FEI San Antonio Chapter: The State of Cybersecurity 2024

Positioning for the changing landscape of cyber risk

David M. Collins

CISSP, vCISO

Summary of experience

Dave brings over 35 years of IT, governance, risk, security/privacy and compliance experience and consultation services to a variety of businesses and industries. His areas of focus include financial, insurance, retail and health care. Dave has worked with organizations from small businesses to Fortune 25 companies.

A former chief information security officer (CISO)/director in the private sector, Dave presently delivers advice and consultation regarding IT and Organizational risk management, information security and privacy controls, as well as governance and compliance requirements and initiatives. Additionally, he is engaged as part of the office of the virtual CISO (vCISO), helping clients build and enhance their overall IT security programs and posture.

Professional affiliations and credentials

HITRUST certified CSF practitioner	**Certified Virtual Chief Information Security Officer (CvCISO, lvl 2)**	**Certified information systems security professional (CISSP)**
Information Systems Audit and Control Association member	**InfraGard member**	**UNIX administration certificate**

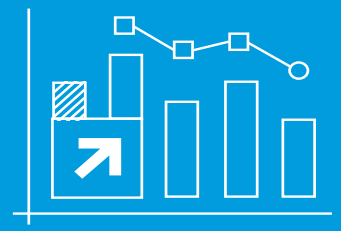
David M. Collins

CISSP, vCISO

Dave.collins@rsmus.com

https://www.linkedin.com/in/dmcollins

Cyber risk by the numbers



Recent cyberattacks from the headlines

OpenAI	Atlassian	Progress Software (MoveIt)	MGM	AT&T
Advanced persistent threat	*Technology stack and supply chain*	*Technology stack and supply chain*	*Ransomware*	*Malicious Actor on a 3rd Party Platform*
A Bug in ChatGPT's open-source library results in leak of personal data of customers	Data breach relating to staff and company facilities and potential exposure of its customers' data	Data breach and service takeover exposed company and personal data of tens of millions of individuals	Names, driver's licenses, and financial account information stolen and held for ransom; hotels operations also locked down	Records of communications during May 1 to Oct. 31, 2022, including the other phone numbers a wireless number interacted with as well as call duration

Causes of Recent cyberattacks from the headlines

OpenAI	Atlassian	Progress Software (MoveIt)	MGM	AT&T
Advanced persistent threat	*Technology stack and supply chain*	*Technology stack and supply chain*	*Ransomware*	*Malicious Actor on a 3rd Party Platform*
INSECURE CODE DEVELOPMENT	INSECURE CODE DEVELOPMENT	INSECURE CODE DEVELOPMENT	SOCIAL ENGINEERING	3rd PARTY SECURITY VULNERABILITY

2023 cyberattacks by the numbers

Frequency of malware

More than [1]

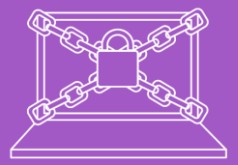
450,000

new malware programs are detected daily

Frequency of phishing emails

3.4 billion

phishing emails are sent everyday totaling 1.2% of all email traffic[2]



Average downtime from ransomware

20+ days

of average system downtime and business interruption from a ransomware attack[3]

Average cost of a breach

Global average cost in 2023 of

$4.45MM

an increase of 15% over the last 3 years[4]

