withum

MAY 6, 2026

Cyber Breach Trends: Anatomy of a Cyberattack

POWER IN THE PLUS™

WE ARE AN INDEPENDENT MEMBER OF

HLB

THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

Today's Presenter

Edward Keck, Jr., CISSP

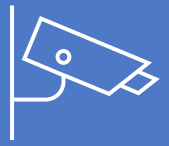
Partner, Practice Leader, Cyber and Information Security Services

Office: 973-867-7447

ekeck@withum.com

Current Trends

Shifting Threats



Moving from highly regulated industries to perceived easier targets

More industries are finding themselves under new regulations or federal “guidance”

Larger corporations have hardened defenses

Startups and mid-size organizations can be just as productive for hackers

All businesses are treasure trove of personal information

Nation state activity continues to expand

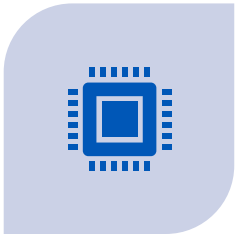
The newest twist….Artificial Intelligence

I asked AI to create a graphic of hackers leveraging AI to create cyber attacks. This is the graphic designed based on my prompt.

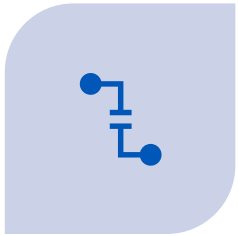
I then asked a different AI large language model to tell me how threat actors are using AI in attacks. Here is what AI shared with me:

•**Crafting convincing scams:** AI can analyze massive amounts of data on people, including social media profiles and leaked information. This allows hackers to craft phishing emails, messages, and even chatbots that appear to be from someone you know, making them much more believable.
•**Generating undetectable malware:** AI can be used to develop malware that can change its behavior to evade traditional security measures. This makes it much harder for antivirus software to detect and block the malware.
•**Launching automated attacks:** Hackers can use AI to automate tasks in cyber attacks, making them much faster and more widespread. This allows them to target a large number of victims in a short period of time.
•**Cracking passwords:** AI-powered tools can be used to analyze password patterns and predict combinations much faster than ever before. This can help hackers crack passwords and gain access to accounts.
•**Finding and exploiting vulnerabilities:** AI can be used to scan large networks for weaknesses and vulnerabilities that hackers can exploit. This can help them find new ways to break into systems.

Emerging Trends and Future Challenges



ARTIFICIAL INTELLIGENCE IN ATTACKS AND DEFENSE: BOTH ATTACKERS AND DEFENDERS ARE DEPLOYING AI TO AUTOMATE TASKS, IDENTIFY PATTERNS, AND BYPASS TRADITIONAL SECURITY CONTROLS.



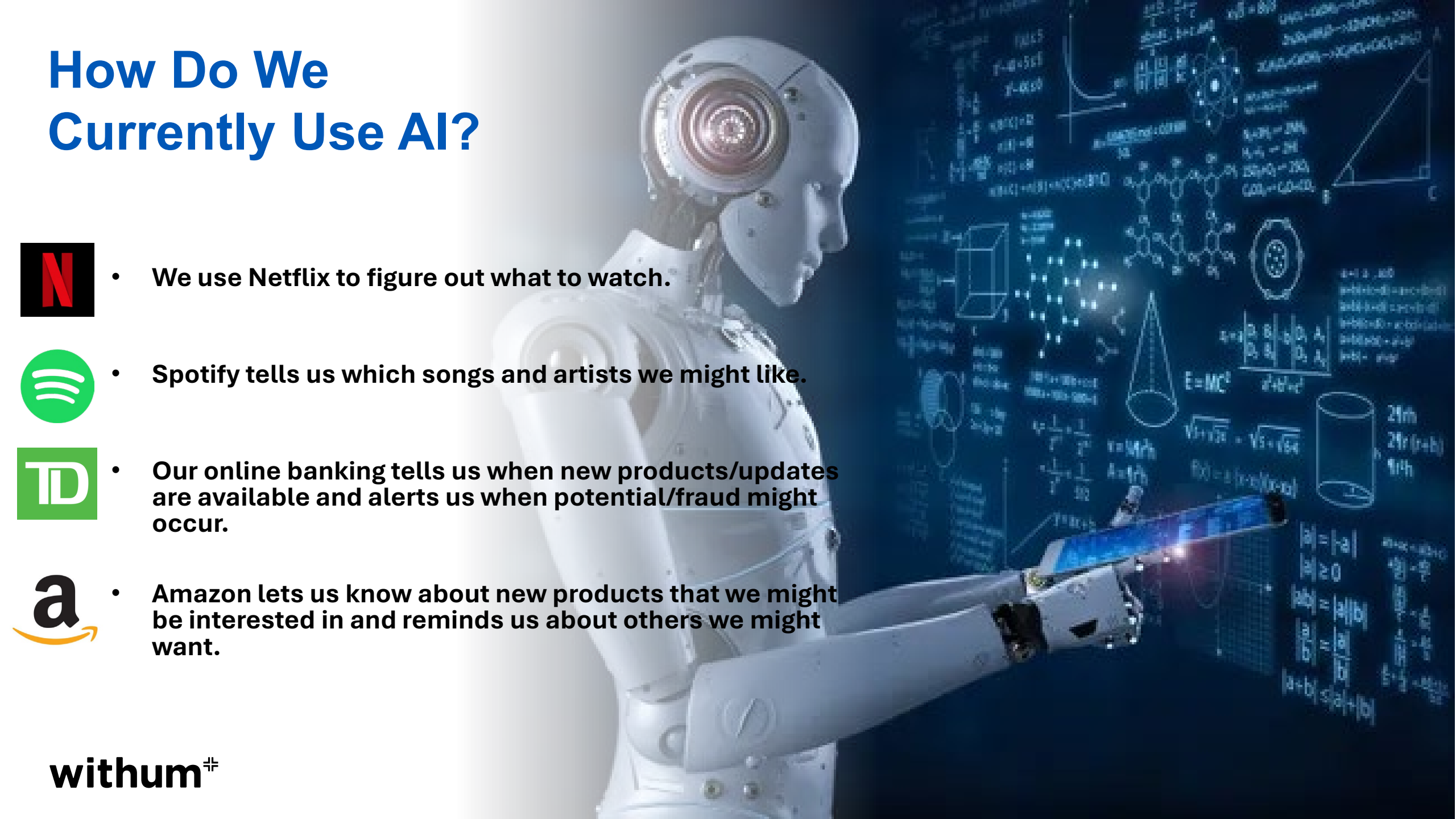
TARGETING OF CRITICAL INFRASTRUCTURE: ENERGY GRIDS, HEALTHCARE SYSTEMS, AND TRANSPORTATION NETWORKS FACE INCREASING THREAT LEVELS FROM SOPHISTICATED ACTORS.

