



Building Strong Cybersecurity Defenses

October 31, 2023
Diane McNally, SVP & National Insurance Practice Leader / Michael Stoyanovich, VP, Administration and Technology Consulting

Segal Select Insurance Services, Inc. is a subsidiary of The Segal Group, Inc., CA License # 0106323.



Today's Presenters



Diane McNally
Senior Vice President and
Insurance Practice Leader



Michael Stoyanovich
Vice President and Senior Consultant,
Administration & Technology

Agenda

Cybersecurity Risks and Threats

Changing Cyber Liability Insurance Market

Regulatory Cybersecurity Guidance

**How to Respond? One Suggested Strategy
and Supporting Tactics**

Risks to Manage and Threats to Mitigate

Risk

Data Privacy

There are multiple different federal data privacy rules, regulations and laws to be aware of.

Risk

Data Security

There are multiple different federal data security rules, regulations and laws to be aware of including recent sub-regulatory guidance from the DOL, etc. All states have breach notification laws.

Risk

Cyber Liability Insurance

Minimum underwriting standards has made it harder to obtain comprehensive coverage with prices fluctuating as well.

Threat

Cyber Criminal Activity

Cyber-criminal activity has increased dramatically: malware, phishing, ransomware and many other such attacks are all up double digits in the past four (4) years.

Also...regulatory investigation activity, related to privacy, security or prompted by criminal activity.

“US Smashes Annual Data Breach Record With Three Months Left”



“There were 2116 reported US data breaches and leaks in the first nine months of 2023, making it the worst year on record with a whole quarter left to go, according to the Identity Theft Resource Center (ITRC).”

“The non-profit, which tracks publicly reported breaches in the US, said there were 733 “data compromises” in Q3 2023, a 22% decline from the previous quarter. However, despite the relative slump, this was enough to drag the total for the year past the previous all-time high of 1862 set in 2021.”

[US Smashes Annual Data Breach Record With Three Months Left - Infosecurity Magazine \(infosecurity-magazine.com\)](https://www.infosecurity-magazine.com)

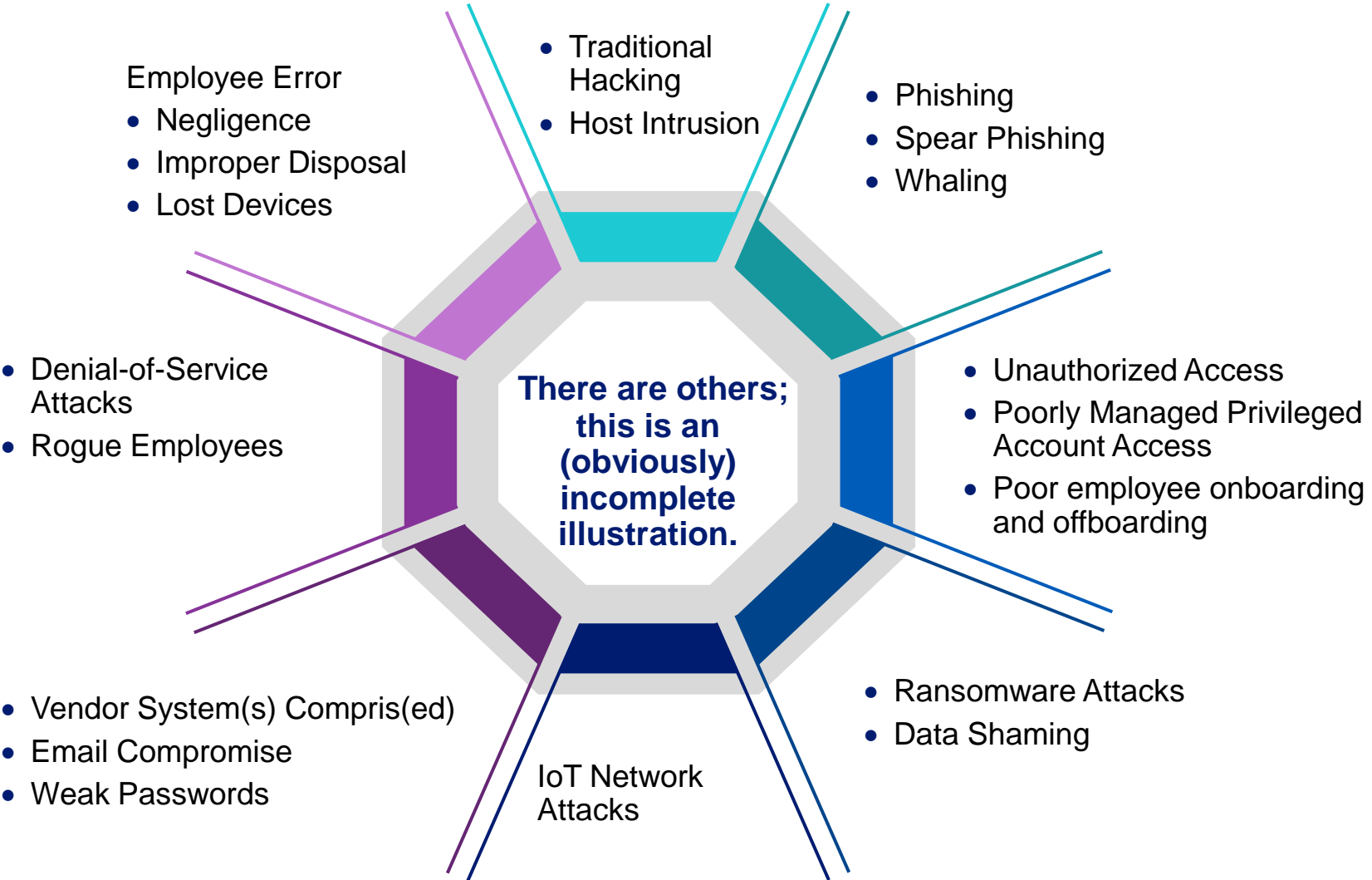
“78% of Healthcare Organizations Suffered a Cyberattack in the Past Year”



“A recent survey of healthcare professionals indicates 78% of healthcare organizations have experienced at least one cybersecurity incident in the past 12 months. 60% of those incidents had a moderate or significant impact on the delivery of care, 15% had a severe impact, and 30% involved sensitive data. Protected Health Information (PHI) was exposed or stolen in 34% of incidents in North America.”

