WELCOME

Cyber Security Risk Management Symposium

February 13, 2025

Thank You to our Partners & Presenters

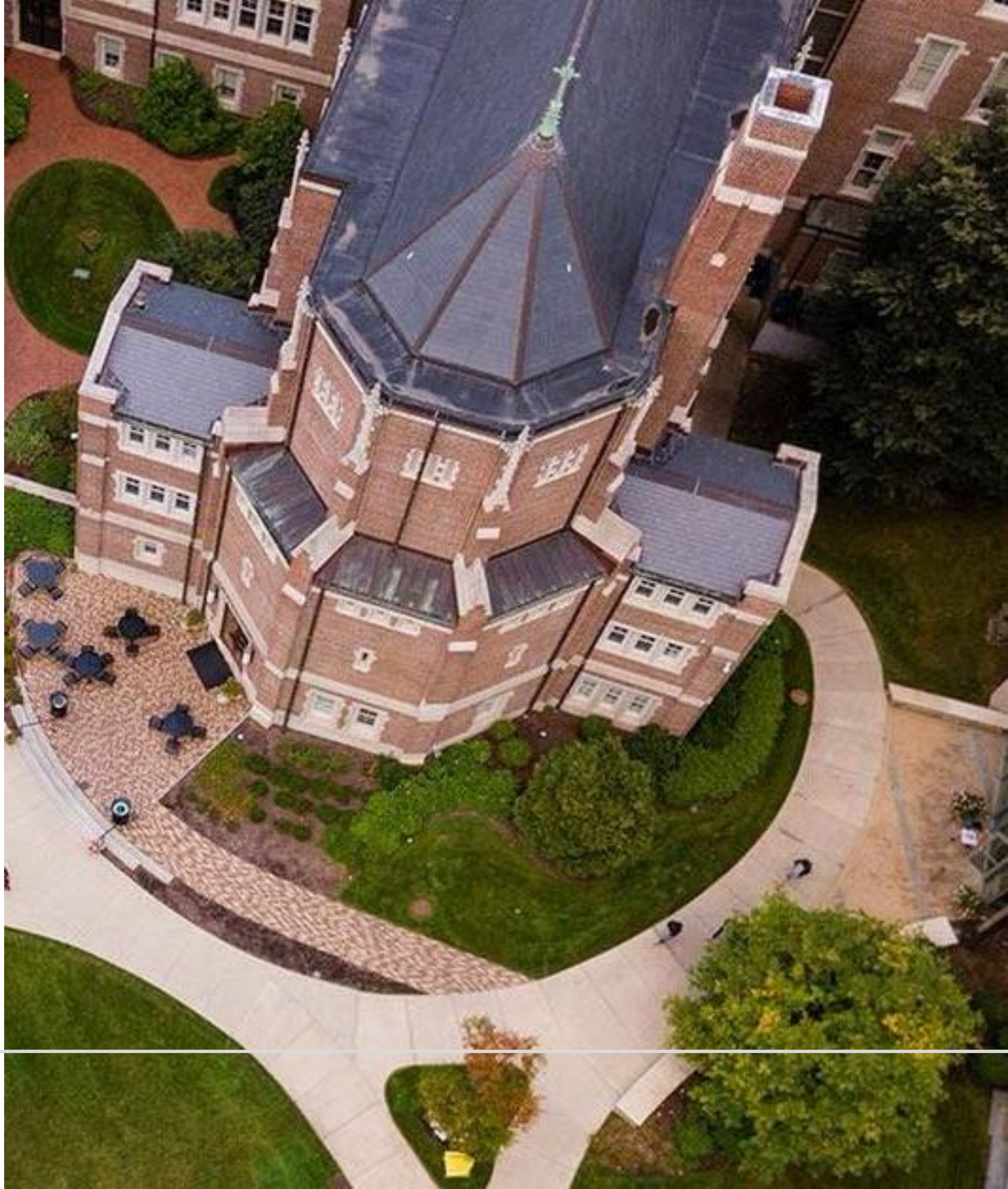
Colleges of the Fenway

Fred C. Church INSURANCE

EST. 1865

Robinson+Cole

beazley



Kathryn M. Rattigan

Partner

Katheryn advises clients on data privacy and security, cybersecurity, and compliance with related state and federal laws. She assists clients in assessing risks related to technology and software contracts, as well as with compliance-related issues with outsourcing and vendor management.

KEYNOTE

THE EVOLVING THREAT LANDSCAPE IN HIGHER EDUCATION

Robinson+Cole

Robinson+Cole

The Evolving Threat Landscape in Higher Education

Kathryn M. Rattigan

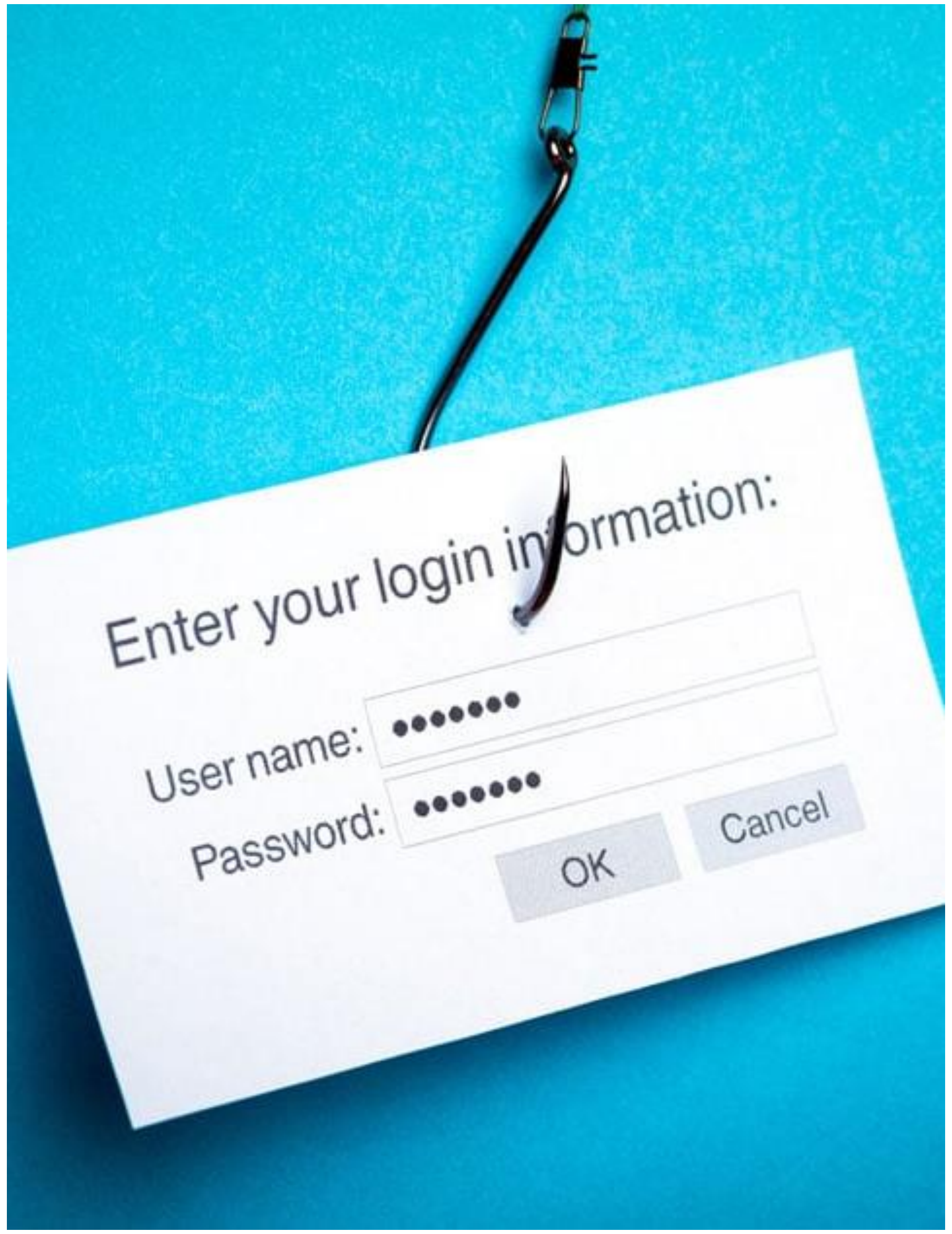
February 13, 2025

Introduction

Higher education institutions are susceptible to cyber risks because they manage large amounts of sensitive data, including student records, financial information, and intellectual property, making them attractive targets for cybercriminals seeking to exploit this data for identity theft, financial fraud, or competitive advantage; this includes personal information, research data, and financial records.

Common cyber threats to higher education institutions:

- Phishing attacks
- Ransomware attacks
- Malware infections
- Insider threats



But this is now. What does the future hold? **Let’s take a look**.

Security Incident Statistics in Higher Education

- Education was the third most targeted sector in Q2 of 2024
- Amounts to a 35% increase in attacks from 2023 to 2024
- Over 35% of attacks result from hacking or malware

Security Incident Statistics in Higher Education (cont'd)

- Unintended disclosers account for 30% of breaches, often due to human error or inadequate data handling practices
- Portable device loss accounts for 17% of breaches attributed to lost or stolen devices, securing portable devices is a critical concern

Security Incident Statistics in Higher Education (cont'd)

High attack volume:

Check Point research indicates the education sector is the most heavily attacked, with an average of 2,454 cyberattacks per organization weekly.

Ransomware prevalence:

Over 60% of higher education institutions reported ransomware attacks in the past year.

Attack methods:

Most attacks involve exploiting vulnerabilities, compromised credentials (like phishing), or malicious emails.

Security Incident Statistics in Higher Education (cont'd)

Backup targeting:

Nearly all adversaries attempt to compromise backups during cyberattacks on higher education institutions.

Security gaps:

A significant percentage of universities lack basic email security configurations and have open database ports.

Understaffing concerns:

Many higher education IT departments are understaffed, making it difficult to manage the volume and complexity of cyber threats.

The Future of Cyber Threats

AI, VR, analytics, hybrid learning, micro-credentials.

It’s easy to brush off these terms as buzzwords, but staying “in the know” about tech innovations is vital to protecting your organization.

- More than 86% of organizations expect to increase their implementation of new and frontier technologies by 2028.
- To ensure students are prepared for their future careers, higher education institutions must keep up with the seemingly breakneck pace of technological advances.

But what are the risks associated with these new technologies?

Generative AI -The New Frontier in Education

Khanmigo, built by nonprofit Khan Academy, is a top-rated AI for education. Save time on prep, tackle homework challenges, and get personalized tutoring.

Let’s take a look:

Generative AI

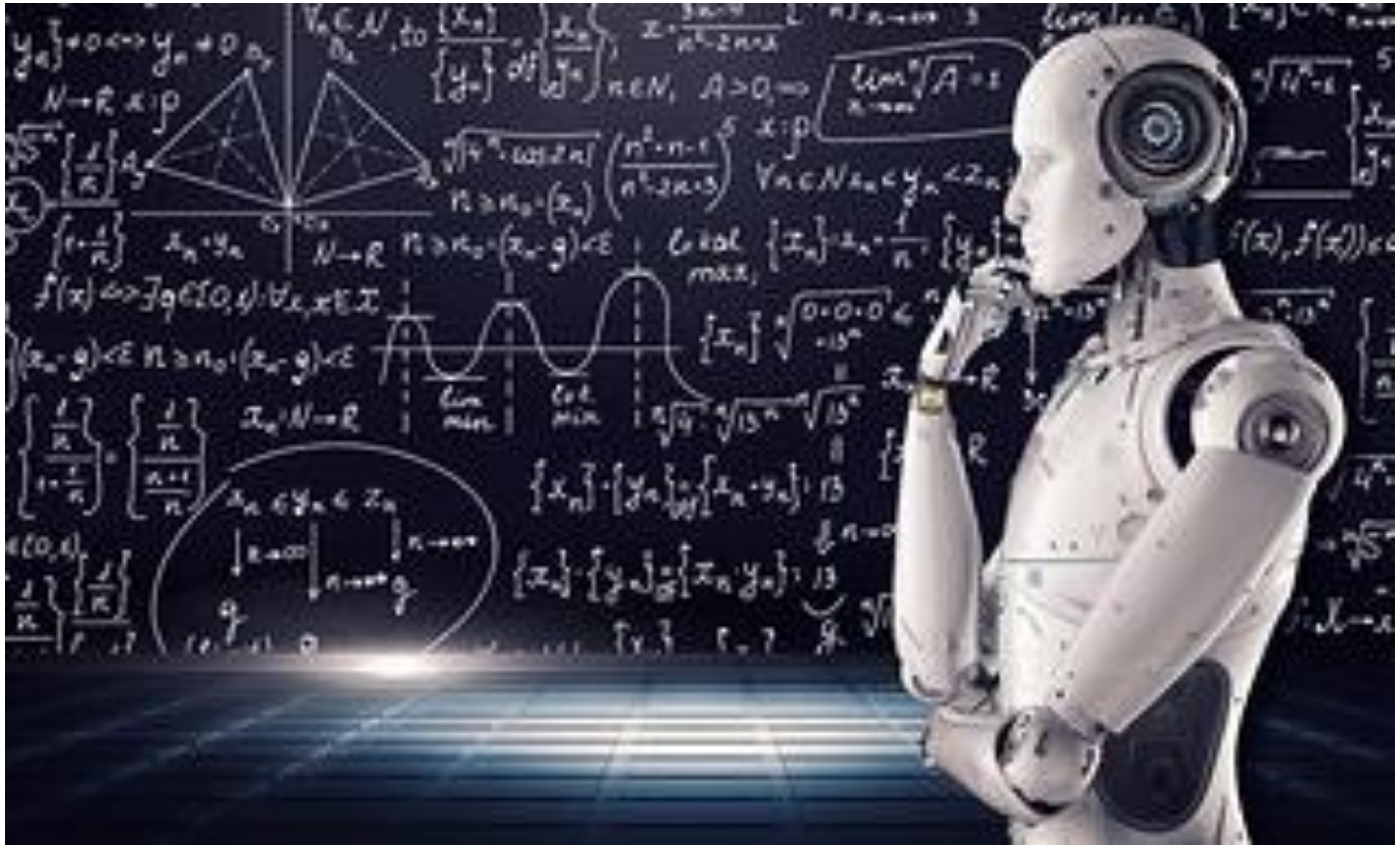
AI refers to a machine's ability to simulate human thought processes, such as analyzing data, learning from patterns, and making informed decisions.

Generative AI or machine learning is a subset of AI that focuses on enabling systems to automatically learn and improve from experience without explicit programming.

AI-powered tools can be used to:

- Write multiple-choice questions
- Generate essay prompts
- Develop training plans
- Evaluate assessments
- Identify at-risk employees
- Provide learners with timely feedback
- Suggest relevant learning content

This automation frees up instructors' time because they're not spending hours or days sourcing material, writing assessments, or aligning learning goals to those of their institution.



Generative AI (cont'd)

AI implementation comes with its challenges.

Ethical considerations and privacy concerns arise when collecting and analyzing **large amounts of student data**.

Generative AI + Cyber Risks

Increasing prevalence of AI will make it easier for threat actors to launch attacks and be successful in those attacks

- Can implement adaptive learning with AI to be more effective
- Hacking with AI may overcome some of the security methods currently used to repel attackers
  - e.g., AI can have ability to bypass MFA

Generative AI + Cyber Risks (cont’d)

By 2026, the majority of advanced cyberattacks will employ AI to execute dynamic, multilayered attacks that can adapt instantaneously to defensive measures.

This escalation in AI usage by both attackers and defenders will transform the cybersecurity landscape into a continuous AI cyber arms race.

Protecting your organization will depend on the convergence of security solutions and data into a unified platform, making strides in establishing governance frameworks and trust in AI, and putting AI at the helm of security operations.

Generative AI + Cyber Risks (cont'd)

The use of artificial intelligence will improve a threat actor's likelihood of gaining access to a system:

- Write more convincing phishing messages that contain fewer errors
- Believable deep-fakes and voice messages
- Quickly scale current operations to output more malicious messages

Generative AI + Cyber Risks (cont’d)

The threat of deep fakes:

Generative AI + Cyber Risks (cont’d)

Data Breaches:

AI models require vast amounts of student data for training, which could be compromised if not properly secured, leading to major privacy violations.

Supply Chain Vulnerabilities:

If AI tools are sourced from third-party vendors, potential security weaknesses in their systems could expose sensitive data within the institution.

Lack of Transparency:

Complex AI algorithms can be difficult to understand and audit, making it challenging to identify and address potential security flaws.

Vendor Contracts for AI Platforms

When negotiating a contract with an AI platform, several key considerations should be addressed to ensure that the agreement is comprehensive and protects the interests of all parties involved. Here are some important aspects to consider:

Data Security and Privacy:

Clearly define the responsibilities for data security and privacy between the AI platform provider and the university. This includes specifying how data will be protected, who has access, and how data breaches will be handled.

Intellectual Property and Copyright:

Address the ownership of AI-generated content. Since AI-generated works may not qualify for copyright protection, it's crucial to clarify who owns the output and any derivative works.

Vendor Contracts for AI Platforms (cont’d)

Liability and Indemnification:

Establish liability clauses that outline the responsibilities of each party in case of damages caused by the AI system. This includes indemnification provisions to protect against third-party claims.

Performance and Service Level Agreements (SLAs):

Define performance metrics and service levels that the AI platform must meet. This includes uptime guarantees, response times, and accuracy of AI outputs.

Vendor Contracts for AI Platforms (cont’d)

Transparency and Explainability:

Ensure that the AI platform provides transparency regarding how its algorithms work and the data used for training. This is important for compliance with ethical standards and regulatory requirements.

Modification and Updates:

Specify how updates and modifications to the AI system will be handled, including any additional costs and how they might affect the system's performance.

Termination and Exit Strategy:

Include provisions for contract termination and an exit strategy that allows for the migration of data and services to another provider if necessary.

Compliance with Regulations:

Ensure that the AI platform complies with relevant regulations and standards, such as data protection laws and industry-specific guidelines.

Augmented and Virtual Reality

While AI tools are streamlining learning tasks, augmented reality (AR) and virtual reality (VR) are two technologies that are bringing learning to life for students through immersion.

AR enhances the environment for learners by overlaying digital information onto live images of the real world, while VR creates entirely virtual experiences that mimic reality.

Cybersecurity Challenges in VR

Vulnerabilities in VR Systems:

As are computing devices, VR headsets are susceptible to cyber threats like data breaches and identity theft.

Exploitable VR hardware and software weaknesses threaten sensitive information and network security.

Targeting Content Marketplaces:

VR headsets connect to content marketplaces for software downloads, presenting additional points of vulnerability.

Malicious actors may compromise these platforms, compromising applications or VR devices.

Cybersecurity Challenges in VR (cont'd)

Unique Data Exploitation:

Collecting user movement data in VR environments enables unauthorized identification or impersonation.

Exploitation of VR data introduces challenges in verifying identity and authenticating transactions.

Cybersecurity Challenges in VR (cont'd)

Social Engineering and Manipulation:

VR's immersive nature facilitates social manipulation and distortion of user perceptions.

Vulnerabilities in VR environments may expose users to manipulated realities and social engineering tactics.