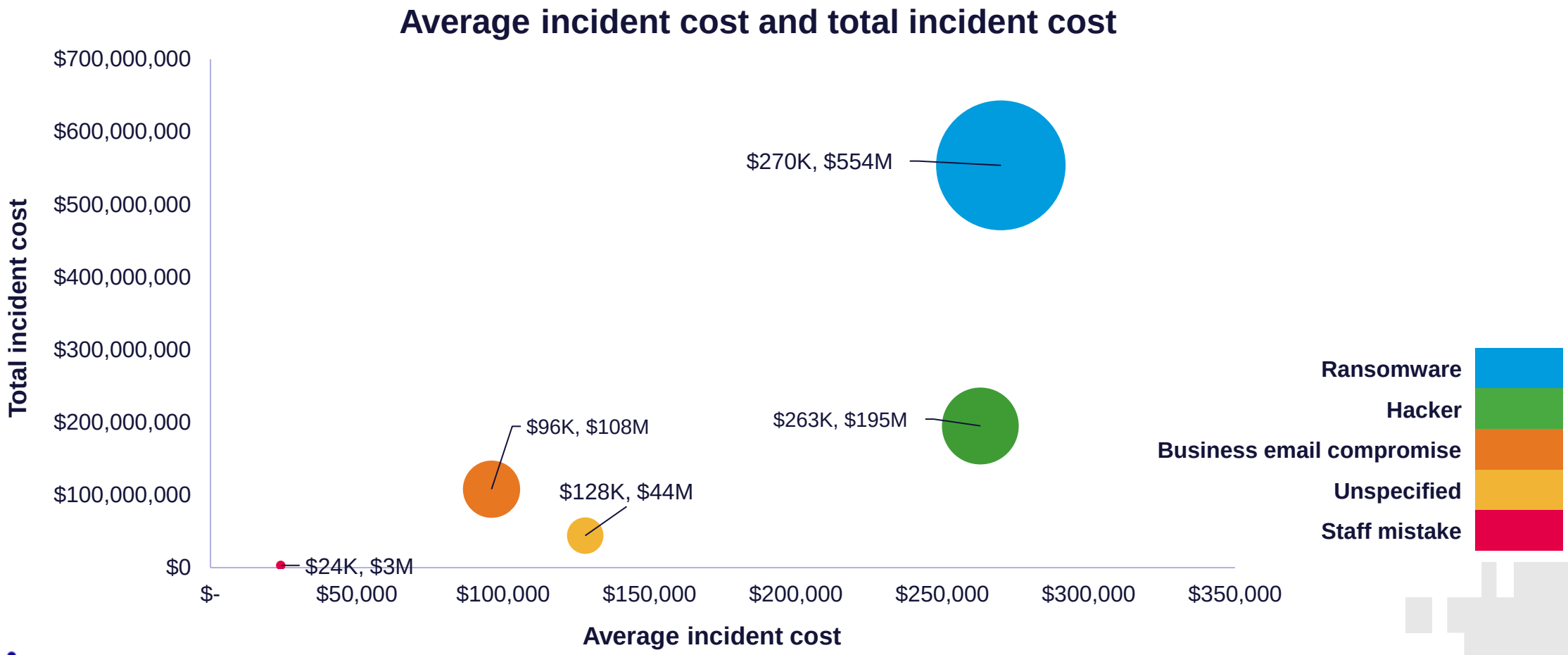
Key trends in the cybersecurity landscape

According to the RSM Middle Market Business Index 2024 cybersecurity report:

- **Significant cybersecurity concerns persist**: 28% of middle market executives claimed their company experienced a data breach last year. (Up from 20% in 2023)
- **Breaches are on the rise:** smaller middle market companies rose to 20% from 12% a year ago, and those at their larger counterparts were up to 37%, compared to 28%.
- **Security is still understaffed:** more than 60% of respondents have two or fewer data security and privacy employees.
- **Technology is changing**: 55% of organizations have moved to the cloud in the past year due to security concerns, up from 50% last year.
- **Cyber liability coverage is also changing:** 76% (68% in 2023) of companies carry a cyber insurance policy, and 70% say premium costs have increased.