[78% of Healthcare Organizations Suffered a Cyberattack in the Past Year \(hipaajournal.com\)](http://hipaajournal.com)

There Are Internal and External Cybersecurity Threats



(Some) Internal and External Cybersecurity Threats

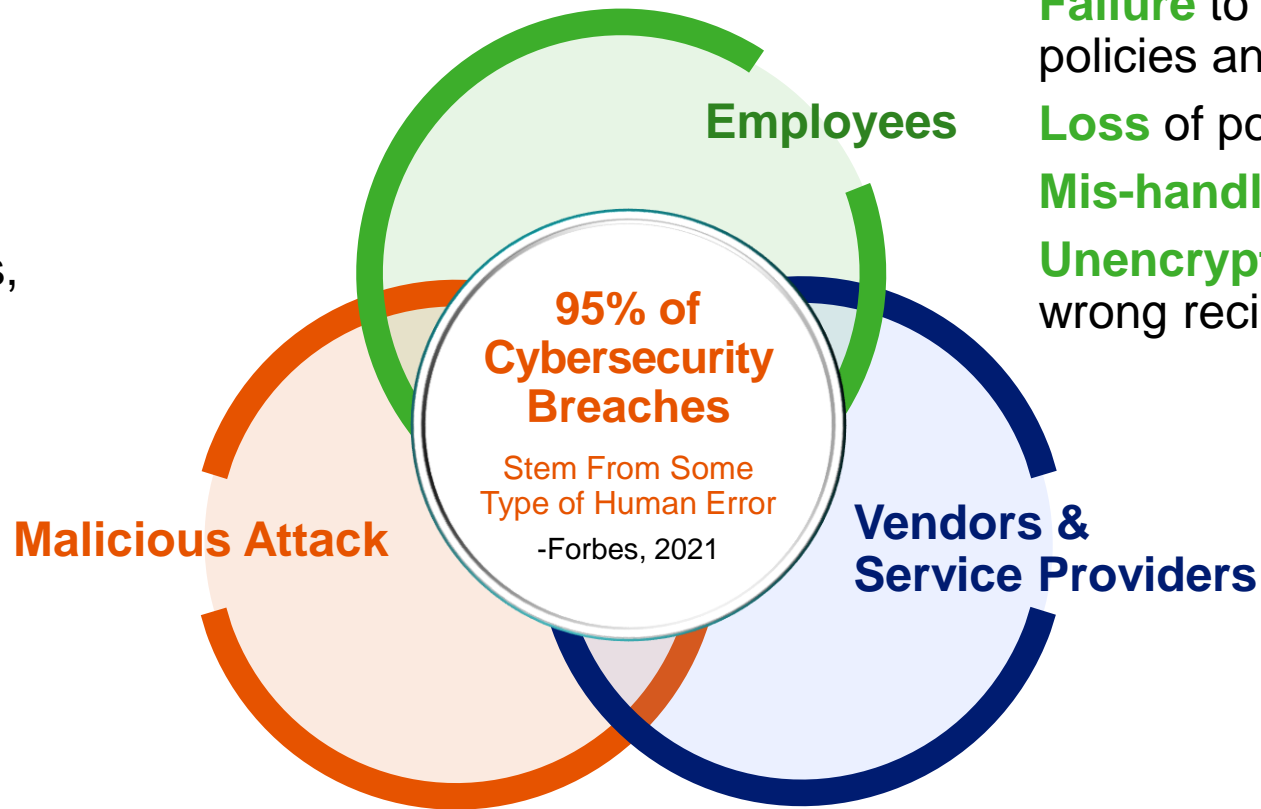
Hackers in your workstations, laptops, servers, email, or **mobile devices**.

Malware and viruses.

Phishing scams.

Theft of desktops, laptops, portable devices, or paper.

Rogue employees.



Negligence related to use and storage of data.

Failure to follow or learn policies and procedures.

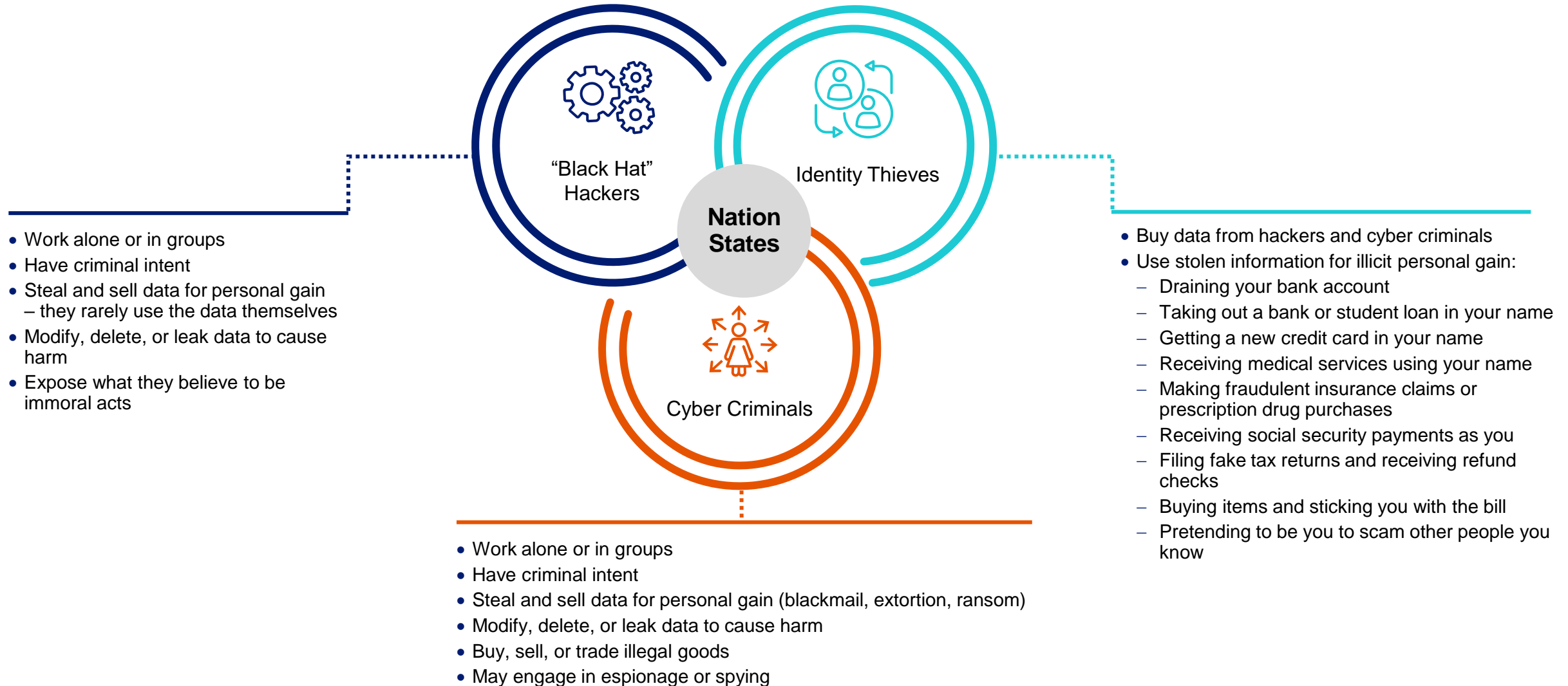
Loss of portable devices.

Mis-handling of paper.

Unencrypted emails to the wrong recipients.

Any of the above can occur to a third-party vendor or service provider with whom data is shared.