QR Codes and Cyber Threats

- Becoming one of the most frequent implementing a cyber attack
- Microsoft Defender blocks more than 15,000 emails per day directed to educational organizations that include malicious QR codes

Robinson+Cole

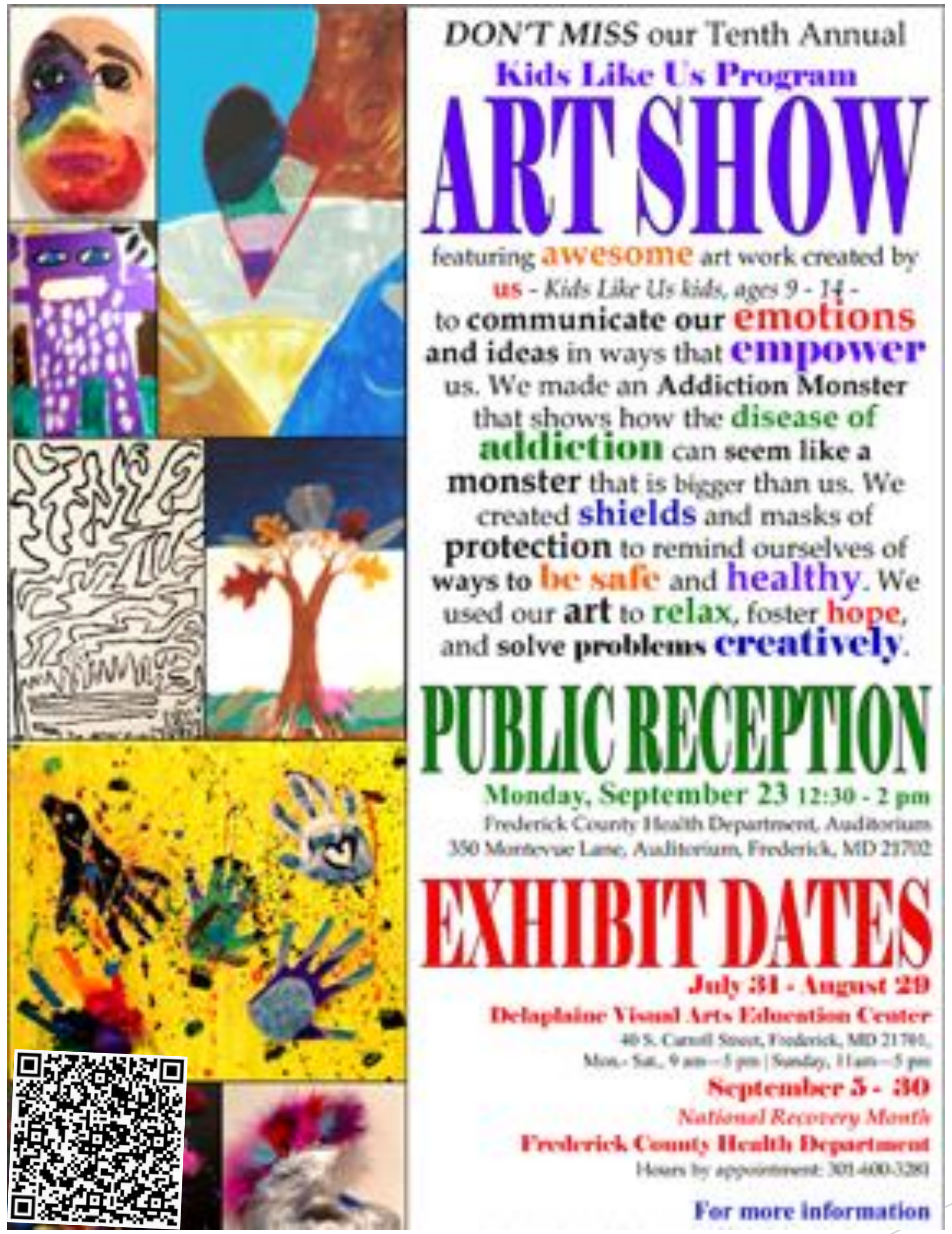
QR Codes and Quishing

- Can be easily manipulated by malicious actors to redirect users to phishing websites, steal personal information, or infect devices with malware

- This can be particularly dangerous as students and staff are often quick to scan QR codes without verifying their legitimacy, making them vulnerable to attacks

QR Codes and Cyber Threats (cont'd)

- Universities traditionally have spaces for students and staff to hang fliers
  - It is easy for a threat actor to hang a flier with a malicious QR code
- Malicious QR codes may also be difficult to detect with traditional email software
- This can lead to compromised student accounts, identity theft, or data breaches



DON'T MISS our Tenth Annual

Kids Like Us Program

ART SHOW

featuring awesome art work created by us - *Kids Like Us kids, ages 9 - 14* - to communicate our emotions and ideas in ways that empower us. We made an Addiction Monster that shows how the disease of addiction can seem like a monster that is bigger than us. We created shields and masks of protection to remind ourselves of ways to be safe and healthy. We used our art to relax, foster hope, and solve problems creatively.

PUBLIC RECEPTION

Monday, September 23 12:30 - 2 pm
Frederick County Health Department, Auditorium
350 Montevue Lane, Auditorium, Frederick, MD 21702

EXHIBIT DATES

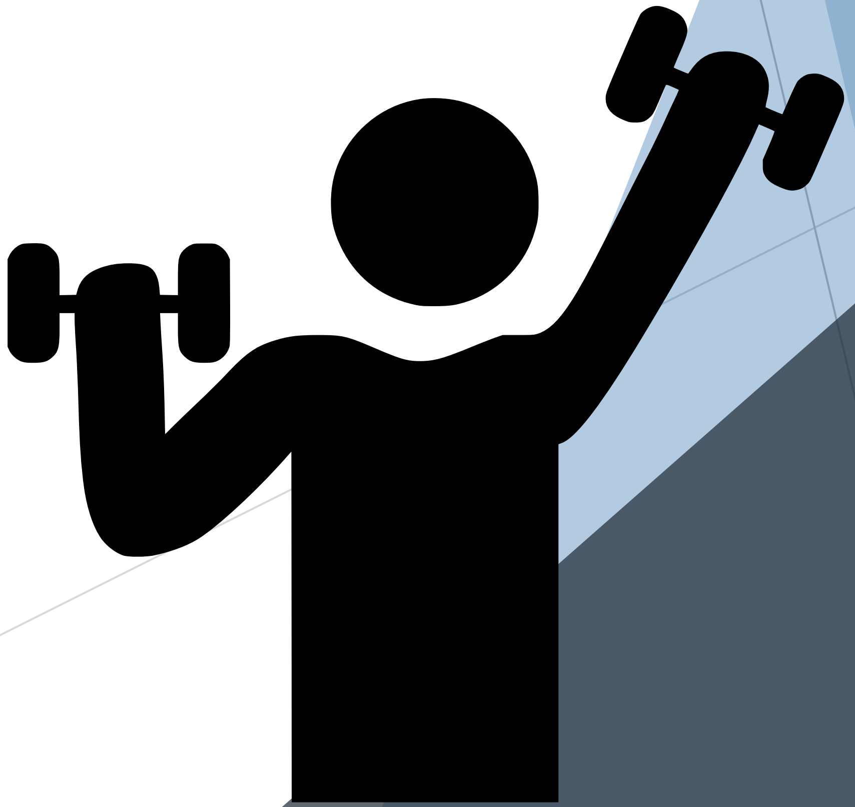
July 31 - August 29
Delaplaine Visual Arts Education Center
40 S. Carroll Street, Frederick, MD 21701,
Mon.- Sat., 9 am—5 pm | Sunday, 11am—5 pm

September 5 - 30
National Recovery Month
Frederick County Health Department
Hours by appointment: 301-600-3280

For more information

Cybersecurity Training

- Minimizing human error is key to reducing an organization's impact from a cyber event
    - Increased trainings help make users more proficient and less likely to make a critical error
    - Users need sufficient knowledge about how to prevent cyber threats as well as proper decision making to act appropriately
- Conduct tabletop trainings
    - Define rolls and strategy for responding to an incident



Zero Trust Approach

- A school's network must support more and more connected devices
  - There are an estimated 18.8 billion connected devices worldwide
  - Number could grow to over 30 billion by 2030
- **Zero-trust approach does not trust any of the devices inside the network**
  - Requires strict verification for every device attempting to access the network
- Incorporated into an organization's cybersecurity program to reduce risk and contain attacks
  - More difficult for a threat actor to gain access to the network through any of the devices
  - Restricts movement of the threat actor

Cyber Resilience as the North Star

Cyber resilience, or the ability to anticipate and adapt to adverse conditions, is key to anticipating cyber threats and staying ahead of growing regulatory requirements. **Simply put, organizations can't build resilience if they don't know what's ahead.**

"When we don't know exactly where we're going, we use our instrumentation to guide us," says Cam Beasley, chief information security officer at the University of Texas at Austin.

But cyber resilience is not something organizations can achieve overnight. Ultimately, cyber resilience comes from an information security risk management program with intentional features:

- Is easy to implement
- Provides visibility
- Helps manage regulatory compliance
- Scales as it matures

Conclusion

Universities may be decentralized across different departments or colleges and include different security protocols, which creates a lack of consistency in defending against and responding to attacks.

Collaboration is KEY to future proofing your organization.

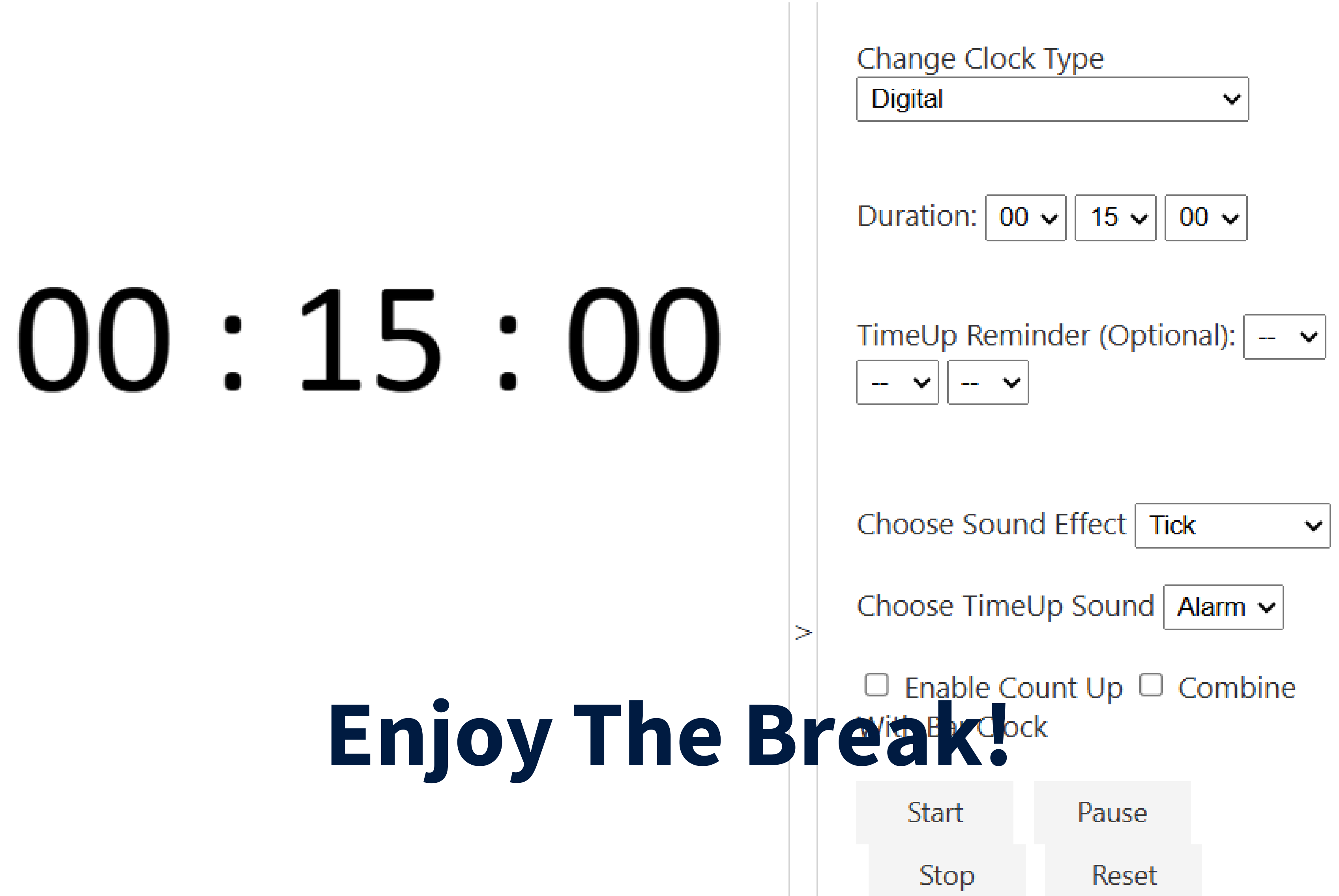
Build a Culture of Information Security.

Thank you!

Kathryn Rattigan
Robinson + Cole
One Financial Plaza
14th Floor
Providence, RI 02903
(401) 709-3357
krattigan@rc.com

Blog: dataprivacyandcybersecurityinsider.com

QUESTIONS?



00 : 15 : 00

Change Clock Type: Digital

Duration: 00 15 00

TimeUp Reminder (Optional): -- -- --

Choose Sound Effect: Tick

Choose TimeUp Sound: Alarm

☐ Enable Count Up ☐ Combine With Bar Clock

Enjoy The Break!

Take a Pause! – The Power of Pause

Did you know ?

"The Power of Pause" refers to utilizing the deliberate act of taking a moment to consider the potential consequences of one's actions to promote better decision making. It's a strategy aimed at preventing mistakes and it is often applied to human-computer interactions to stop inadvertent data loss!

Tom O’Neill

Management Liability & Cyber Practice Leader

Tom joined Fred C. Church in 2019 as the coverage specialist for Cyber, Management Liability, and Professional Liability coverage lines. In coordination with the commercial insurance marketing team, he consults with clients about their risk management strategies and negotiates coverage programs with our partner carriers.

Preferred Practices In Cybersecurity for Higher Education

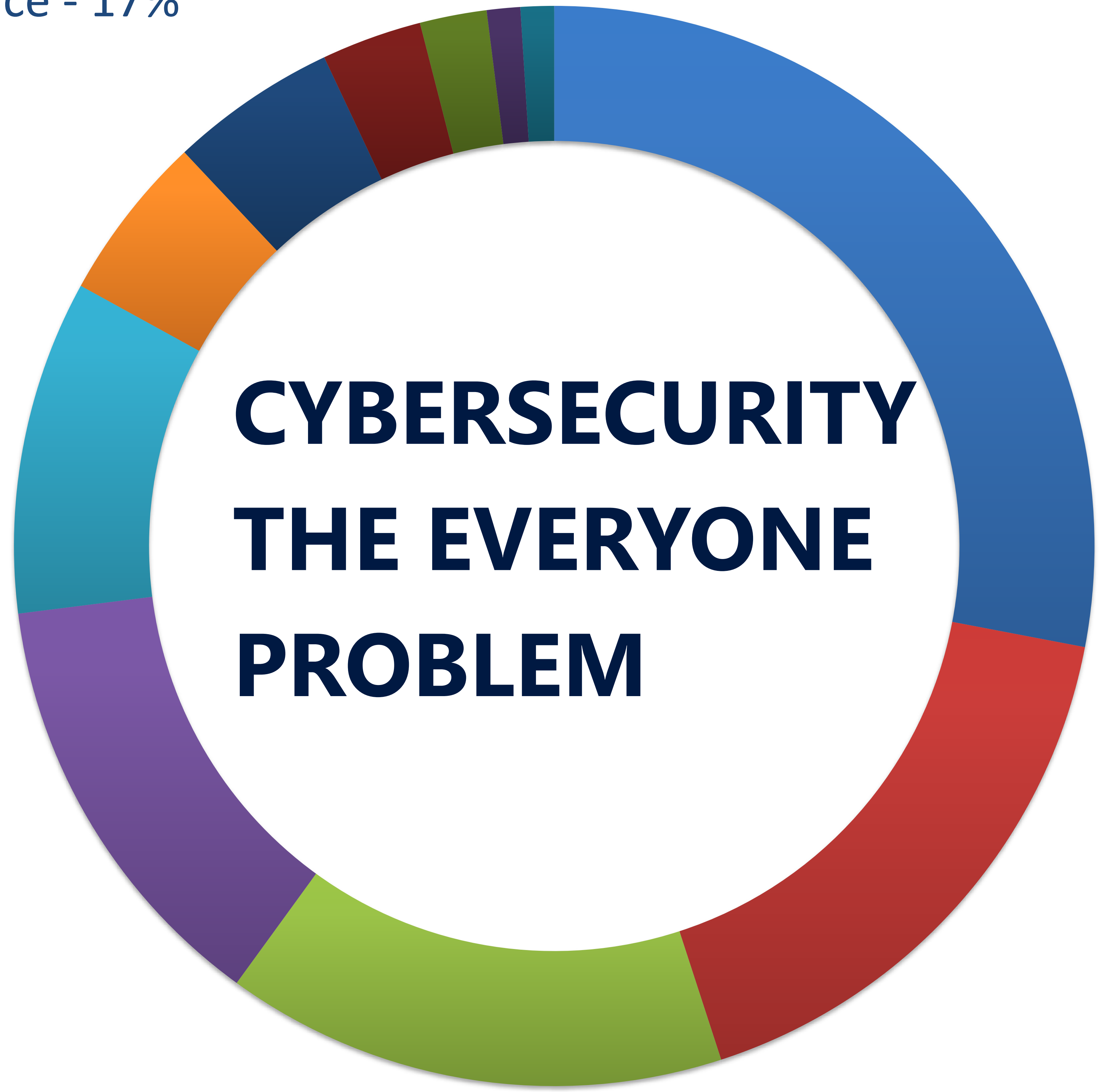
CYBERSECURITY
THE EVERYONE PROBLEM

- In the past five years, cybersecurity controls have improved on a macro level, but there is still a high rate of attempts against higher education institutions.
- Threats remain:
  - Users still love to click
  - And, threat actors continue to develop new strategies

2021	2022	2023	2024
44%	64%	79%	66%

Source: Sophos, Percent of higher education institutions hit by ransomware.

CYBERSECURITY THE EVERYONE PROBLEM



🟦 Health Care - 28%

🟥 Finance and Insurance - 17%

🟩 Business and Professional Services -15%

🟪 Education - 13%

🟦 Retail, Restaurant, and Hospitality - 10%

🟧 Manufacturing - 5%

🟦 Technology - 5%

🟥 Government - 3%

🟩 Non-Profit - 2%

🟪 Energy - 1%

🟦 Other - 1%

- The other side of the risk management coin: risk mitigation / incident response.
- We can’t put cybersecurity in a silo.
- Preparation, prevention, and mitigation is paramount.

Source: Baker Hostetler, 2024 Cyber Incident Response Report

ENTERPRISE CYBER RISK MANAGEMENT

Building a culture that uses collaboration to embrace cyber risk management as an everyone problem creates the foundation on which an enterprise risk management approach can thrive.

Loss prevention & incident preparation

(Cyber Incident)

Incident response and mitigation

Presented By : Tom O’Neill

THE LEFT OF BOOM…
LOSS PREVENTION & INCIDENT PREPARATION

Scan:

In your web browser:

Join at slido.com
#1529931

ⓘ Start presenting to display the joining instructions on this slide.

Who is the most likely person in your community to click a phishing link? (This is anonymous!)

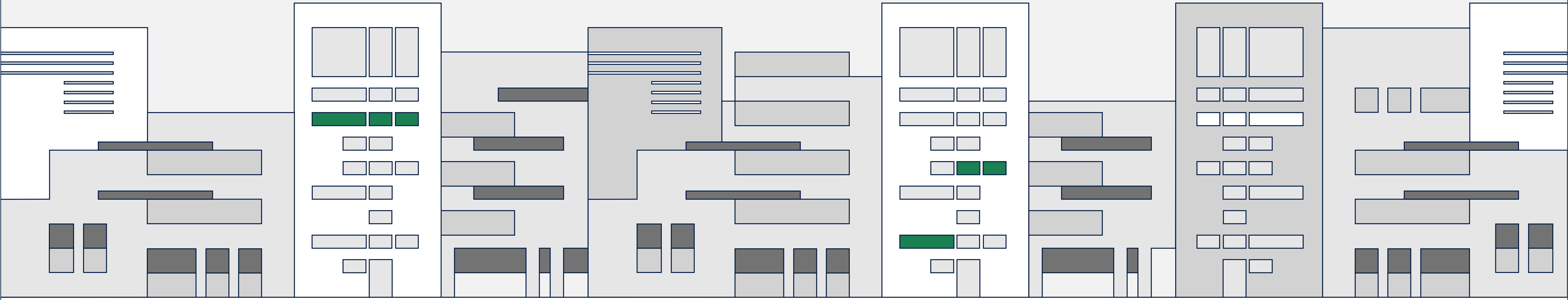
Join at slido.com
#1529931

ⓘ Start presenting to display the poll results on this slide.