Average and total cost by attack vector: 2017-2021

Small and Medium Businesses - SMB



NetDiligence®

2023 Cyber Claims Study

Source: https://rsmus.com/insights/services/risk-fraud-cybersecurity/the-cost-of-a-data-breach.html

Upcoming cybersecurity trends

Navigating the shifting cyber risk landscape

01

Impact of global economic headwinds

With high levels of uncertainty around inflation, challenges in the supply chain and shrinking profit margins, cyber leaders are being asked to do more with less

02

Growing complexity of cyber solution landscape

The Cybersecurity software industry is experiencing exponential growth resulting in an explosion of tools in the market; however, there are limited ways to assess solution value, overlap with existing solutions, and validate each is fully configured

03

Lack of board-level understanding of cyber-risk

While cyber more often has a seat at the table, boards of directors are challenged to put cyber-risk in context with business operations and its enterprise risks

04

Increasing gap in the cyber workforce market

The cyber workforce shortfall continues to grow, leaving millions of positions unfilled and an increasing fight for talent

05

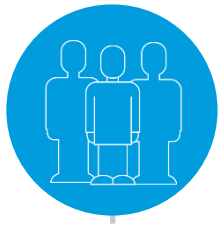
Minding the gap of shared responsibility

Vendors play an increasingly important role in cybersecurity (e.g., outsourcing and cloud) but there is a lack of understanding regarding the division of responsibilities

Preparing for the evolving trends of cybersecurity

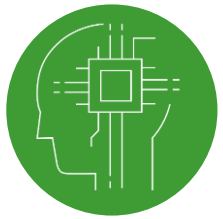
Identity is the new perimeter

Changing borders of the workplace and IT landscape have forced a shift from network boundaries to a focus on digital identity defenses



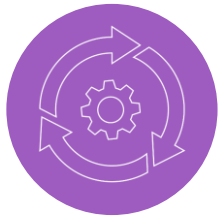
Tomorrow's cyber workforce is being built today

The war for talent is driving investments into internal staff development through both retooling and upskilling the workforce



Responsibility must align with "as a service"

Complex vendor ecosystem requires constant alignment and communications while also adapting to evolving technologies and regulatory needs



Automation will drive action over alerts

Automation will need to extend beyond detection and orchestration in order to drive decisioning in near real time

Data will fuel risk and opportunity in cyber

Data will serve as an increasingly valuable business and cyber asset but with tightening regulation and growing risk to organizations

Cyber service and platform markets will consolidate

Anticipate vendor convergence to expand core capabilities, drive margin, enhance interoperationality and unify disparate solutions

IDENTITY IS THE NEW PERIMETER

“If identity is the new perimeter, then Bob in accounting is the new Port 80”

- Richard Bird, former Ping identity leader [8]

WHAT DOES IT MEAN?

- Traditional cybersecurity approaches have focused on securing network perimeters
- Emphasis has now shifted to **protecting user identities** (e.g., customer, workforce, system) **and their devices as the primary line of defense**

WHY DOES IT MATTER?

- **Traditional perimeter is gone** as workers move remotely and IT moves to the cloud
- Over the past few years, the **majority of cyberattacks were mostly credential-based**
  - Eight out of 10 cybersecurity attacks occur with compromised credentials[6]
  - Over 1,200 password attacks every second; over 111 million per day[7]

HOW DO WE START TO ADDRESS IT?

- Inventory **who is accessing what, from where**
- **Start small with multifactor authentication (MFA)**; critical to stop attacks on credentials
- Build an **identity and access management (IAM) road map;** incrementally deploy across both use cases and key assets
- Assess and strategize future of **architecting with zero trust**

RSM

ACTION-ORIENTED AUTOMATION

When an attack is in progress, you have on average of one minute to detect it, 10 minutes to understand it and one hour to contain it. [11]

WHAT DOES IT MEAN?

- **Past automation focused on passive correlation** and alerting as well as streamlining workflows
- Solutions shouldn't just prevent or detect but they should **support response at the speed of the attack** in order to minimize its blast radius

WHY DOES IT MATTER?

- **Cyber attacks** are increasing in prevalence and complexity, **overloading analysts and bypassing preventative controls**
- **AI and machine learning** integrated with your cyber tools (e.g., EDR) **allow you to take immediate action** to tailored alerts while your team works on its formal response including:
  - Quarantine assets (e.g., ransomware)
  - Disable access to systems or accounts
  - Modify device configuration

HOW DO WE START TO ADDRESS IT?