Criminals (And a Few of Their Motivations)



Cybersecurity Staffing and Skills — Too Few and Not Experienced Enough



“59% of leaders indicating their teams are understaffed. This isn’t merely a numbers game; it’s about equipping teams with the right skills.”

“The State of Cybersecurity (ISACA) report underscores that demand for technical skills such as identity and access management (49%), cloud computing (48%), data protection (44%), incident response (44%), and DevSecOps (36%) is on the rise. Alongside these, soft skills are gaining prominence. Communication is at the forefront with 55%, followed by critical thinking (54%), problem-solving (49%), teamwork (45%) and attention to detail (36%).”

[State of Cybersecurity 2023: Navigating Current and Emerging Threats \(isaca.org\)](https://www.isaca.org)

Changing Cyber Liability Insurance Market

Segal Select Insurance Services, Inc. (“Segal Select”), a subsidiary of The Segal Group, is a specialty retail broker insurance. Any information and/or opinions herein provided by third parties have been obtained from sources believed to be reliable, but accuracy and completeness cannot be guaranteed. The contents of this presentation and any opinions expressed herein are intended for general education purposes only and not as professional advice specific to any person, entity or circumstance. It is not intended for use as a basis for making insurance-related decisions, including determinations of appropriate types or levels of insurance coverage, nor should it be construed as advice designed to meet the needs of any particular person, entity or circumstance. Please contact Segal or another qualified insurance professional for advice regarding the evaluation of any specific information, opinion, or other content. Of course, on all matters involving legal interpretations and regulatory issues, you should consult legal counsel.

Cyber Crime Around the World



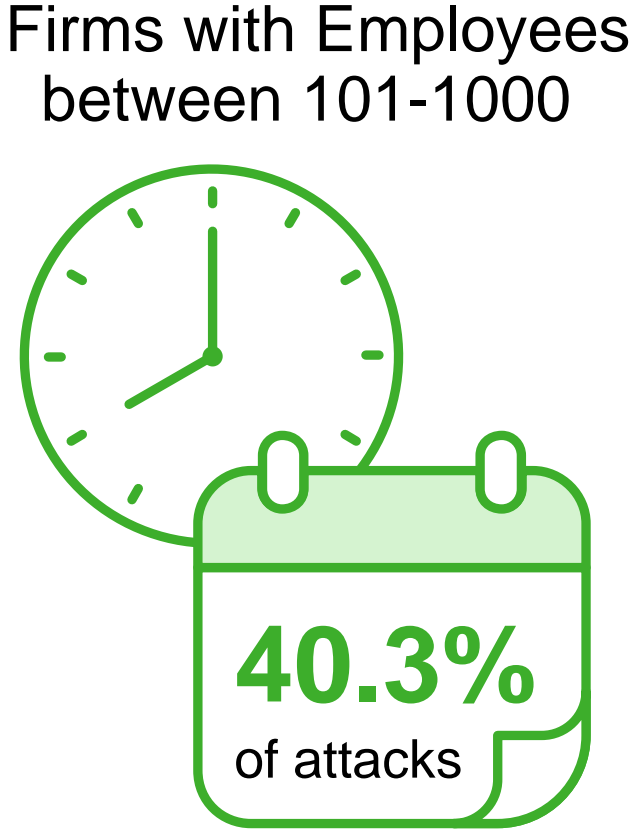
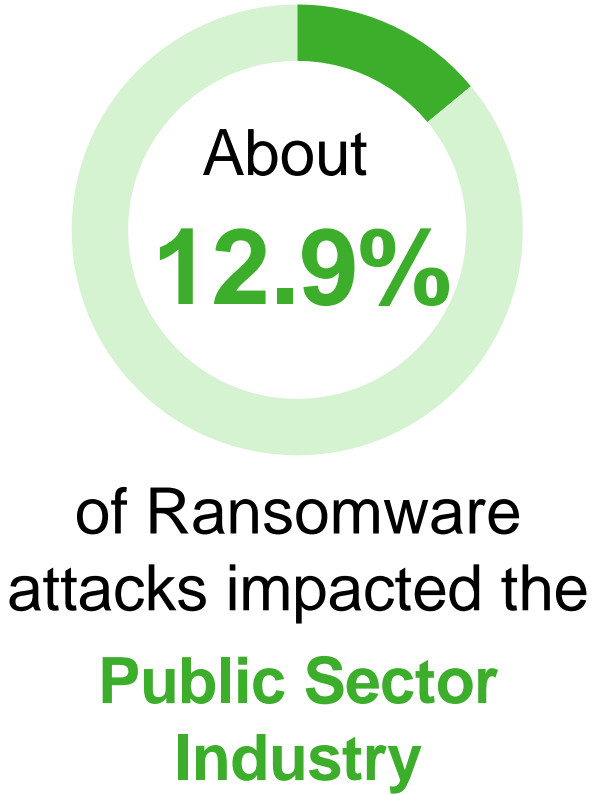
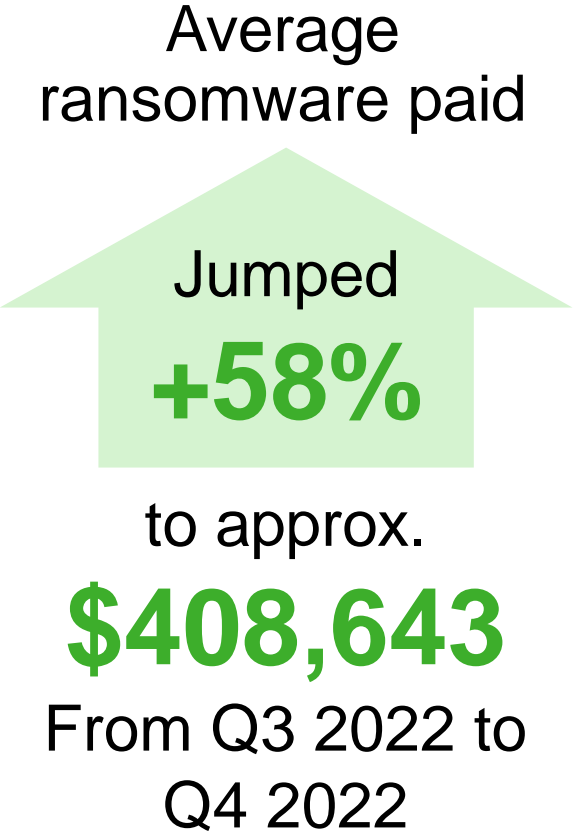
Many incidents include more than one threat



Source: Verizon 2022 Data Breach Investigations Report, Verizon.com

Recent Ransomware Statistics

4Q 2022



<https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments#types>

State of the Cyber Insurance Market

01

There remains an onus on Insureds for minimum/base controls

Including: implementation of MFA; Secure RDP's; robust backup procedures, training and Incident Response Plans

02

Rate increases have slowed

More stability in premiums, including some decreases

03

Broader Terms/Conditions

Reduction/removal of co-insurance; lower retentions; and increase in sublimits

04

Increase in Cyber Liability Capacity YOY

Existing markets increase capacity as well as the introduction of additional market capacity

State of the Cyber Insurance Market

05

Increase in automatic renewals

Automatic renewals can still include changes to premium and terms, but no application requirement usually seen as a positive

06

Inconsistency with admitted/non-admitted markets still exists

Many carriers continue to use non-admitted paper to allow greater flexibility on rate and coverage changes

07

Move towards universal applications

Still evolving. Limited flexibility on terms

08

Interest in additional products/limits

Increased purchasing of Excess Social Engineering Fraud coverage

What is Cyber Liability Insurance?

Incident Response

Coach Services

Legal Services

Forensics

Notification

Credit Monitoring

Public Relations

First-Party

Extortion/Ransomware

Data Recovery/
Restoration

Business Interruption/
Extra Expense

Crime/Social
Engineering

Third-Party

Privacy Liability

Regulatory

Payment Card

Network Liability

Media Liability

Insurance for Ransomware Attacks

- Plan records, Plan contributions or Total participants
- Rates can vary with types of data stored
- Protected Health Information
- Prior claims or data breaches could increase rates
- Encryption and other cybersecurity protections will support rate credits
- Overall market conditions



Insurance for Social Engineering Fraud

Attacks are generally covered by most carriers when malware is added, data is stolen or held hostage, or money transferred:

- The coverage may have exclusions and require certain procedures to be followed in order to have a covered claim (independent call back provisions, etc.)
- If money is stolen, the primary policy limits are often sublimited to between \$50K and \$250K regardless of the full policy limit
- There may be similar coverage in other policies such as a fidelity bond or crime insurance
- Larger coverage limits are usually only available by having excess carriers participate in the cyber program

Insurance for Social Engineering Fraud

Standalone excess policies available for social engineering fraud

- Typical attachment point of \$250,000;
- Requested limits are usually \$1-million to \$5-million;
- Appetite can depend on which carrier writes primary



Insurance for Social Engineering Fraud

Key Application Questions



Average volume and frequency of fund transfers over last 12 months, largest to totals? Domestic and foreign



Anti-fraud training for detection of phishing and social engineering scams?



Do you authenticate vendor instructions?



Who is authorized to direct accounts payable to pay an invoice and authenticate instructions in place?












Authority on wire transfers, verbally, in writing and banking instructions?

Cyber Coverage Issues

- Some policies only cover certain types of “data” and/or limit coverage based on when and where it exists
- Watch for sub-limits and potential coinsurance requirements for ransomware losses
- Are insiders/employees covered?
 - Some policies only cover loss caused by outsiders
- Review for limitations does not require “updated software protections”
 - This may artificially limit coverage for many plans
- Review carefully time element limitations to when coverage applies

Beware of Cyber Policy Exclusions

-  Professional services
-  Criminal or Intentional acts of employees
-  “Failure to Follow Minimum Required Practices”
-  Acts prior to the inception of the policy
-  Unencrypted data exclusion
-  Mechanical/electronic failure such as when a computer stops functioning
-  Laptops and other portable electronics such as cell phones and tablets
-  Patent, software, copyright Infringement
-  War or Terrorism

Typical Incident Response Services

Crisis Hotline →

Reporting Urgent event

#800 or through a Cyber App

Response → Coaches

To triage a cyber-event

- Maintain client privilege
- Consultation, hours can vary
- Tender a claim to the carrier

Response → Specialists

Support response

- Forensics
- Public Relations
- Notification Services
- Call Center
- Extortion
- Business Interruption

What's in your client's Incident Response plan?

How Rates Are Determined

- Plan records, Plan contributions or Total participants
- Rates can vary with types of data stored,
- i.e., protected health information (for health plans)
- Prior claims or data breaches could increase rates
- MFA applications and other cyber protections



Key Tips for Insurance Applications

- Who is responsible for data security?
- Is there an information security policy and how are violations handled?
- What protections exist for Multi Factor Authentication controls?
- Is there an incident response plan in place?
- Is there on-going security training?
- Are there contracts in place for 3rd parties who process, host or store sensitive information?
- What has the breach experience been and how was it handled?

Separate questionnaires are now often required to address COVID, Ransomware and Social Engineering Fraud exposures.

Beware Warranty Statements



- In general, warranty statements are very broad attestations that the proposed insureds are not aware of any incident, act, knowledge, error, or omission which might result in a claim under the policy
- Usually required for first year of coverage, but an important factor when applying for renewals and considering changing carriers
- Disputes can arise with the insurance company regarding the knowledge that may lead to insurance claim denials or even policy recession by the carrier

Sample Application Questions

Do you use multi-factor authentication (MFA) for cloud-based email account access?

Do you regularly (at least annually) provide cyber security awareness training, including anti-phishing, to all staff who have access to your organisation's network or confidential/personal data?

Do you implement critical patches (within 2 months)?

Do you scan incoming emails for malicious attachments and/or links?

Do you protect all of your devices with anti-virus, anti-malware, and/or endpoint protection software?

Do you regularly back-up critical data?

Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose?

Are your backups encrypted?

What remote access technology does the Applicant provide that allows for users to connect into the environment from outside of the office? (select all that apply)

- Remote Desktop (RDP)
- Virtual Private Network (vendor and product): _____
- Citrix
- Remote access software (e.g. LogMeIn) (vendor and product): _____
- Other: _____

Is multi-factor authentication ("MFA") technology in use and, if so, where is it used by the Applicant? (select all that apply)

Solution (vendor and product): _____

- All external remote access (RDP, VPN, etc.)
- Email
- Vendor access
- Privileged account usage
- Administrative access to servers
- Not used

Sample Application Questions

Do you use an endpoint detection and response (EDR) tool that includes centralized monitoring and logging of all endpoint activity across your enterprise?

If "Yes", please select your EDR provider:

If "Other", please provide the name of your EDR provider:

Do you use MFA to protect access to privileged user accounts?

Do you manage privileged accounts using privileged account management software (e.g., CyberArk, BeyondTrust, etc.)?

If "Yes", please provide the name of your provider:

Do you actively monitor all administrator access for unusual behavior patterns?

If "Yes", please provide the name of your monitoring tool:

Do you roll out a hardened baseline configuration across servers, laptops, desktops and managed mobile devices?

- Does your company use any software or hardware that is no longer supported or has been identified as end-of-support by the software or hardware vendor?
- Please confirm the use of multifactor authentication for remote access, emails, on personal devices and for privileged access.
 - If no MFA is present, please provide details and dates for implementation

Third Party Network Scans

Cyber liability insurance carriers relying more on third party networks scans:

- Bitsight
- CyRisk Insight Engine
- In-house proprietary scans

Mixed feedback from clients

- Scanning wrong urls (e.g., union's site rather than fund's site);
- Outdated scans

Scans done periodically throughout the year

May require response midterm or prior to next renewal

Takeaways

The threat environment has only become increasingly risky during the pandemic environment due to an increased number of remote workers and system vulnerabilities



A robust Cyber Liability Insurance policy is a 'must have' in today's perilous environment; ensure you have the appropriate coverage for your organization



Ransomware attacks and Social Engineering attacks are becoming more prevalent, more expensive, and more sophisticated in their ability to trick users



Having knowledgeable professional providers to review your insurances



Regulatory Guidance to Strengthen Security

Three (3) DOL Publications for Fiduciaries and Organizations to Understand and Embrace



EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR
CYBERSECURITY PROGRAM BEST PRACTICES

ERISA-covered plans often hold millions of dollars or more in assets and maintain personal data on participants, which can make them tempting targets for cybercriminals. Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

The Employee Benefits Security Administration has prepared the following guidance for use by recordkeepers and other service providers responsible for maintaining plan records and data, and for plan fiduciaries making prudent decisions on the service providers they should hire. Plans' service providers should:

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and risk assessments.
7. Conduct periodic cybersecurity awareness training.

EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR
TIPS FOR HIRING A SERVICE PROVIDER WITH STRONG CYBERSECURITY PRACTICES

As sponsors of 401(k) and other types of pension plans, business owners often rely on other service providers to maintain plan records and keep participant data confidential and plan accounts secure. Plan sponsors should use service providers that follow strong cybersecurity practices.

To help business owners and fiduciaries meet their responsibilities to participants, select and monitor such service providers, we prepared the following tips for providers of all sizes:

1. Ask about the service provider's information security standards and audit results, and compare them to the industry standard for your type of institution.
 - Look for service providers that follow a recognized standard for information security and use an outside (third-party) auditor to verify their cybersecurity. You can have much more confidence in the security of its systems and practices are backed by a third-party audit that verifies information security, system/data availability, product confidentiality.

EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR
ONLINE SECURITY TIPS

You can reduce the risk of fraud and loss to your retirement account by following these basic rules:

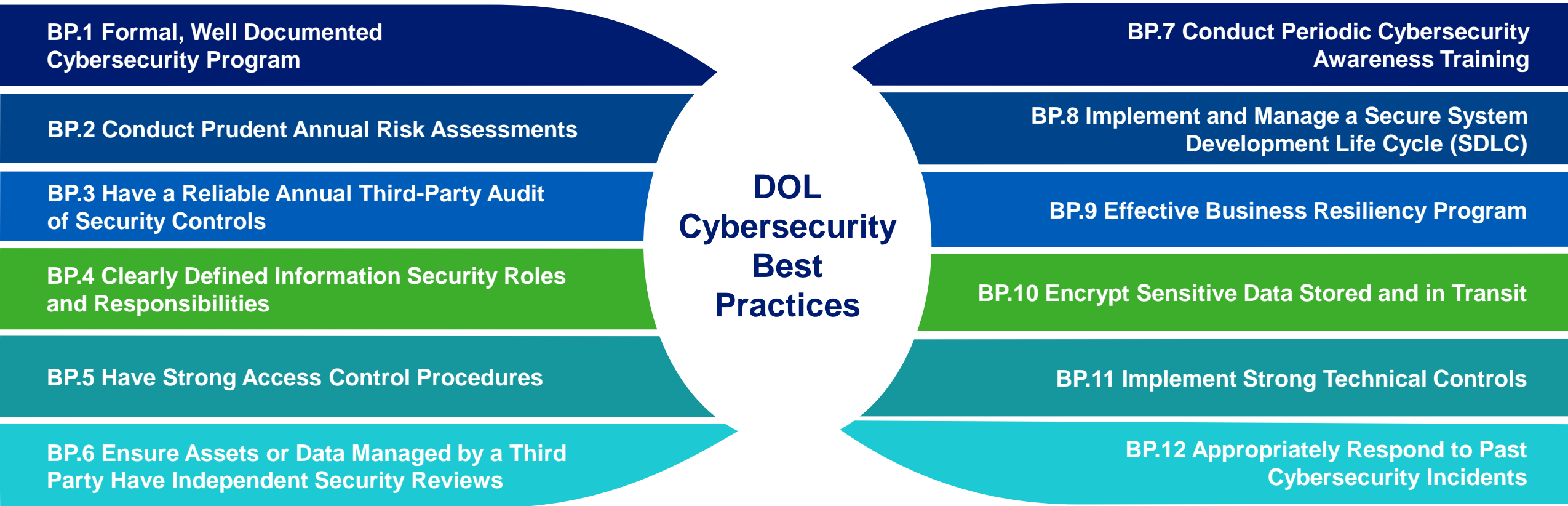
- **REGISTER, SET UP AND ROUTINELY MONITOR YOUR ONLINE ACCOUNT**
 - Maintaining online access to your retirement account allows you to protect and manage your investment.
 - Regularly checking your retirement account reduces the risk of fraudulent account access.
 - Failing to register for an online account may enable cybercriminals to assume your online identity.

<https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf>

<https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf>

<https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf>

DOL Cybersecurity Best Practices Overview



Segal has seen weakness is seen in all the above categories 1 – 12. It is endemic throughout administrative, technical and (even) physical controls.

Hire a Service Provider With Good Cybersecurity Practices

The Plans' stakeholders should implement processes and procedures that will allow them to survey, assess (and then monitor) third-party vendors, trading partners and service providers' cybersecurity programs. As part of this process, the Plan should:

- Consider establishing an information security governance committee (ISGC) or alternative governing and reporting structure
- In partnership with other stakeholders that ISGC should confirm or identify the third-party vendors to survey
- In partnership with other stakeholders that ISGC should establish how to survey those vendors (agree upon the actual survey of questions)
- Manage the survey process and score and report upon the individual vendor surveys

Risk to Manage: DOL Cybersecurity Guidance (*And There **Has** Been DOL Data Gathering Activity*)

- They have asked for any documents relating to any cybersecurity or information security programs that apply to the data of the Plan, whether those programs are applied by the sponsor of the Plan or by any service provider of the Plan.
- From what we understand, they have asked for information related to:
 - Cybersecurity policies, procedures, etc.
 - Data governance, including how that data is classified, managed and disposed of (at end of life)
 - Access controls related to that data – from a cybersecurity as well as a privacy perspective
 - Business continuity plans
 - Disaster recovery plans
 - Incident response plans
 - Any cybersecurity risk assessments that have been performed
 - Training related to cybersecurity (for staff); ongoing awareness education, as well
 - Any information related to third-party service providers (that is, any information related to how they are managed in relation to Plan data (e.g., notification if they have a breach, limits on how they can use Plan data, other information related to their cybersecurity environment)
 - Etc.

There are other topics as well...this is just a partial list of potentially requested data and information, as we understand.

SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies



The screenshot shows the SEC website's press release page for the announcement of new cybersecurity rules. The page features the SEC logo and navigation menu at the top. A sidebar on the left lists various content categories, with 'Press Releases' highlighted. The main content area displays the title of the press release, a 'FOR IMMEDIATE RELEASE' notice, the release number '2023-139', the date 'July 26, 2023', and a summary of the rules. A quote from SEC Chair Gary Gensler is also included.



<https://www.sec.gov/news/press-release/2023-139>

The Actual Fact Sheet

FACT SHEET

Public Company Cybersecurity Disclosures; Final Rules



The Securities and Exchange Commission adopted final rules requiring disclosure of material cybersecurity incidents on Form 8-K and periodic disclosure of a registrant's cybersecurity risk management, strategy, and governance in annual reports.

Background

In March 2022, the Commission proposed new rules, rule amendments, and form amendments to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and material cybersecurity incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. The Commission observed that cybersecurity threats and incidents pose an ongoing and escalating risk to public companies, investors, and market participants. It noted that cybersecurity risks have increased alongside the digitalization of registrants' operations, the growth of remote work, the ability of criminals to monetize cybersecurity incidents, the use of digital payments, and the increasing reliance on third party service providers for information technology services, including cloud computing technology. The Commission also observed that the cost to companies and their investors of cybersecurity incidents is rising and doing so at an increasing rate. All of these trends underscored the need for



<https://www.sec.gov/files/33-11216-fact-sheet.pdf>

Quick Summary

Caveat, I Am Not an Attorney

The SEC's new cybersecurity rule is intended to ensure that public companies are more transparent about their cybersecurity practices and incidents. The rule has two main components:

- A requirement to disclose any material cybersecurity incident within four business days after determining its materiality, unless the Justice Department requests a delay for national security or law enforcement reasons. A material cybersecurity incident is one that has a significant impact or is reasonably likely to have a significant impact on the company's business, operations, financial condition, reputation, or stock price.
- A requirement to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance, including the board of directors' oversight and management's role and expertise in this area. The disclosure should also describe the company's processes for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects or reasonably likely material effects of risks and incidents on the company.

Quick Summary

- The rule aims to provide investors with more consistent, comparable, and decision-making relevant information about how public companies are managing cybersecurity risks and responding to incidents.
- The rule also intends to encourage public companies to improve their cybersecurity policies and procedures and to foster greater accountability and responsibility for cybersecurity matters.
- The rule will become effective 30 days after publication in the Federal Register and will apply to annual reports for fiscal years ending on or after December 15, 2023.

HIPAA Security Rule – Still Important!

- Recall that the HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity, as noted by HHS.
- The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
 - The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.
 - View the combined regulation text of all HIPAA Administrative Simplification Regulations found at 45 CFR 160, 162, and 164.

[The Security Rule | HHS.gov](https://www.hhs.gov/hipaa/for-professionals/security/index.html)

How to Respond?

Consider Embracing a Defense-in-Depth Cybersecurity Strategy

Recognizing the above noted risks and threats associated with securing and managing confidential, sensitive, nonpublic data and information...what is to be done?



Embrace a defense-in-depth strategy.

The Assumptions of Defense-in-Depth

Technology alone cannot save you; technology is not magic.

- Defense in depth is a security strategy in which multiple security techniques are employed. If one fails, the others are expected to hold.
- Assumes that any individual dimension of your cybersecurity defenses cannot be counted on to succeed in its assigned task.
- Assumes that you need **Administrative, Technical and Physical** controls.



1

2

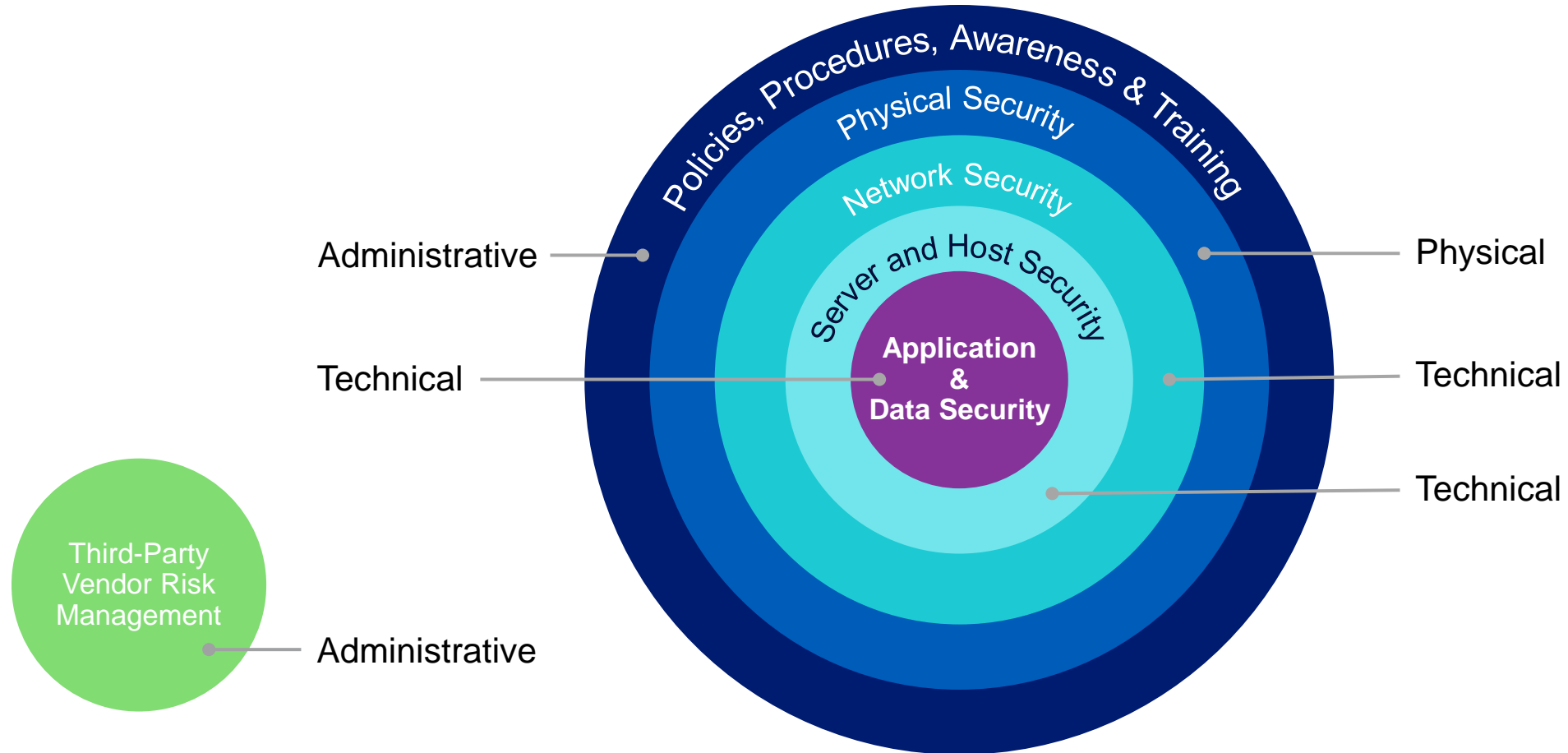


Proactive cybersecurity is hard; do it anyway.

