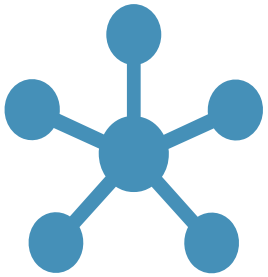
# CYBER WARS – CYBER SECURITY STRATEGIES IN THE DIGITAL INSURANCE LANDSCAPE

IAC Conference 2024:Cancun, Mexico

# KEY TOPICS

- Changing Risk Landscape
- “Fun” Facts
- A View from the C-Suite
- Changing Threat Actors
- State of Cyber Crime
- AI and Evolving Threats
- Key Philosophies – Healthy Paranoia
- Impact on Cyber Insurance
- Key Takeaways

# THE RISK LANDSCAPE IS EVER CHANGING



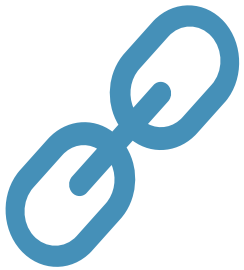
## Digitization

The push to digitize business processes has expanded the attack surface that must be defended.

## Privacy

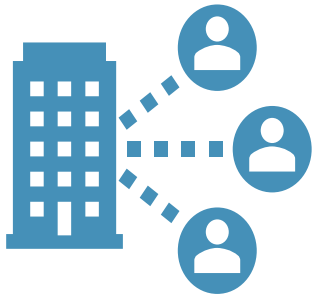
New rules recognize the rights of data subjects as data owners.

Specific rights include access, correction, portability, erasure, consent, and appeal.



## Vendors and Partners

Cyber security risks posed by otherwise trusted vendors who provide a wide array of services to the Enterprise.



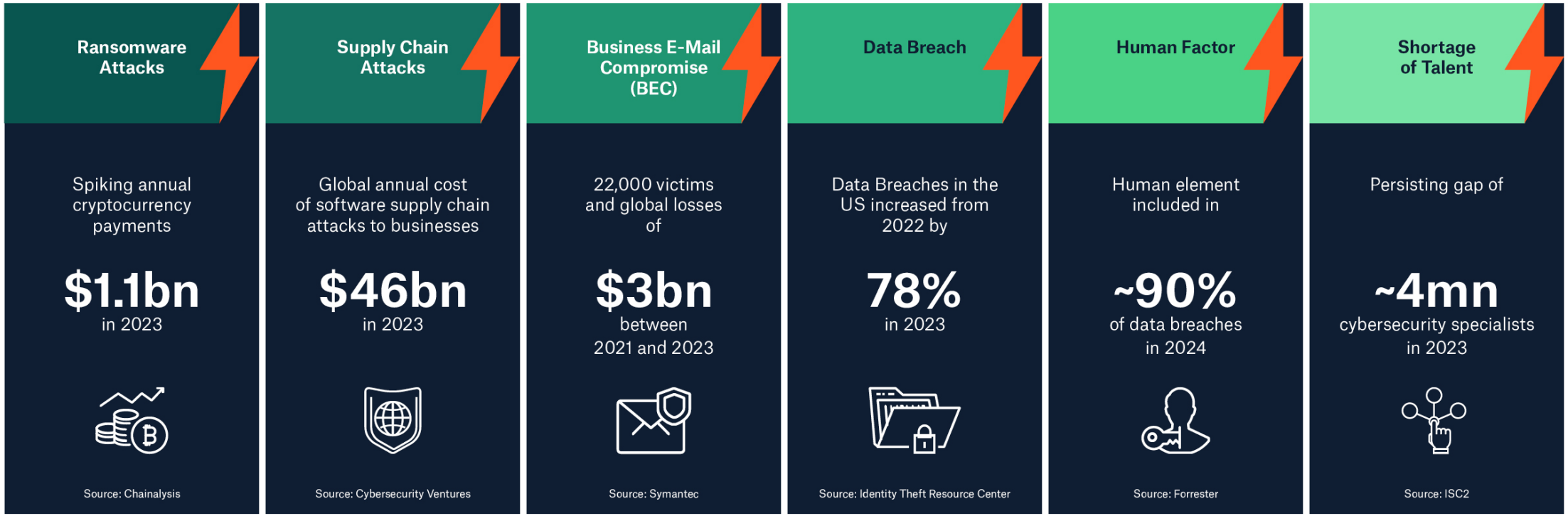
## Remote Work

The shift to working offsite has expanded the challenge to effectively defend systems, operations, as well as the workforce from both intentional and unintentional acts.

