A VIEW FROM THE EXPERTS – DOL CYBERSECURITY GUIDANCE: WHAT IT MEANS AND HOW TO IMPLEMENT IT

Morgan Lewis

Presenters

Matthew M. Hawes
(Moderator)
Partner, Morgan Lewis

Anthony J. Ferrante
Senior Managing
Director, FTI Consulting

Elizabeth S. Goldberg
Partner, Morgan Lewis

Michael J. Gorman
Associate, Morgan Lewis

Morgan Lewis

FTI CONSULTING

Introduction

Morgan Lewis

FTI CONSULTING

Legal Background

- ERISA's duty of prudence requires fiduciaries to act "with the care, skill, prudence, and diligence under the 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."
- It has become generally accepted that ERISA fiduciaries have *some* responsibility to mitigate the plan's exposure to cybersecurity events. But, prior to this guidance, it was not clear what the DOL expected of a "prudent" fiduciary with respect to cybersecurity risks.
- Cybersecurity events may implicate other fiduciary duties (e.g., loyalty) but the focus is on prudence.

Reports Highlighting Cybersecurity Risks

In November 2016, the ERISA Advisory Council published a report to the Secretary of Labor titled "Cybersecurity Considerations for Benefit Plans," which included questions regarding data protection that it thought may be helpful to plan fiduciaries contracting with and evaluating service providers.

In March 2021, the GAO published a report examining the data that plan sponsors and their service providers exchange during the administration of defined contribution plans and the associated cybersecurity risks.

- The report recommended that the DOL formally state whether it is an ERISA plan fiduciary's responsibility to mitigate cybersecurity risks in defined contribution plans and to establish minimum expectations for addressing cybersecurity risks in such plans.

Cybersecurity is a Priority for the DOL

- The Deputy Secretary of Labor, Julie Su, has stated that cybersecurity will be an area of focus for the DOL.
- Timothy Hauser, the Deputy Assistant Secretary for National Office Operations of the U.S. Department of Labor (DOL), has repeatedly commented on cybersecurity matters.
  - "Plans hold lots and lots of money, and with lots of money there's lots of temptations for bad actors . . . So far I think we've been fairly lucky in the plan universe. We have not had a huge catastrophic loss yet. But I do fear that may just be a matter of time."

DOL Focus Arises During Uptick in Private Litigation

- In the backdrop of this renewed DOL focus on cybersecurity is high profile litigation over alleged identity theft and fraudulent distributions.
- Prior court precedent is relatively favorable to plan fiduciaries, but there is some concern that the law will become less favorable as additional cases (with worse facts) are heard.
  - The most prominent cases focus on whether the fiduciary has a prudent process and whether that process was followed.
- There has also been increased litigation alleging that plan fiduciaries have failed to properly secure plan data.
  - While this presentation focuses on the threat of identity theft and fraudulent distributions, cybersecurity events involving plan data are also a major concern.

The DOL Issues First-of-Its-Kind Cybersecurity Guidance

- The DOL has repeatedly signaled that it would be turning its focus toward the intersection of cybersecurity practices and ERISA's fiduciary duties.
- On April 14, 2021, issued three pieces of subregulatory guidance addressing the cybersecurity practices of retirement plan sponsors, their service providers, and plan participants respectively.
- While this subregulatory guidance is not entitled to deference — and arguably does not even have the persuasive authority of an Advisory Opinion — it provides a window into the DOL's expectations for a "prudent" plan fiduciary's cybersecurity practices.

New Guidance

- Each of the three new pieces of guidance addresses a different audience.
- *Tips for Hiring a Service Provider with Strong Cybersecurity Practices* provides guidance for plan fiduciaries when hiring a service provider, such as a recordkeeper, trustee, or other provider that has access to a plan's nonpublic information.
- *Cybersecurity Program Best Practices* is a collection of best practices for recordkeepers and other service providers, which may be viewed as a reference for plan fiduciaries when evaluating service providers' cybersecurity practices.
- *Online Security Tips* contains online security advice for plan participants and beneficiaries.

Could Best Practices Be More Than Best Practices?

- While the DOL characterizes the guidance for fiduciaries and service providers as "tips" and "best practices," the language in the body of the guidance is stronger.
  - For example, *Tips for Hiring a Service Provider* states, "Plan Sponsors **should** use service providers that follow strong cybersecurity practices." (emphasis added).
  - Similarly, *Cybersecurity Program Best Practices* introduces a list of its 12 best practices as what "Plan's service providers **should**" do (emphasis added).
- This distinction is particularly important given the ongoing enforcement initiative focusing on ERISA plan cybersecurity practices.

