Your Attention Please:

A Cybersecurity Overview

ERISA Advisory Council Activity (2022) / DOL Guidance (2021); What This Means and Suggested Responses

September 2022 / Michael Stoyanovich

Segal

Today's Presentation

1. **Background**
2. **DOL ERISA Advisory Council Activity (2022)**
3. **DOL EBSA Guidance (2021)**
4. **DOL Audit/Investigation Activity**
5. **Cybersecurity Risks & Threats**
6. **Mitigating With a Defense-in-Depth Strategy**

Background

Some Key Background Information

- ERISA Duty of Prudence.
  - To paraphrase – my understanding as an operations and IT executive (*not* a legal interpretation):
    - ERISA's duty of prudence requires fiduciaries to act with care, skill, prudence and diligence under circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims.
  - This has meant (previously) that ERISA fiduciaries have some responsibility to try to limit risks associated with a plan's cybersecurity exposure.
    - Then the DOL (Employee Benefits Security Administration (EBSA)) issued its guidance in April of 2021
    - It is now clearer what the DOL expects a prudent fiduciary to do.

Also…the ERISA Advisory Council of 2016 published a report directed to the Secretary of Labor titled "Cybersecurity Considerations for Benefit Plans". This report raised questions about data protection for Plan fiduciaries – as it related to third parties that provided services to the Plan.

Also…in 2021 the GAO published a report that looked at that topic in more detail – specifically for defined contribution (DC) Plans and the third parties they share(d) data with to provide services to the Plan (and participants). It noted associated cybersecurity risks and recommended the DOL make it clear (formally) whether it is an ERISA fiduciary responsibility to mitigate cybersecurity risks (specifically for DC plans). The GAO recommended minimum expectations be set.

The DOL has publicly stated the cybersecurity is a priority, especially considering the size of assets that Plans hold.

There has also been private litigation related to fiduciaries' responsibility to protect Plan data and information.

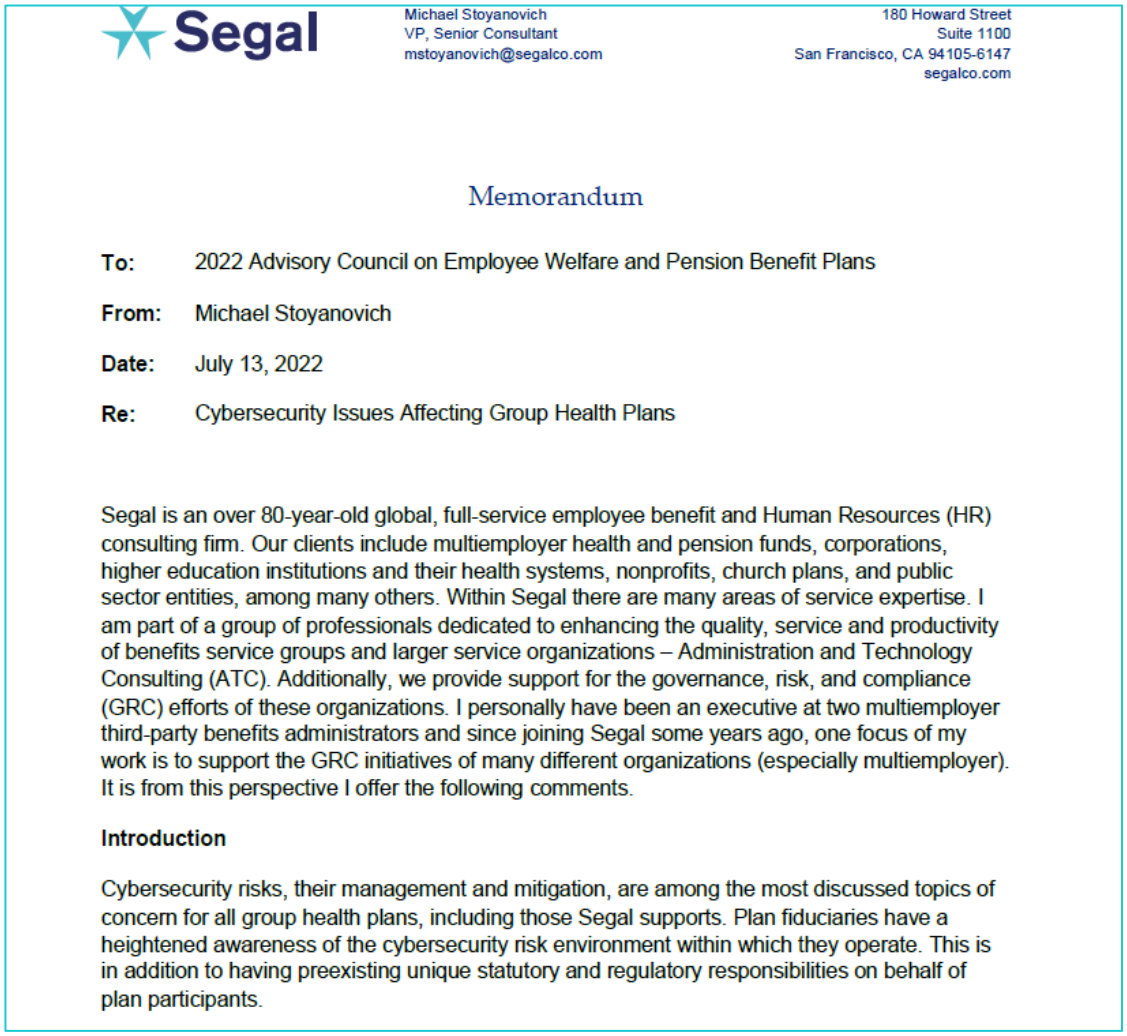
DOL ERISA Advisory Council Activity (2022)

Most Recently

From the ERISA Advisory Council (2022) Issue Statement (on Cybersecurity)

"The 2022 Advisory Council will examine cybersecurity issues affecting health benefit plans. The examination will identify issues and vulnerabilities affecting these plans and faced by plan sponsors, fiduciaries, and service providers, as well as how those may differ by plan size. The Council will also examine existing relevant frameworks, approaches and initiatives tailored to health care and health plan cybersecurity concerns and the interaction between overlapping regulatory regimes for health plans…"