- **Assess existing vendor landscape** for current capabilities; build incremental road map to deploy
- Document **what actions** you are willing to take **on what assets**
- Review use cases and fit of security solutions such as identity threat detection and response (ITDR), endpoint detection and response (EDR) and extended detection and response (XDR)

RSM

RESPONSIBILITY MUST ALIGN WITH "AS A SERVICE"

"Bottom line … you can outsource activities, but you don't want to outsource responsibility."

- Richard Freeman, Harvard economics professor [10]

WHAT DOES IT MEAN?

- **Critical IT, regulatory and cyber capabilities** are being increasingly **outsourced to third parties**
- **Security and compliance are assumed to be baked in** "as a service" resulting in potential for significant program gaps

WHY DOES IT MATTER?

- **Organizations are responsible for their data** and associated security events (e.g., Target breached via HVAC vendor)
- Growing digital supply chain has created increasing **ripple of vendor breach impacts** (e.g., SolarWinds, Kaseya)
- No standard responsibility matrix and many cloud contracts cannot be negotiated

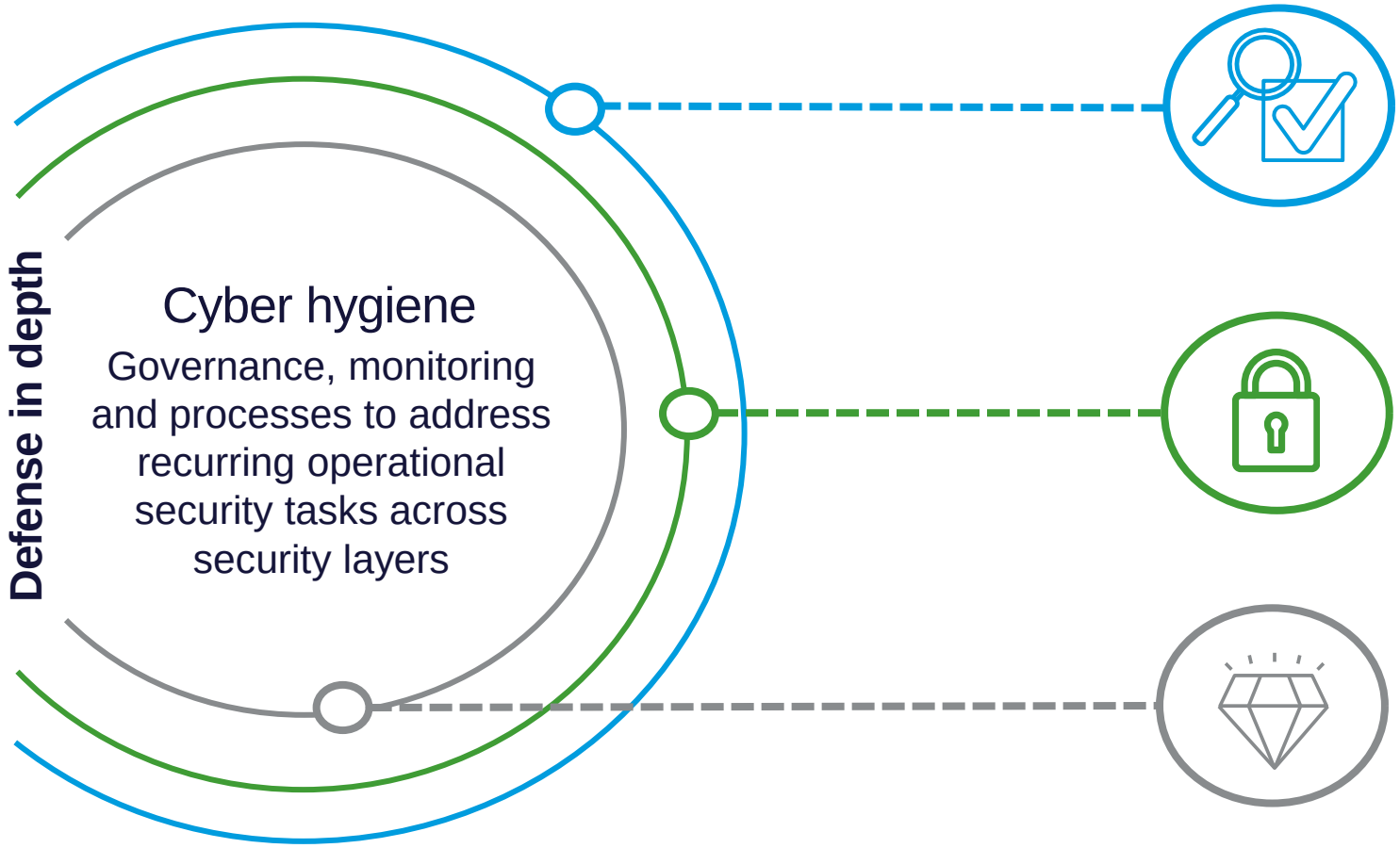
HOW DO WE ADDRESS THIS ISSUE?