The Role of Cybersecurity Professionals

- While legal counsel can assist plan fiduciaries in developing a prudent process to monitor cybersecurity risks consistent with the DOL guidance, lawyers may not be well situated to evaluate the strength of a vendor's cybersecurity practices.
- Thus, it may be appropriate for the plan fiduciary to engage a third-party cybersecurity vendor to evaluate the plan's vendors' cybersecurity practices.
  - To satisfy its duty of prudence, a fiduciary is not required to be an expert; but the fiduciary may need to consult an expert.
- Plan fiduciaries and their third-party cybersecurity vendors (if any) may benefit from working hand-in-hand with the plan sponsor's IT professionals to develop a uniform response to cybersecurity threats.

Summarizing the Guidance

Morgan Lewis

FTI CONSULTING

Tips for Hiring a Service Provider

Tips for Hiring a Service Provider outlines factors for "business owners and fiduciaries" to consider when selecting retirement plan service providers.

More specifically, this guidance recommends steps that a plan fiduciary should take when hiring a service provider. These steps include:

- Asking about the service provider's data security standards, practices, and policies and audit results and benchmark those against industry standards.

- Analyzing the service provider's security standards and security validation practices.

- Confirming that the agreement with the service provider permits the plan fiduciary to review cybersecurity compliance audit results.

- Evaluating the service provider's track record in the industry (e.g., security incidents, litigation, etc.).

- Asking about past security events and responses.

- Confirming that the service provider has adequate insurance coverage for losses relating to cybersecurity and identity theft events, including losses caused by internal threats (e.g., the service provider's employees) and external threats (e.g., third party fraudulent access of participant accounts).

- Ensuring that the services agreement between the plan fiduciary and the service provider includes provisions requiring ongoing compliance with cybersecurity standards.

FTI CONSULTING

Morgan Lewis

Tips for Hiring a Service Provider – Legal Commentary

- Conspicuously absent from this guidance is a clear statement regarding a fiduciary's obligations with respect to current service providers. However, it is reasonable to expect that the DOL may assert on audit that a plan fiduciary should have reevaluated their current service providers' practices and their current agreements in light of this guidance.
- Thus, fiduciaries may want to consider evaluating current agreements to better understand the service provider's obligations, sending questionnaires to service providers regarding their cybersecurity programs, and exercising audit rights. Depending on the terms of the agreement, a fiduciary may want to propose amending the services agreement to better align with the *Tip for Hiring a Service Provider*.
- Plan fiduciaries could consider using the *Tips for Hiring a Service Provider* when preparing requests for information (RFI) and requests for proposal (RFP).
- When entering into a new agreement, the plan fiduciary could engage in meaningful negotiations over the terms of the agreement implicated in this guidance (e.g., cybersecurity, protection and use of confidential data, insurance coverage, etc.).

Cybersecurity Program Best Practices

- *Cybersecurity Program Best Practices* is directed squarely at ERISA plan recordkeepers and other service providers who have access to plan-related IT systems and plan data.

- It summarizes 12 "best practices" that plan service providers "should" implement to mitigate exposure to cybersecurity risks. Although this guidance is specific to service providers, the DOL points out that plan fiduciaries "should" be aware of these best practices to enable them to make prudent decisions when hiring a service provider.

- As discussed above, this implies that the DOL may take the position on audit that a plan fiduciary is being imprudent if they fail to ensure that the plan's service providers engage in these best practices. Arguably the DOL could take this position with respect to service providers hired prior to the issuance of this guidance (and even with respect to services rendered prior to the issuance of this guidance).

Cybersecurity Program Best Practices (1-2)

The *Cybersecurity Program Best Practices* provide that:

1. service providers **should** have a formal, well-documented cybersecurity program that consists of policies and procedures designed to protect the infrastructure, information systems, and data from unauthorized access and other malicious acts by enabling the service provider to (1) identify the risks, (2) protect the assets, (3) detect and respond to cybersecurity events, (4) recover from cybersecurity events, (5) appropriately disclose the event, and (6) restore normal operations.
2. service providers **should** design and codify annual risk assessments that help identify, estimate, and prioritize risks to the information systems.