Segal's Position (Testimony)… to Paraphrase



Segal

Michael Stoyanovich
VP, Senior Consultant
mstoyanovich@segalco.com

180 Howard Street
Suite 1100
San Francisco, CA 94105-6147
segalco.com

Memorandum

To: 2022 Advisory Council on Employee Welfare and Pension Benefit Plans

From: Michael Stoyanovich

Date: July 13, 2022

Re: Cybersecurity Issues Affecting Group Health Plans

Segal is an over 80-year-old global, full-service employee benefit and Human Resources (HR) consulting firm. Our clients include multiemployer health and pension funds, corporations, higher education institutions and their health systems, nonprofits, church plans, and public sector entities, among many others. Within Segal there are many areas of service expertise. I am part of a group of professionals dedicated to enhancing the quality, service and productivity of benefits service groups and larger service organizations – Administration and Technology Consulting (ATC). Additionally, we provide support for the governance, risk, and compliance (GRC) efforts of these organizations. I personally have been an executive at two multiemployer third-party benefits administrators and since joining Segal some years ago, one focus of my work is to support the GRC initiatives of many different organizations (especially multiemployer). It is from this perspective I offer the following comments.

Introduction

Cybersecurity risks, their management and mitigation, are among the most discussed topics of concern for all group health plans, including those Segal supports. Plan fiduciaries have a heightened awareness of the cybersecurity risk environment within which they operate. This is in addition to having preexisting unique statutory and regulatory responsibilities on behalf of plan participants.

1. Group Health Plans already comply with many different laws that protect the sensitive health information they are entrusted with.
2. Additionally, the sub-regulatory guidance published by the DOL in 2021 mirrors much of that pre-existing effort (e.g., HIPAA-HITECH).
3. Internal risk mitigation concerns at group health plans and external commercial pressures are also prompting most group health plans to embrace improvement activity related to their cybersecurity stance (e.g., using the NIST (CSF) framework, ISO, SOC, or other (including the DOL's sub-regulatory guidance as a framework)).
4. Considering this, no additional guidance from the DOL is necessary currently.

From the ERISA Advisory Council (2022) Issue Statement (on Cyberliability Insurance)

"Concerns regarding cyber-attacks, cyber theft and the need for strong cybersecurity measures continue to grow in prominence. The 2022 Advisory Council intends to examine the role that cybersecurity insurance plays in addressing cybersecurity risks for employee benefit plans…"

NCCMP's and Segal's' Position (Testimony)… to Paraphrase

NATIONAL COORDINATING COMMITTEE FOR MULTIEMPLOYER PLANS

815 16TH STREET, N.W., WASHINGTON, D.C. 20006 • PHONE 202-737-5315 • FAX 202-737-1308

MARIAH M. BECKER
DIRECTOR OF RESEARCH AND EDUCATION
E-MAIL: MBECKER@NCCMP.ORG

Septemb

ERISA A
U.S. Dep

Re: Cyb
Cyb

Dear Me

The Nat
opportun
multiem
on behal
an Enrol
Committ

The NC
multiem
organiza
families
assure a
retireme

Segal

Diane McNally
Senior Vice President
T 212.251.5146
M 929.240.1433
drmcnally@segalco.com

333 West 34th Street
New York, NY 10001-2402
segalco.com
CA License No. 0I06323

Memorandum

To: 2022 Advisory Council on Employee Welfare and Pension Benefit Plans

From: Diane McNally

Date: September 6, 2022

Re: Cybersecurity Insurance and Employee Benefit Plans

I have been asked to address the topic of "Cybersecurity Insurance and Employee Benefit Plans" as a representative of the National Coordinating Committee for Multiemployer Plans (NCCMP). Specifically, I will provide an overview of cyber liability insurance and provide an understanding of the cybersecurity market for employee benefit plans.

I am a Segal Senior Vice President and the National Practice Leader of Segal Select Insurance Services, Inc. Segal Select is a wholly owned subsidiary of The Segal Group and operates as a national retail insurance brokerage firm. Segal Select specializes in financial and commercial insurance products including cyber liability insurance.

Segal is an over 80-year-old full-service employee benefit and human resources consulting firm. Our clients include multiemployer funds, corporations, higher education institutions, health systems, nonprofits and public sector entities, among many others.

Key Point(s):

- Underwriting requirements have changed in recent years in response to the increase in data breach events; with insurers requiring many more obligations from insureds, including items such as:
  - Multifactor authentication
  - Sound backup and encryption procedures
  - Patching and vulnerability scanning procedures
  - Strong email security
  - Training and awareness related to cybersecurity
  - Privileged account restriction and monitoring
  - Endpoint detection and response

DOL (EBSA) Guidance (2021)

The Department of Labor (DOL) issued three pieces of non-regulatory guidance on reducing cybersecurity risks in April of 2021. These items are the first official guidance from the DOL.

DOL Published First Ever Guidance on Cybersecurity

News Release

US DEPARTMENT OF LABOR ANNOUNCES NEW CYBERSECURITY GUIDANCE FOR PLAN SPONSORS, PLAN FIDUCIARIES, RECORD-KEEPERS, PLAN PARTICIPANTS

Guidance seeks to help protect an estimated $9.3T in assets

WASHINGTON, DC – The U.S. Department of Labor today announced new guidance for plan sponsors, plan fiduciaries, record keepers and plan participants on best practices for maintaining cybersecurity, including tips on how to protect the retirement benefits of America's workers. This is the first time the department's Employee Benefits Security Administration has issued cybersecurity guidance. This guidance is directed at plan sponsors and fiduciaries regulated by the Employee Retirement Income Security Act, and plan participants and beneficiaries.

Three (3) Key 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 cyber-criminals. Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

The Employ
use by reco
and data, a
should hire.

1. Ha
2. Co
3. Ha
4. Cle
5. Ha
6. Ens
pro
ass
7. Co

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 under ERISA to prudently select and monitor such service providers, we prepared the following tips for plan sponsors of

1.

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 identify.