- Formalize/mature your **vendor (risk) management program**
- Document vendor handoffs and contractual lines
- **Test as an integrated team** in tabletops and/or red teaming
- Hold vendors accountable; **develop and monitor KPIs/KRIs** against defined service-level agreements

RSM

While keeping a focus on addressing the basics

No matter where your IT lives, the basics don't change;
it requires constant discipline to address today's automated and financially motivated cyberattacks



Know your property

Build and maintain an inventory of all IT assets in order to implement and validate security coverage.

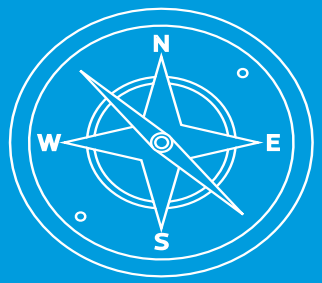
Lock your doors and get a good alarm

Deploy preventative controls across IT layers (e.g., network, laptops, applications). Build alerts to detect and respond to abnormal system behavior. Establish and test ability to quickly recover to business as usual.

Secure and insure your valuables

Identify your crown jewels (data/systems), prioritize their security and cover their value with cyber insurance.

Cyber landscape of the future



The role of transformative and emerging technology

Cyber leaders must balance securing their current IT landscape against economic headwinds while also enabling the organization to evaluate the new IT buzzwords that have the potential to revolutionize how and where companies deliver on their mission

Cloud

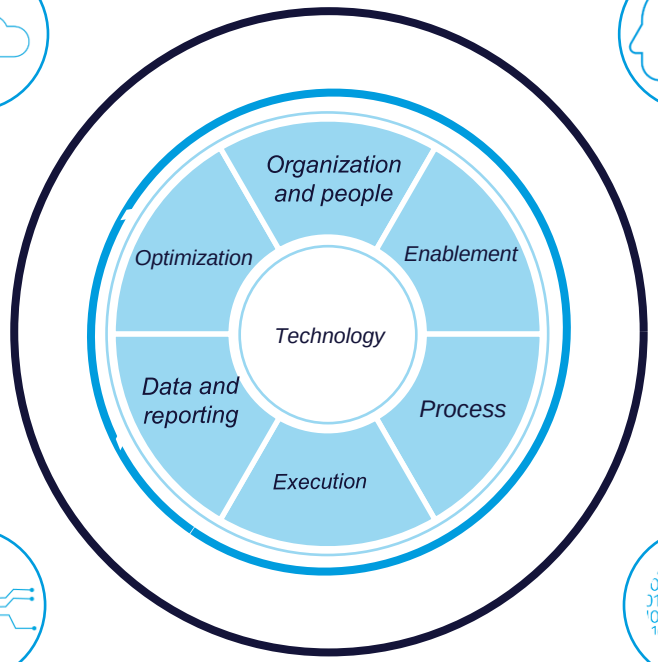
- Cloud-first has become business-as-usual with security needing to become in-line to keep pace