Cybersecurity Program Best Practices (3-4)

3. service providers **should** have a third-party auditor assess the service provider's security controls on an annual basis. The DOL indicated that as part of its review of an effective audit program, the DOL would expect to see, among other things, audit reports and audit files prepared and conducted in accordance with appropriate standards, penetration test reports, and documented correction of any weaknesses.
4. service providers **should** clearly define and assign information security roles and responsibilities, with management of the cybersecurity program at the senior executive level and execution of the cybersecurity program by qualified personal who have sufficient experience and certifications, undergo background checks, receive regular update and training on current cybersecurity risks, and have current knowledge of changing threats and countermeasures.

Cybersecurity Program Best Practices (5-6)

5. service providers **should** have strong access control procedures, including limiting access to authorized users; limiting access privileges based on role and the "need-to-access" principle; establishing a policy to review access privileges every three months; requiring unique, complex passwords; using multifactor authentication wherever possible; establishing policies, procedures, and controls to monitor authorized users and detect unauthorized access; establishing procedures to ensure participant or beneficiary sensitive information in the service provider's records matches the plan's information; and confirming the identity of authorized fund recipients.
6. service providers **should** ensure that any cloud or third-party managed storage system used by the service provider to service the plan is subject to proper security reviews and independent security assessments.

Cybersecurity Program Best Practices (7-8)

7. service providers **should** conduct periodic cybersecurity awareness training for all personnel pursuant to a comprehensive program that sets clear cybersecurity expectations and educates everyone to recognize sources of attack, help prevent incidents, and respond to threats.
   - The DOL emphasized identity theft—individuals posing as plan officials, fiduciaries, participants, or beneficiaries—as a leading cause of fraudulent distributions that should be considered a key topic of training.
8. service providers **should** implement and manage a secure "system development life cycle" (SDLC) program addressing both in-house developed applications and externally developed applications and that includes activities such as penetration testing, code review, and architecture analysis.

Cybersecurity Program Best Practices (9-10)

9. service providers **should** have an effective business resiliency program that addresses business continuity, disaster recovery, and incident response and allows for the organization to maintain continuous operations and safeguard people, assets, and data during periods of disruption.
10. service providers **should** implement current, prudent standards for the encryption of sensitive nonpublic information both while it is at rest and while in transit.

Cybersecurity Program Best Practices (11-12)

11. service providers **should** implement technical security controls consistent with best security practices, including hardware, software, and firmware that is kept up to date; firewalls and intrusion detection and prevention tools; current and updated antivirus software; routine patch management (preferably automated); network segregation, system hardening; and routine data backup (preferably automated).
12. service providers **should** respond appropriately to cybersecurity incidents that have occurred, including notifying law enforcement; notifying the appropriate insurer; investigating the incident; giving affected plans and participants information to prevent or mitigate harm; honoring contractual or legal obligations and fixing any problems that would prevent recurrence.

Online Security Tips

- *Online Security Tips* recommends 9 security tips for plan participants and beneficiaries as ways to better protect their online information and retirement accounts.
- These tips include the use of multifactor authentication, keeping contact information current, and avoiding phishing attacks.
- Plan fiduciaries may help mitigate the plan's exposure to cybersecurity threats by encouraging participants and beneficiaries to follow these tips.
- Plan fiduciaries may better satisfy their fiduciary duties, and better protect themselves in the event of a cybersecurity event, by emphasizing to participants the importance of following these tips.

Open Questions

- The DOL guidance issued on April 14, 2021 leaves open many questions. For example:
  - How should plan fiduciaries and service providers address existing arrangements that do not comport with the guidance?
  - Does the DOL believe that ERISA preempts state data privacy laws as they relate to ERISA benefit plans?
  - Does the DOL expect fiduciaries to communicate the *Online Security Tips* to participants and beneficiaries, and, if so, how often?
- Notwithstanding these unanswered questions, this guidance is a helpful starting place for ERISA plan fiduciaries trying to understand how their duty of prudence applies to the world of cybersecurity.

How to Respond to this Guidance (Legal Perspective)

Morgan Lewis

FTI CONSULTING

Practical Steps to Respond to this Guidance

Review the guidance and consider working with service providers to ensure that existing data security protocols reflect the best practices set forth by the DOL.

Consider establishing formal procedures designed to ensure that cybersecurity issues are regularly considered and properly addressed.

Consider fiduciary training on how best to address fiduciary exposure to cybersecurity events.

Consider educating participants as to their obligations with respect to cybersecurity and advising them of the DOL's *Online Security Tips*.

Consider reviewing plan documents, including SPDs and participant communications.

- The cybersecurity world is rapidly evolving, and it may make sense to tweak plan provisions to better protect the plan, its fiduciaries, and participants.