DOL Audit/Investigation Activity

If the Topic is In the 2021 Publications, They May Request Data and Information

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 cyber-criminals. Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

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 under ERISA to prudently select and monitor such service providers, we prepared the following tips for plan sponsors

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 identify.

It appears that if the topic is related to one of these publications; organizations may be asked about it in a DOL investigation.

And There *Has* Been DOL Data Gathering Activity

- The 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.

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

Cybersecurity Risks & Threats

(Some) Cybersecurity Risks to Manage and Threats to Counter

Risk

Data Privacy Obligations

There are multiple different federal data privacy rules, regulations and laws to be aware of: E.g., HIPAA-HITECH, ADA, GINA, ERISA, FTC Act, FERPA as well as CCPA/CCRA and other state laws.

Risk

Data Security Obligations

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

Risk

Cyber Insurance Needs

Recent strengthening of underwriting standards has made it harder to obtain comprehensive coverage with prices escalating as well.

Threat

Cyber Criminal Activity

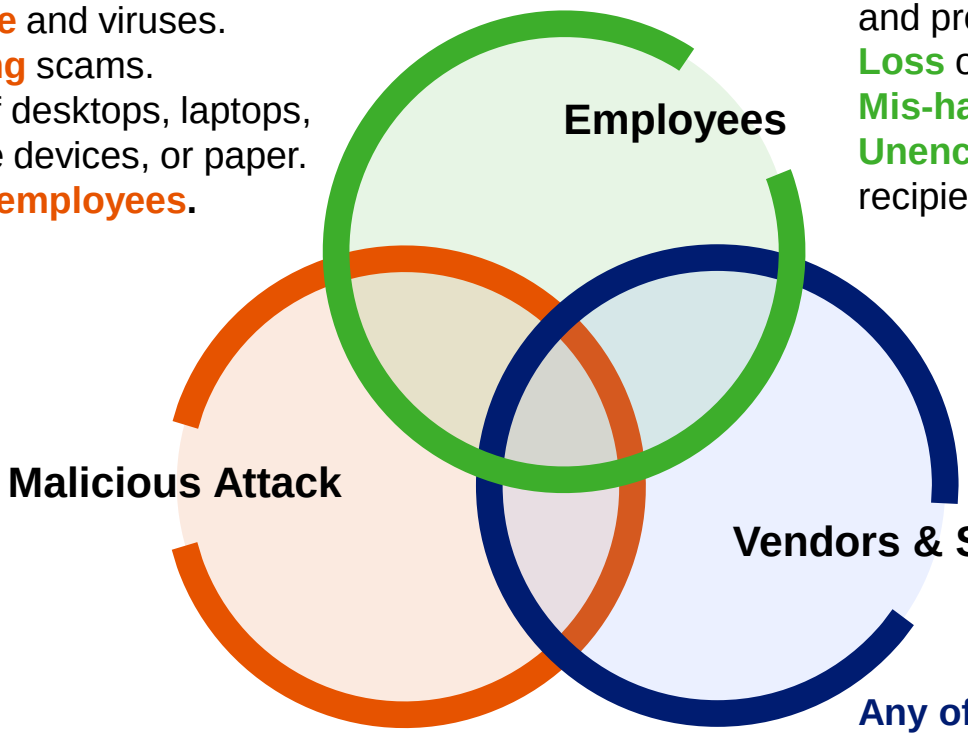
Cyber-criminal activity has increased dramatically: malware, phishing, ransomware and many other such attacks are all up double digits in the past four (4) years.

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

Sources of Cybersecurity Risks and Threats (…and thus, potential incidents)

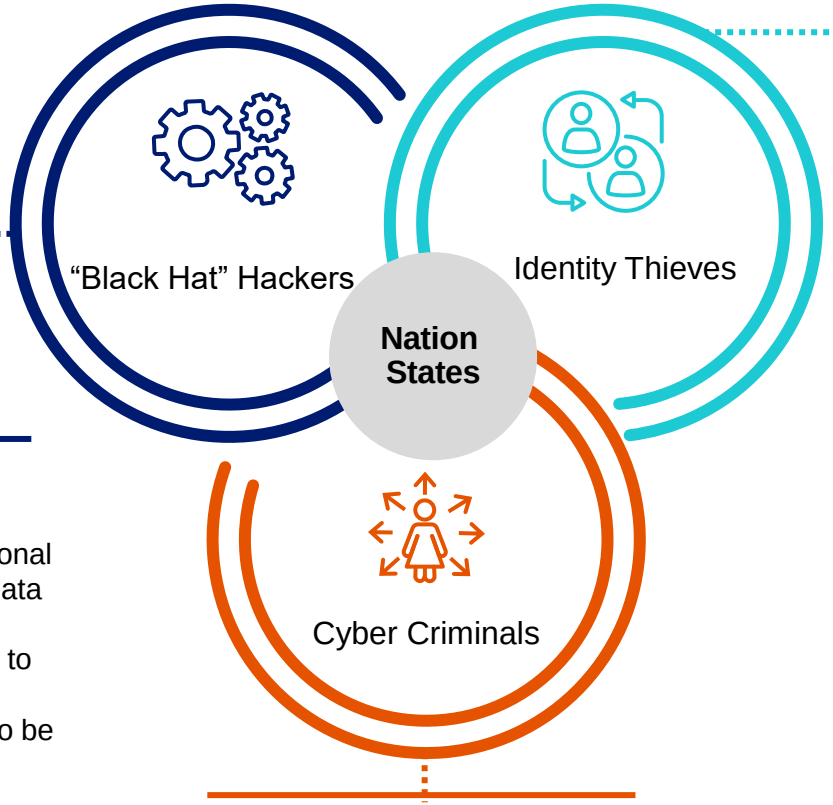
Hackers in your workstations, laptops, servers, email, or *mobile devices.*
Malware and viruses.
Phishing scams.
Theft of desktops, laptops, portable devices, or paper.
Rogue employees.

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.

Who Are The Criminals (and why do they want your data)?