DEEPFAKES AND DISINFORMATION: ADVANCES IN SYNTHETIC MEDIA MAKE IT EASIER TO SPREAD FALSE INFORMATION AND CONDUCT SOCIAL ENGINEERING CAMPAIGNS.

QUANTUM COMPUTING: THE RISE OF QUANTUM TECHNOLOGIES MAY RENDER CURRENT ENCRYPTION OBSOLETE, PRESENTING NEW CHALLENGES FOR CYBERSECURITY (GOOGLE'S SYCAMORE/WILLOW VS TRADITIONAL SUPERCOMPUTER-EL CAPITAN FROM HP).

PRIVACY CONCERNS: THE BALANCE BETWEEN SECURITY AND PERSONAL PRIVACY IS UNDER CONSTANT NEGOTIATION AS SURVEILLANCE TECHNOLOGIES BECOME MORE PERVASIVE.

How Do We Currently Use AI?



- We use Netflix to figure out what to watch.
- Spotify tells us which songs and artists we might like.
- Our online banking tells us when new products/updates are available and alerts us when potential/fraud might occur.
- Amazon lets us know about new products that we might be interested in and reminds us about others we might want.

withum

Modern Threat Landscape

Modern Threat Landscape…

+ **AI / Deepfake:** AI deepfake cyberattacks use artificial intelligence to create hyper-realistic, fabricated videos, images, or audio designed to impersonate individuals for malicious purposes like fraud, identity theft, and sophisticated social engineering attacks.

+ **Malware and Ransomware:** Malware remains a foundational threat, encompassing viruses, worms, trojans, spyware, and adware. Ransomware attacks encrypt victims' data and demand payment for its release, often targeting businesses, healthcare providers, and municipalities.

+ **Phishing and Social Engineering:** Phishing is among the most successful and pervasive attack methods, leveraging deception to trick users into revealing credentials, downloading malware, or transferring funds. Social engineering techniques exploit human psychology and trust rather than technical vulnerabilities, making them difficult to defend against with technical solutions alone. Spear phishing, wherein attackers craft highly customized messages for specific targets, poses a significant risk to executives and high-profile individuals.

+ **Advanced Persistent Threats (APTs):** Advanced Persistent Threats represent a class of attacks often associated with nation-state actors or organized criminal groups. These adversaries use sophisticated tools and tactics to infiltrate networks, maintain access over extended periods, and extract sensitive data or disrupt operations.

Modern Threat Landscape…

- **Supply Chain Attacks:** One of the most insidious recent developments is the rise of supply chain attacks. By compromising software providers or trusted vendors, attackers can infiltrate multiple organizations simultaneously. The 2020 SolarWinds hack exemplifies the dangers of this approach, as malicious code inserted into legitimate updates propagated to thousands of customers, including government agencies and Fortune 500 companies.

- **IoT and Cloud Vulnerabilities:** The proliferation of Internet of Things (IoT) devices and the migration to cloud services have expanded attack surfaces. IoT devices, often deployed with minimal security, can be hijacked for use in botnets, surveillance, or as entry points into more secure networks. Similarly, cloud misconfigurations and weak access controls are frequently exploited to steal data or disrupt services.

- **Insider Threats:** Not all threats come from external actors. Insider threats, malicious, negligent, or compromised employees, can cause significant damage. Whether motivated by financial gain, ideology, or coercion, insiders may steal sensitive information, sabotage systems, or enable external attacks. Detecting and mitigating insider threats requires a blend of technical controls and robust organizational policies.

- **Distributed Denial of Service (DDoS) Attacks:** DDoS attacks aim to overwhelm systems with traffic, rendering websites, applications, or even entire networks unusable. Though not typically used to steal data, DDoS attacks can disrupt business operations, damage reputations, and serve as a smokescreen for more targeted intrusions.

46% of all Cyber Attacks are aimed Small-Medium Sized Business.

85% of all Email Attachments are Harmful.