Consider engaging counsel and third-party vendors to conduct a benefit plan cybersecurity audit to analyze potential weaknesses in cybersecurity practices and the best way to resolve such weaknesses.

- There may be value to engaging third-party vendors through counsel in order to maintain privilege.

Vendor Questionnaires

- The DOL guidance asks that plan fiduciaries be aware of their vendors' cybersecurity practices, which may be essential to allowing the plan fiduciary to fulfill its monitoring obligation.
- One way to gain an understanding of the vendors' cybersecurity practices is through the use of a questionnaire.
- The questionnaire would also enable the plan fiduciary to gather the context and historical information that the DOL highlights in the *Tips for Hiring a Service Provider*.

Vendor Agreements

- Another step that plan fiduciaries may wish to take is to have counsel review the relevant vendor agreements to ensure that the contract terms identified in the *Tips for Hiring a Service Provider* are included (or excluded) consistent with this guidance.
- This will also provide an opportunity for the plan fiduciaries to seek representations and warranties from the vendor as to its compliance with the *Cybersecurity Program Best Practices*.

How to Respond to this Guidance (Cybersecurity Advisory Perspective)

Morgan Lewis

FTI CONSULTING

Working With Your Service Provider

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 all sizes:

1. Ask about the service provider's information security standards, practices and policies, and audit results, and compare them to the industry standards adopted by other financial institutions.
   - Look for service providers that follow a recognized standard for information security and use an outside (third-party) auditor to review and validate cybersecurity. You can have much more confidence in the service provider if the security of its systems and practices are backed by annual audit reports that verify information security, system/data availability, processing integrity, and data confidentiality.
2. Ask the service provider how it validates its practices, and what levels of security standards it has met and implemented. Look for contract provisions that give you the right to review audit results demonstrating compliance with the standard.
3. Evaluate the service provider's track record in the industry, including public information regarding information security incidents, other litigation, and legal proceedings related to vendor's services.
4. Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.
5. Find out if the service provider has any insurance policies that would cover losses caused by cybersecurity and identity theft breaches (including breaches caused by internal threats, such as misconduct by the service provider's own employees or contractors, and breaches caused by external threats, such as a third party hijacking a plan participants' account).
6. When you contract with a service provider, make sure that the contract requires ongoing compliance with cybersecurity and information security standards – and beware contract provisions that limit the service provider's responsibility for IT security breaches. Also, try to include terms in the contract that would enhance cybersecurity protection for the Plan and its participants, such as:
   - **Information Security Reporting**. The contract should require the service provider to annually obtain a third-party audit to determine compliance with information security policies and procedures.

Cybersecurity Due Diligence

- Choose a provider that prioritizes security
  - Assess their policies, procedures, and processes against best practice and industry standards, such as NIST, CIS, or ISO
  - Interview management and staff to understand how policies and procedures are carried out
  - Verify or validate implemented cybersecurity processes or procedures through testing
- Review their cybersecurity incident history, such as past breaches, their response, and remediation actions
- Tie information security management to service level agreements
  - Right to audit, obligations, incident response, compliance standards, insurance
- Understand if the provider has cyber insurance and what their policy covers

Assess the operational reality of the provider and how they *actually* manage risk vs. what's documented on paper

Conducting a Cybersecurity Assessment

The objective of a cybersecurity assessment is to analyze cybersecurity maturity and to identify gaps or deficiencies in current controls as compared to standards and applicable obligations (regulatory, contractual, etc.).

Policy Review

- Does the policy have…
  - Clear purpose?
  - Endorsement?
  - Target audience?

Security Controls

- Typically compared against a cybersecurity framework
- Is the control…
  - Defined in IT security policy?
  - Implemented?

Vulnerability Assessment (Level 2)

- Identify flaws in software, missing patches, and application misconfigurations
  - Internal
  - External

Penetration Testing (Level 2)

- Test the effectiveness of security controls in preventing and detecting attacks
  - Internal
  - External
  - Application
  - Wireless

Cybersecurity Assessment Example

IT Security Policy	Concise Purpose (Yes / No)	Endorsed by IT Management (Yes /No)	Target Audience (Yes / No)	Conclusions
Business Continuity - Radio and TV Discussion_2012.pptx	Yes Document defines a purpose for the assessment	Yes Document assumes endorsement from Corporate IT	Yes Document defines Corporate IT as the target audience	FTI Consulting believes the document is defined
Response - BusContinuity.docx	Yes Document defines a purpose for the audit	No Document doesn't show endorsement from the Director of IT	Yes Document defines Corporate IT as the target audience	The document doesn't show endorsement from IT Director. Endorsement is assumed by Corporate IT/IS
Procedure for Change Management.docx	Yes Document defines a purpose for the policy and procedure	Yes Document assumes endorsement from Corporate IT	No Document doesn't define a target audience	Unclear if this document applies specifically to Corporate IT or other groups within the company. The target audience is not defined
Response - changemgmt.docx	Yes Document defines a purpose for the audit	No Document doesn't show endorsement from the Director of IT	Yes Document defines Corporate IT as the target audience	The document doesn't show endorsement from IT Director. Endorsement is assumed by Corporate IT/IS