- Work alone or in groups
- Have criminal intent
- Steal and sell data for personal gain – they rarely use the data themselves
- Modify, delete, or leak data to cause harm
- Expose what they believe to be immoral acts

- Work alone or in groups
- Have criminal intent
- Steal and sell data for personal gain (blackmail, extortion, ransom)
- Modify, delete, or leak data to cause harm
- Buy, sell, or trade illegal goods
- May engage in espionage or spying

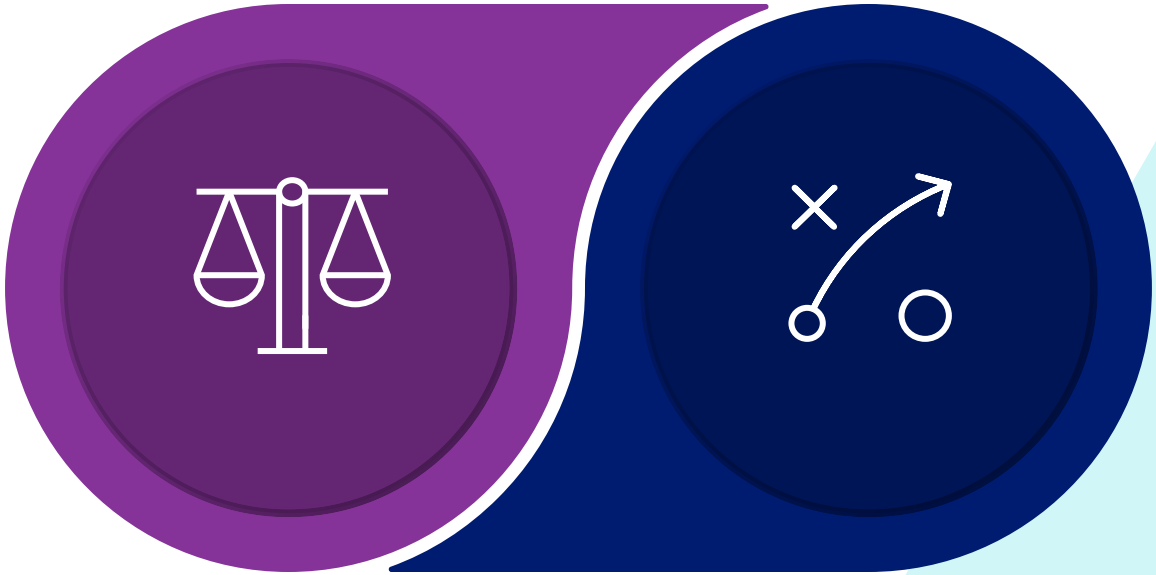
- Buy data from hackers and cyber criminals
- Use stolen information for illicit personal gain:
  - Draining your bank account
  - Taking out a bank or student loan in your name
  - Getting a new credit card in your name
  - Receiving medical services using your name
  - Making fraudulent insurance claims or prescription drug purchases
  - Receiving social security payments as you
  - Filing fake tax returns and receiving refund checks
  - Buying items and sticking you with the bill
  - Pretending to be you to scam other people you know

How can you respond to both these risks and threats?

Mitigating With a Defense in Depth Strategy

Consider Embracing a Defense-in-Depth Strategy

Recognizing the previously noted regulatory obligations and criminal risks associated with securing and managing your confidential, sensitive, non-public data and information…what is to be done?