Blockchain

- Expanding use cases, such as digital contract, require cybersecurity to be embedded in these products up front

Generative AI and machine learning

- Users expect that AI will be a daily part of their productivity
- Cyber criminals have adopted large language models to advance attacks



Metaverse and augmented reality

- Metaverse adoption has been slow, but augmented reality devices and use cases continue to grow

Big data

- Expect expanded efforts toward improved usage of data balanced with privacy and other regulatory requirements

Quantum

- Once thought of as only “over the horizon,” quantum computing is now becoming a reality causing current state encryption to become obsolete

Converging with the increasingly complex compliance landscape

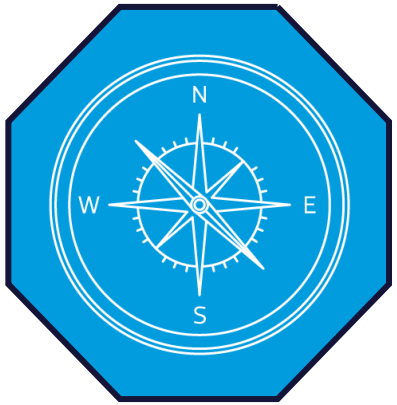
12 states now with data privacy laws and 7 more states in the pipeline*

** As of October 2023*

Release of White House national cybersecurity strategy

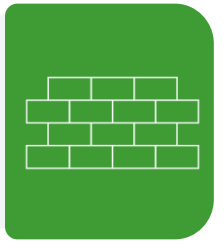
EU data protection board continues to issue major fines against U.S. companies

Enacted SEC rule for reporting of material cybersecurity incidents

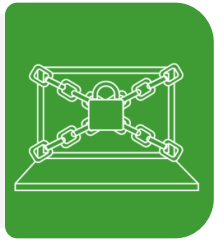


Major version change to NIST CSF controls framework

Federal government agency mandate for aligning to zero-trust standards



Expanded scope of organizations affected by FTC safeguards rule



New York proposes significant expansions to existing cyber regulations

References

[1] https://www.av-test.org/en/statistics/malware/

[2] https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

[2] https://www.zdnet.com/article/three-billion-phishing-emails-are-sent-every-day-but-one-change-could-make-life-much-harder-for-scammers/[2] 90+ Cyber Crime Statistics 2023: Cost, Industries & Trends (getastra.com)

[3] https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack-global/

[4] https://www.ibm.com/reports/data-breach

[5] *Source: Lockton Companies – For further information please contact Ashley Jones (abjones@lockton.com) at Lockton*

[6] https://www.mimecast.com/blog/the-rise-of-identity-based-attacks/

[7] https://www.microsoft.com/en-us/security/blog/2023/01/09/microsoft-entra-5-identity-priorities-for-2023

[8] https://www.forbes.com/sites/forbestechcouncil/2019/06/14/identity-is-not-the-new-cybersecurity-perimeter-its-the-very-core/?sh=1d7884603abb

[9] https://www.isc2.org/Research/Workforce-Study

[10] https://www.core-econ.org/the-economy/book/text/richard-freeman_you-cant-outsource-responsibility-transcript.html

[11] https://www.crowdstrike.com/resources/crowdcasts/the-1-10-60-minute-challenge-a-framework-for-stopping-breaches-faster/

[12] IDC's DataSphere and StorageSphere reports

[13] https://panaseer.com/reports-papers/report/2022-security-leaders-peer-report/

[14] https://www.forbes.com/sites/silberzahnjones/2016/03/15/without-an-opinion-youre-just-another-person-with-data/?sh=4b9d85e8699f

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING