SAFER

Cyber Insight Day

July 29, 2021

Agenda

- Cyber Trends
- Coverage Review
- Overview of Best Practices, Impact on Deductible & Pre-loss Solutions
- Incident Response/Claim Process
- Q&A

Disclaimer

The material presented in this presentation is not intended to provide legal or other expert advice as to any of the subjects mentioned, but rather is presented for general information only. You should consult knowledgeable legal counsel, forensic experts, or other knowledgeable experts as to any legal or technical information.

Panelists

Jacqui Spencer-Sim, Hamilton
Underwriter

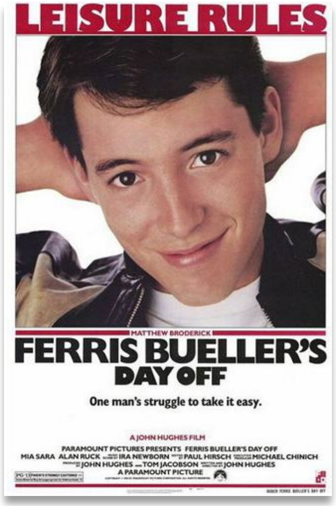
Bill Hardin, Charles River Associates
Forensics Expert

John Loyal, Cipriani and Werner
Breach Counsel

Chris Gissing, CyberScout
Breach Response Expert

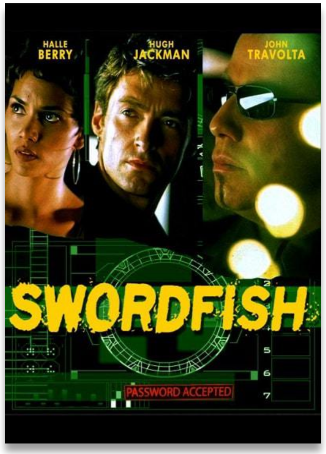
Neutral

Hollywood Impact



OLIVER STONE
THE ONLY SAFE PLACE IS ON THE RUN
SNOWDEN
JOSEPH GORDON-LEVITT // SHAILENE WOODLEY
DIRECTED BY OLIVER STONE
SCREENPLAY BY KIERAN FITZGERALD & OLIVER STONE

DESPERATE TIMES DESPERATE MEASURES
TOM CRUISE
MISSION: IMPOSSIBLE
ROGUE NATION
IN THEATERS AND IMAX JULY 31



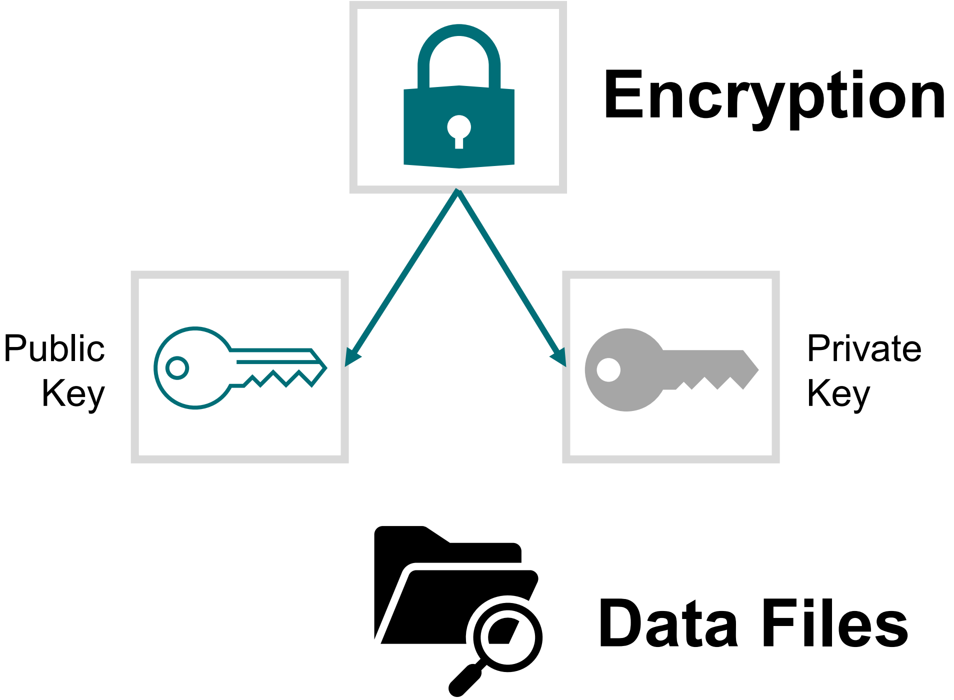
Inattentional Blindness

Focus on one thing and we fail to see other things in plain sight.

EMBER is Burning

1. **E**xtortion
2. **M**alware
3. **B**usiness Email Compromise
4. **E**ngineering
5. **R**egulatory