## AI

Adoption of AI creates new areas of Risk. Attackers' use of AI enhances existing attacks and provides new methods that must be defended.

# FUN FACTS: CYBER ATTACKS AND SOURCES OF RISK




https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html

# A VIEW FROM THE C-SUITE

- Munich Re estimates that global cyber insurance premiums in 2023 were approximately US$14 billion, with projections soaring to approximately US$29 billion by 2027.
- In April 2024, Munich Re published findings from their 3rd annual survey which analyzed responses from > 7,500 participants from 15 countries across various sectors.
- Despite heightened awareness to cyber security risks, 87% of all C-level respondents reported that their company is not adequately protected against cyber attacks.
- Organizations must balance the increasing relevance of AI, cloud services, and data analytics across industries with business risk.
  - Technological advancements also bring heightened vulnerabilities and potential security gaps.
  - These necessitate new proactive measures to safeguard against cyber threats.

# CHANGING THREAT ACTORS

## Early Day Threat Actors

- Early on, hacking had little to do with financial gain. Motivated by a desire to learn and explore, the term "hacker" was a badge of honor.
- In the ’80s, the profile of a hacker begins to evolve from a heroic figure to a young coder who is hacking into big institutions. Motive was bragging rights.
- By the ‘90s, hackers were heralded as being super-smart and could hack into almost anything within a remarkably brief time. Hollywood hackers.

# CHANGING THREAT ACTORS

## Current Day Threat Actors

- Our world now demands constant connectivity. The attack surface has increased drastically; from cell phones to smart devices, we are always online both professionally and personally.
- The new main motives are money and the advancement of political and/or personal agendas.
- No longer simply driven by curiosity, hackers are now operating on advanced AI enabled technology.
- The modern-day hacker is a collection of organized criminals, state sponsored hackers, cyber terrorists, and hacktivists.

# THE STATE OF CYBERCRIME

- The cybercrime underground economy is a diverse but interrelated ecosystem where nearly every criminal business is both a producer and a consumer . . . they leverage solutions provided by others and offer solutions in the marketplace as well.
- The industry is mature and operates on principles similar to legitimate businesses
  - Competitive advantage, profitability, and market share
- It operates with all the attributes of traditional businesses
  - Markets and exchanges
  - Specialist operators
  - Outsourcing service providers
  - Integrated supply chains, etc.
- Narrow point solutions as well as comprehensive solutions are available for sale
- Even the most basic criminal business utilizes several different tools or services . . . and all are readily purchased on the black market.

# INTRODUCING FRAUD GPT

- Similar to the ethical marketplace, AI has found its way into the development of malware or malicious tools. Large Language Models (LLMs) are well-suited to social engineering hacks.
- Criminals use GPT-based technology to craft scam scripts and scale up production on phishing campaigns, correct spelling and grammar mistakes, etc.
- Benefits include the ability to convey key elements such as a sense of urgency and the ability to translate text in different languages.
  - This has opened new markets that were previously inaccessible because of language barriers.
- The dark web is offering millions of phishing email samples upon which to train your effort.
- There are >6,000 source code references for malware as well as automated scripts to replicate logs/cookies
- Code obfuscation and custom data sets based on your uploaded HTML sample
- Bot creation of virtual machines (VMs) and accounts . . . Licensed for 1 VM per month

https://www.privacyaffairs.com/dark-web-price-index-2023/

# FRAUD GPT THREATS

## Phishing

- Makes phishing attack stages easier, makes custom phishing emails accessible to more bad actors
- Research targets at scale with tailored messaging
- Grammar and spelling corrections

## Vishing

- Makes voice spoofing much more effective as fraudsters make calls to phish for information

## Smishing

- Allows for more tailored SMS-based phishing campaigns that are also easier to deploy

Deep fake videos, photographs, and voices add credibility to BEC/BCC attacks and fraud

# KEY PHILOSOPHIES FOR CYBERSECURITY

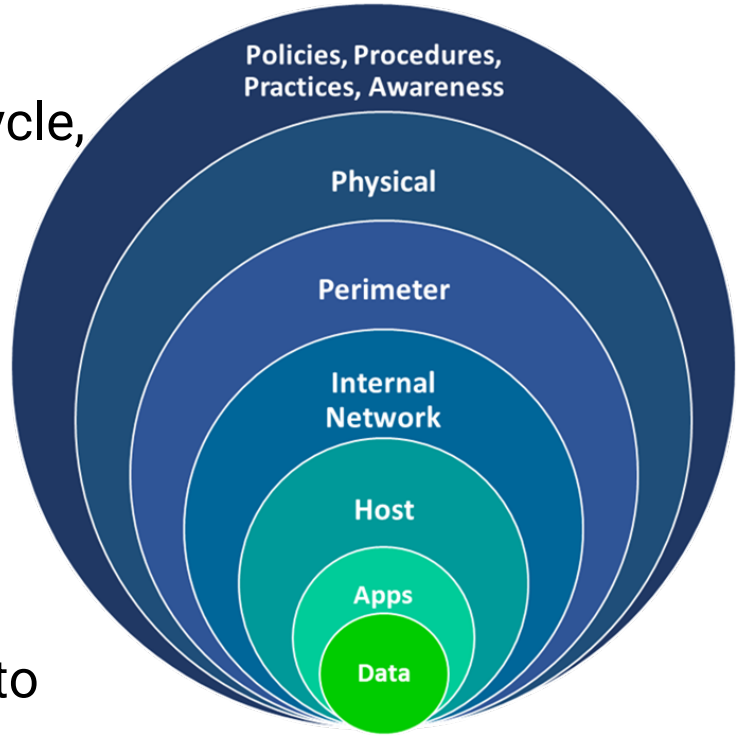
**Healthy Paranoia**

- Apply a Defense in Depth approach to reduce risk by relying on multiple overlapping controls
- Continuous testing to adjust defenses based on prevailing attack vectors and techniques
- Attack simulations test efficacy of existing tools against emerging threats and identify solutions to address gaps that emerge
- Security awareness training, advisories, and tech tips allow end users to become part of the solution
- Embedding security and privacy concepts into your software development life cycle
- Enhanced vendor onboarding to enhance overall security posture
- Vigilance, measurement, and continuous improvement promote a virtuous cycle

"Success breeds complacency. Complacency breeds failure. Only the paranoid survive." - Andy Grove

# DEFENSE IN DEPTH

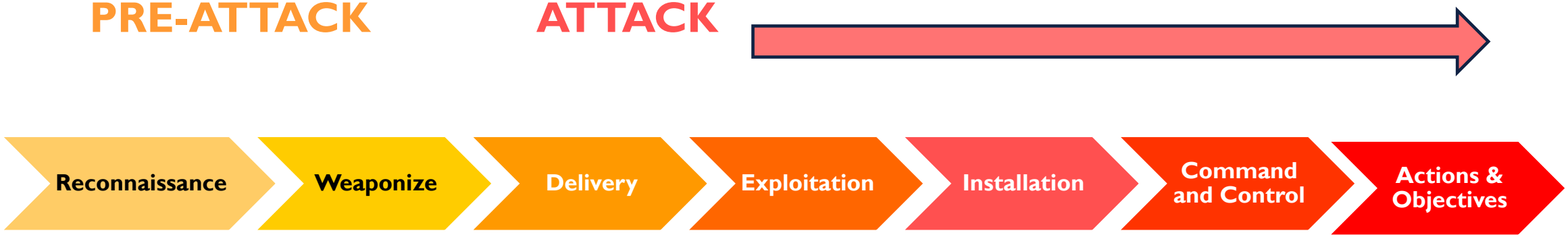
- Employ a layered security approach designed to reduce risk across your organization by relying on multiple overlapping controls.
- Controls are aimed at stopping attacks at all stages in the attack life cycle, from the point of initial compromise to that of data exfiltration.
- Design strives to protect data relating to customers, prospects, partners, and financial performance regardless of an adversary's knowledge regarding your deployment landscape.
- Continuous testing should be conducted regularly to tweak defenses.
- Attack simulations should be performed to test the efficacy of existing tools against emerging threats and identifying technological solutions to address gaps.
- Conduct "tabletop" exercises throughout the year to practice responses should a major cyber event occur.  Exercises must mimic real world events that have affected organizations across the globe.