Consider employing 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

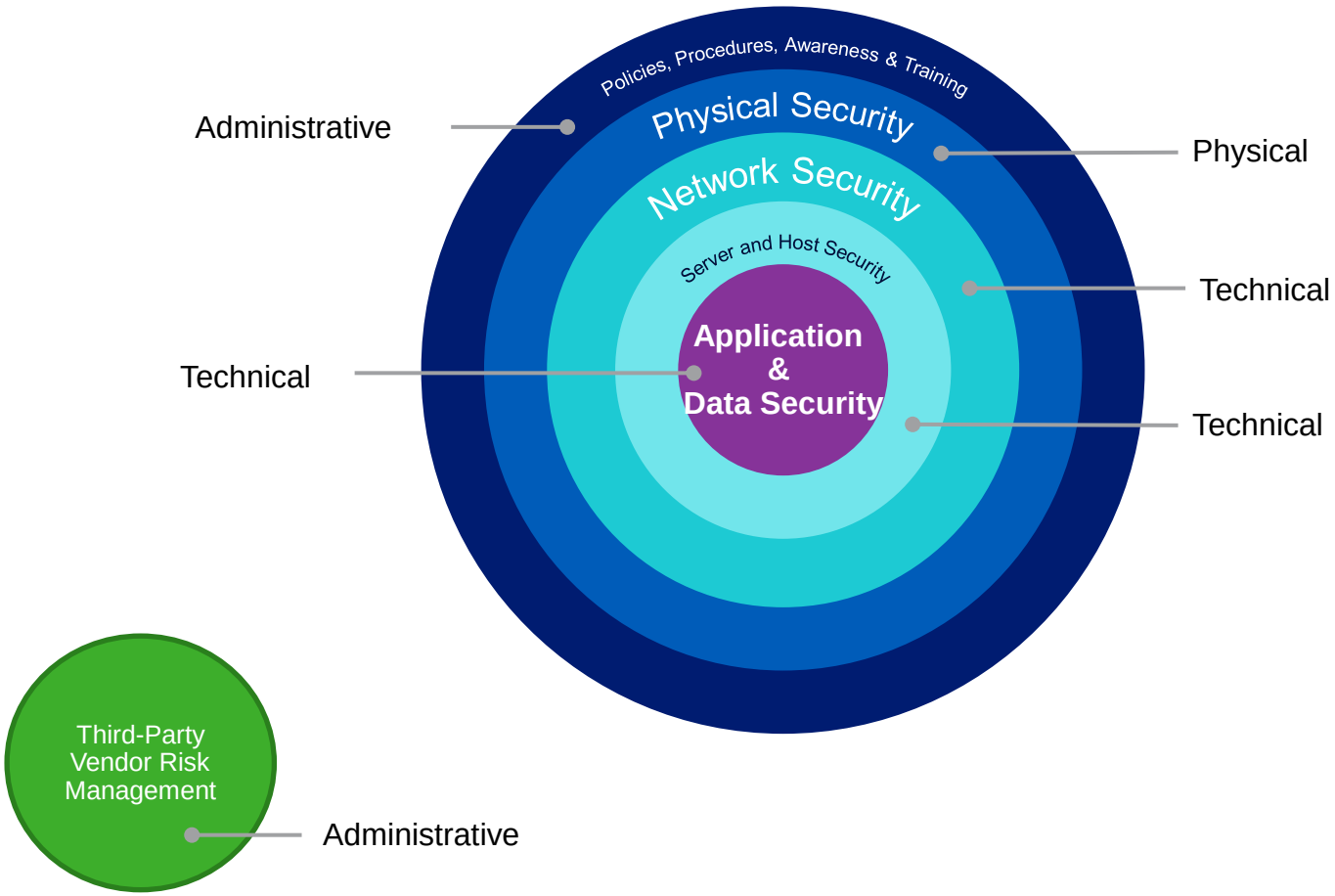
2

- 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.

Proactive cybersecurity is hard; do it anyway.

The Layers of Defense-in-Depth

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



Illustrating Each Dimension

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).

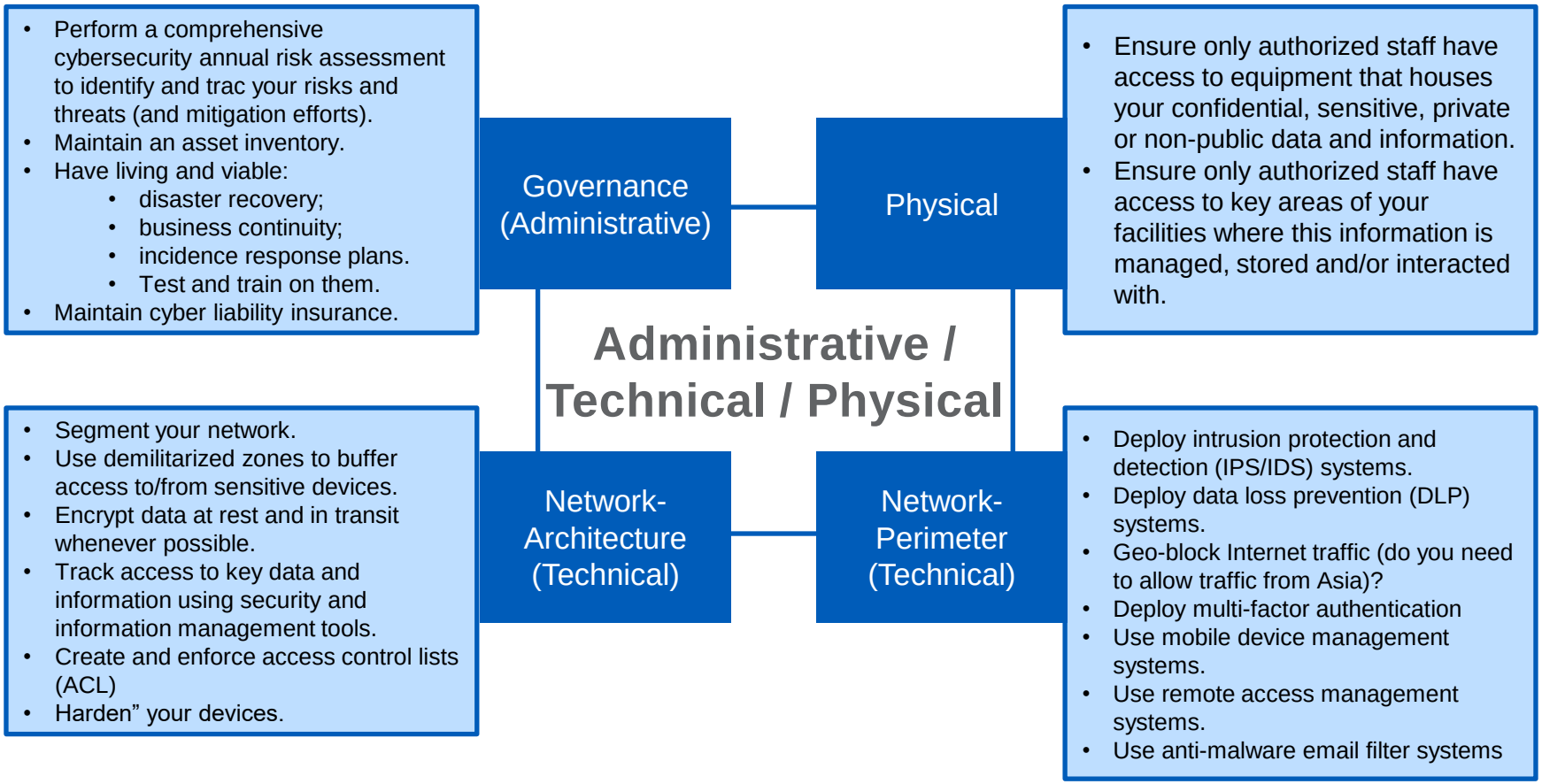
Network - Leveraging tools and technologies to block direct internet access to key sensitive systems – either at all – without appropriate architectural and other safeguards in place (e.g., DMZ, MFA, IPS/IDS, XDR (with anti-virus), etc.)

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.

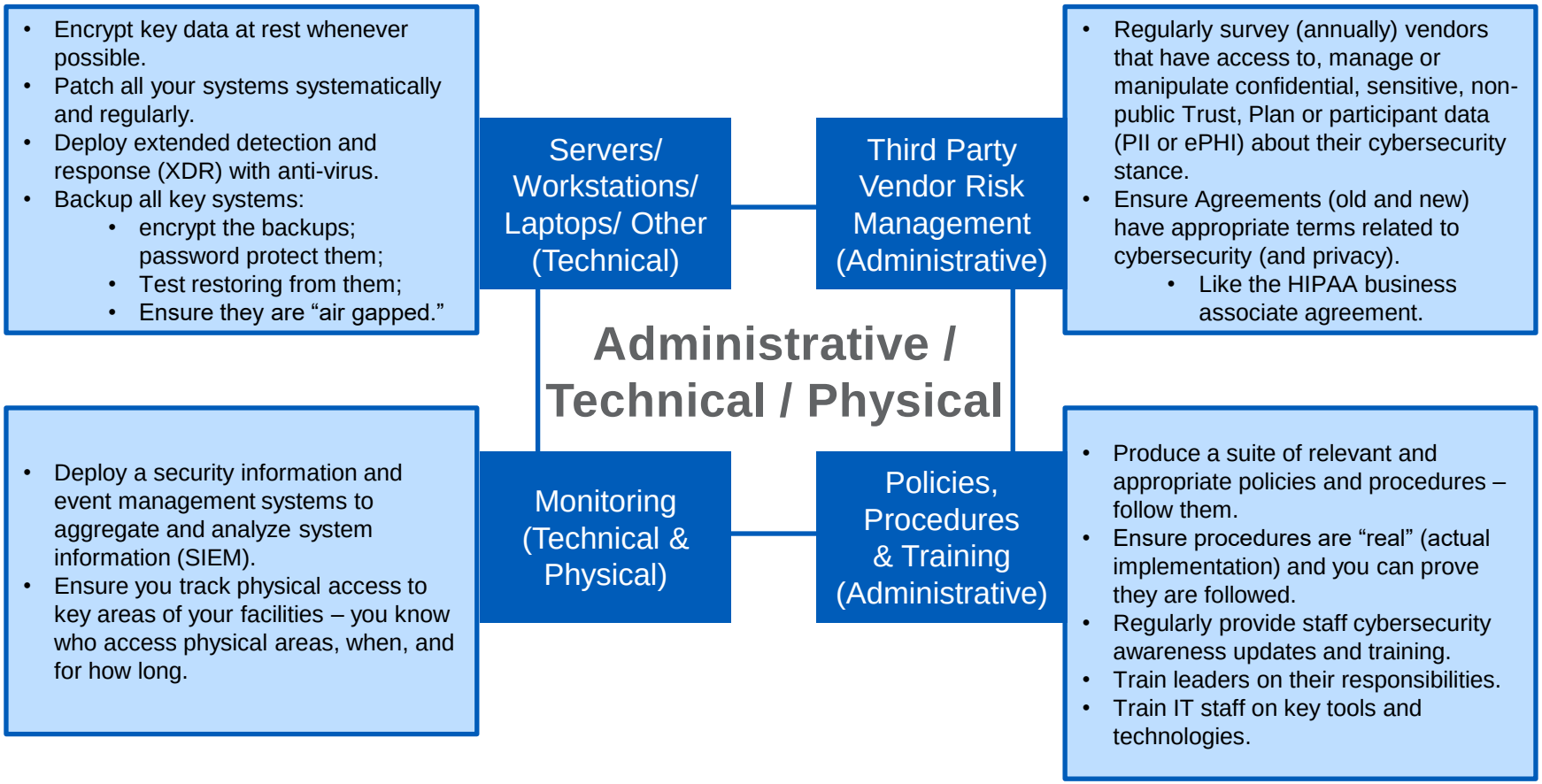
Applications - Restricting access to certain application functions via role-based security and per user accounts and passwords, again with MFA deployed. Tracking access to and changes of key data and information via log files and reporting – sent to SIEM tools, or not.

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)



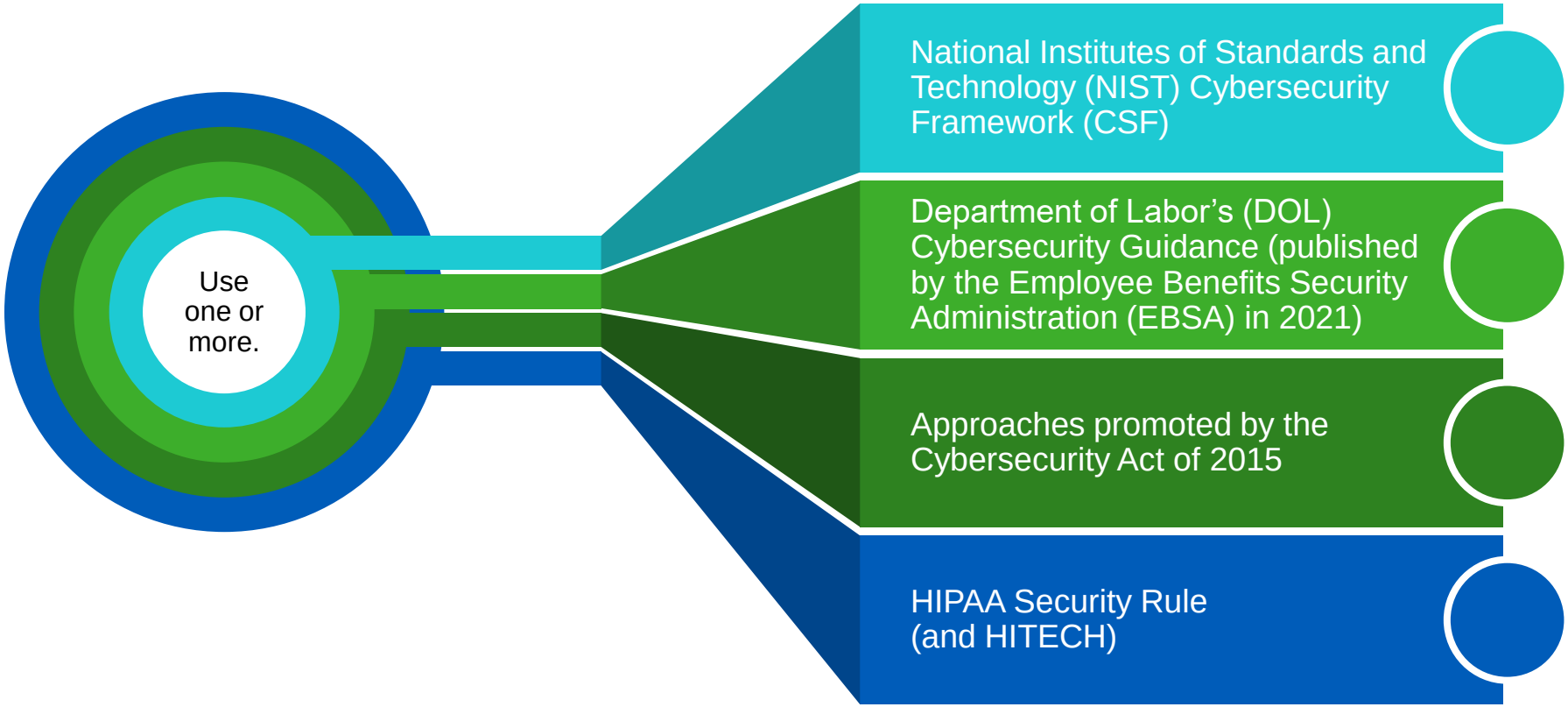
Illustrating *Some* Key Elements (*not* the only elements)