Extortion Game – Ransomware



Encryption

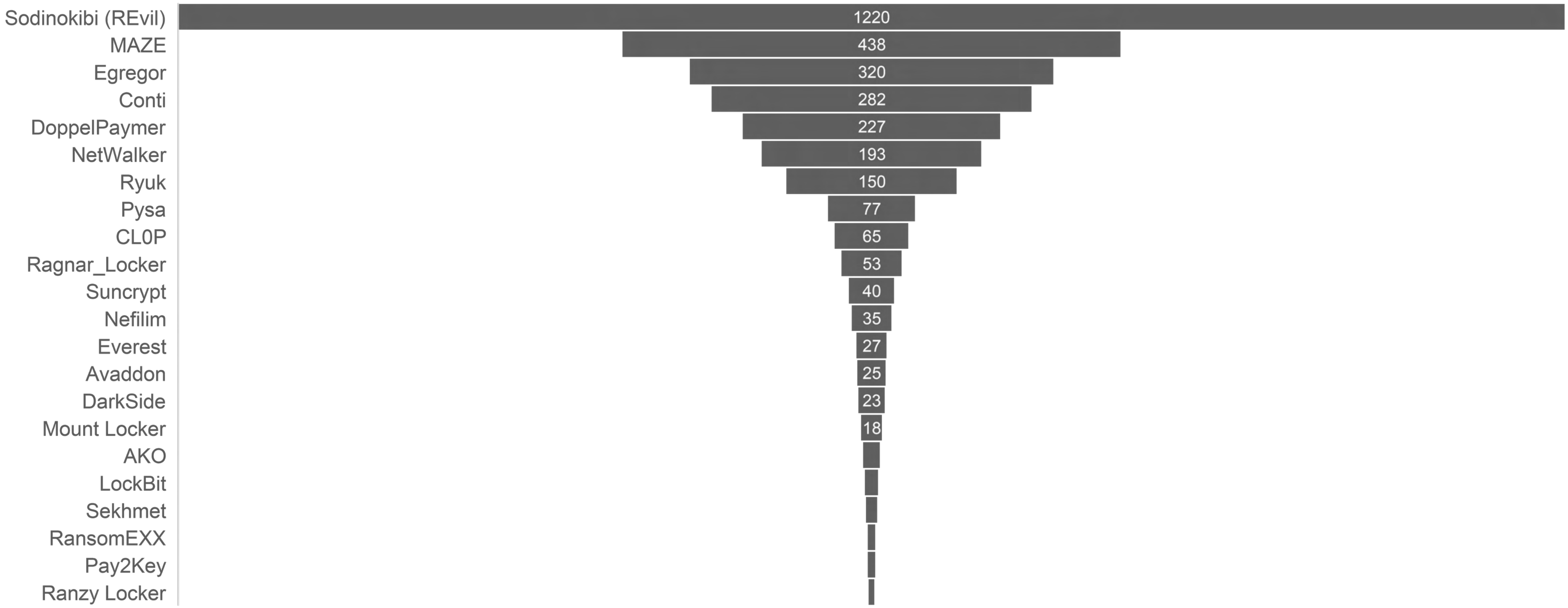
Public Key

Private Key

Data Files

Payment

2020 Threat Actor of the Year Awards



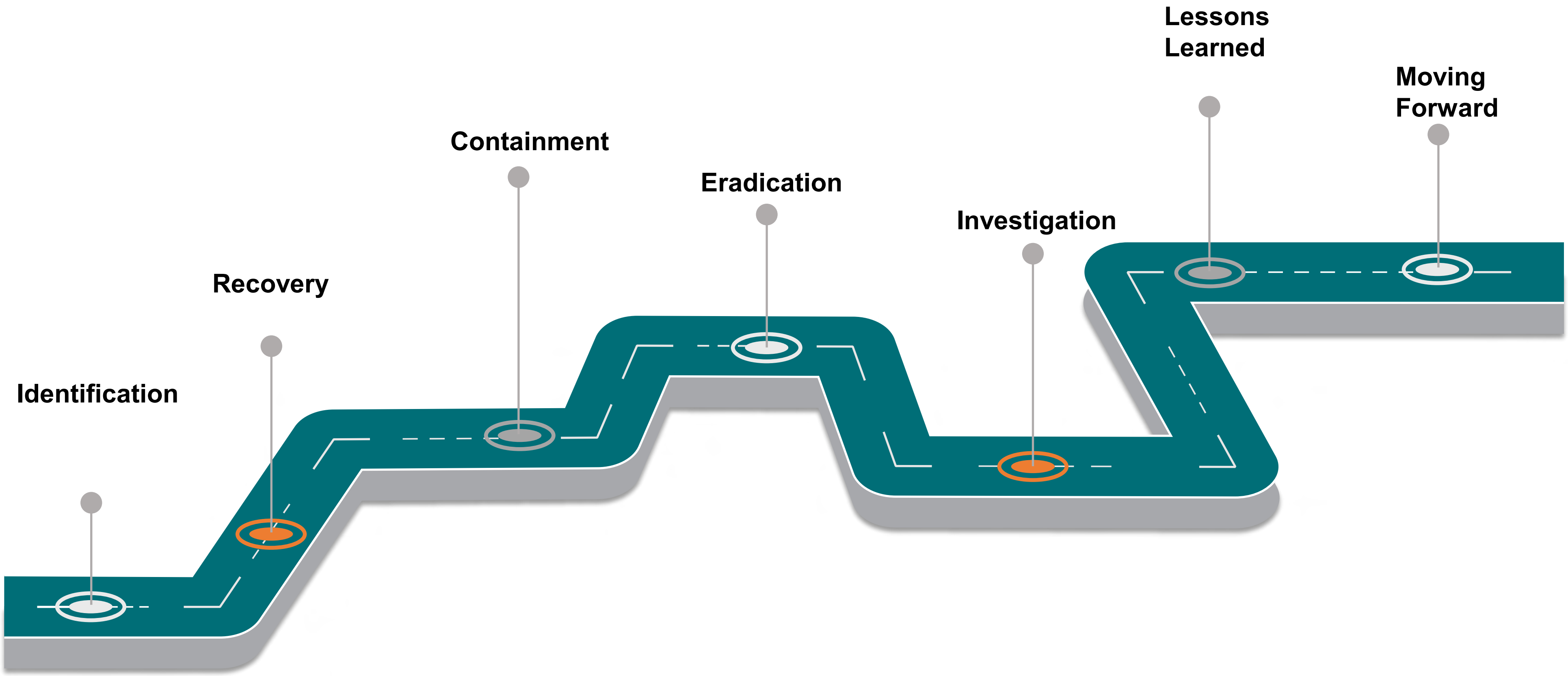
Economics

Maze Campaign – RETIRED

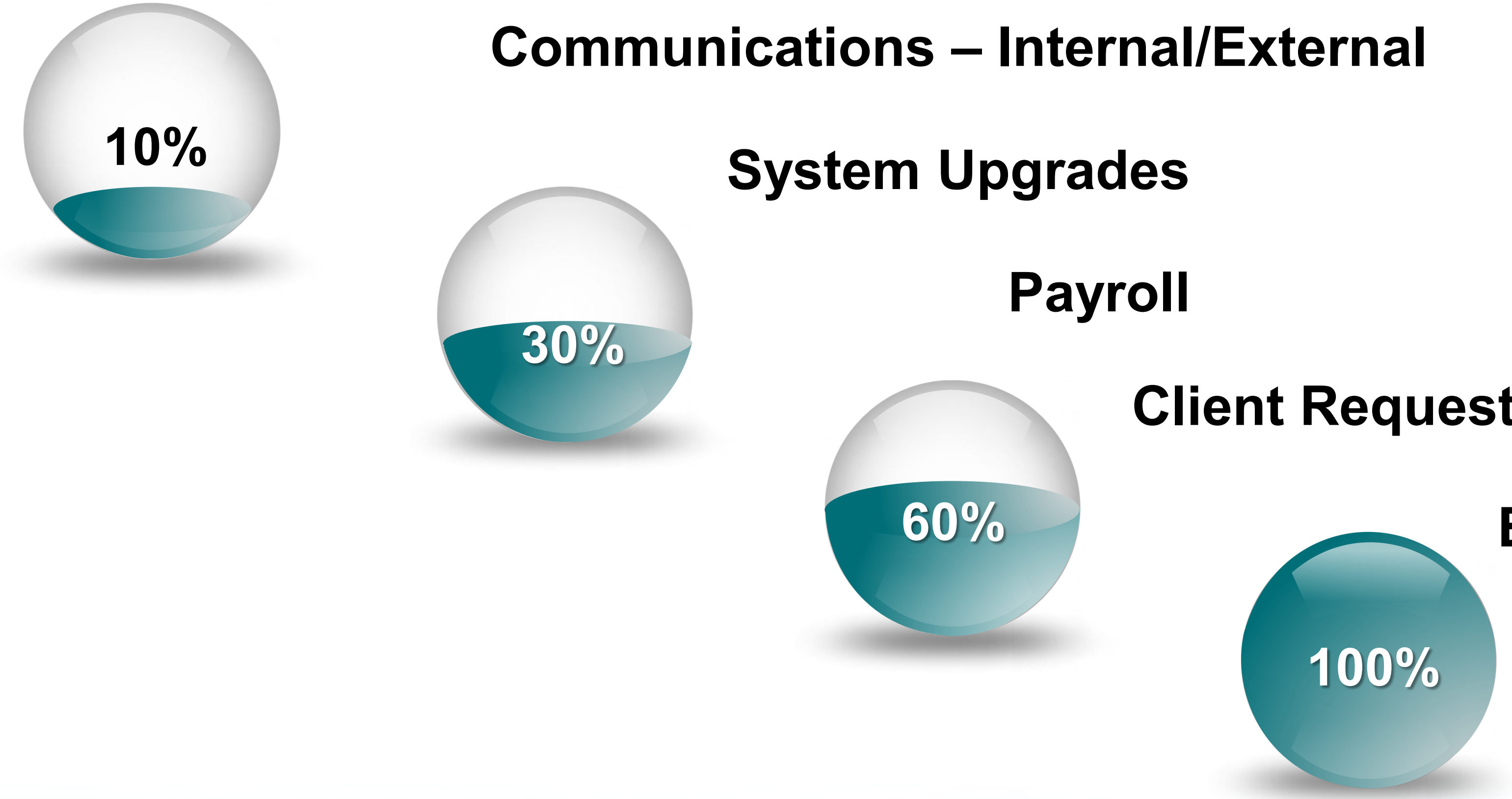
- **Ransom payment ranges:** $50,000 to $35,000,000
- **Operational impact**: Backup and production systems
- **Targets:** All operating companies around the world
- **First seen:** July 2019
- **Data exfil:** High
- **Potential profits from campaign: $750 million**
- **eCrime syndicate locations:** Multiple continents
- **Deployment:** Known to sell the code to other eCrime syndicates for franchise fees
- **Evolving:** Attack kit now includes functionality to search for sensitive information to extract before encryption occurs