# LAYERED SECURITY CONTROLS

**Diagram Reference: Lockheed Martin Cyber Kill Chain**

**PRE-ATTACK** **ATTACK**




- Motivation
- Preparation
- Listening

- Exploit Development
- Packaging
- Register look-a-like domain

- Mechanism of Delivery
- Infection Vector

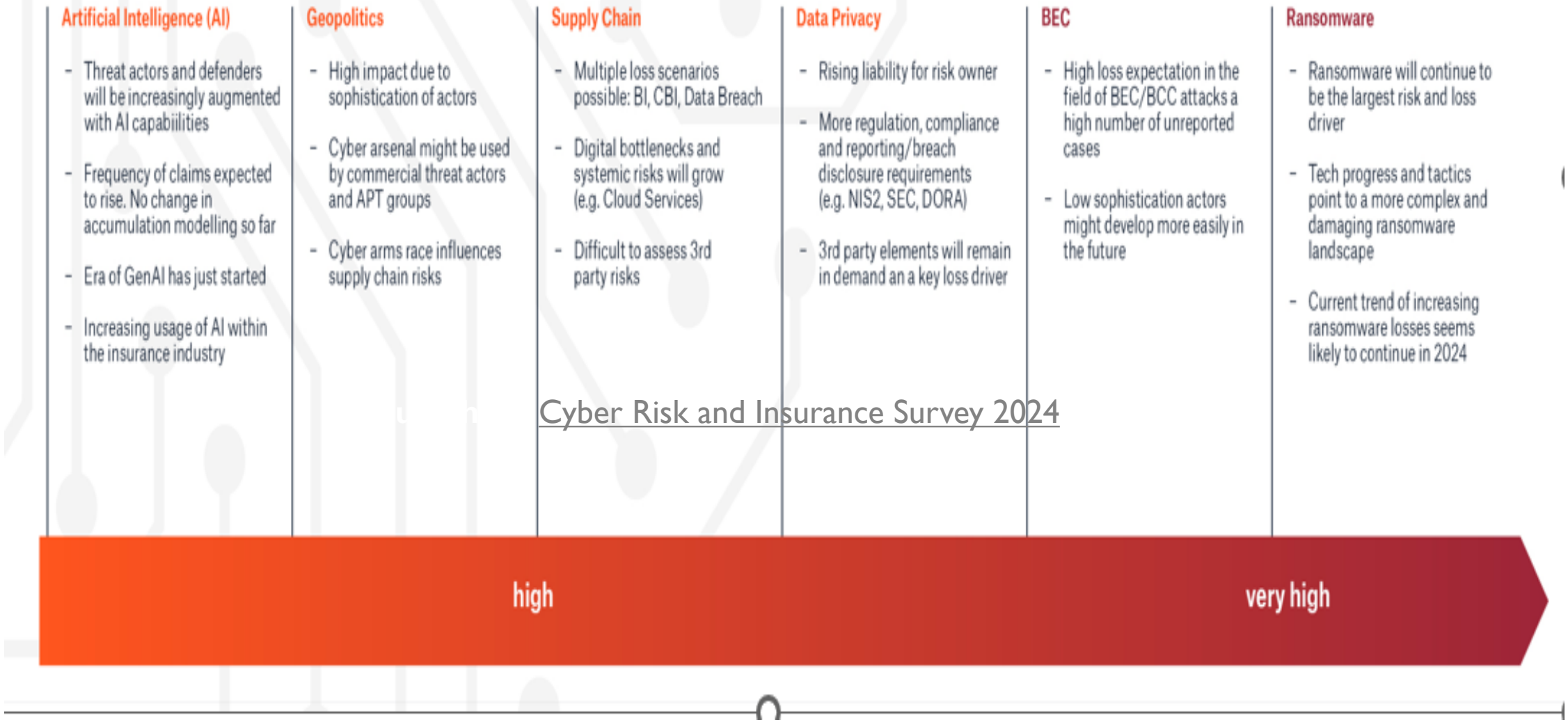
- Applications affected
- Method & Characteristics

- Persistence
- Characteristics of change
- Acquiring additional components

- Communication between victim & adversary

- Action by adversary once they have control

# IMPACT ON CYBER INSURANCE




Cyber Risk and Insurance Survey 2024

Source: Munich Re Global Cyber Risk and Insurance Survey, April 2024

# IN CLOSING

## Key Takeaways

- All other things being equal, threat actors will choose the more vulnerable target to attack.
- Threat actors develop capabilities and change their attack vectors to take the least difficult approach to their target.
- Exploitation of Zero Day vulnerabilities are on the rise

- Track industry trends; this can assist in understanding attack vector changes and inform protective mitigation strategies.
- Apply a Defense in Depth approach with overlapping defenses.
- Create the ability to disrupt an attack across attack stages.
- Patch, Patch, Patch - Vulnerable technology is susceptible to attack.
- Drive social engineering awareness; it remains a leading technique to acquire initial access . . . Train your workforce and partners.

# THANK YOU