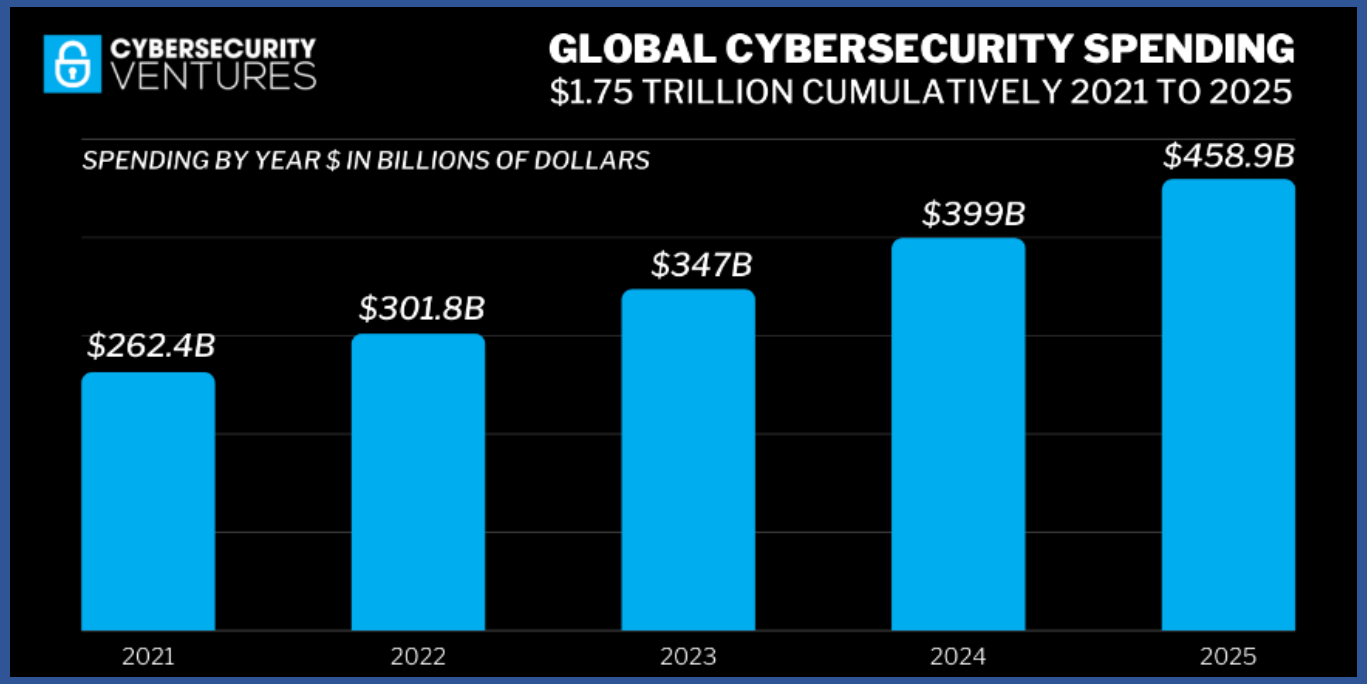
MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations

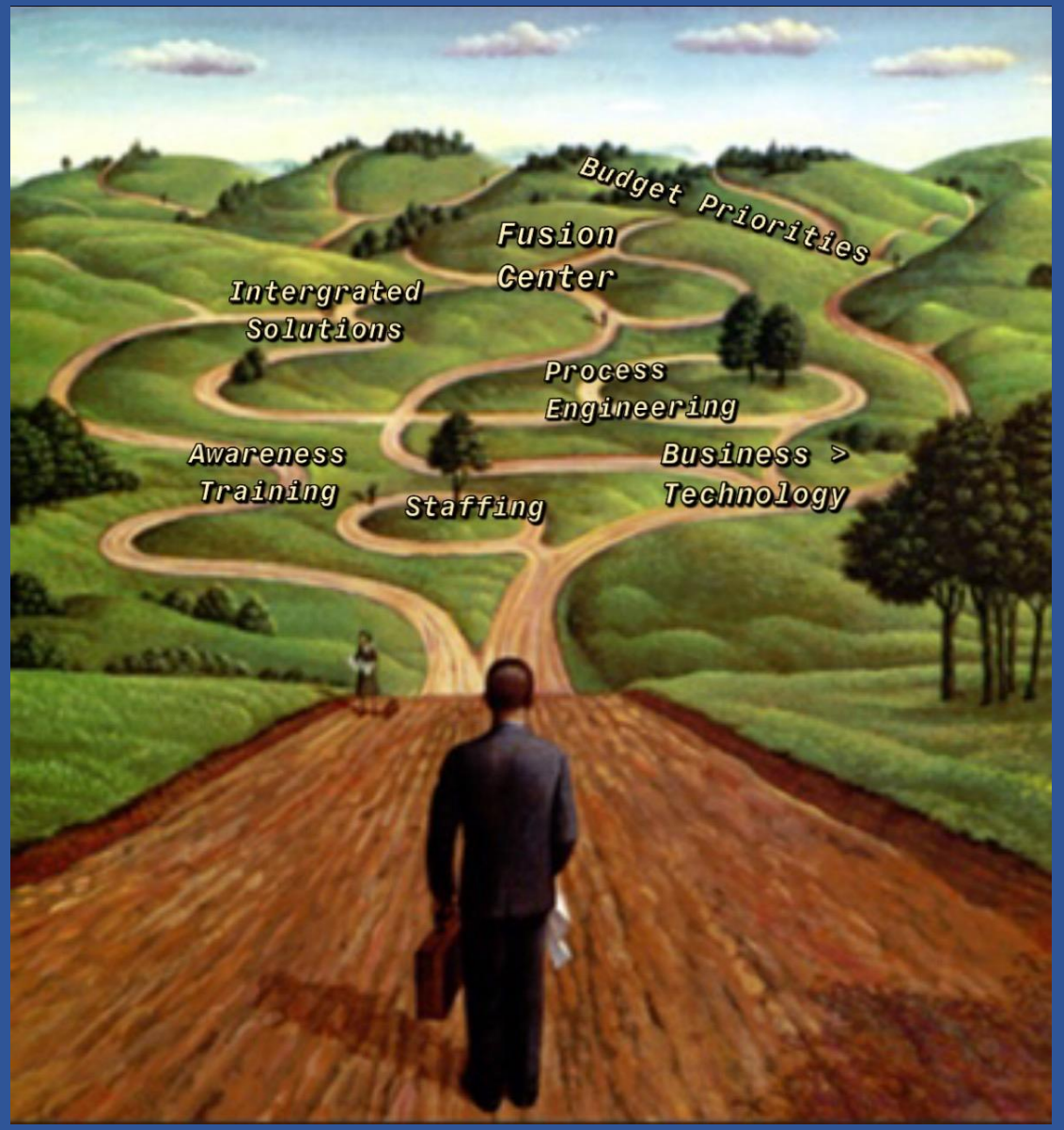
SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies - 2024

ISO is an independent, international NGO with a membership of 165 national standards bodies. ISO has developed over 23400 International Standards .

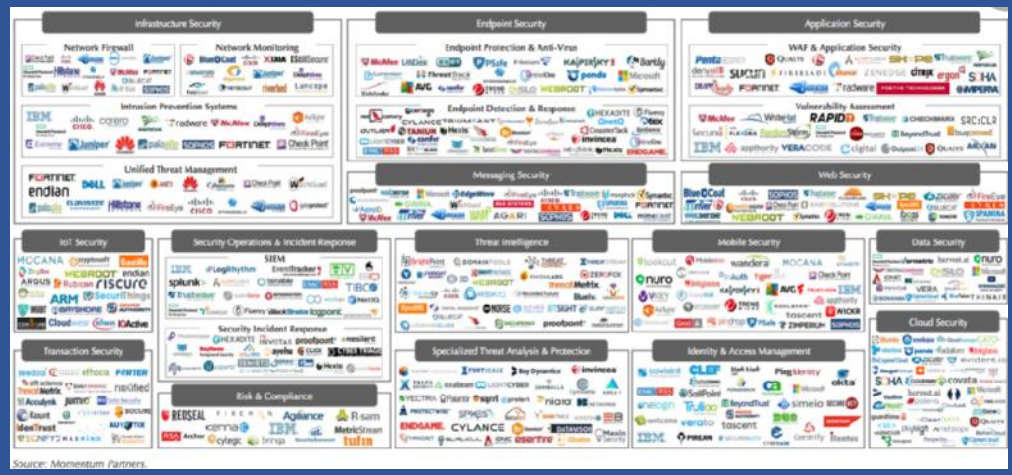
conclusion: go forward with solutions that make a difference

Take a Giant Step Forward in the Cyber Security Journey





Businesses Must Understand Technology and NOT be Driven by Technology – Focus on the *Problems at Hand*



Mis-Aligned
Overwhelming
Undigestible
Incompatible
Incomplete
Too Complex
Burn-out
Unmanageable
Unnecessary
Redundant

Organization Wide, Organization Deep

Silent Breach

Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

thank you