Ransom Notes: The Message of Threat Actors

Understanding the Event



Business Interruption



Systems Impacted

Communications – Internal/External

System Upgrades

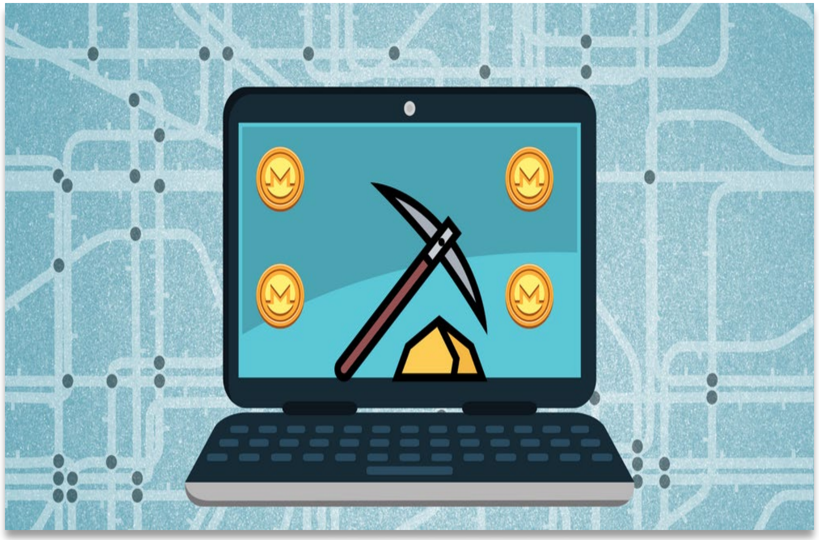
Payroll

Client Requests

Business Competitors

Malware

- Malware as a Service
- Zero Day Exploit Kits
- Emotet
- Trickbot
- Dridex
- Crypto Mining



Business Email Compromise

- COVID-19 statistics
- Storage space exceeded
- Security alert
- Password expiring
- UPS delivery notice
- Job satisfaction survey
- DocuSign document T247218
- Bill shared a file with you

- USPS: Failed delivery notice
- Unusual sign-in activity: Verify your identity
- Microsoft: Your account will be deactivated

Business Email Compromise

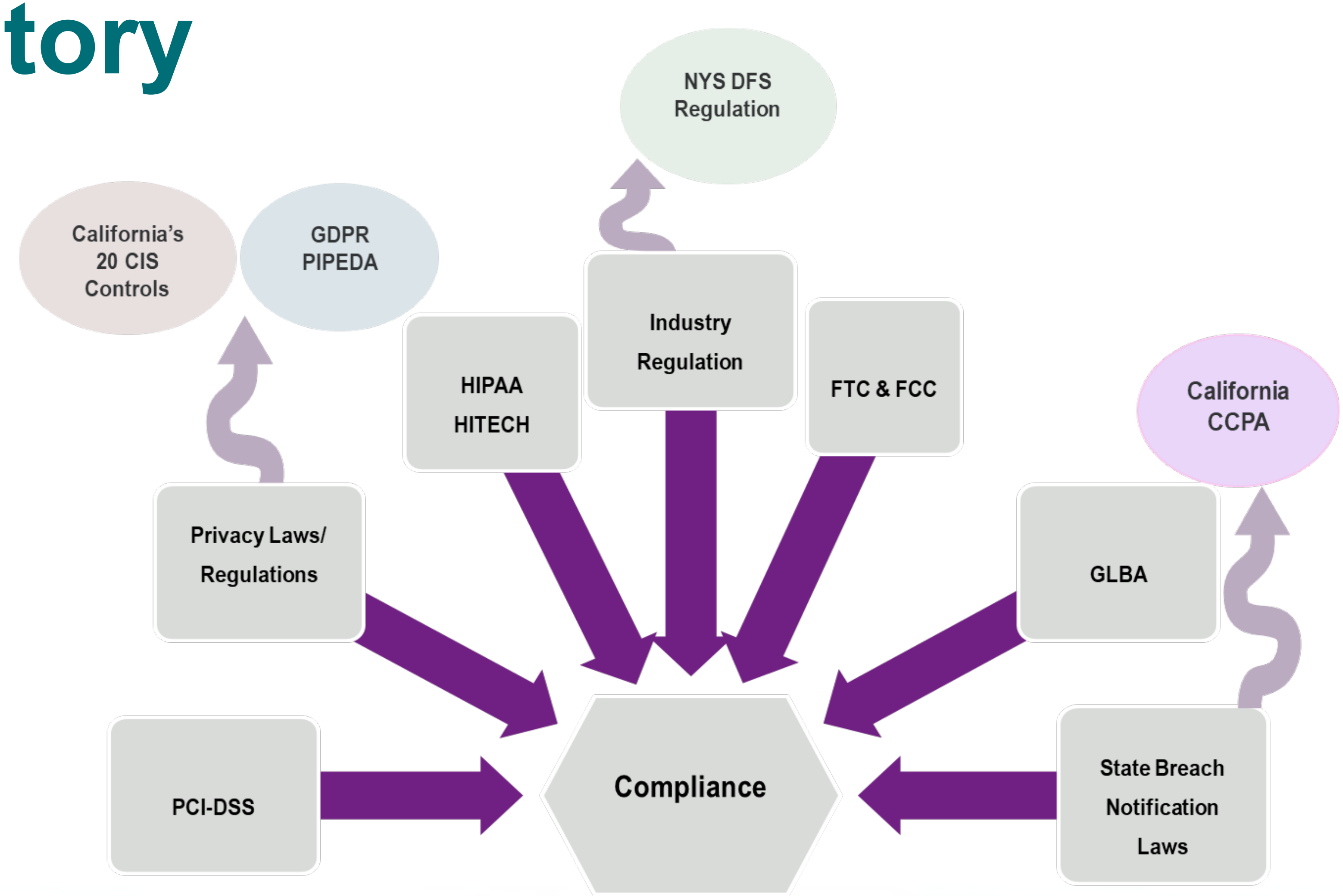
Attack methodology, information, and theft

Phishing/spam emails	Email spoofing and impersonation	Unauthorized inbox rules/ forwarding	Malware
Malicious macros/PDFs	Contact harvesting	PCI (Payment Card Industry)	PHI (Protected Health Information)
PII (Personally Identifiable Information)	Passwords stored in email	Other platforms exposed	Compromised VPN (Virtual Private Network) credentials
Wire/bank fraud	Direct deposit/ payroll fraud	Tax return fraud	Theft of intellectual property

Engineering

1. Synthetic IDs
2. Smishing
3. Vishing
4. Bio hacking
5. Social media profiles
6. Code injections
7. Bug bounties

Regulatory


NYS DFS Regulation
California's 20 CIS Controls
GDPR PIPEDA
Industry Regulation
HIPAA HITECH
FTC & FCC
California CCPA
Privacy Laws/ Regulations
GLBA
PCI-DSS
Compliance
State Breach Notification Laws

Coverage Overview

$15M Policy Aggregate

Members may select aggregate limits of $1M, $3M, $5M

3rd party coverage	1st party coverage
Privacy Liability Privacy Regulatory Claims Security Liability	Cyber Extortion Digital Asset Restoration Security Breach Response Cyber Crime Bricking/Hardware