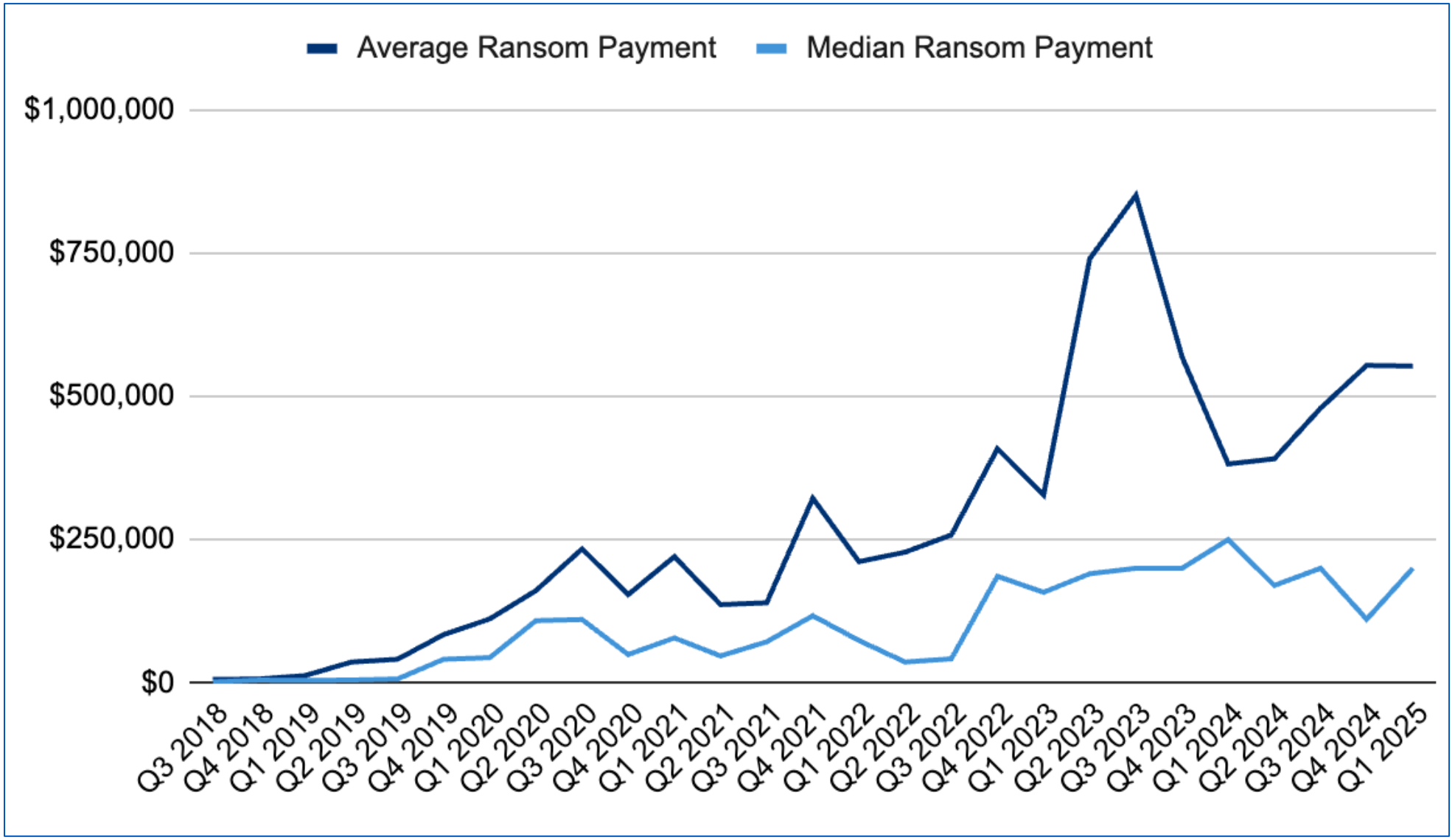
91% of Attacks are launched from Phishing.

Cyber Crime will cost 20 Trillion in 2026.

60% of Businesses close permanently following a Ransomware Attack.

A Business is hit with a Ransomware Attack every 11.5 seconds.

Ransom Payments by Quarter



Average Ransom Payment

$552,777

-0.2% from Q4 2024

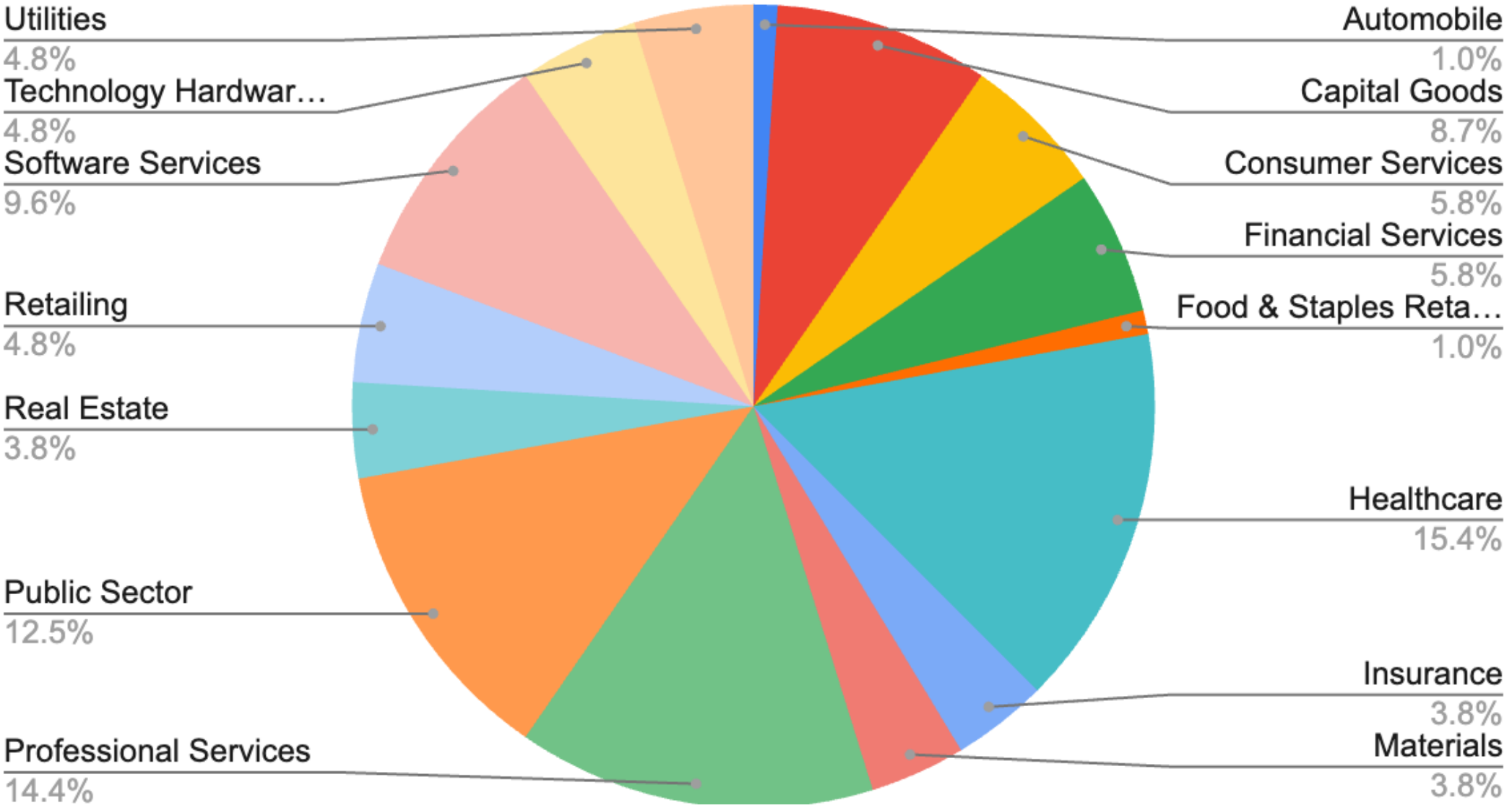
Median Ransom Payment

$200,000

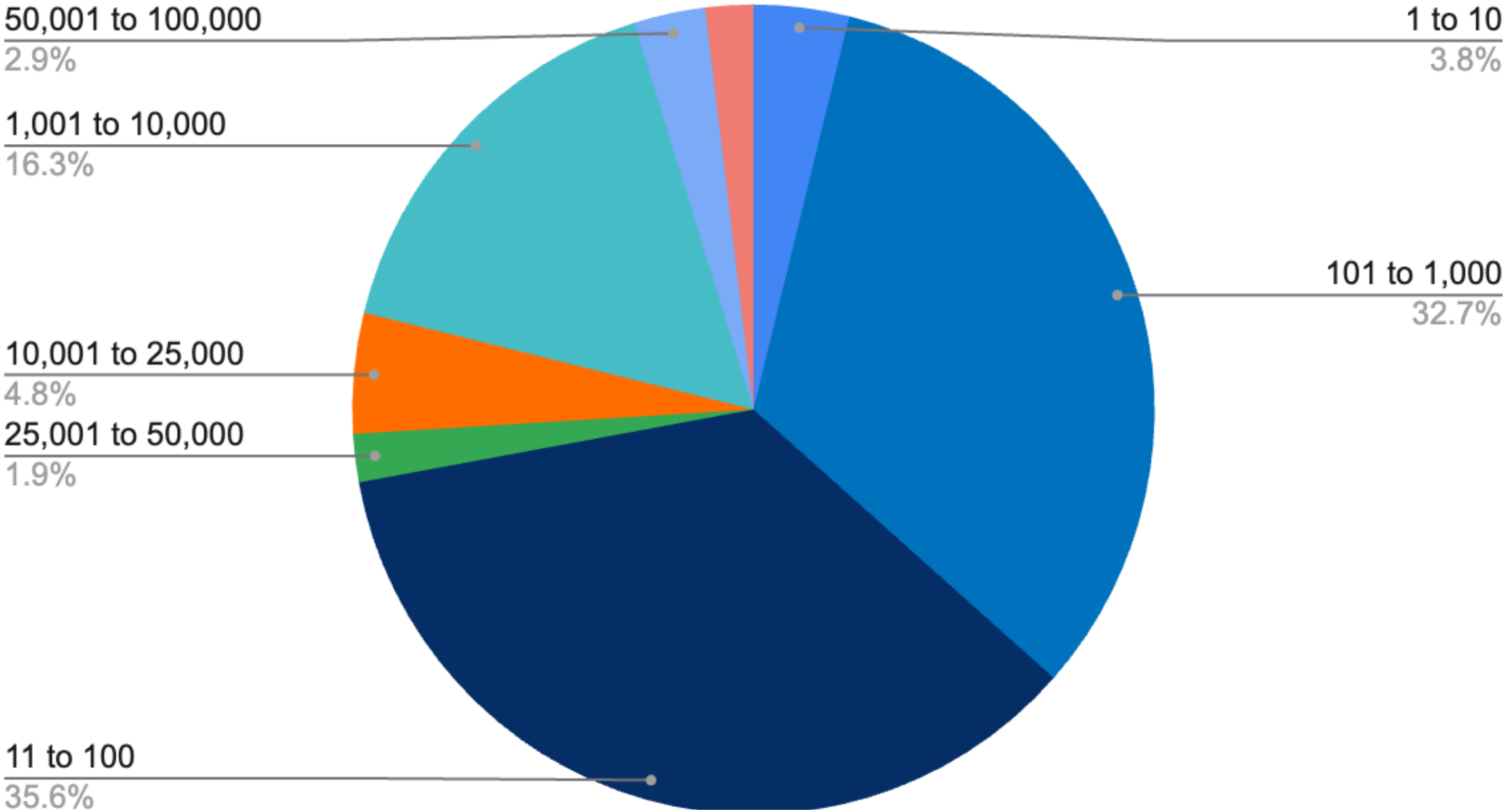
+80% from Q4 2024

withum

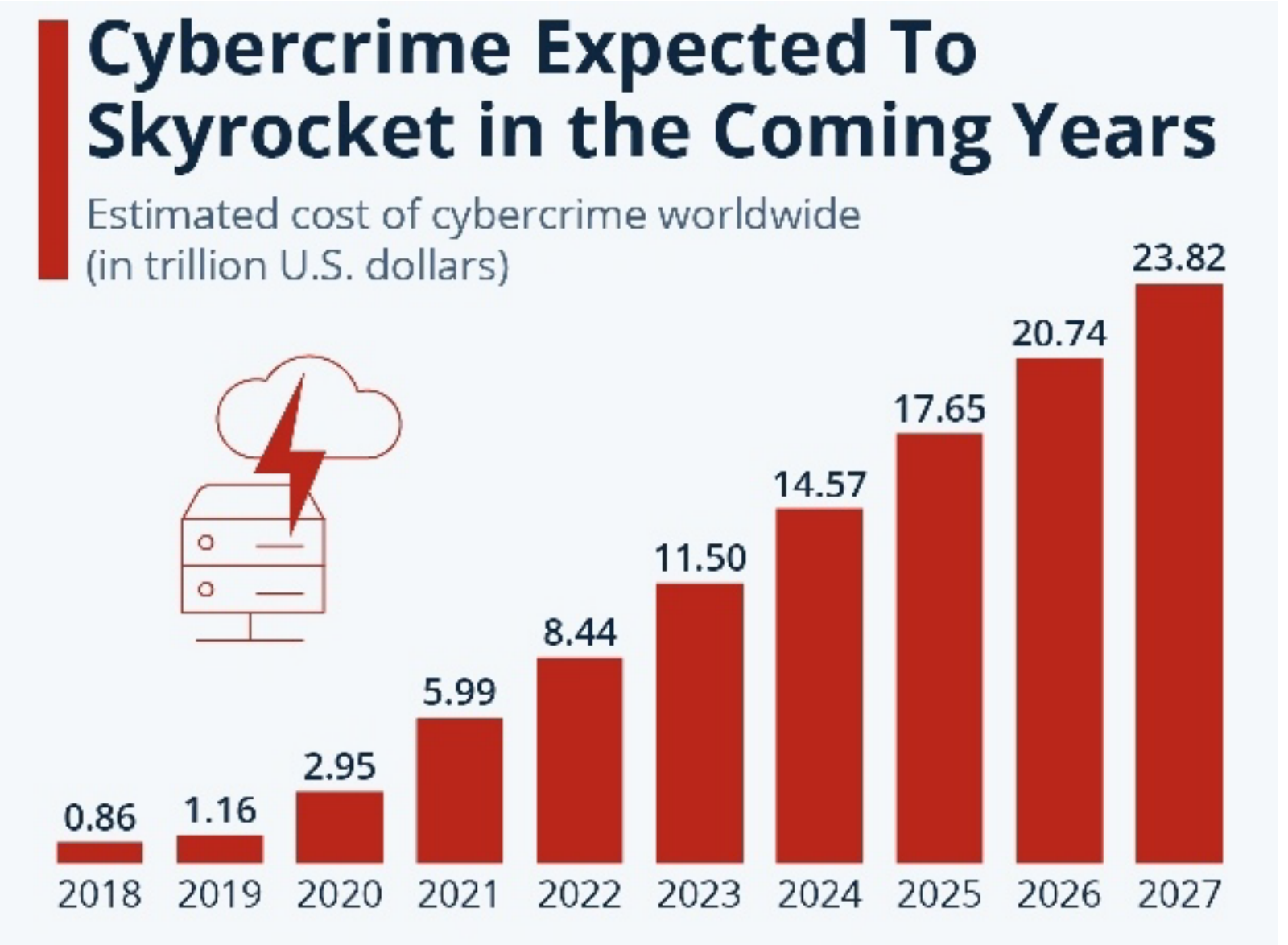
Industries Impacted by Ransomware



Ransomware Business Impact by Size



The Cost of Cyber-Crime

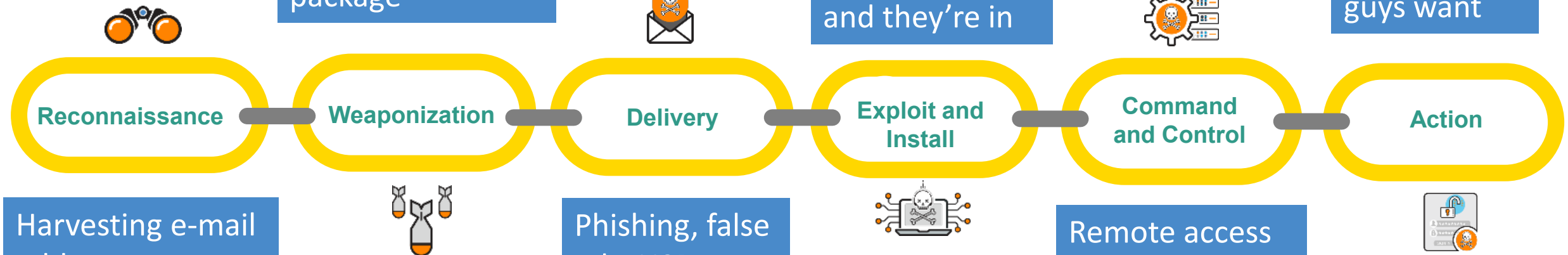


Cyberattack Stages

STAGES OF A CYBERATTACK

- **Reconnaissance:** Attackers conduct research for weeks or months, mapping an organization's digital footprint and seeking points of entry. OSINT (Open-Source Intelligence) and social engineering are especially prevalent in this phase (Social Media / Public Records).
- **Initial Compromise:** The first "crack" in the armor often comes through phishing or exploiting unpatched software. Understanding these vectors is vital to prevention.
- **Establishing a Foothold**: Once inside, attackers deploy malware, sometimes remaining undetected for months.
- **Escalation and Lateral Movement:** With a foothold, adversaries escalate privileges and move laterally to access more sensitive systems.
- **Actions on Objectives:** Attackers pursue their goals - be it theft, disruption, or destruction. Exfiltration of data or deployment of ransomware often marks the climax of an attack.

Cyberattack Chain…



Harvesting e-mail addresses, LinkedIn, Website, etc

Taking Exploits + backdoors to build package

Phishing, false ads, USB, Hacking, and more

Unpatched systems, clicked links, and they're in

Remote access through malware to allow the bad guys to drive

Whatever goal the bad guys want

Early Warning Signs

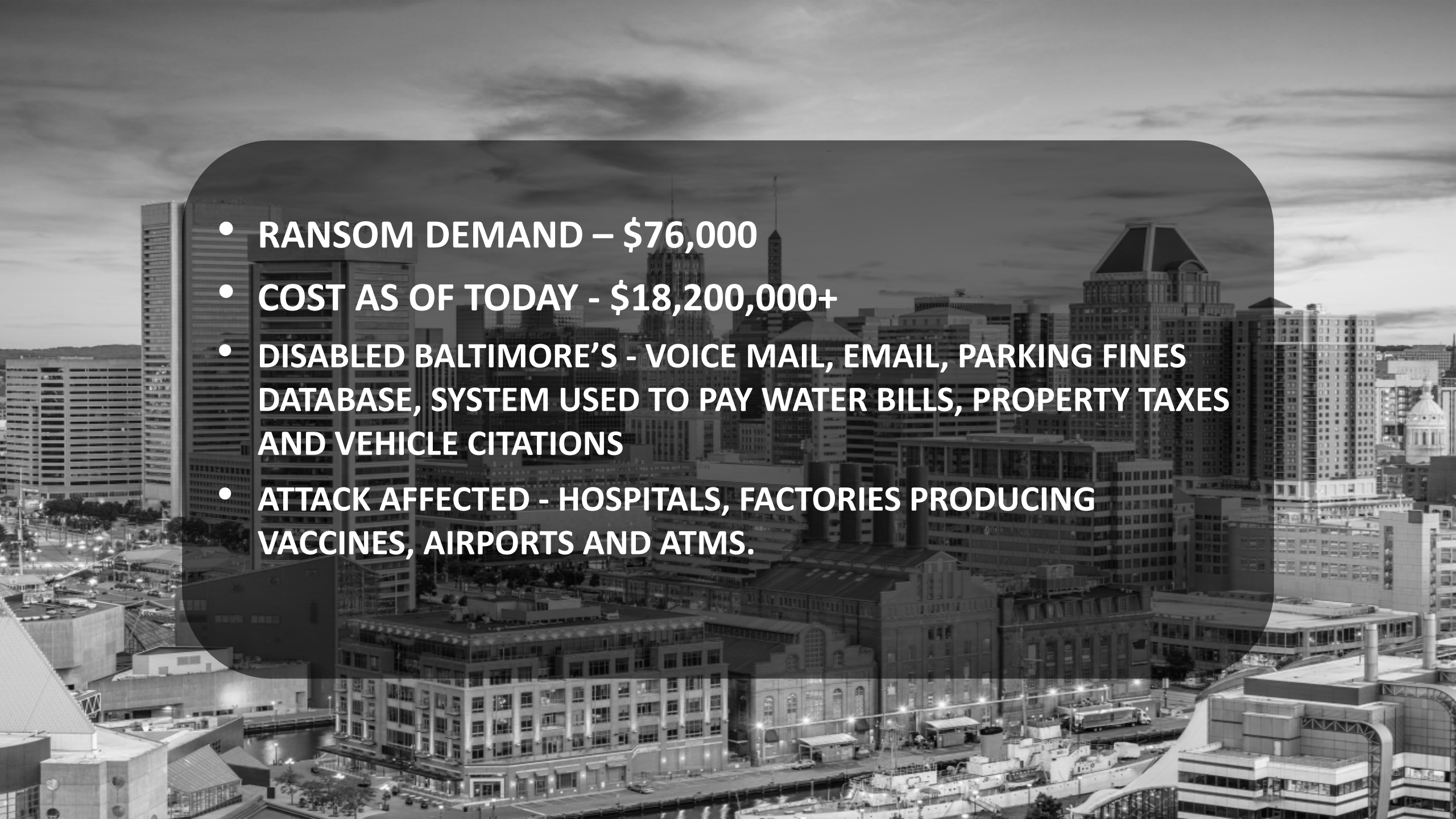
- Unusual login activity, such as logins at odd hours or from unexpected locations.
- Sudden spikes in network traffic or unexplained bandwidth usage.
- Frequent system crashes, slowdowns, or unexpected reboots.
- Appearance of unfamiliar software, processes, or toolbars on devices.
- Files that become inaccessible, disappear, or are unexpectedly encrypted.
- Unauthorized changes to system settings, configurations, or user accounts.
- Unexplained outgoing communications, including emails or data transfers.
- Multiple failed login attempts or account lockouts.
- Alerts from security software or intrusion detection systems.
- Unexpected pop-ups, warnings, or demands for ransom (ransomware).
- Disabled antivirus or firewall protection without authorized action.
- Unusual activity in system logs, such as unfamiliar IP addresses or access patterns.
- External contacts reporting receipt of suspicious emails or communications from your accounts.
- Discovery of known malware or suspicious files during routine scans.
- Unexplained changes in file sizes, timestamps, or metadata.

Case Studies

The Atlanta Ransomware Attack


Ransom Ask - $52,000
City Paid - $2,700,000
Paid Another - $9,500,000
Total Investment - $12,200,000
Annual It Budget - $35,000,000
7 years of police dash-cam video lost
-CBS reports 21 million was-
actually spent on data recovery


BALTIMORE



- RANSOM DEMAND – $76,000
- COST AS OF TODAY - $18,200,000+
- DISABLED BALTIMORE'S - VOICE MAIL, EMAIL, PARKING FINES DATABASE, SYSTEM USED TO PAY WATER BILLS, PROPERTY TAXES AND VEHICLE CITATIONS
- ATTACK AFFECTED - HOSPITALS, FACTORIES PRODUCING VACCINES, AIRPORTS AND ATMS.

Ransomware Crippled Police & Fire Department Servers –Police Dept Loses 10 months of Work to Ransomware – Infected a Second Time within a month

Very Recent…

- On October 20, 2025, AWS experienced an outage caused by internal networking issues in the US-EAST-1 region, which is a major hub for its data centers. The problem involved failures in the Domain Name System (DNS) and an underlying subsystem for monitoring network load balancers. This led to many services that rely on AWS, such as Snapchat, Reddit, and Venmo, being unable to connect to their data for several hours, even though the data itself was stored safely.
- On August 31, 2025, a cyberattack on Jaguar Land Rover (JLR) forced the company to shut down its global production, costing tens of millions of pounds daily and impacting the entire supply chain. The breach, which is speculated to have been ransomware, resulted in the theft of company data. The attack led to widespread factory closures in the UK, Slovakia, India, and Brazil, and prompted the company to focus on restoring its IT systems.
  - **Data Compromise**: The company eventually confirmed that sensitive customer and company data was compromised during the breach.
  - **Claim of Responsibility:** A group called "Scattered Lapsus$ Hunters" claimed responsibility for the attack, which combined elements of the **Scattered Spider**, Lapsus$, and ShinyHunters hacking groups.

Defending Against Cyberattacks

How Can I Protect My Organization?

- Install all security updates within 2 weeks of their release (ideally this would be 1 week of release)
  - This includes computers, servers, firewalls, and other network devices
  - If you can automate this task by using a third party software that pushes out approved updates, this is even better
- Provide risk-based cybersecurity training for all of your employees
  - Recommendation is at least quarterly (monthly is even better)
- Use Multi-Factor Authentication….everywhere
- Back your data up daily and store it offline
- Implement the practice of least privilege
- Have a cybersecurity expert you can seek for advice. This can often take the form of a virtual CISO (vCISO) that serves as a consultant for your team. Listen to them and take their advice seriously.

What Should I Do if My Organization is a Victim of Ransomware?

- Make sure you have a team of professionals in place to assist you. It will be more difficult to vet and hire professionals during a crisis
- Have a communication plan in place
- Have an Incident Response Plan and practice it
- Make every effort to NOT pay the ransom
- After the root cause of the ransomware has been determined and the incident has been contained:
  - Reformat all impacted systems
  - Restore your data from secure/clean backups
  - Following your reporting requirements (stakeholders, law enforcement, regulators, etc)

Cyber Insurance

How to obtain cyber insurance?

First understand the requirements

- Have a written Information Security Program
- Use Multi-Factor Authentication
- Use industry standard endpoint protection
- Perform regular backups that are testing and stored offline
- Have a patch management program
- Encrypt your data (at rest and in transit)
- Perform a risk assessment
- Provide security awareness training to all employees

Cyber insurance

After you have the previous items in place, then contact an insurance broker to get you quotes from various carriers.

Make sure that coverage is adequate to cover you in the event of an incident

Coverage is being limited

- Under $1m likely approval
- Over $1m required full underwriting review

Insurers are requiring proof of implemented controls

- Don’t overstate your controls on your application. Insurance carriers will verify the controls are in place if an event happens and could deny coverage if they are not fully implemented (there are current cases that support this)

Information Security Policies

- First, why do you even need policies?
  - A Written Information Security Program defines every aspect of your organization's information security posture
  - They clearly outline expectations as it relates to information security
  - It is a requirement to obtain cyber insurance (but don't do this to simply check a box)
  - Without a formal Written Information Security Program, you end up doing one of two things:
    - Completely ignore cybersecurity and hope it won't impact your organization
    - You are blindly throwing darts at cybersecurity hoping that you will hit something that protects your organization (you might get lucky, but most likely will not)

Third Party Vendor Management

- Third Party Vendor Management Policy
  - This is one of the most important and often neglected policies
  - This policy defines your organization's oversight of all third party vendors, your risk assessment of each vendor and your ongoing management of each vendor and understanding of their information security posture
  - You will want to specify minimum contract provisions for these vendors

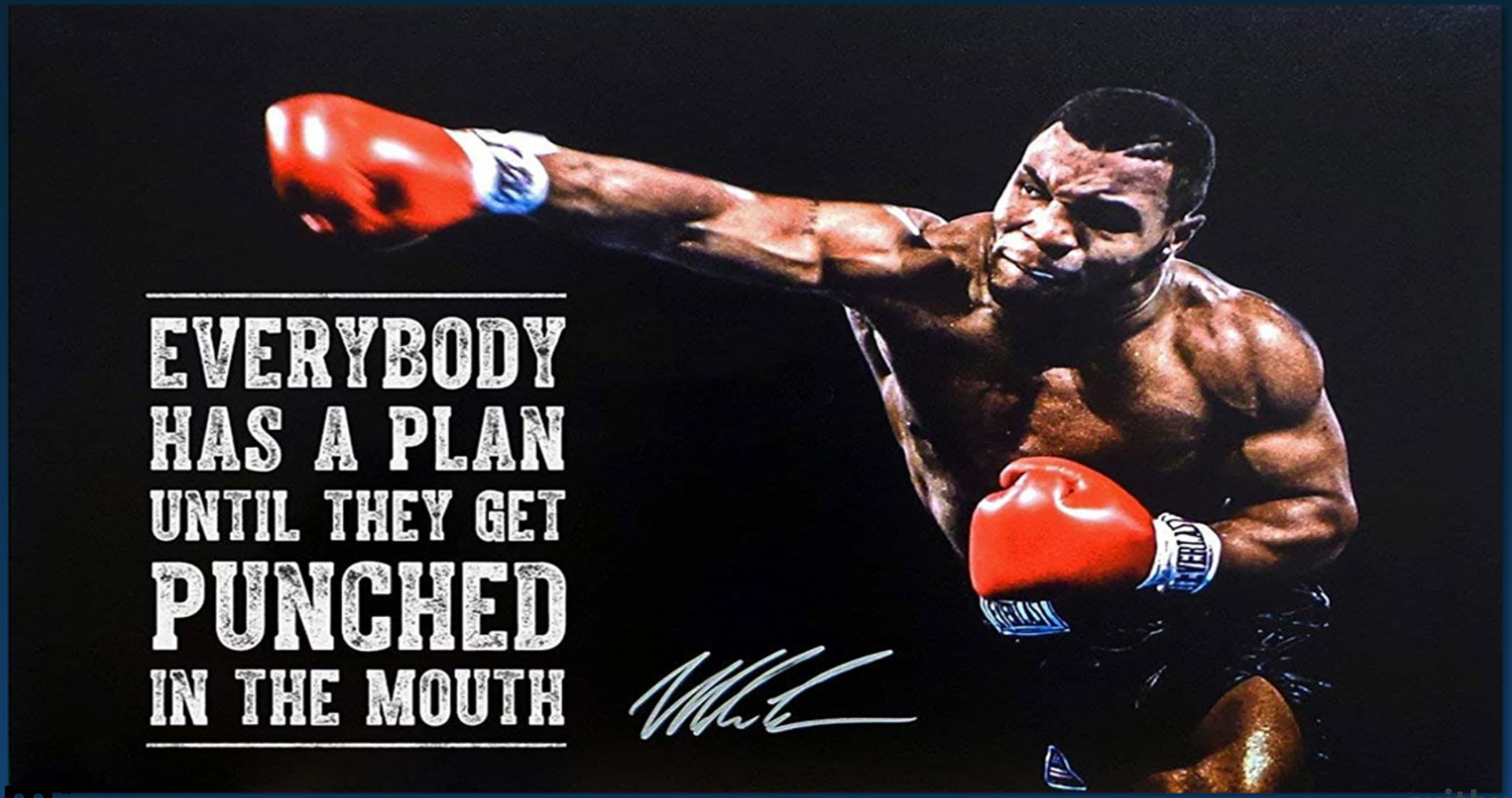
Cybersecurity Isn’t Just for Businesses

- Phishing emails
- Identity Theft
- Email spoofing
- Cyber stalking

Cybersecurity Best Practices

- Strong Passwords
- Patch your systems
- Use caution with email
- Encrypt your hard drive
- Use quality endpoint protection
- Use multifactor authentication whenever possible (especially with financial based transactions)

Test Your Cybersecurity Plan



Next Steps...

- ✓ Create a culture of security.
- ✓ Engage a trusted cyber partner that understands your business.
- ✓ Independently assess your cyber program.
- ✓ Practice good cyber hygiene
- ✓ Educate employees (Targeted training where needed)
- ✓ Have a plan and practice.
- ✓ Obtain/maintain the appropriate level of cyber insurance

Questions

Free DarkWeb Scan for our event attendees.