- Vulnerabilities can exist anywhere on your physical premises or your logical IT systems (workstations, laptops, mobile devices, thin clients, etc.) – on premises or in your “cloud”.
- Threats are a result of unmanaged vulnerabilities.
- Threats, and those who initiate them may be criminal and malicious, accidental, or a result of random chance.
- Threats can be both external and internal in their source.

The Dimensions of Defense-in-Depth

Addressing one or two dimensions is not enough.
You should seek to address them all.

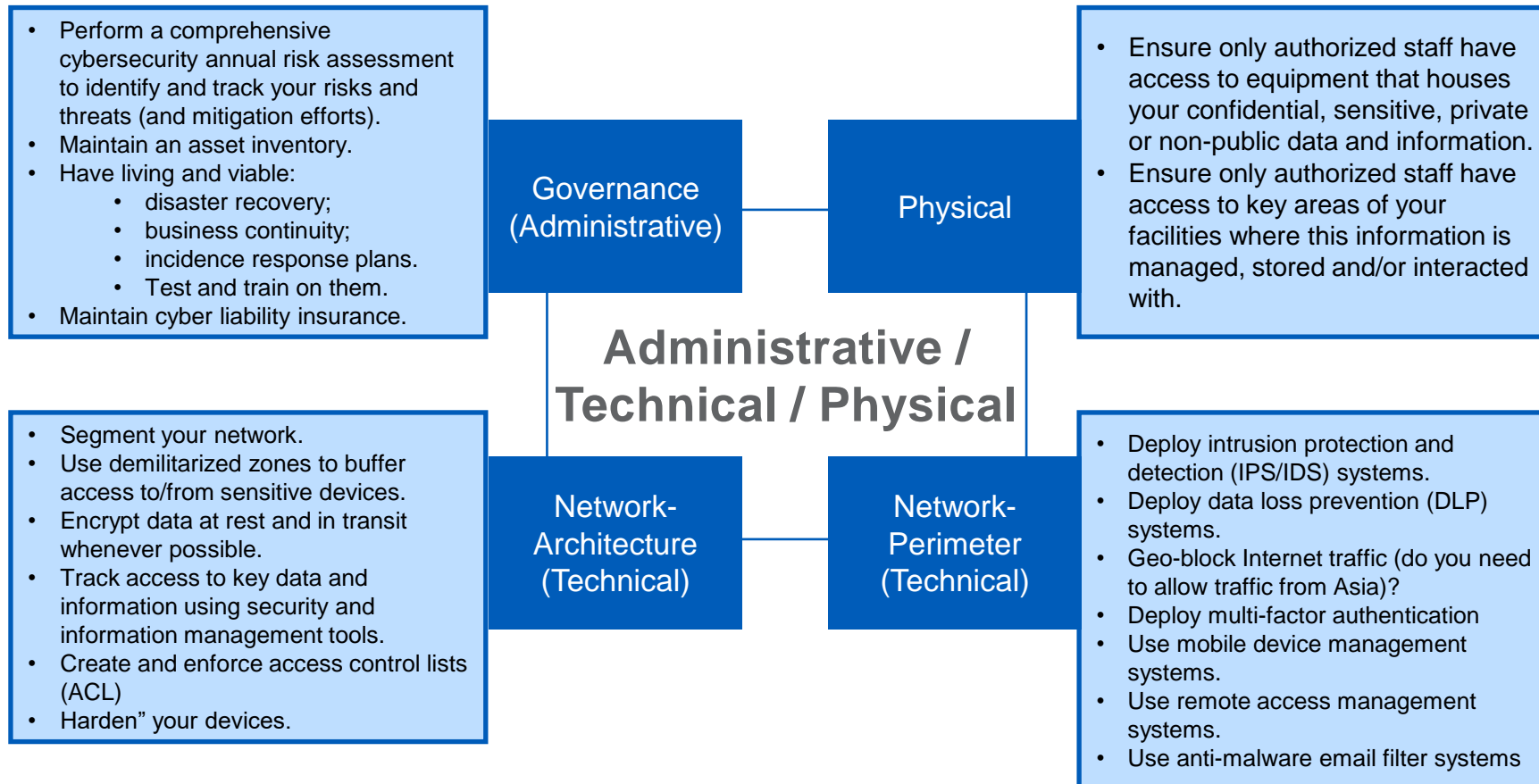


Illustrating Each Dimension

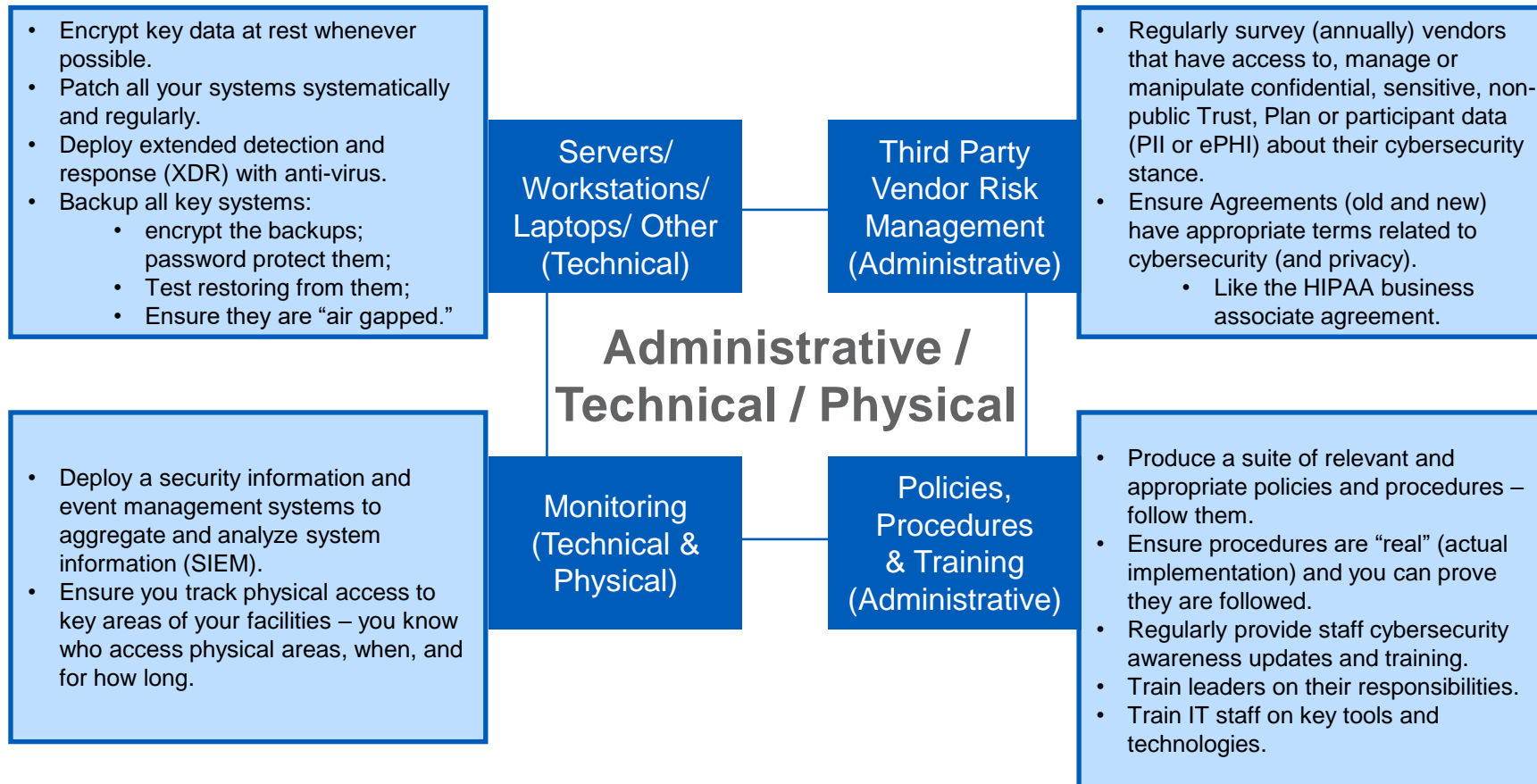
Defense-in-Depth

Policy	Accountability through the attribution of actions, such as recording who enters and exits a building or specific – restricted – areas (e.g., who can go into the claims payment area).
Procedure	Each person must enter the facility one at a time. No tailgating. You should have the ability to prove this procedure is followed (key card log files with video monitoring of key access points, etc.).
Training & Awareness	Employees should, given their role, know who they typically work with. Observing unknown people in unexpected locations or at unexpected times comes across as suspicious and is reported to managers or designated personnel. They should be trained and have a policy to follow that supports this.
Physical	Configuring physical premises to restrict access to the area as well as restricting hardware to prevent connecting unauthorized USB drives to computing devices of any type (in that area or elsewhere).
Network	Leveraging tools and technologies to block direct internet access to key sensitive systems – either at all – without appropriate architectural and ensure other safeguards in place (e.g., DMZ, MFA, IPS/IDS, XDR (with anti-virus), etc.)
Servers/workstations/ laptops, etc. (aka, “Hosts”)	Redundant power backed up by Uninterruptable Power Supplies (UPS) or generators to extend uptime in the event of a power loss. Extended detection and response (XDR) with anti-virus should be deployed.