Use Frameworks to Guide Your Implementation of Defense-in-Depth

Supplement by Using One *or More* Frameworks

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



And there are many others!

Using the DOL's Published Guidance as a Cybersecurity Framework

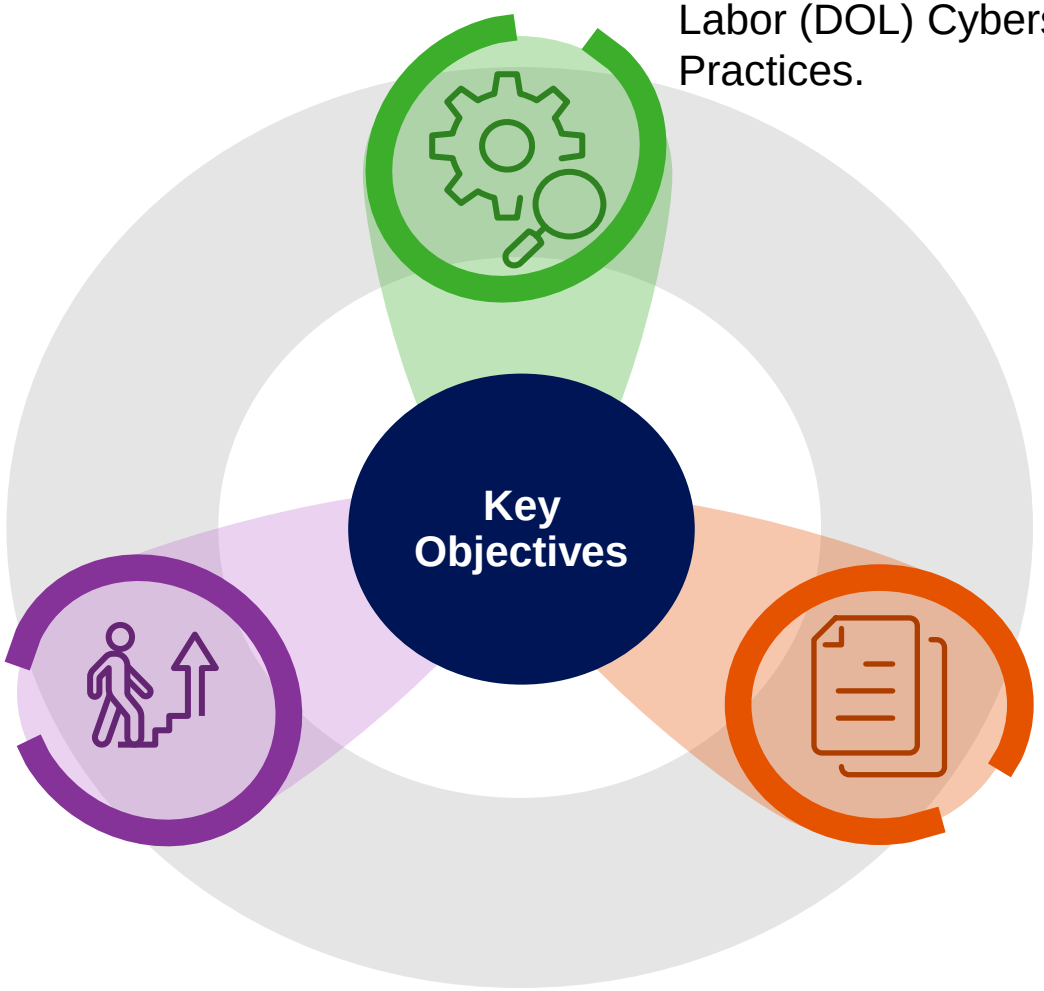
These goals are structured to help your Trust(s) / Plan(s) act in accord with the three (3) DOL published pieces related to cybersecurity guidance.

A DOL Cybersecurity Best Practices Evaluation Suite of Objectives

Assess your current cybersecurity activities against the Department of Labor (DOL) Cybersecurity Best Practices.