Who signs the Cyber Insurance Application?

Join at slido.com
#1529931

ⓘ Start presenting to display the poll results on this slide.

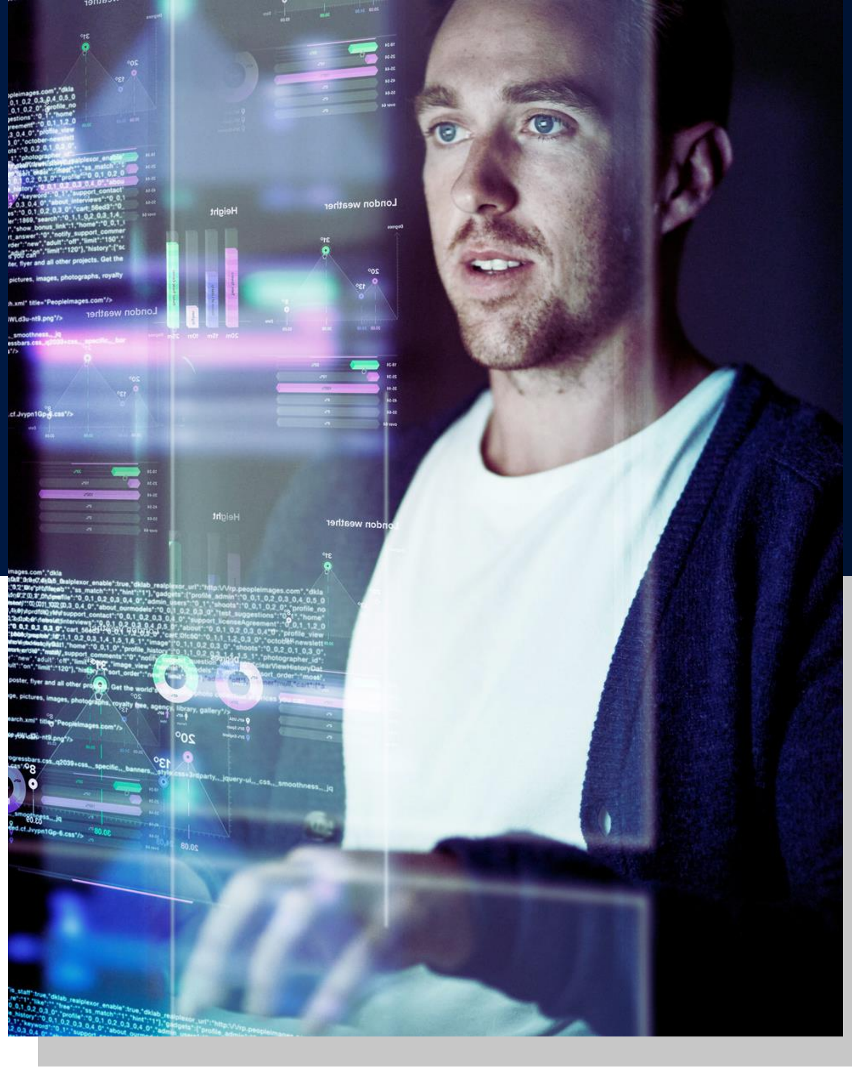


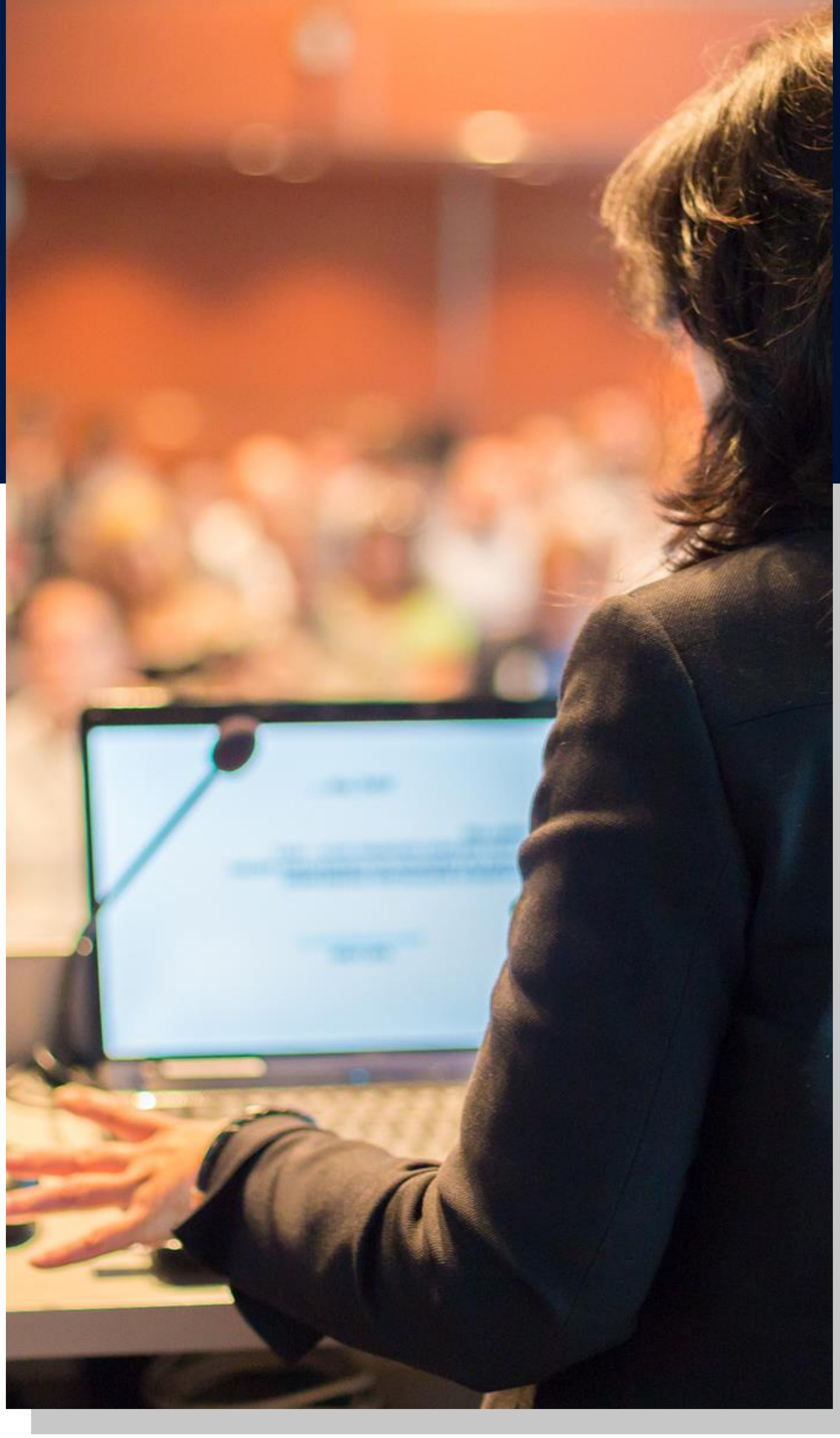
Who approves the IT budget?

Join at slido.com
#1529931

ⓘ Start presenting to display the poll results on this slide.

WHAT DO THESE RESPONSES TELL US ABOUT RISK MANAGEMENT?





- Everyone across the enterprise touches technology at some or multiple levels.
- Users are the weakest link.
- Collaboration is key — cyber insurance and the IT budget are examples of this.

LOSS PREVENTION—KEY CONTROLS

Multifactor Authentication (MFA)

Email, Remote Network Access, Privileged Accounts Access

24/7 Security Operations Center

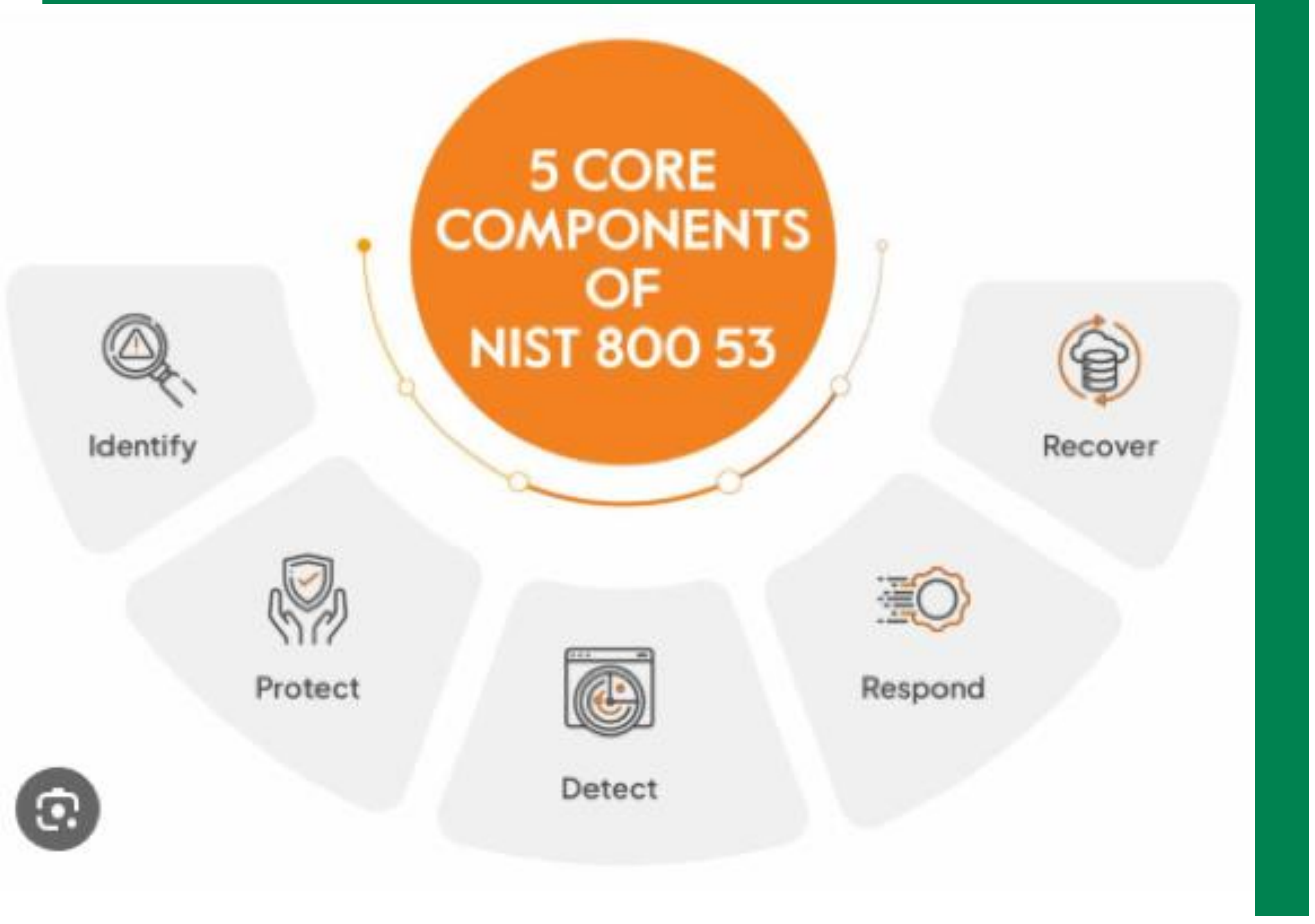
Endpoint Detection & Response
Managed Detection & Response

Secure Backups

Encrypted, immutable, protected by MFA if cloud-based, disconnected from the network, and tested.

RISK ASSESSMENT

- The list of controls is long and always developing, but where to begin?
- What governs your information security policy?
- Cyber Risk Assessment—NIST 800 53
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover



IDENTIFYING YOUR RISK
WHAT ARE THE CROWN JEWELS?

In a ransomware situation, what are the last things that you would want a threat actor to get their hands on and threaten to release on the dark web?

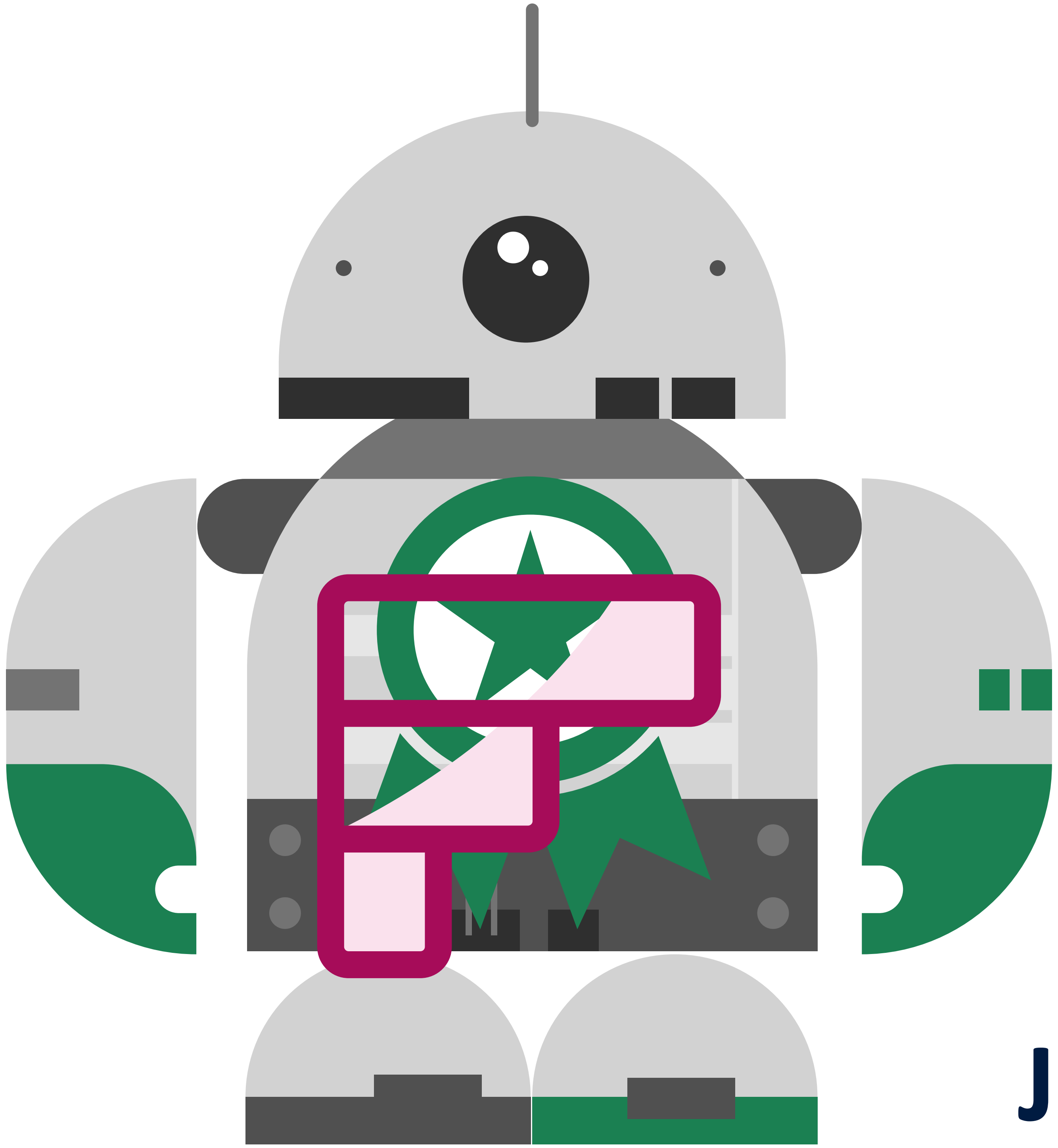
- PII/PHI
- Proprietary Research Information
- HR Employee Files
- Student Disciplinary Files

THE RIGHT OF BOOM…
RISK MITIGATION

Whose responsibility is it to notify members of the community if there is a cyber incident?

Join at slido.com
#1529931

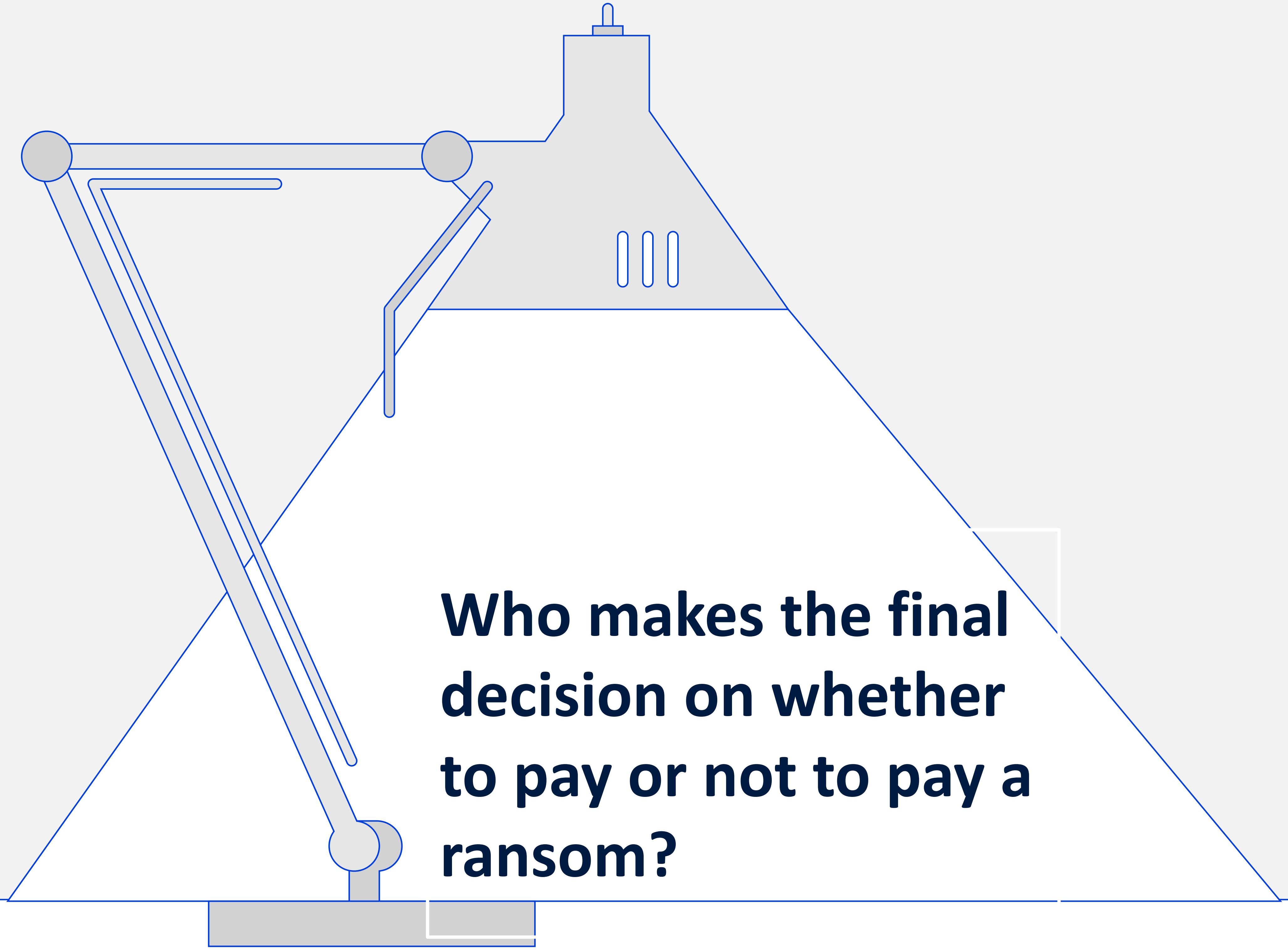
ⓘ Start presenting to display the poll results on this slide.



Who leads your Cyber Incident Response Team?

Join at slido.com
#1529931

ⓘ Start presenting to display the poll results on this slide.



Who makes the final decision on whether to pay or not to pay a ransom?

Join at slido.com
#1529931

ⓘ Start presenting to display the poll results on this slide.

WHAT DO THESE RESPONSES TELL US ABOUT RISK MANAGEMENT?

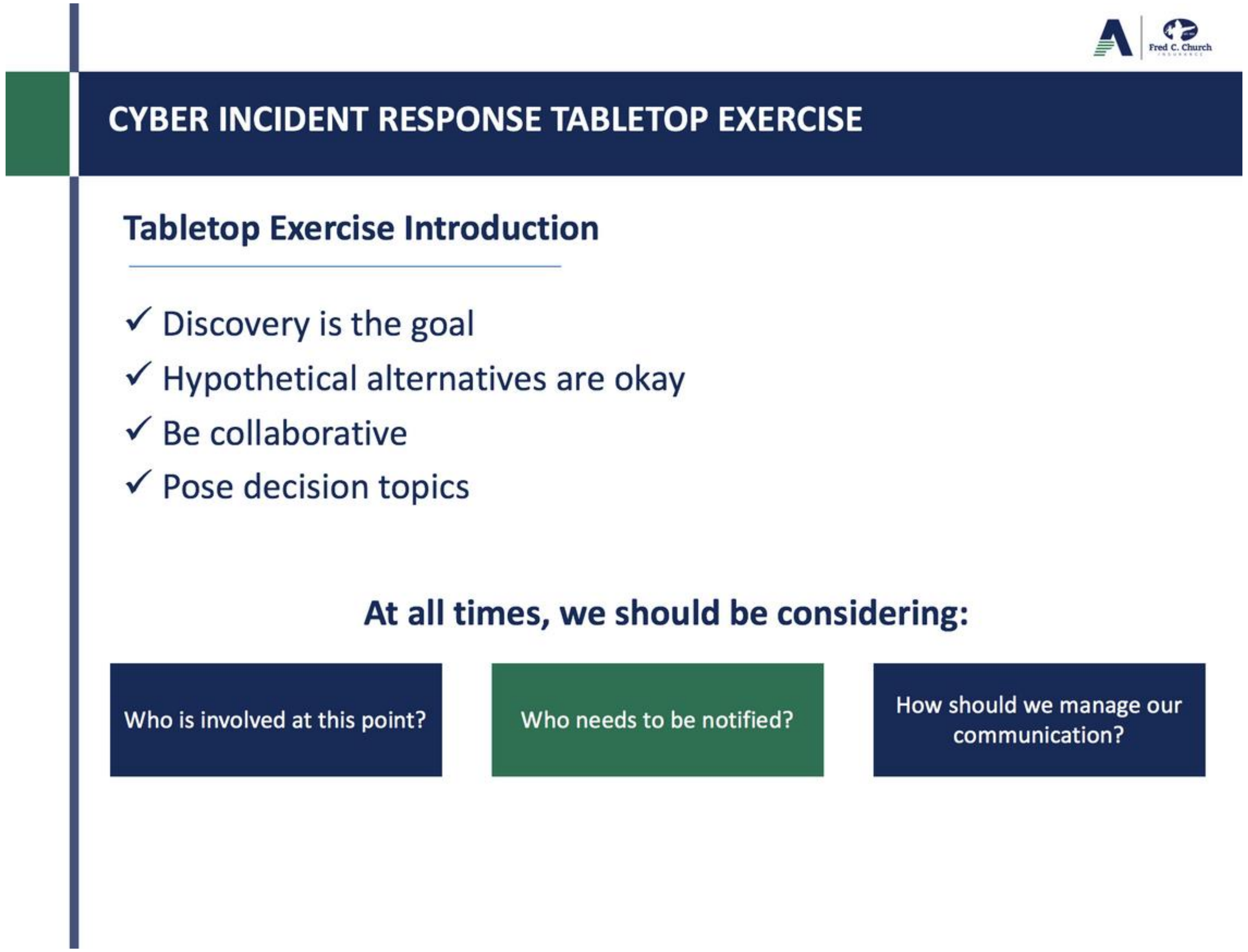
- Individuals across various departments will be involved in incident response.
- Designating a leader is important. This does not necessarily have to be an IT person. Remember, they will have a lot on their plate.
- Collaboration is key.

PREFERRED PRACTICES IN CYBER INCIDENT RESPONSE

- You can’t put the toothpaste back in the bottle.
- Cyber Incident Response plans are your playbook.
- Have an onboarding meeting and get to know your Cyber Insurance carrier.

CYBER INCIDENT RESPONSE TABLETOP

- Enterprise level versus IT only?
- Who is involved at what times? Who needs to be brought into the loop internally and externally, and when is the appropriate time to communicate to the community?
- Example incidents: Ransomware, Business Email Compromise, Third-Party Incident



CYBER INCIDENT RESPONSE TABLETOP EXERCISE

Tabletop Exercise Introduction

- ✓ Discovery is the goal
- ✓ Hypothetical alternatives are okay
- ✓ Be collaborative
- ✓ Pose decision topics

At all times, we should be considering:

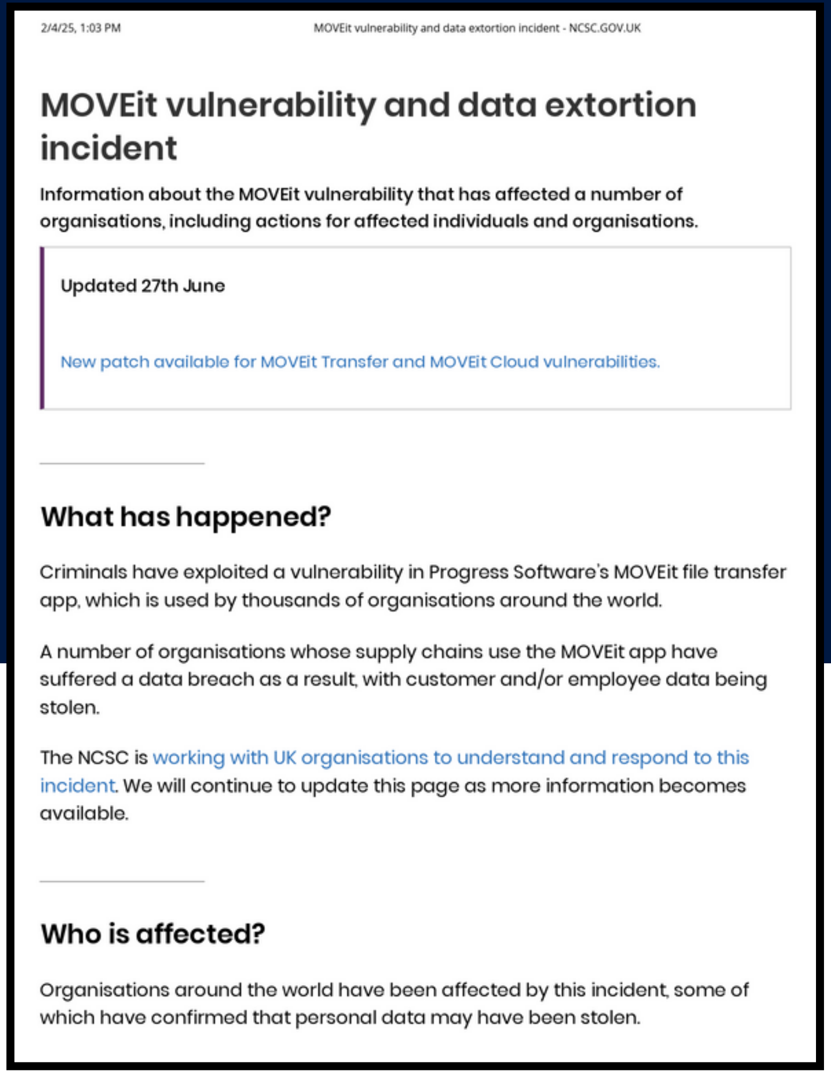
Who is involved at this point?

Who needs to be notified?

How should we manage our communication?

THIRD-PARTY RISK MANAGEMENT

2024 INCIDENTS MAKE HEADLINES



2/4/25, 1:03 PM MOVEit vulnerability and data extortion incident - NCSC.GOV.UK

MOVEit vulnerability and data extortion incident

Information about the MOVEit vulnerability that has affected a number of organisations, including actions for affected individuals and organisations.

Updated 27th June

New patch available for MOVEit Transfer and MOVEit Cloud vulnerabilities.

What has happened?

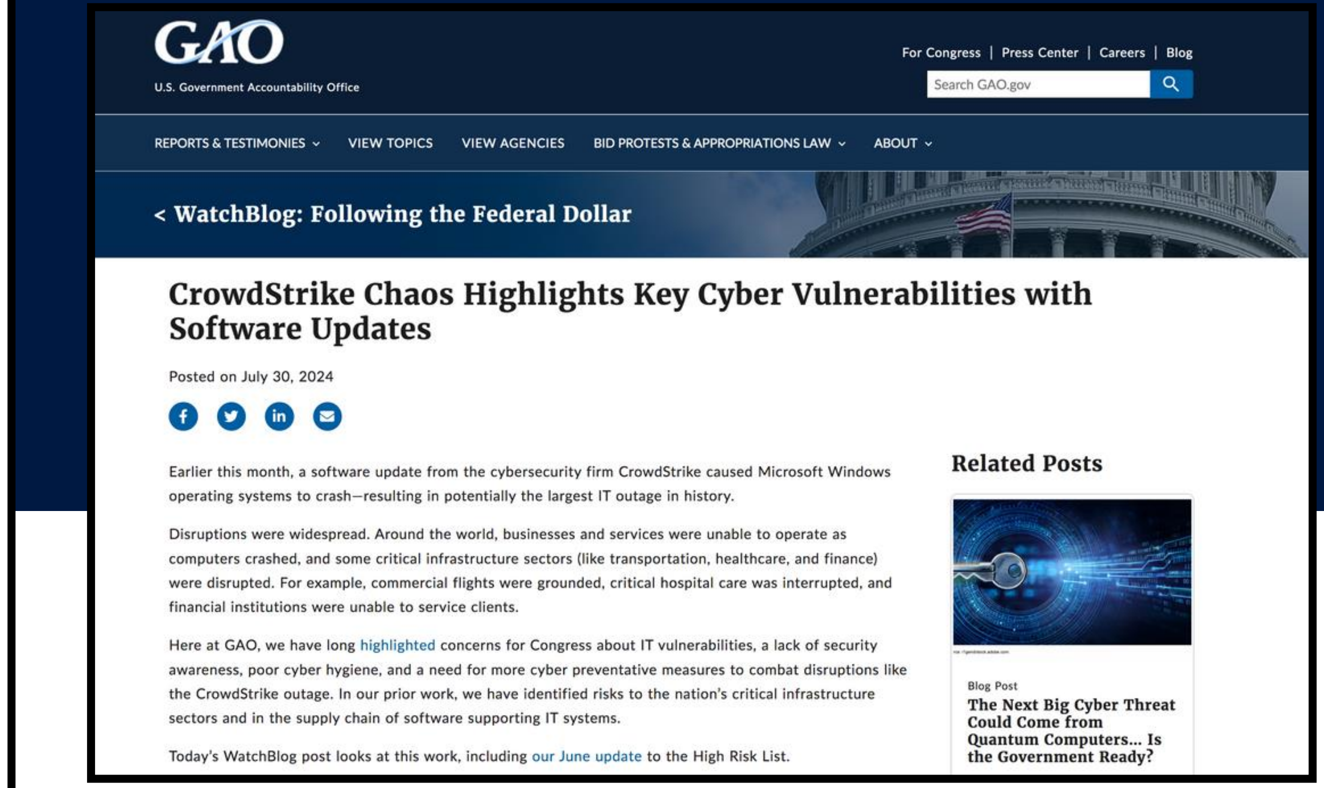
Criminals have exploited a vulnerability in Progress Software's MOVEit file transfer app, which is used by thousands of organisations around the world.

A number of organisations whose supply chains use the MOVEit app have suffered a data breach as a result, with customer and/or employee data being stolen.

The NCSC is working with UK organisations to understand and respond to this incident. We will continue to update this page as more information becomes available.

Who is affected?

Organisations around the world have been affected by this incident, some of which have confirmed that personal data may have been stolen.


GAO
U.S. Government Accountability Office
For Congress | Press Center | Careers | Blog
Search GAO.gov
REPORTS & TESTIMONIES
VIEW TOPICS
VIEW AGENCIES
BID PROTESTS & APPROPRIATIONS LAW
ABOUT

< WatchBlog: Following the Federal Dollar

CrowdStrike Chaos Highlights Key Cyber Vulnerabilities with Software Updates

Posted on July 30, 2024

Earlier this month, a software update from the cybersecurity firm CrowdStrike caused Microsoft Windows operating systems to crash—resulting in potentially the largest IT outage in history.

Disruptions were widespread. Around the world, businesses and services were unable to operate as computers crashed, and some critical infrastructure sectors (like transportation, healthcare, and finance) were disrupted. For example, commercial flights were grounded, critical hospital care was interrupted, and financial institutions were unable to service clients.

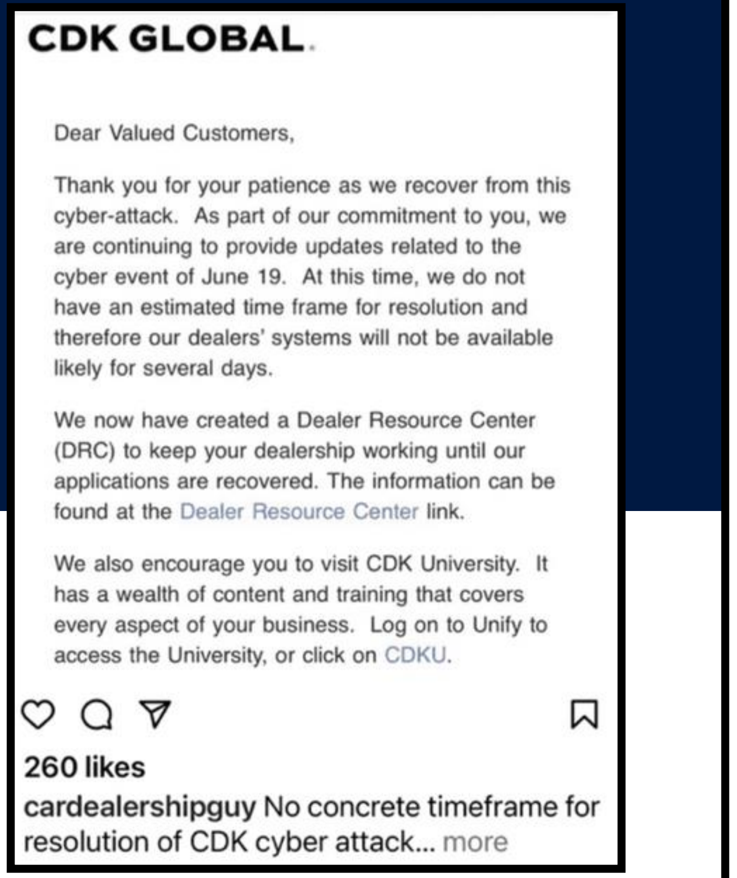
Here at GAO, we have long highlighted concerns for Congress about IT vulnerabilities, a lack of security awareness, poor cyber hygiene, and a need for more cyber preventative measures to combat disruptions like the CrowdStrike outage. In our prior work, we have identified risks to the nation's critical infrastructure sectors and in the supply chain of software supporting IT systems.

Today's WatchBlog post looks at this work, including our June update to the High Risk List.

Related Posts

Blog Post

The Next Big Cyber Threat Could Come from Quantum Computers... Is the Government Ready?



Dear Valued Customers,

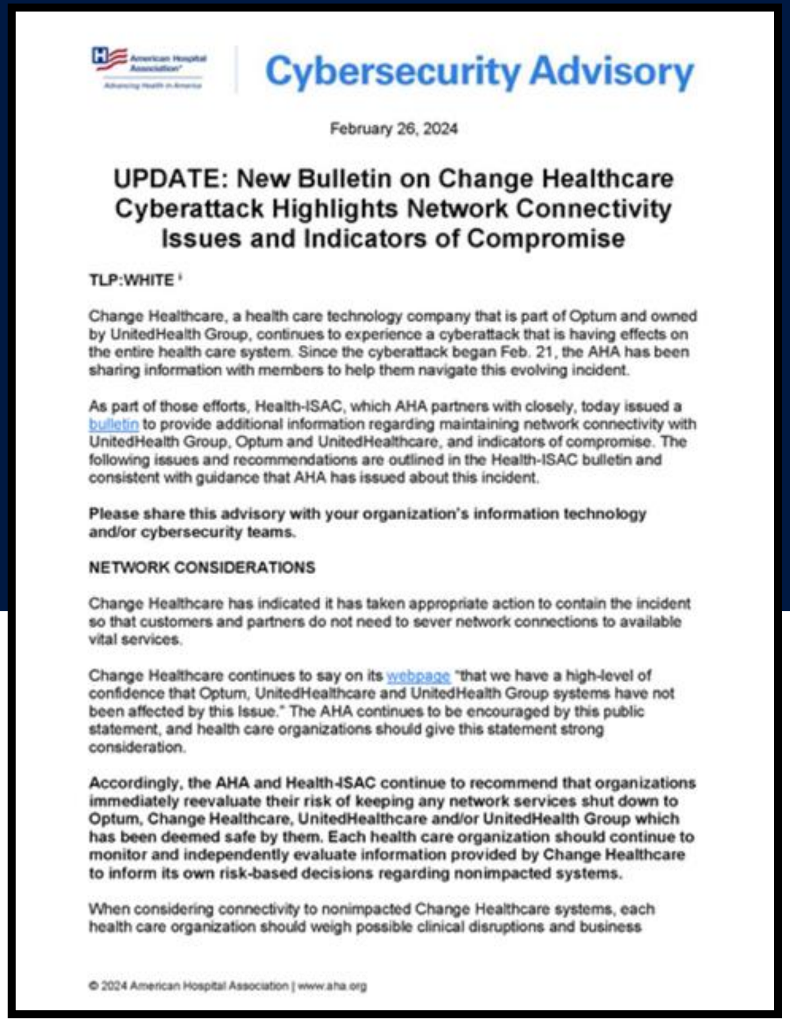
Thank you for your patience as we recover from this cyber-attack. As part of our commitment to you, we are continuing to provide updates related to the cyber event of June 19. At this time, we do not have an estimated time frame for resolution and therefore our dealers' systems will not be available likely for several days.

We now have created a Dealer Resource Center (DRC) to keep your dealership working until our applications are recovered. The information can be found at the Dealer Resource Center link.

We also encourage you to visit CDK University. It has a wealth of content and training that covers every aspect of your business. Log on to Unify to access the University, or click on CDKU.

260 likes

cardealershipguy No concrete timeframe for resolution of CDK cyber attack... more



Cybersecurity Advisory

February 26, 2024

UPDATE: New Bulletin on Change Healthcare Cyberattack Highlights Network Connectivity Issues and Indicators of Compromise

TLP:WHITE [i]

Change Healthcare, a health care technology company that is part of Optum and owned by UnitedHealth Group, continues to experience a cyberattack that is having effects on the entire health care system. Since the cyberattack began Feb. 21, the AHA has been sharing information with members to help them navigate this evolving incident.

As part of those efforts, Health-ISAC, which AHA partners with closely, today issued a bulletin to provide additional information regarding maintaining network connectivity with UnitedHealth Group, Optum and UnitedHealthcare, and indicators of compromise. The following issues and recommendations are outlined in the Health-ISAC bulletin and consistent with guidance that AHA has issued about this incident.

Please share this advisory with your organization's information technology and/or cybersecurity teams.

NETWORK CONSIDERATIONS

Change Healthcare has indicated it has taken appropriate action to contain the incident so that customers and partners do not need to sever network connections to available vital services.

Change Healthcare continues to say on its webpage "that we have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this Issue." The AHA continues to be encouraged by this public statement, and health care organizations should give this statement strong consideration.

Accordingly, the AHA and Health-ISAC continue to recommend that organizations immediately reevaluate their risk of keeping any network services shut down to Optum, Change Healthcare, UnitedHealthcare and/or UnitedHealth Group which has been deemed safe by them. Each health care organization should continue to monitor and independently evaluate information provided by Change Healthcare to inform its own risk-based decisions regarding nonimpacted systems.

When considering connectivity to nonimpacted Change Healthcare systems, each health care organization should weigh possible clinical disruptions and business

Presented By : Tom O'Neill

THIRD-PARTY CYBER RISK MANAGEMENT BEST PRACTICES

Contract Review

Cyber Insurance Requirements

Hold Harmless Language

Third-Party Scanning Tools

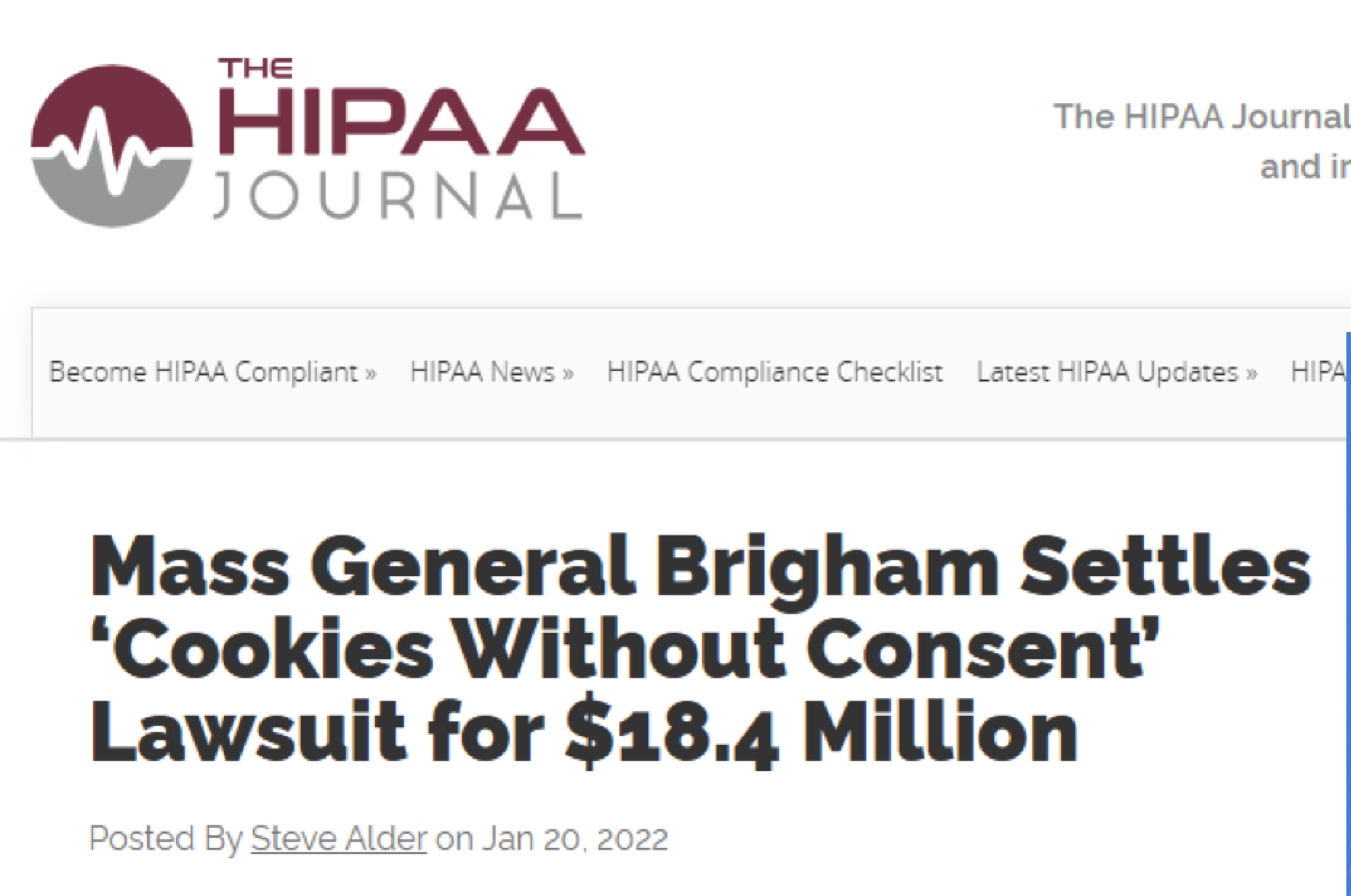
Limitation of Liability

Incorporating Third-Party Losses to IRP

Presented By : Tom O'Neille

CONCLUSION—THE PITCH FOR CYBER

LESSONS FROM LOSS



THE HIPAA JOURNAL

The HIPAA Journal is th
and indep

Become HIPAA Compliant » HIPAA News » HIPAA Compliance Checklist Latest HIPAA Updates » HIPA

Mass General Brigham Settles 'Cookies Without Consent' Lawsuit for $18.4 Million

Posted By Steve Alder on Jan 20, 2022

Becky Donovan

Risk Management Consultant

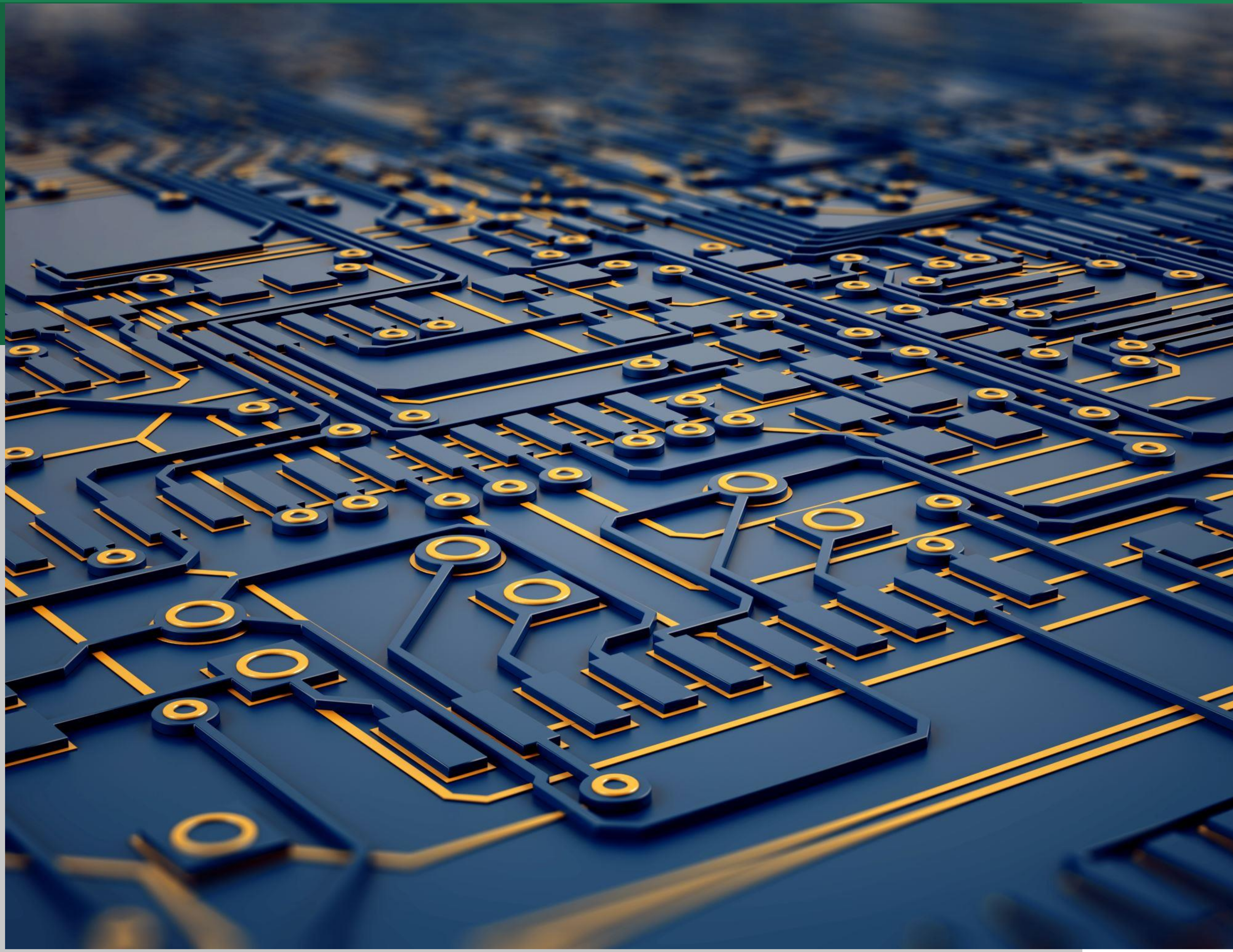
Throughout her decade-long career in the industry, Becky has honed her expertise in contract design and review, safety policy and procedure creation, as well as relationship and team building. As the Risk Management Consultant at Fred C. Church, she works hand in hand with the Sales Executives across all industry specialties. She is an essential partner in the risk management process.

Developing a Cybersecurity Culture & Awareness Program

WHAT'S IN IT FOR ME?

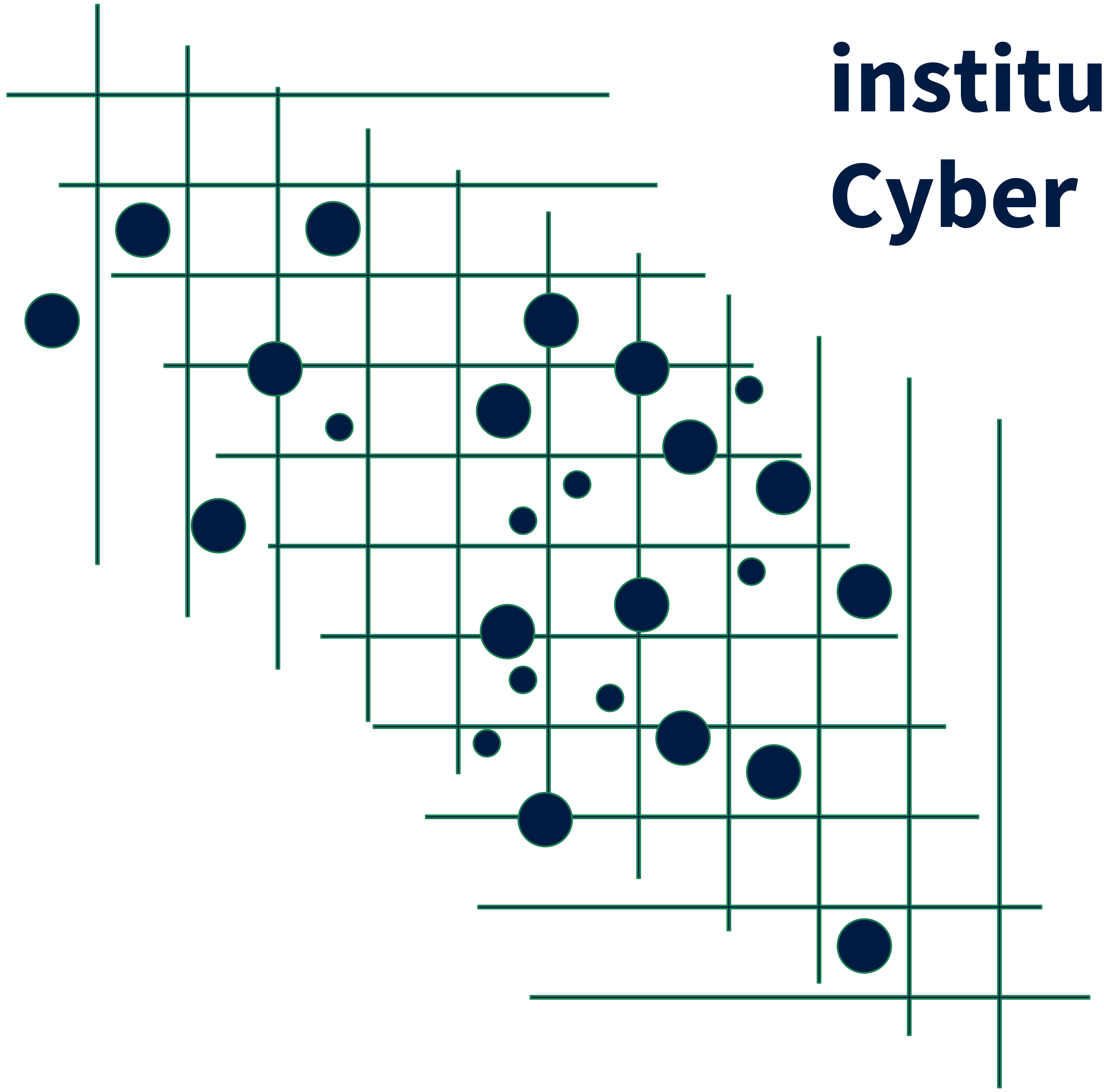
KEY TAKEAWAYS FOR YOU, AND YOUR TEAM:

- Why is a culture of risk needed in your institution?
- Defining and designing a cybersecurity culture.
- Developing a cybersecurity awareness program and how to evaluate it.
- Engaging your entire institution.



MIND THE GAP!
Thinking about your institution as a whole:

<u>In one word:</u> **What level or stakeholder group in your institution do you feel has the biggest gap in Cyber Risk Management Awareness?**



Join at slido.com
#1529931

ⓘ Start presenting to display the poll results on this slide.

UNDERSTANDING THE NEED FOR A CYBERSECURITY CULTURE

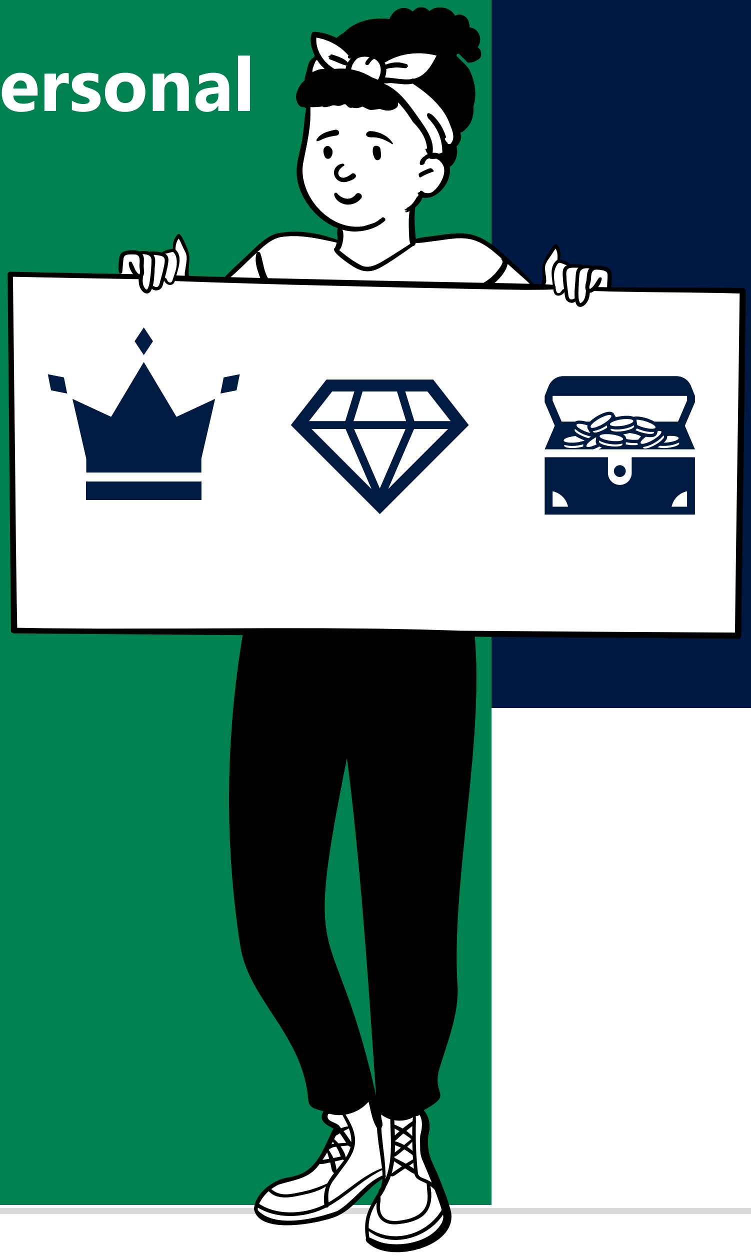
Human Element

- Diverse user base—students, faculty, and staff.
- Varying levels of knowledge and expertise in cybersecurity understanding.
- Stakeholders under different pressures.

UNDERSTANDING THE NEED FOR A CYBERSECURITY CULTURE

Crown Jewels—supporting the protection of your high-value data (research/personal information).

- **What are the jewels you hold?**
  - **Institutional responsibilities to stakeholders.**
  - **Trust and reputation.**
  - **Future-proofing against the growing threat landscape.**



One word that describes what other crown jewels are in your "cyber tiara?"

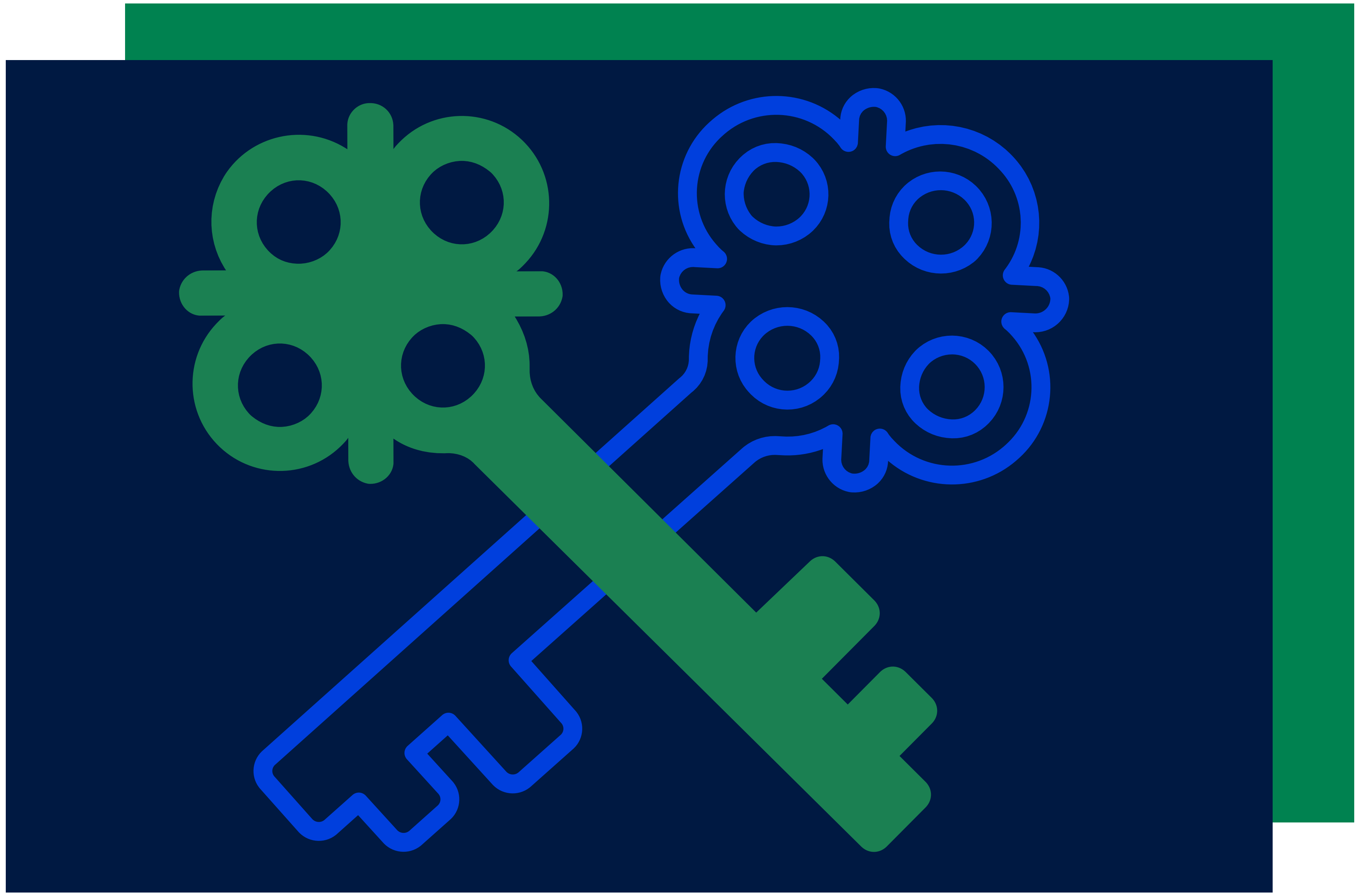
i.e.; Forms of data, key stakeholders, vendors, support resources, ect.?

ⓘ Start presenting to display the poll results on this slide.

KEY COMPONENTS OF A POSITIVE CYBERSECURITY CULTURE

● Awareness and Training

- Regular cybersecurity training for all stakeholders.
- Phishing simulations, cyber tabletop exercises, and awareness campaigns.



KEY COMPONENTS OF A POSITIVE CYBERSECURITY CULTURE

● Policies and Procedures

- Clear and actionable cybersecurity policies.
- Incident response plans and regular real time exercises.

KEY COMPONENTS OF A POSITIVE CYBERSECURITY CULTURE

● Collaboration and Communication

- Cross-departmental collaboration.
- The need for third-party cross collaboration.
  - Utilizing the onboarding call.
  - Using third-party resources.
- Open lines of communication for reporting and addressing cyber risks.

Rating – Out of five stars - what rating would you give your assessment of the current state of cybersecurity awareness at your institution?

Join at slido.com
#1529931

ⓘ Start presenting to display the poll results on this slide.

BUILDING A CULTURE OF CYBERSECURITY RISK MANAGEMENT—LAYING THE FOUNDATION

- Assess the current state of cybersecurity awareness.
- Set goals and objectives for the program to align with organizational policy.
- Identifying key stakeholders and their roles.
  - Teaching users as key stakeholders.
  - Giving students and other lower-level access users empowered knowledge.
    - Solutions with a cost vs. cost-free solutions.
  - Preparing students for decision making after educational years.

DEVELOPING A CYBERSECURITY AWARENESS PROGRAM

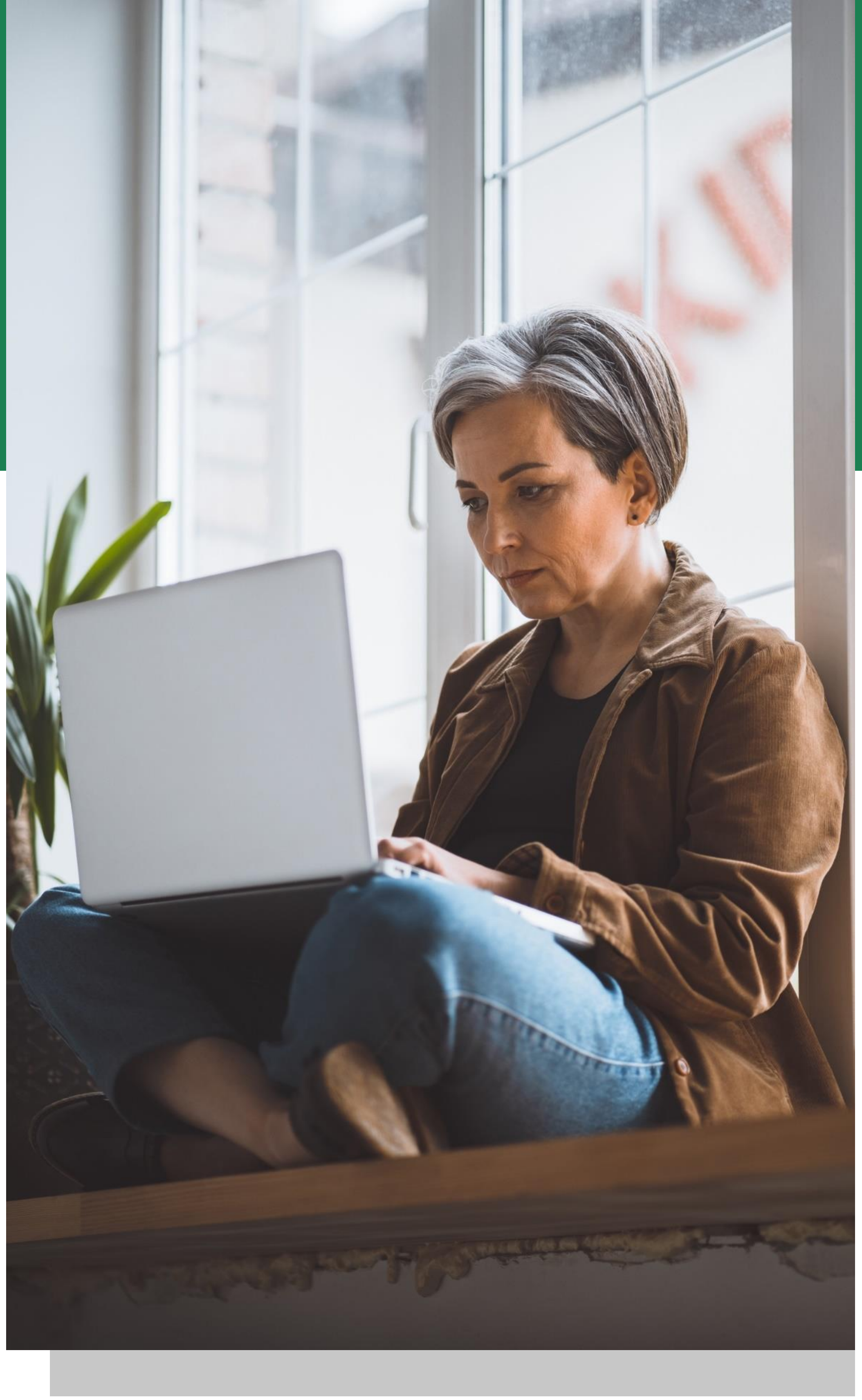
BUILDING THE FRAMEWORK

● Creating Engaging Training Content:

- Interactive training modules and workshops.
- Real-life scenarios and case studies.
- Gamification and rewards for participation.

DEVELOPING A CYBERSECURITY AWARENESS PROGRAM

IMPLEMENTING THE PROGRAM

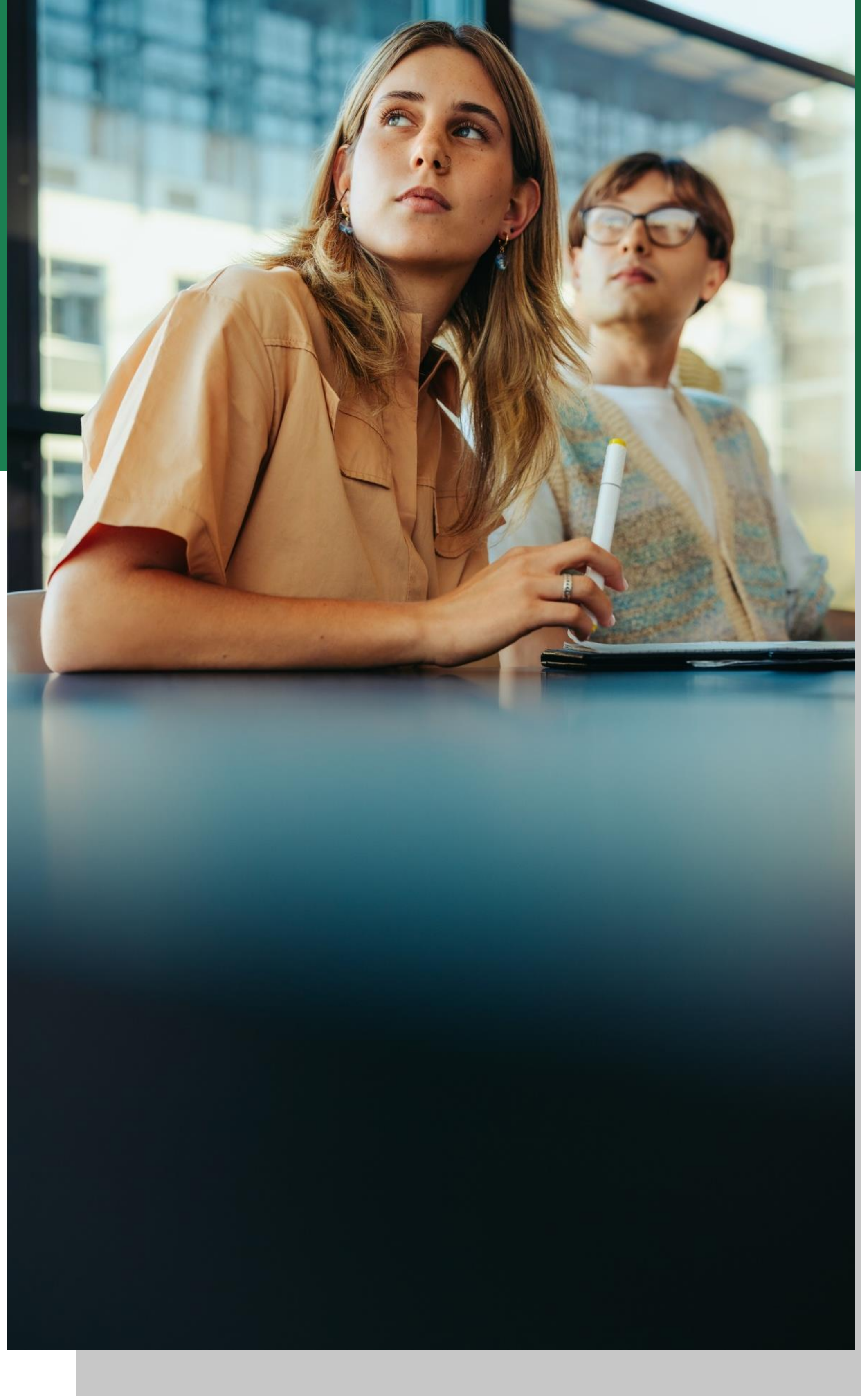


Reinforce the message:

- Scheduling regular training sessions.
- Utilizing various communication channels (emails, posters, webinars).
- Encouraging continuous learning and improvement.

DEVELOPING A CYBERSECURITY AWARENESS PROGRAM

ENGAGING THE ENTIRE INSTITUTION



Students, Faculty, and Staff all have roles to play:

- Defining roles.
- Creating buy-In and ownership.
    - Strategies to engage and motivate different stakeholders.
    - Using successful engagement initiatives.

DEVELOPING A CYBERSECURITY AWARENESS PROGRAM

MAINTAINING THE EFFECTIVENESS AND EVOLVING

● Tracking the program success:

- More phishing reports submitted through email button.
- Engagement in cybersecurity efforts etc.
- Reports of accidental risk exposure—promoting a blameless, educational space.

● Feedback and Improvement:

- Collecting feedback from participants.
- Regularly reviewing and updating the program based on feedback and new threats.

Lift Up

- Break down Silos”
  - Everyone is on the same team to go up against the threat actors and other cyber threats.
  - Get all stakeholders speaking the same “language.”
  - Support all stakeholder levels to keep them invested in the common goal.

Goal Up

- Invested people work together better with a team mentality.

- Team mentality prevents losses when working for cyber security as the group goal.

- Invested teams are less likely to have a member attempt legal action in the event a concern occurs. They can see and be a part of the efforts, leaving no stone unturned, knowing everyone did their best.

- Identifying the common goal for steak holders through education and awareness will band everyone together starting on the left of the boom, and traveling to the right should a cybersecurity incident occur.

Wrap Up

- Remember when presenting, teaching, and communicating a culture of cyber risk:
  - Educate others to have understanding, not just to check a box.
  - Transparently teach the importance of the why – without scare tactics.
  - Consistently Foster a positive and inclusive culture of risk management.

Questions?

- Enter questions in SLIDO or feel free to jump in!
- How do you feel about your institution's risk appetite to build a culture of cyber risk?

00 : 15 : 00

Duration: 00 15 00

TimeUp Reminder (Optional): -- -- --

Choose Sound Effect Tick

Choose TimeUp Sound Alarm

☐ Enable Count Up ☐ Combine With Bar Clock

Something to think about while on break:

1. The global cost of cybercrime is $6 trillion.
2. The average cost of a data breach is $4.88 million.
3. 88% of cybersecurity breaches are caused by human error.
4. The average time to identify a breach is 194 days.

MANAGING CYBER RISK ACROSS MULTIPLE DEPARTMENTS

Jim McFarland

Associate Vice President, Digital Technology Services, Wentworth Institute of Technology

Kristen Howard

Information Security Officer, Simmons University

Matt Murphy

Claims Manager for Cyber and Technology, Beazley

MANAGING CYBER RISK ACROSS MULTIPLE DEPARTMENTS

How can institutions prepare for the potential cyber threats through collaboration and cross-disciplinary input?

MANAGING CYBER RISK ACROSS MULTIPLE DEPARTMENTS

- How can organizations proactively ensure timely and accurate reporting of cyber incidents to their insurers?

MANAGING CYBER RISK ACROSS MULTIPLE DEPARTMENTS

- What challenges do organizations face when adopting new cyber vendor technologies?

MANAGING CYBER RISK ACROSS MULTIPLE DEPARTMENTS

Submit your Questions in Slido, or feel join in live!

ⓘ Start presenting to display the audience questions on this slide.

Matt Murphy
Risk Management Consultant

Matt joined Beazley in 2023 as a Claims Manager for Cyber and Technology with a focus on ransomware matters. Prior to joining Beazley, he was Senior Counsel at a law firm, providing clients with advice on cyber insurance and other lines of coverage and edited the firm's privacy newsletter. Prior to becoming a lawyer, Matt worked a software engineer and has a Master's Degree in Computer Science.

Incident Response and Cyberattack Recovery

beazley

beazley

Incident Response and Recovery

Planning Starts Before an Event

- Prepare a Written Information Security Plan
  - Policies and procedures to protect the sensitive personal information
  - Knowing what time of information is collected, and where and how it is stored on systems can help streamline forensics efforts.

- Proper planning means a Culture of Awareness
  - Table-Top Exercises
  - Phishing awareness
  - Continual training
  - Understand the roles and relationships with outside vendors

- Incident Response Plan
  - What to do? Who to call? Broker and Insurance Company
  - Many policies have “panel requirements” for certain Breach Response Services

Policy T&Cs

The Policy

- Read your policy
- Claims Made and Reported
- Triggers i.e. data/security breach?

The Vendors

- BBR, Infosec or WTW wording?
- Panel vendors vs non panel
- Costs vs experience

The Notification

- Early communication
- Prior consent needed?
- Breach Response Costs
- Cyber Extortion
- Defence Costs
- Settlement

Ransomware

The three most common threat vectors

- Social Engineering / Phishing
  - Relatively speaking, these attacks requires less technical skill
  - The use of AI has made the crafting of phishing emails both easier and more convincing

- Exploits / Vulnerabilities
  - Defenders try to patch as soon as possible vs Attackers that are trying to leverage the weaknesses
  - Sometimes there are no security patches available – temporary workarounds are only temporary

- Exposed Services that are under secured
  - There are millions of credentials on the internet
  - Many people reuse passwords for work / personal purposes
  - If there are no additional controls to verify who is accessing a service remotely, attackers can use legitimate remote access services for malicious purposes

beazley

Incident Response and Recovery

Incident Response

- Attorney
  - Evaluate obligations pursuant to Breach Notice Laws

- Forensics
  - Evaluate the cause and scope of an actual or reasonably suspected Data Breach
  - Containment

- Public Relations

- Data Mining
  - Doc Review

- Notification
  - Letters
  - Call Center
  - Credit Monitoring

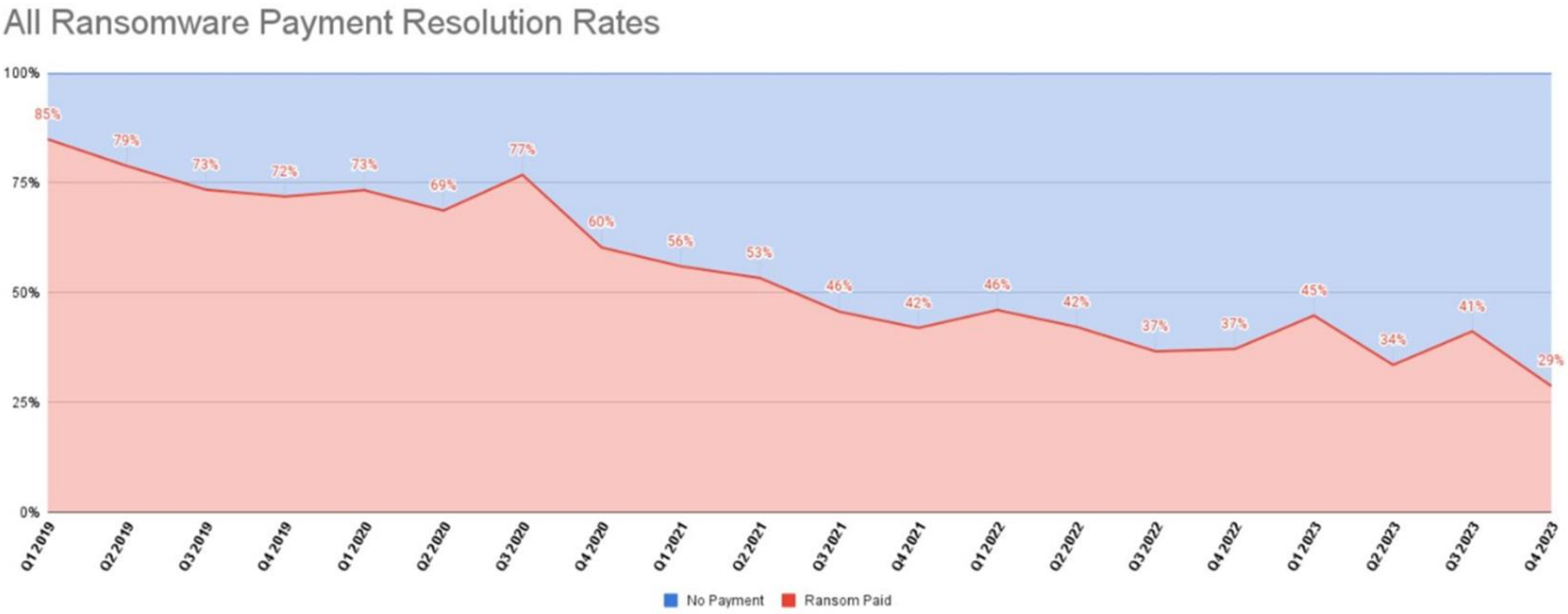
Data Exposed – Decision to pay Ransom?

You can't always trust cybercriminals

- More often, companies who pay are paying to avoid data being posted online
- We have always suspected cybercriminals made additional copies of stollen data
- We finally have proof of this
  - Lockbit was one of the most active cybercriminal group for at least the past in 2023 and the first half of 2024
  - They were taken down by law enforcement last year but have promised a comeback in February 2025.
  - Britain's National Crime Agency (NCA) discovered "some of the data on LockBit's systems belonged to victims who had paid a ransom to the threat actors."

Source: LockBit held victims' data even after receiving ransom payments to delete it (therecord.media)

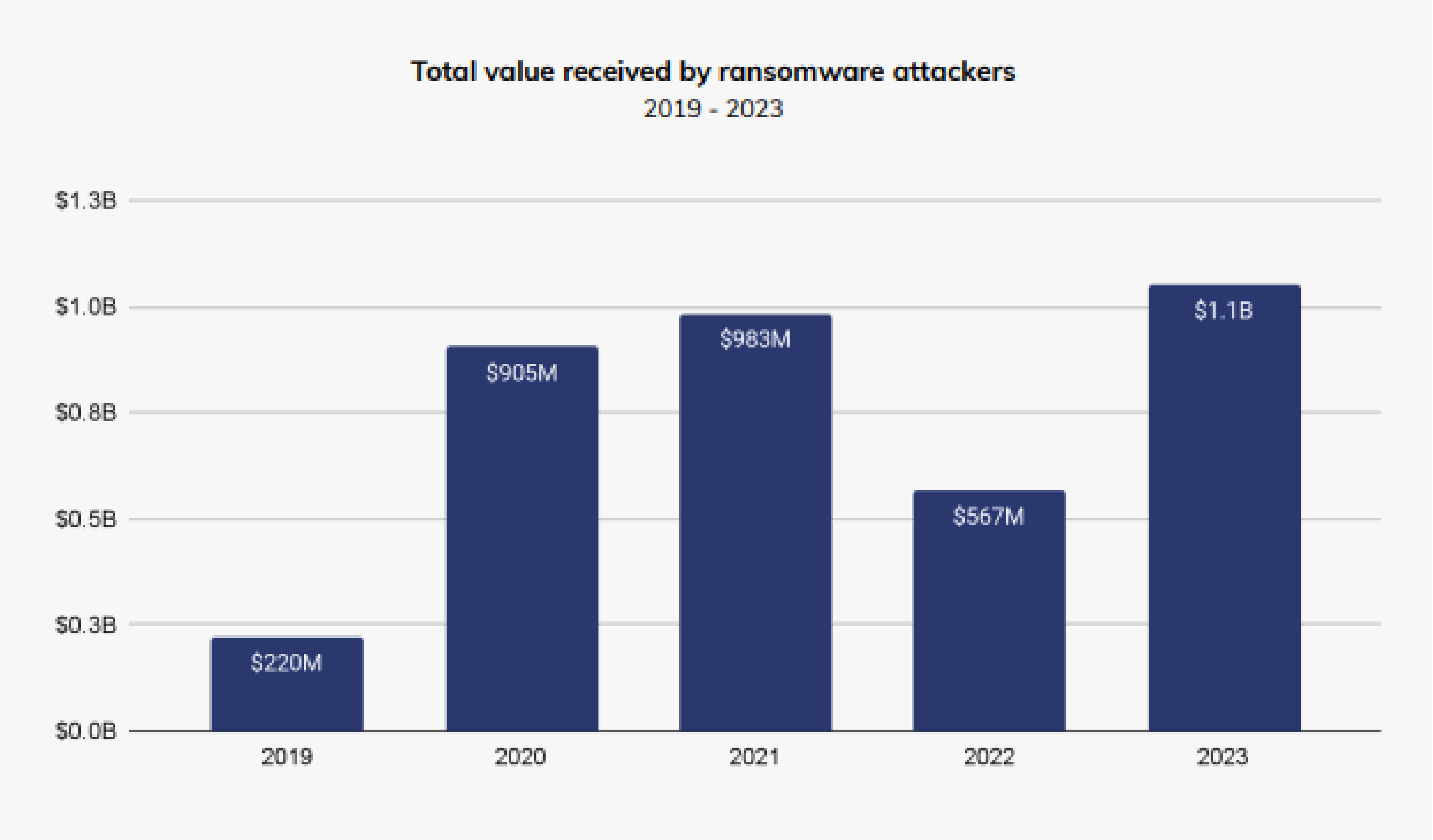
Ransomware – how often do people pay?



All Ransomware Payment Resolution Rates

COVEWARE

Ransomware – how much are people paying?



beazley

beazley

Data Recovery

Data Recovery

- Reasonable and necessary costs to regain access to, replace, or restore Data, or if Data cannot reasonably be accessed, replaced, or restored then the reasonable and necessary costs incurred by the Insured Organization to reach this determination

- Getting the right vendors in is key

- Avoid duplication of effort

Source: LockBit held victims' data even after receiving ransom payments to delete it (therecord.media)

- Data Recovery policies are intended for the **existing technology configuration**

  - and the reasonable and necessary efforts towards recovering that to that baseline

- Indemnity costs are attributed to returning the environment to its **prior** operating configurations

- Coverage is not intended to indemnify IT Capital Project Improvements; i.e. **Betterment**

beazley

Business Interruption Loss

Beazley's Business Interruption Cyber Guide and Resources

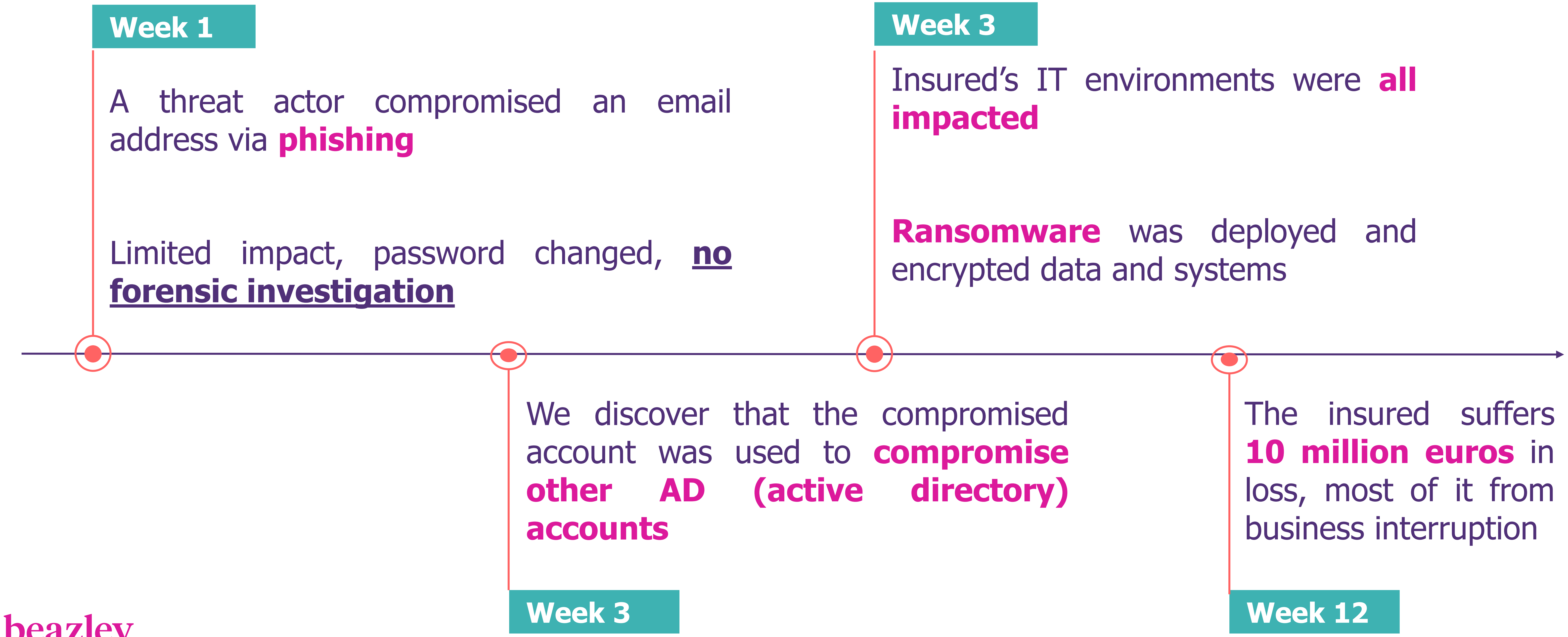
- Our **online cyber business interruption guide** includes:
  - ✓ Process overview – step by step timeline of adjusting a cyber BI loss
  - ✓ Policy wording – use our interactive policy explainer to learn more about our insuring agreements and key policy terms
  - ✓ Claims examples – see how we adjust claims in real life examples
  - ✓ Common misconceptions – answers to common questions raised by insureds.

- Proof of Loss
  - Beazley's internal forensic accountant is available to discuss any questions regarding the Proof of Loss preparation/submission with Insureds.
  - If the Insured Organization is unable to prepare the Proof of Loss, there is a **Claims Preparation Cost** allowance to contract with a third party prepare a Proof of Loss in excess of retention.

beazley

Claims Examples

Business Email Compromise – Large Retailer in Europe



Week 1

A threat actor compromised an email address via **phishing**

Limited impact, password changed, **no forensic investigation**

Week 3

We discover that the compromised account was used to **compromise other AD (active directory) accounts**

Week 3

Insured’s IT environments were **all impacted**

Ransomware was deployed and encrypted data and systems

Week 12

The insured suffers **10 million euros** in loss, most of it from business interruption

How our policy supported our client for the duration of the incident

Incident Type: Ransomware
Industry: Financial Services
Revenue: <£10m

Crime ~~In~~tended

Our client suffered a ransomware attack where the criminal's initial demand was £500K.

How our Cyber Cover & Services responded

Our client contacted their dedicated Cyber Services Manager.	**Cyber Services** **Incident Helpline**
The Cyber Services Manager appointed a lawyer and IT forensics services to determine the extent of the incident. They revealed that 500gb of data had been stolen in addition to the confidential files of 4,500 customers.	**Cyber Services** **Digital forensics, Legal Services**
Our client opted to pay the ransom to avoid the data and confidential files being publicised. We reimbursed our client for the ransom payment.	**First Party Loss** **Cyber extortion**
The Cyber Services Manager also appointed a Notification Centre to handle the communication with the 4,500 affected customers.	**Cyber Services** **Notification**
After retrieving the data, we helped our client reconstitute the data, and get their computer network back up and running.	**First Party Loss** **Data Recovery, Business interruption**
The total claim paid was £790k which included: - The reimbursement of the ransom payment- £500k - Business interruption and data recovery- £100k - Fees for Legal, Forensics & The Notification Centre- £190K	**Claims Support**

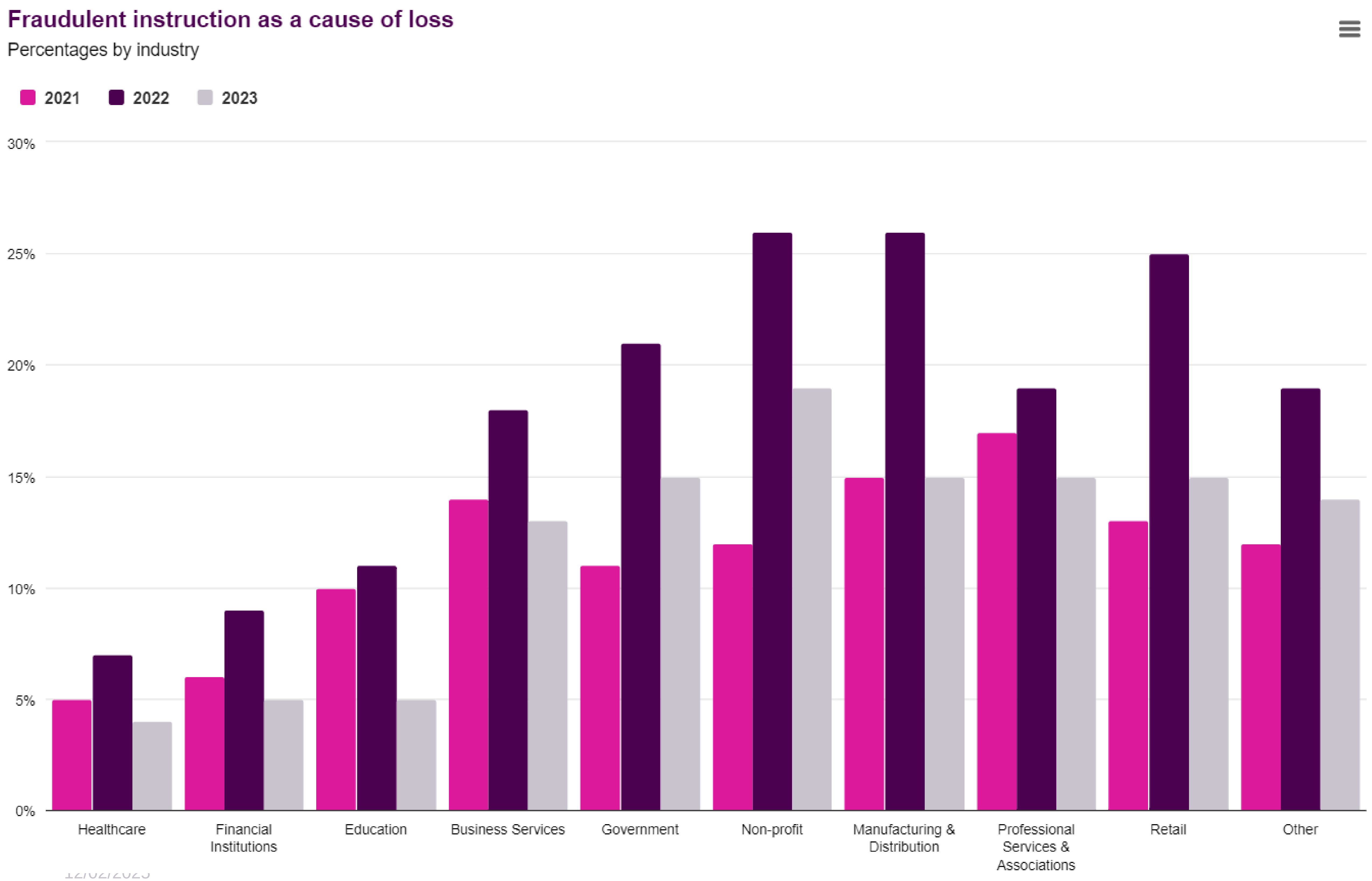
beazley

The descriptions contained in this communication are for preliminary informational purposes only. Coverages are underwritten by Beazley Solutions International Limited on behalf of Beazley syndicates at Lloyd's or Lloyd's Insurance Company S.A. ("LLoyd's Brussels" - a subsidiary of Lloyd's and authorised by the National Bank of Belgium) or Beazley Insurance dac and will vary depending on individual country law requirements and may be unavailable in some countries. The exact coverage afforded by the products described in this brochure is subject to and governed by the terms and conditions of each policy issued. For more information, visit www.beazley.com.

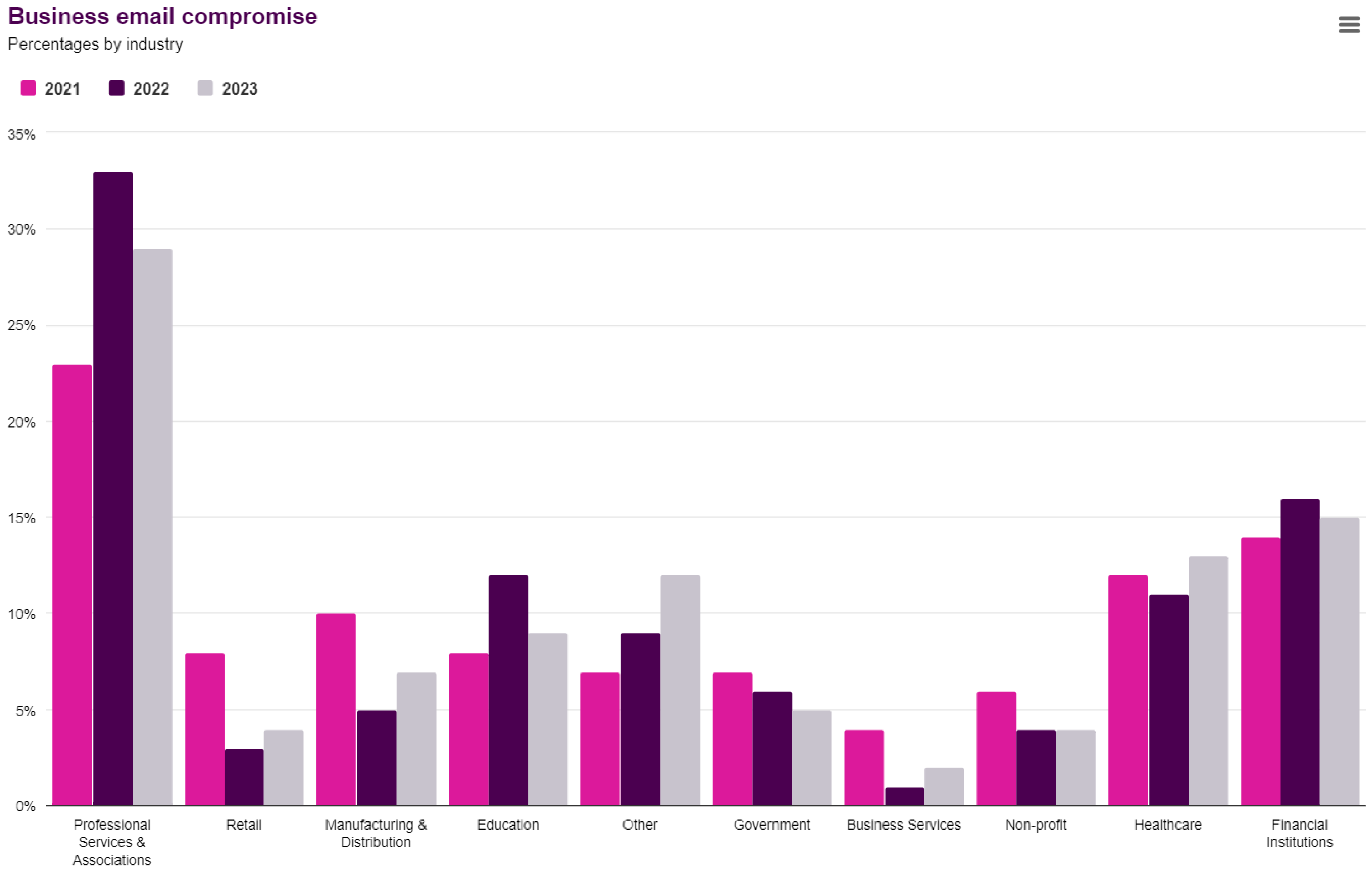
beazley

Claims Data

Fraudulent Instruction as a Cause of Loss

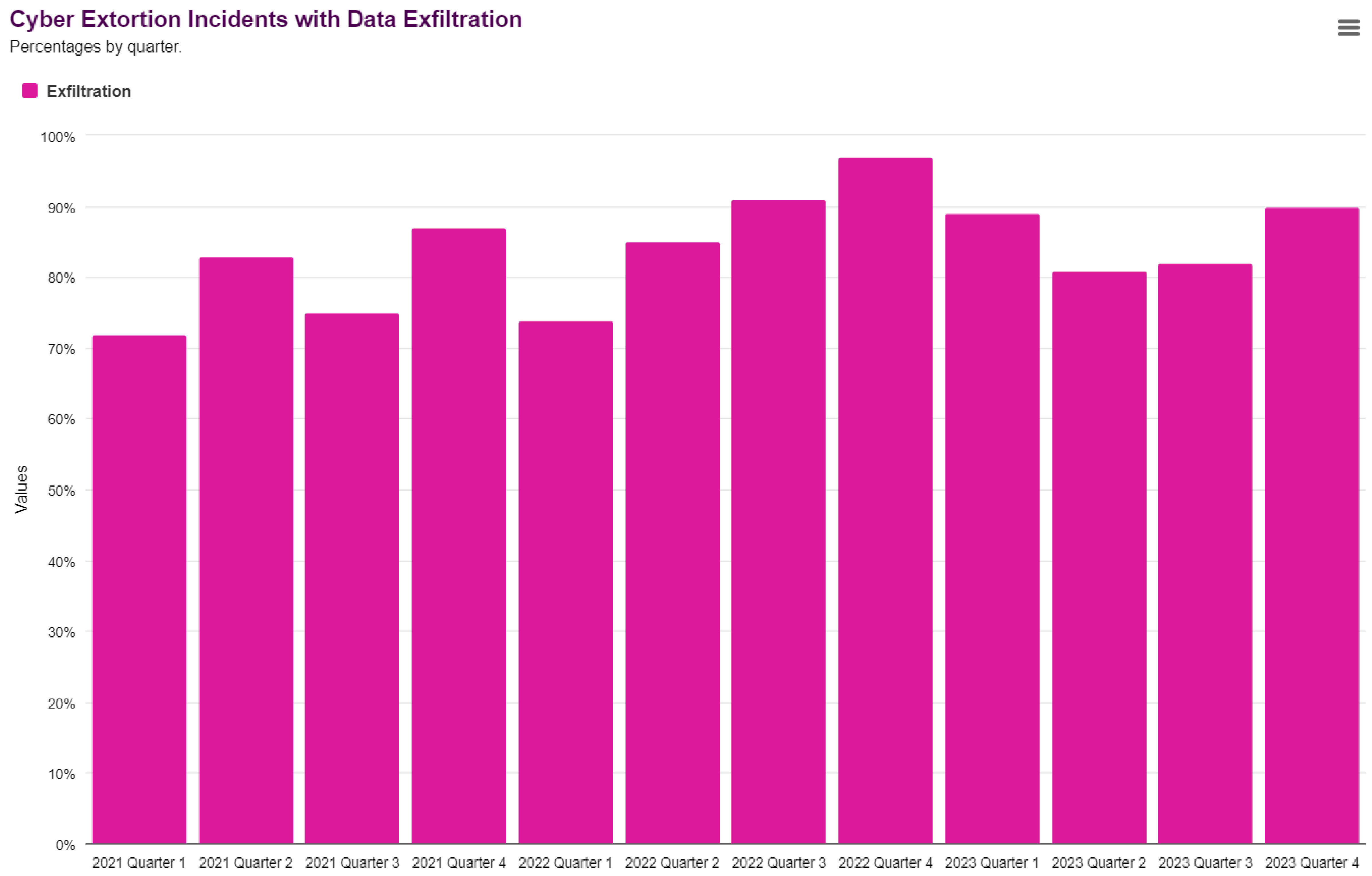


Business email compromise

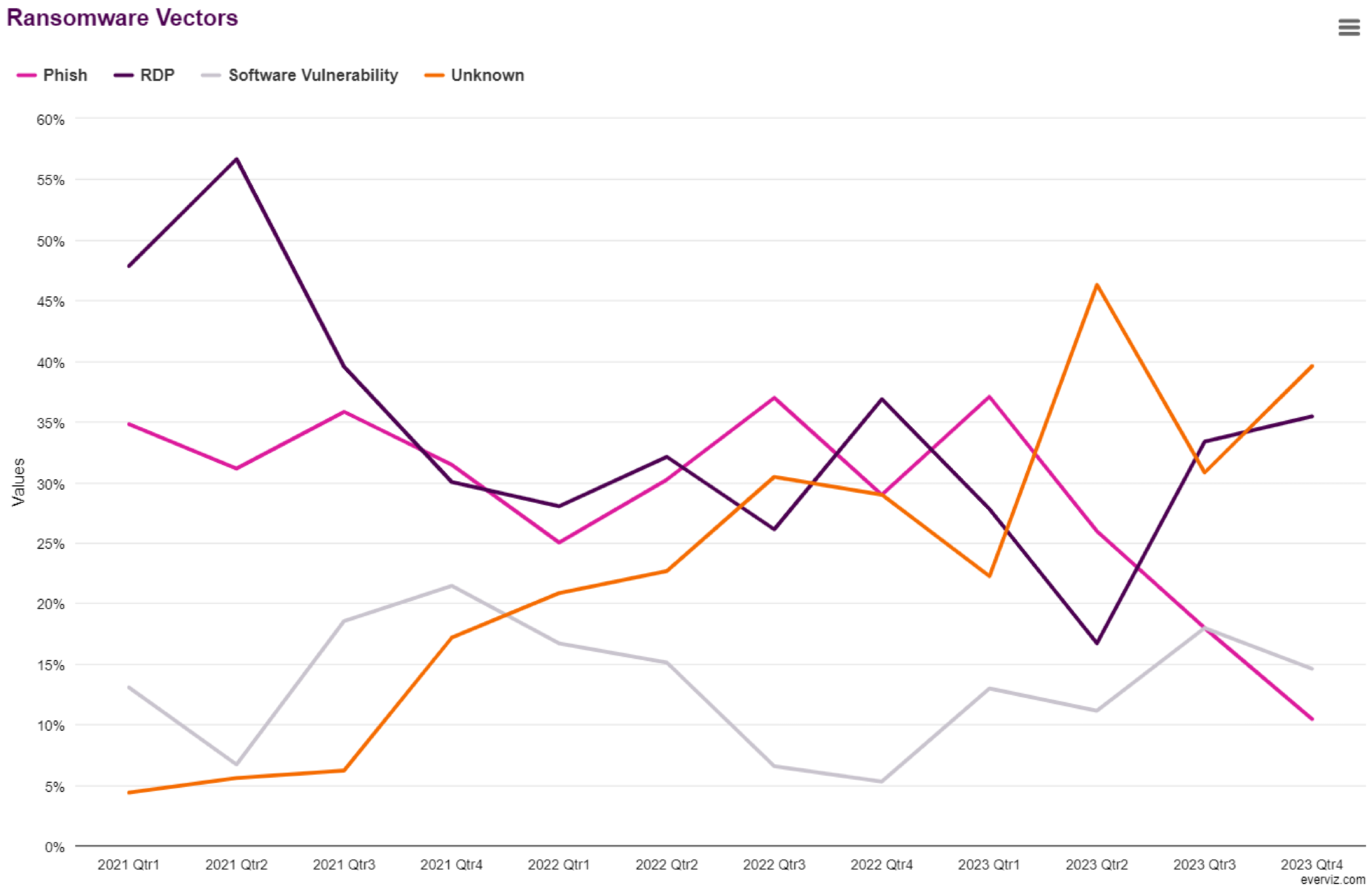


beazley

Cyber extortion incidents with data exfiltration



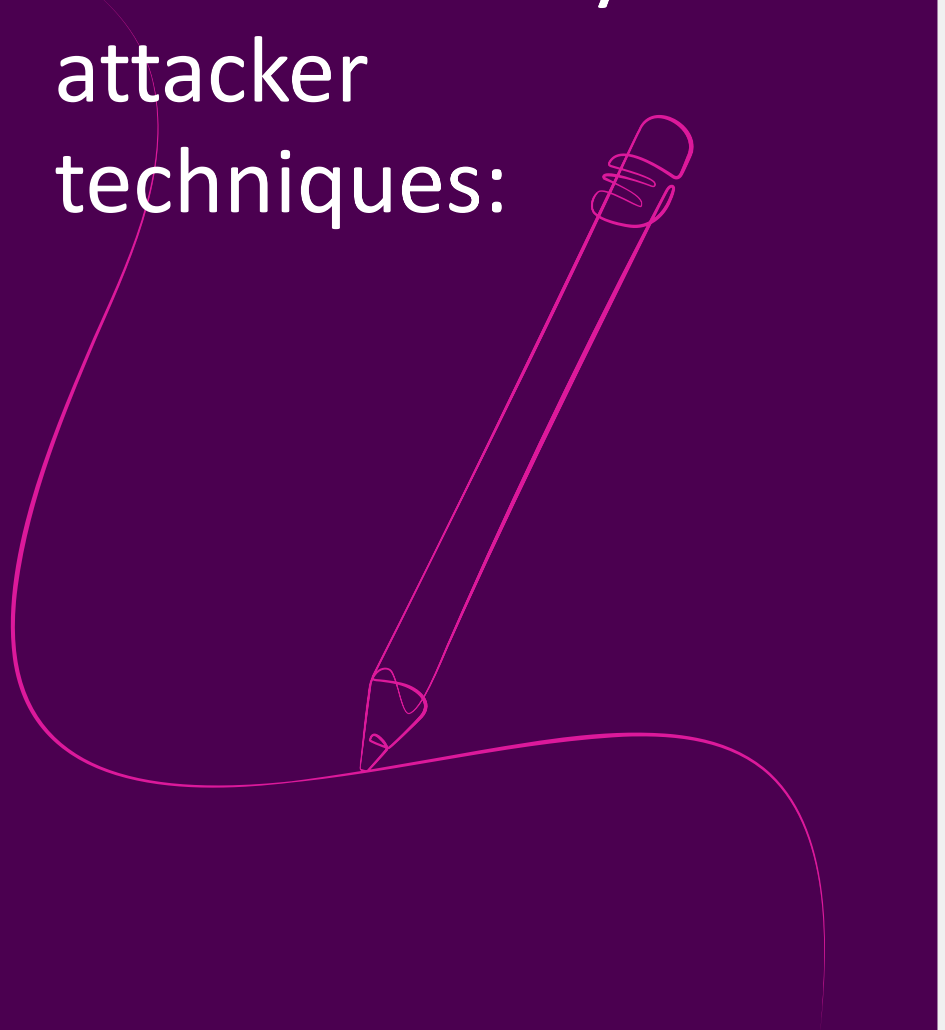
Ransomware vectors



beazley

Predictions

By staying ahead of cyber threats and updating controls we can combat the evolution of cyber attacker techniques:



01

The evolution of social engineering techniques

Cybercriminals imitate IT support staff to trick employees into installing and accessing tools, they also impersonate employees to deceive IT support staff into inadvertently allowing access.

02

Attackers find new ways to bypass security controls

Customised, specific security training provides a strong first line of defence. Phishing-resistant forms of MFA can make it harder for cybercriminals to impersonate your employees. By using hardware tokens or passkeys instead of passwords its harder for a criminal to enter a network.

03

Getting to know “known” threat groups

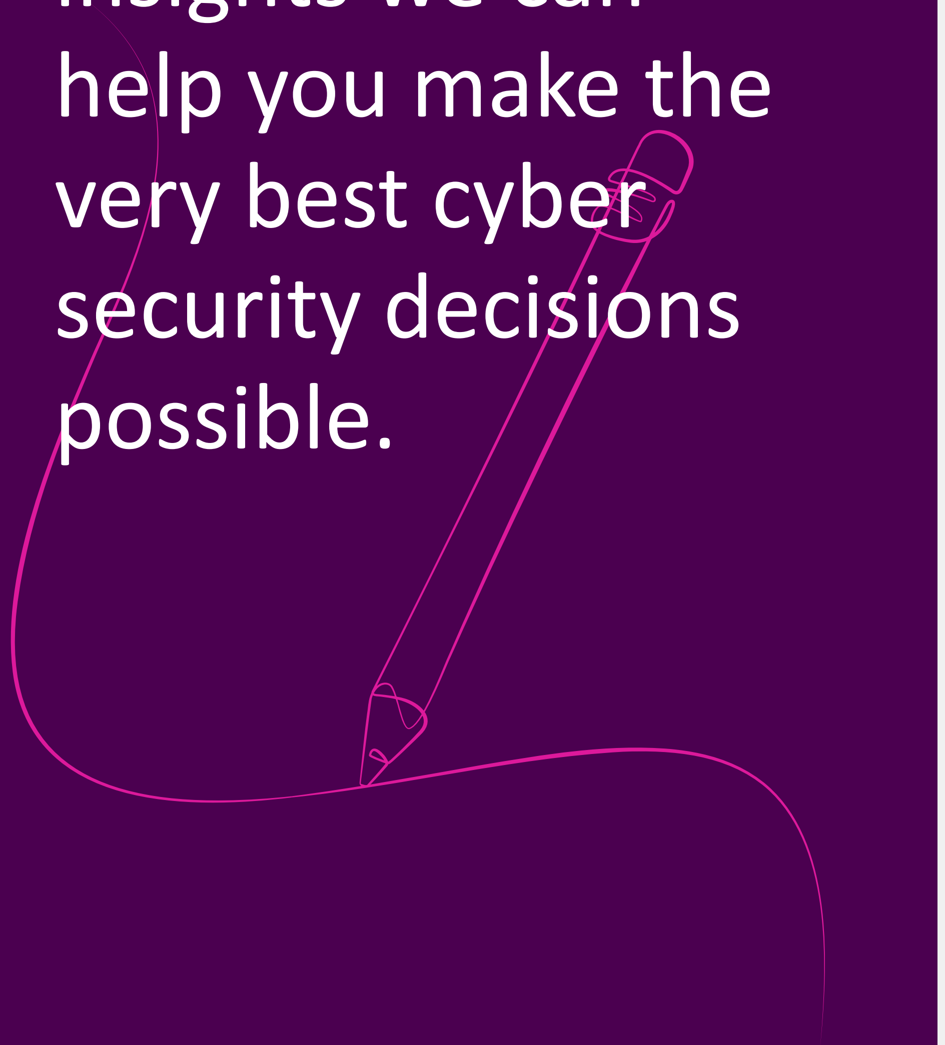
Keeping tabs on cybercriminal groups and threat intel reports can help tailor your cyber defences. Understanding groups like **Scattered Spider** and **The CL0P**, and their techniques, can help with incident negotiation and outcomes.

04

Keeping pace with the risks

Recent attacks demonstrate that motivated cybercriminals will eventually compromise a network; organisations must continually improve their ability to respond if a cyber hacker gets past their initial defences.

By tracking the cyber trends and paying close attention to the insights we can help you make the very best cyber security decisions possible.



01

AI’s considerable impact will play out in the courts in 2025

With high-profile lawsuits pending against key players like Open AI and Meta we’re likely to see US courts rendering a patchwork of decisions affecting several key categories.

02

Global regulatory change is likely to influence behaviours

What happens in one region could impact other regions around the world, including possible ripple effects to cover and policies.

03

Privacy and tracking claims are likely to reach a tipping point

Privacy will be a continued and exacerbated theme for 2025 especially for the US, where more privacy and tracking claims are anticipated.

04

Attackers will employ a wider range of strategies and tactics

Cybercriminals are constantly evolving their tactics to increase pressure on their victims, as they seek to maximise the monetary value of their attacks.

05

AI will increase the threat landscape in 2025

Regulation will continue to evolve over the course of the year and there will also be greater pressure on firms who suffer a data breach or cyberattack to notify official privacy bodies, which could create additional knock-on effects following an incident.

Find out more and read the new Cyber Services Snapshot:

https://www.beazley.com/en-001/cyber-services-snapshot/the-evolution-of-cyber-attacker-techniques/

To read all previous Cyber Services Snapshots visit:

https://www.beazley.com/en-001/cyber-services-snapshot

How we work to protect your client in the first 48 hours after a ransomware incident

Preserve

- Take steps to preserve evidence for forensic investigation where possible
- Preserve the firewall logs before they are over written
- Take a least one copy of the backups offline if this has not been done already
- Switch to more secure communications ("Out of Band")

Investigate

- Attempt to locate the ransom note. Make note of any threats of data leak and the name of the group used in the note.
- Appoint a forensics investigator and provide the necessary forensics evidence
- Determine the scope of the attack
  - Determine if your business critical data has been made unusable
  - Determine if there has been unauthorised access to personal data
- Verify the viability of the backups
- Appoint a lawyer
- Appoint a ransomware negotiator

Minimise

- Consider isolating the affected environment until the situation has been sufficiently contained
  - At the direction of a forensics firm, allow external connections to only IP addresses that are explicitly trusted
- Disconnect suspected compromised devices from the network
- Reset passwords for all accounts
- Appoint a PR agency

Recover

- Establish a new way of working; given the limited capacity
- Form action plan for a secure and quick recovery
  - Create a secure IT environment that can be used for recovering backups (e.g. cloud)
  - Scan and assess the newly restored backup to check for any sign of malware or cybercriminal activity
  - Install critical patches and limit services that are exposed to the internet

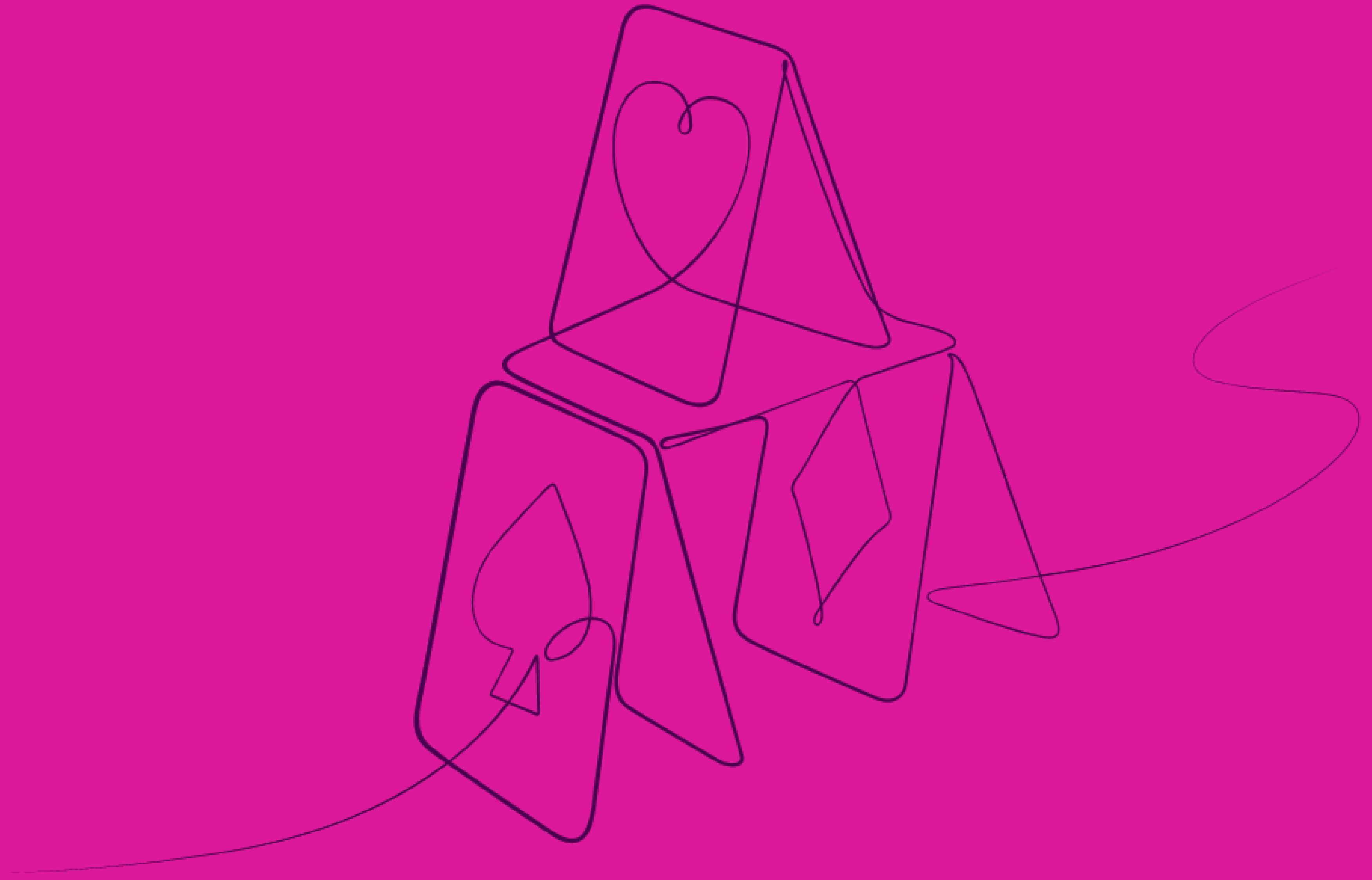
You are obligated to notify the regulator of any data breach no later than 72 hours after discovery click here

beazley

disclaimer

The information set forth in this document is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Beazley has not examined and/ or had access to any particular circumstances, needs, contracts and/or operations of any party having access to this document. There may be specific issues under applicable law, or related to the particular circumstances of your contracts or operations, for which you may wish the assistance of counsel. Although reasonable care has been taken in preparing the information set forth in this document, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.

Thank You



beazley

Thank You

Scan the QR code to view and download today's Cybersecurity Toolkit