Coverage Overview

✓ Best Practices Implemented

$25,000 each claim K12s < 9,000 ADA

$50,000 each claim K12s > 9,000 ADA

$75,000 each claim Community Colleges

✗ Best Practices Not Implemented

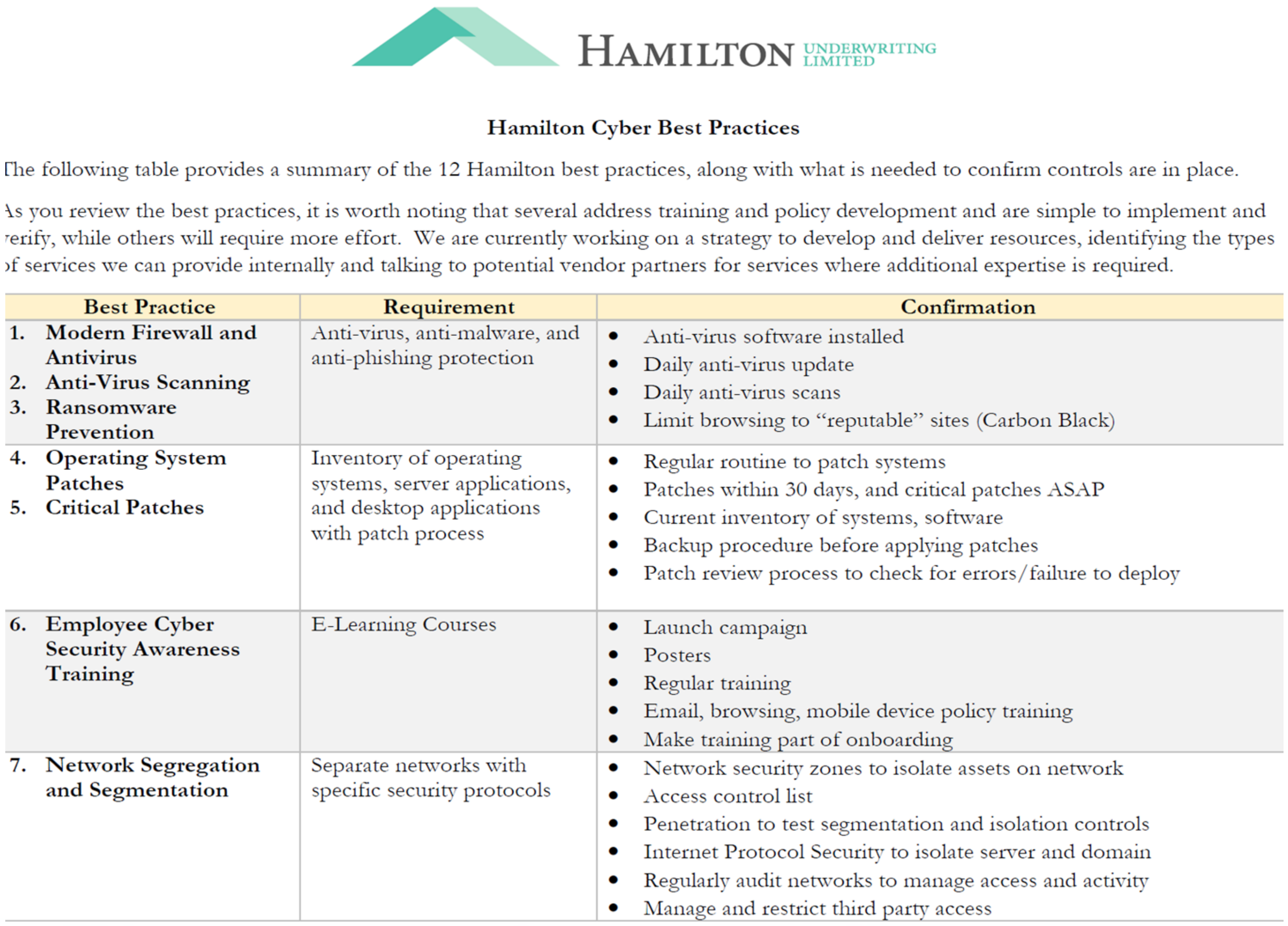
$50,000 each claim K12s < 9,000 ADA

$100,000 each claim K12s > 9,000 ADA

$150,000 each claim Community Colleges

Best Practices Overview

- Modern firewall and antivirus are in place
- Regular antivirus scanning
- Firewalls are configured to prevent ransomware
- Operating systems patches are kept up to date
- Critical patching is completed as soon as possible
- Employee cyber security awareness training and best practices are in place
- Confirm that schools are not connected/segregated
- Privilege access management is limited
- Two-factor authentication is in place
- Strong password policy is in place
- Off-site backup is in place
- Email filtering to prevent spam reaching employees



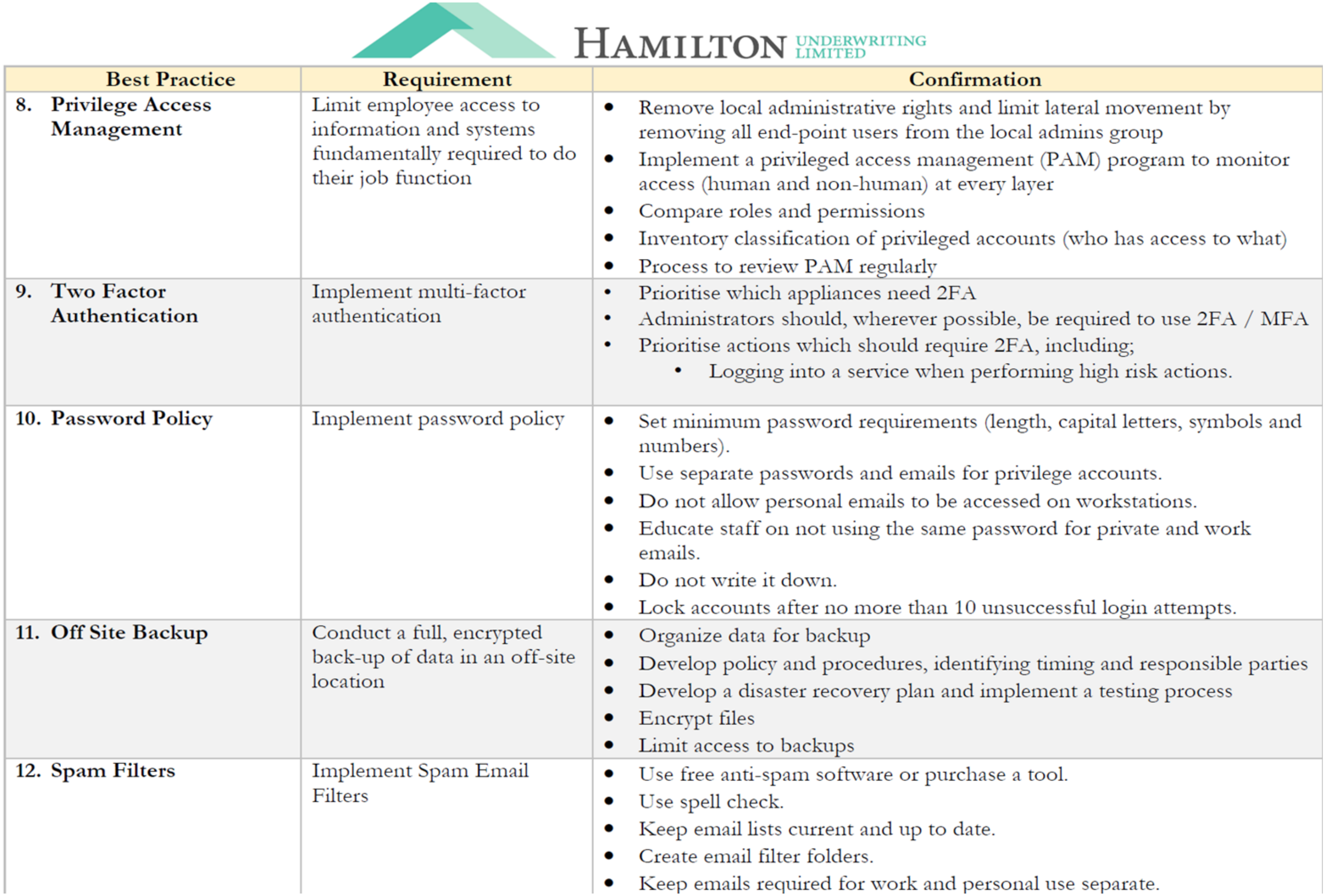
HAMILTON UNDERWRITING LIMITED

Hamilton Cyber Best Practices

The following table provides a summary of the 12 Hamilton best practices, along with what is needed to confirm controls are in place.

As you review the best practices, it is worth noting that several address training and policy development and are simple to implement and verify, while others will require more effort. We are currently working on a strategy to develop and deliver resources, identifying the types of services we can provide internally and talking to potential vendor partners for services where additional expertise is required.

Best Practice	Requirement	Confirmation
1. Modern Firewall and Antivirus **2. Anti-Virus Scanning** **3. Ransomware Prevention**	Anti-virus, anti-malware, and anti-phishing protection	• Anti-virus software installed • Daily anti-virus update • Daily anti-virus scans • Limit browsing to "reputable" sites (Carbon Black)
4. Operating System Patches **5. Critical Patches**	Inventory of operating systems, server applications, and desktop applications with patch process	• Regular routine to patch systems • Patches within 30 days, and critical patches ASAP • Current inventory of systems, software • Backup procedure before applying patches • Patch review process to check for errors/failure to deploy
6. Employee Cyber Security Awareness Training	E-Learning Courses	• Launch campaign • Posters • Regular training • Email, browsing, mobile device policy training • Make training part of onboarding
7. Network Segregation and Segmentation	Separate networks with specific security protocols	• Network security zones to isolate assets on network • Access control list • Penetration to test segmentation and isolation controls • Internet Protocol Security to isolate server and domain • Regularly audit networks to manage access and activity • Manage and restrict third party access



HAMILTON UNDERWRITING LIMITED

Best Practice	Requirement	Confirmation
8. **Privilege Access Management**	Limit employee access to information and systems fundamentally required to do their job function	• Remove local administrative rights and limit lateral movement by removing all end-point users from the local admins group • Implement a privileged access management (PAM) program to monitor access (human and non-human) at every layer • Compare roles and permissions • Inventory classification of privileged accounts (who has access to what) • Process to review PAM regularly
9. **Two Factor Authentication**	Implement multi-factor authentication	• Prioritise which appliances need 2FA • Administrators should, wherever possible, be required to use 2FA / MFA • Prioritise actions which should require 2FA, including; • Logging into a service when performing high risk actions.
10. **Password Policy**	Implement password policy	• Set minimum password requirements (length, capital letters, symbols and numbers). • Use separate passwords and emails for privilege accounts. • Do not allow personal emails to be accessed on workstations. • Educate staff on not using the same password for private and work emails. • Do not write it down. • Lock accounts after no more than 10 unsuccessful login attempts.
11. **Off Site Backup**	Conduct a full, encrypted back-up of data in an off-site location	• Organize data for backup • Develop policy and procedures, identifying timing and responsible parties • Develop a disaster recovery plan and implement a testing process • Encrypt files • Limit access to backups
12. **Spam Filters**	Implement Spam Email Filters	• Use free anti-spam software or purchase a tool. • Use spell check. • Keep email lists current and up to date. • Create email filter folders. • Keep emails required for work and personal use separate.

Submitted Questions

- Will Hamilton be auditing members or will the survey be their method of compliance assessment?
- To achieve full compliance, do we need to have all practices in place before September 1st? If we have a couple in development would that be acceptable?
    - If not acceptable, will we be able to alert Hamilton when we have all deployed or will it have to wait until 2022 renewal?
- Do these points pertain to all computers, such as for student use and computer labs, or do they apply only to business-related computers/servers/processes?
- If the best practices list a specific vendor, do we have to use that vendor (i.e. Carbon Black)?

Best Practices 1, 2 & 3

1. Confirm modern firewall and antivirus

The modern firewall should provide protection against both basic and advanced cyber threats. This requires both core prevention technology – such as antivirus, anti-malware, and anti-phishing protection – as well as the ability to ingest threat intelligence feeds and use them to identify more sophisticated attacks. A firewall acts as a mechanism to filter out malicious traffic before it crosses the network perimeter.

2. Regular anti-virus scanning

Keeping your computer protected from viruses and malware maintains the integrity of your system and prevents you from unknowingly infecting other systems. Antivirus programs provide a way to protect against known threats.

Best Practices 1, 2 & 3

3. Confirm that firewalls are configured to prevent ransomware

- Your firewall and endpoint security can protect against attacks getting onto the network in the first place, and if an attack should somehow penetrate your network, they can prevent it from spreading and infecting other systems.
- Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks.

★★★ Top Tips ★★★

- Examine trusted sources or reviews for different antivirus programs to decide what is best for you
- Ensure antivirus program updates daily, at a time when your computer is not in use, for it to be most effective
- Ensure scans are performed at regular intervals (daily)
- Visit only reputable sites to limit exposure

Submitted Question

In our county, the schools connect to the districts; the districts connect to the COE; the COE connects to “the world.”

If the COE has a “modern firewall,” does that also count for the districts and schools since their path to “the world” would be through the COE's firewall? Or will each district/school be required to have their own modern firewall?

Best Practices 4 & 5

4. Confirm that critical patching is completed

- Product vendors provide fixes for vulnerabilities identified in products that they still support, in the form of software updates known as “patches.” Patches may be made available to customers immediately or on a regular release schedule.
- Patches are part of essential preventative maintenance necessary to keep machines up-to-date, stable, and safe from malware and other threats. You can’t know what you need to patch until you know what you have. You have operating systems, server applications and desktop applications. You also need to patch servers, PCs, mobile devices, hardware-based appliances, such as firewalls, routers, SANs, etc.

5. Confirm that operating system patching is up-to-date

Operating system (OS) patching is an important part of keeping IT systems and applications in your cloud or on-premise environment safe from malicious users that exploit vulnerabilities. The timely deployment of patches dramatically reduces risk.

Best Practices 4 & 5

★★★ Top Tips ★★★

- Apply patches 30 days from their release to allow for testing unless an immediate threat is announced
- Set a regularly scheduled routine to patch your systems
- Be aware of what systems you need to patch by identifying what software you are using
- Ensure you back up your systems before applying patches
- Take time to review the patches after they have deployed to check for errors or failure to deploy

Submitted Question

Most of our districts and even our COE are very small; we only have a handful of computers. Is manual patching via the OS's built-in patching function by tech support staff adequate or do we need a patch management software beyond the built-in OS patching software?

Best Practice 6

6. Confirm that employee Cybersecurity Awareness Training and Best Practices are in place

- Anyone who uses computers, mobile phones or tablets in their day-to-day work should be trained in cybersecurity and how to spot potential scams. Cybersecurity training ensures that staff can identify data threats and take action to ensure that these threats don’t affect the company. Cybersecurity training will not only help employees in the workplace, but at home too – keeping their own personal data safe and secure.
- By conducting employee cybersecurity training, your staff will be better equipped to identify and respond to any cyber threat.

Best Practice 6

★★★ Top Tips ★★★

- Campaign launch that states your intention to address cyber security
- E-learning training courses for awareness
- Visual reminders – posters to reinforce your company culture, e-mail signatures that highlight your awareness program
- Cyber champions
- Frequent employee training for cybersecurity awareness and regular cyber security briefings
- Emphasize the importance of reporting cyber security incidents
- Teach employees to recognize phishing attempts
- Revise policies to include rules for email, browsing, and mobile devices
- Make cybersecurity a part of onboarding
- Ensure employees recognize the importance of cybersecurity training and raise awareness around current cyber threats

Submitted Questions

- Do the Keenan SafeSchools or SafeColleges courses satisfy the requirement to conduct cyber security training for all employees? **Yes**
- Would posting flyers satisfy the requirement?
- Would an email campaign comply (training best practice requirement)?
- We bought a cybersecurity training service (KnowBe4) and will implement it as school starts, but it may not have gotten out to all district personnel completely by the August 31 deadline since some schools won't be in session by then. Does this meet the requirement?

Best Practice 7

7. Confirm that schools are not segregated or connected

- Segmentation improves cybersecurity by limiting how far an attack can spread. For example, segmentation keeps a malware outbreak in one section from affecting systems in another.
- Network segregation and segmentation are highly effective strategies an organization can implement to limit the impact of a network intrusion, making it significantly more difficult for a hacker to locate and gain access to an organization’s more sensitive information. It also increases the likelihood of detecting hacker activity in a timely manner. Each separate network should have specific security protocols applied.

Best Practice 7

★★★ Top Tips ★★★

- Prevent single point of failure
- Create network security zones to isolate assets on the network
- Create an access control list
- Have a penetration test to test how well existing segmentation controls are isolating different network zones
- Implementing server and domain isolations using Internet Protocol Security (IPSec)
- Restrict the level of access users have to sensitive information only to those who need it; use the **principles of privilege** across the organization
- Audit your networks regularly to enable the organization to manage access and activity, regular audits are critical to the segmentation process and will help identify security gaps
- Manage and restrict third party access

Submitted Questions

- Can you further define “domain”? Do you mean Windows Active Directory domain? Or Internet domain name? Or some other domain type?
- Can you define and explain more about “software-defined access technology”?

Best Practice 8

8. Confirm that Privilege Access Management is limited

- Privileged user accounts are a prime target for attackers who wish to hijack the account to access data or introduce malware. Management of privileged accounts and sensitive assets is key for visibility and control.
- It is good practice to review these regularly and to use a least privilege-based approach, meaning that all users should only have access to the information and systems fundamentally required for their job functions. By doing this, companies minimize the danger of insider and external threats, which otherwise could end up as a data breach.

Best Practice 8

★★★ Top Tips ★★★

- The Principle of Least Privilege – remove local administrative rights, restrict access to what is required
- Implement a privileged access management (PAM) program to effectively monitor where privileged access exists at every layer, understand which users (both human and non-human) have access to what, detect and alert on malicious or high-risk activity
- Compare roles and permissions
- Establish and enforce a comprehensive privilege management policy
- Address the inventory and classification of privileged accounts
- Enforce password security best practices
- Follow the Zero-trust model and apply the principle of least privilege
- Review privilege access and administrative rights regularly and remove where required, e.g job roles
- Limit lateral movement by removing all end-point users from the local admins group

Submitted Question

- Can you give an example of “control/manage privileged access management to contain elevated privileges”?

Technology: Do You Have Backup?

What is a backup? Holding your data files in a secure location that you can readily and easily access.

What are the benefits of a backup?

- Access your files anywhere
- More efficient storage

What are the *true* benefits of a backup? It can potentially negate ransomware, as files, drives etc. can be reinstalled after wiping

Best Practice 9

9. Confirm that Two-Factor Authentication (2FA) is in place

- 2FA is the single best thing you can do to improve the security of your important accounts. It has low complexity, which makes it an easy addition, and can be rolled out quickly without busting your budget.
- It works by adding an additional layer of security to accounts. It requires an additional login credential – beyond just the username and password – to gain account access. Getting that second credential requires access to something that belongs to you which only you can access.
- All users should use 2FA or MFA (multifactor authentication) when using cloud and other internet-connected services. This is particularly important when authenticating to services that hold sensitive or private data.

★★★ Top Tips ★★★

- Prioritize which appliances need 2FA
- Administrators should, wherever possible, be required to use 2FA/MFA
- Prioritize actions which should require 2FA, including logging into a service when performing high risk actions

Best Practice 10

10. Confirm that a strong password policy is in place

Passwords provide the first line of defense against unauthorized access to your computer or personal information. The stronger the password, the more protected your computer will be. A password should be a meaningless word, number, symbol and be at least 8 characters long.

★★★ Top Tips ★★★

- Set minimum password requirements (length, capital letters, symbols, and numbers)
- Use separate passwords and emails for privilege accounts
- Do not allow personal emails to be accessed on workstations
- Educate staff on not using the same password for private and work emails
- Do not write it down
- Lock accounts after no more than 10 unsuccessful login attempts

Best Practice 11

11. Confirm that off-site backup is in place

- Backups are a way of securing data in a different location. If you just perform regular backups to a nearby external hard drive or in the same location, your data is not protected, as there is still a single point of failure. Off-site backup is literally backups stored in a different location. This could be storing data on tapes or a hard drive, automatically backing up to a remote server or in the cloud.
- Off-site back ups are crucial when faced with a cyber attack. Conducting a full, encrypted backup of your data in an off-site location will allow you to restore your data in the event of an attack. It is critical to know what needs to be backed up, how frequently backups should be done and how to restore the data from a backup. Using off-site back ups will help reduce the risks of a ransomware attack impacting a company's backups and will provide a better foundation for recovery in the event of an infection.

Best Practice 11

★★★ Top Tips ★★★

- Organize your data and learn what is needed for a backup and put a schedule in place
- Familiarize yourself with your backup policy and procedures. Make sure you know who is responsible for backups
- Have a disaster recovery plan in place and make sure it is tested and works
- Stick to the 3-2-1 approach: 3 copies of your data (your production data and two backup copies) on 2 different media with 1 copy stored off-site
- Encrypt your files
- Limit access to backups

Best Practices 12

12. Confirm email filtering to prevent spam reaching employees

- Spam filters detect unsolicited, unwanted, and virus-infested email from getting into your inbox
- By allowing email filtering, you allow the software to independently analyze incoming emails for red flags that signal spam/phishing content and automatically move those emails to a separate folder

★★★ Top Tips ★★★

- Use free anti-spam software or purchase a tool
- Use spell check
- Keep email lists current and up to date
- Create email filter folders
- Keep emails required for work and personal use separate

What’s Your Culture?

What are the *true* benefits of an open and honest culture?

- Less exposure/incidents
- Reduced time on claims/BI costs/operational losses
- Reputational loss

Someone…

Hacked Me

Ransomed Me

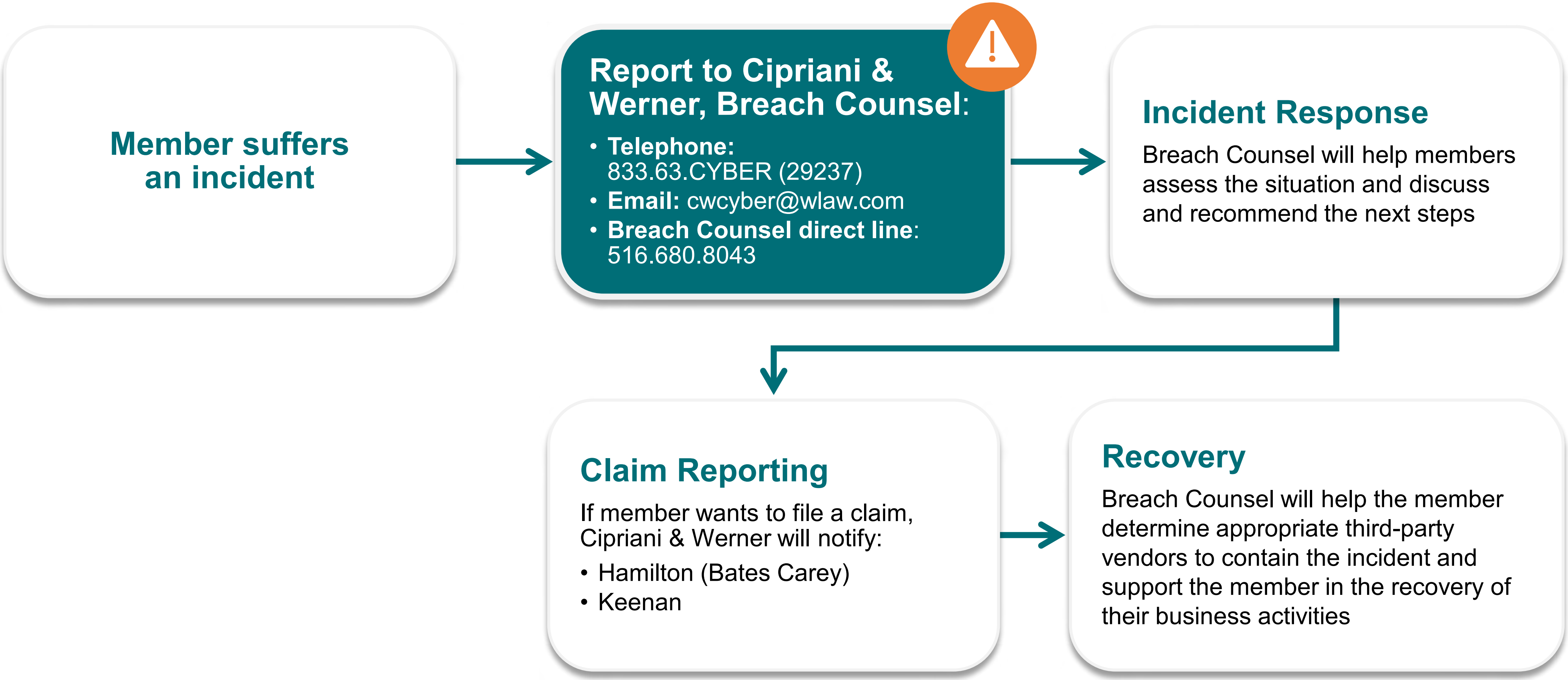
Phished Me

Accidentally Released PII/PHI

Fraudulently Transferred Data or Money

What now?

Incident Response/Claims Process



Member suffers an incident

Report to Cipriani & Werner, Breach Counsel:

- **Telephone:** 833.63.CYBER (29237)
- **Email:** cwcyber@wlaw.com
- **Breach Counsel direct line**: 516.680.8043

Incident Response

Breach Counsel will help members assess the situation and discuss and recommend the next steps

Claim Reporting

If member wants to file a claim, Cipriani & Werner will notify:

- Hamilton (Bates Carey)
- Keenan

Recovery

Breach Counsel will help the member determine appropriate third-party vendors to contain the incident and support the member in the recovery of their business activities

SAFER

Questions?

Disclaimer – Keenan & Associates is an insurance brokerage and consulting firm. It is not a law firm or an accounting firm. We do not give legal advice or tax advice and neither this presentation, the answers provided during the Question and Answer period, nor the documents accompanying this presentation constitutes or should be construed as legal or tax advice. You are advised to follow up with your own legal counsel and/or tax advisor to discuss how this information affects you.

SAFER

Thank you for your participation!