Applications	Restricting access to certain application functions via role-based security and per user accounts and passwords, again with MFA deployed. Tracking access to and changes of key data and information via log files and reporting – sent to SIEM tools, or not.
Data	Encrypting data at rest and in transit, and only enabling specific roles or accounts to decrypt that data.

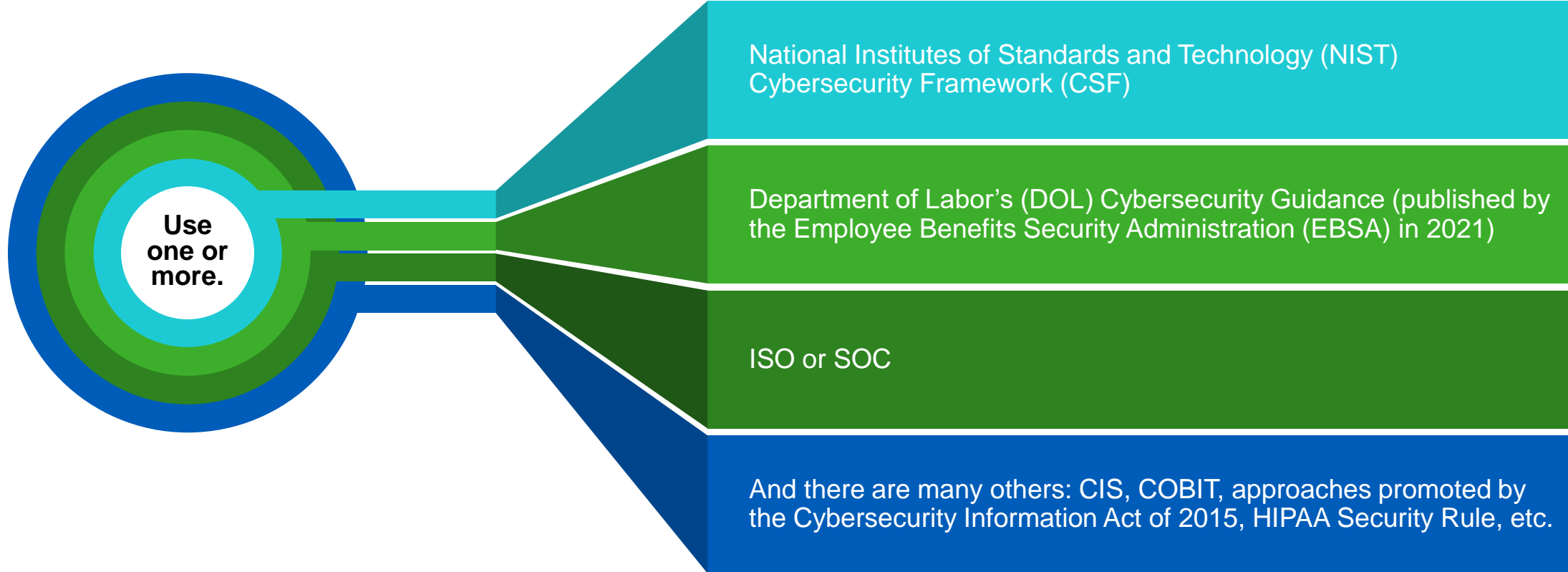
Illustrating *Some* Key Elements (*not* the only elements)



Illustrating *Some* Key Elements (*not* the only elements)



Implement the Strategy by Using One or More Frameworks With Associated Tactics



One or more of these can — and should — be used in conjunction to support your defense in depth cybersecurity strategy.

Tangible Next Step(s) to Take?

- Have an outside assessor perform a risk assessment of your (internal) operations against one or more of your preferred frameworks
 - We have seen significant weakness when we performed such assessments against the NIST (CSF), DOL “best practices” or HIPAA security rule
- Ensure that you also have a third-party risk management (TPRM) assessment
 - Your third parties are a significant source of your organization’s risk
 - Ignoring assessing and then seeking to ensure they are acting in accord with your risk management standards is a potentially significant source of risk
 - TPRM risk is a **cumulative** risk (the more vendors with your confidential, sensitive, nonpublic data and information, the higher the risk)

Questions?



Diane McNally

Senior Vice President and
Insurance Practice Leader
drmcnally@segalco.com



Michael Stoyanovich

Vice President and Senior
Consultant, Administration
& Technology
mstoyanovich@segalco.com



**Please scan QR code
to provide feedback
on today's webinar**

Thank You!



**Please scan QR code
to provide feedback
on today's webinar**