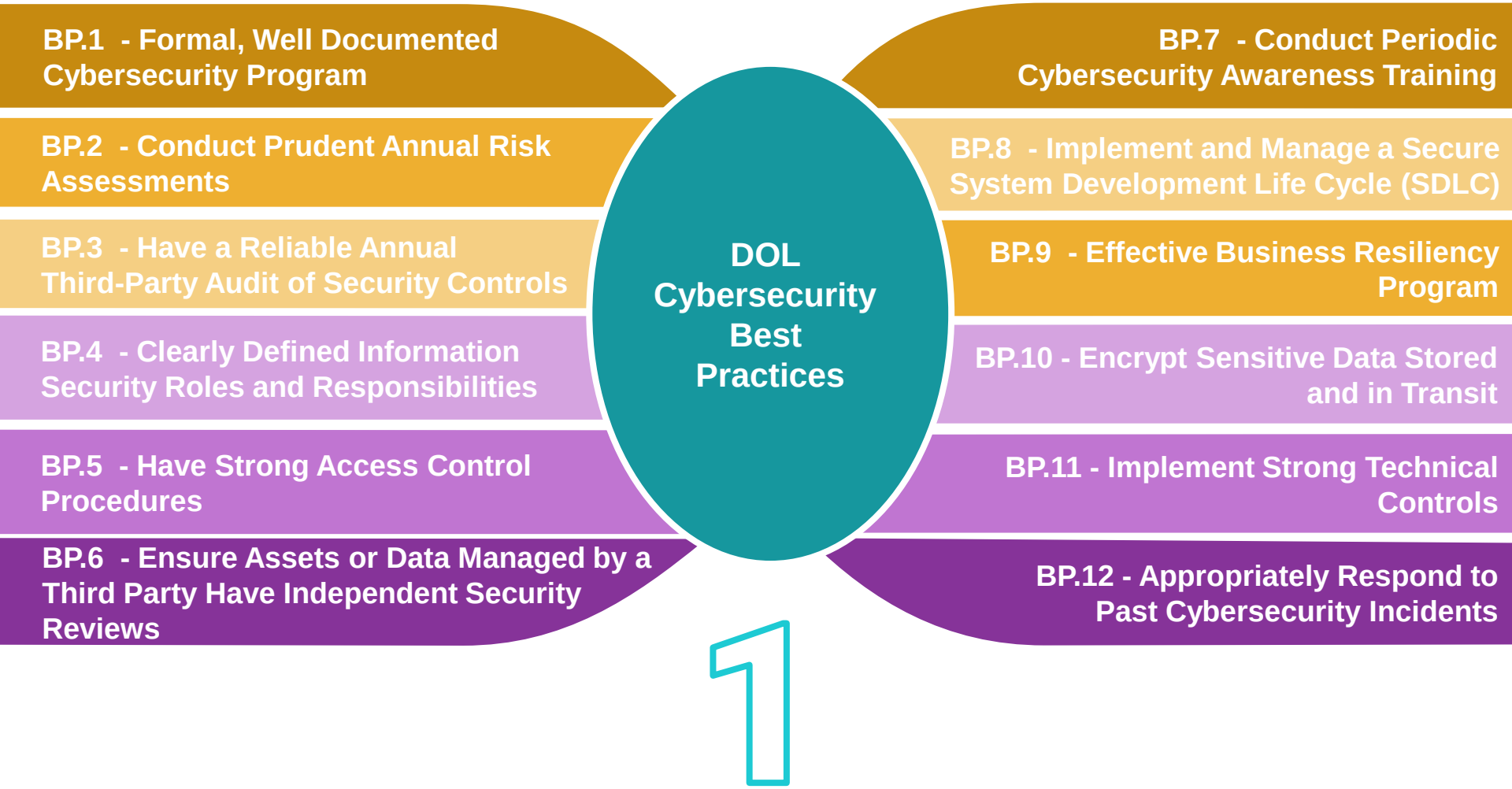
1

Recommend improvement opportunities and next steps.



Produce a detailed report illustrating specific actions you can take to enhance your cybersecurity protection.

DOL Cybersecurity Best Practices Overview



Tips for Hiring a Service Provider

2

Survey Agreed Upon Vendors

- Inquire about information security standards, practices and policies, and audit results, and compare that information to industry standards adopted by other service providers
- Ask how the service provider validates its cybersecurity practices and what levels of security standards are in place
- Evaluate the service provider's "track record" in the industry
- Ask about past security breaches and how the service provider responded to them
- Find out if the service provider has any insurance policies that cover losses from cybersecurity and identity theft breaches

Contracting

- Contracting was also referenced in the Guidelines.
- Work with legal counsel to ensure existing agreement are updated in accord with the published guidance.
- Ensure new agreements contain the appropriate language.

Hire a Service Provider With Good Cybersecurity Practices

2

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

Desirable (Tangible) Deliverables / End Goals for a Hypothetical "DOL Framework" Assessment

- After reviewing and analyzing the data and information provided, the third-party assessor should generate a report that assess the Plans' cybersecurity stance in relation to the DOL's "Best Practices" and indicate specific recommendations for improvement.

- The third party should review in conjunction with the Trust or Plan and then distribute one or more versions of a survey to the agreed upon vendors. Upon completion, those questionnaires should be scored by individual vendor and produce vendor specific reporting made available as well as aggregate reports based on various criteria (grouping vendors who have "advanced," "intermediate," "basic" and "insufficient" cybersecurity, e.g.).

- The DOL also published tips that should be distributed (freely available).
- Supplement these with other tips that – also – are freely available.

> Everyone is a target, most anywhere, most all the time.
>
> No organization is too small, or too big, to improve their cybersecurity stance.
>
> This is *continuous* work.

Thank You

Michael Stoyanovich, CDPSE

VP and Senior Consultant, San Francisco, CA.

Expertise

Mr. Stoyanovich is a Vice President and Senior Consultant in Segal's Administration & Technology Consulting practice. He has over 25 years of experience in the technology and benefits industries. Mr. Stoyanovich has extensive expertise in employee benefits plan administration and technology and considerable experience working with multiemployer plans.

Professional Background

Prior to Segal, Mr. Stoyanovich served as the Chief Information and Chief Operating Officer at Associated Third Party Administrators (ATPA). Earlier in his career he also served as Chief Information Officer of BeneSys. He has worked for a variety of other organizations in executive operational, consulting and leadership roles (a national pharmacy benefits manager, IT consulting companies, etc.).

Education/Professional Designations

Mr. Stoyanovich received a Bachelor or Arts degree from the University of Michigan and a Master of Public Administration degree from Michigan State University. Mr. Stoyanovich has earned a Certified Data Privacy Solutions Engineer (CDPSE) credential, issued by the Information Systems Audit and Control Association® (ISACA).

Publications/Speeches

Mr. Stoyanovich speaks at a variety of industry events and conferences, including the International Foundation of Employee Benefits Plans annual conferences and the Foundation's Trustees and Administrators Institutes. He has authored several articles that have been published in Benefits & Compensation Digest. He has testified before the ERISA Advisory Council (of the DOL) and spoken at the NCCMP annual conference.

Prior to joining Segal, Mr. Stoyanovich served as a member of the Steering Committee for Segal's annual Multiemployer IT Summit.

Michael Stoyanovich, VP, Senior Consultant
mstoyanovich@segalco.com
248.910.2637
segalco.com