Policy Review

CIS Controls	(CIS Control 2) Inventory and Control of Software Assets
Definition of CIS Controls	Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
CIS Controls Mapped to NIST Cybersecurity Framework v1.0	ID.AM-2, PR.DS-6
Controls Defined in IT Written Policy 1. Not written 2. Partially written 3. Written	2. Partially written
Controls Procedures Implemented by IT 1. Not implemented 2. Partially implemented 3. Implemented	2. Partially implemented
Priority Ranking of CIS Controls	Very High
Conclusions	FTI Consulting recommends the Client consider utilizing application whitelisting software to ensure that only authorized software libraries, such as (.dll, .ocx, .so) are allowed to load into a system process. The Client should consider documenting and implementing the following CIS sub-controls for full compliance: 2.8,2.9.

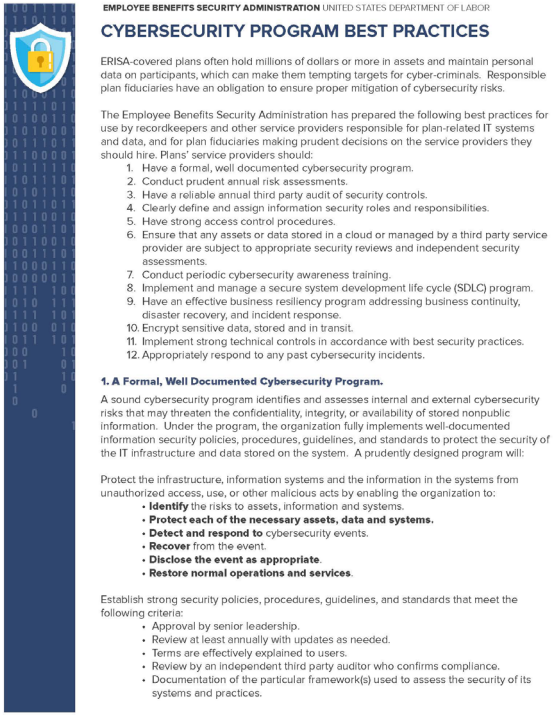
Control Review

RECOMMENDATIONS TO ACHIEVE BEST PRACTICE

Recommendation	Explanation of Recommendation	Priority Ranking
Continuous monitoring, inventory and Control of Hardware Assets	FTI Consulting recommends the Client consider utilizing an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory. Utilize port level access control, following 802.1x standards, to control which device can authenticate to the network.	Very High
Continuous monitoring, inventory and control of Software Assets	FTI Consulting recommends the Client consider utilizing application whitelisting software to ensure that only authorized software libraries are allowed to load into a system process.	Very High
Establish a Vulnerability Management and Remediation Process	FTI Consulting recommends the Client consider investing in a Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan for network vulnerabilities on a weekly basis to proactively identify potential vulnerabilities on the network.	Very High
Actively manage the secure configuration of Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	FTI Consulting recommends the Client consider investing in a SCAP compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur. Maintain secure images or templates for all systems in the enterprise based on the Client's approved configuration standards.	Very High

Recommendations

Additional Cybersecurity Program Best Practices



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 Employee Benefits Security Administration has prepared the following best practices for use by recordkeepers and other service providers responsible for plan-related IT systems 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 independent security assessments.
7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

1. A Formal, Well Documented Cybersecurity Program.

A sound cybersecurity program identifies and assesses internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of stored nonpublic information. Under the program, the organization fully implements well-documented information security policies, procedures, guidelines, and standards to protect the security of the IT infrastructure and data stored on the system. A prudently designed program will:

Protect the infrastructure, information systems and the information in the systems from unauthorized access, use, or other malicious acts by enabling the organization to:

- **Identify** the risks to assets, information and systems.
- **Protect each of the necessary assets, data and systems.**
- **Detect and respond to** cybersecurity events.
- **Recover** from the event.
- **Disclose the event as appropriate.**
- **Restore normal operations and services.**

Establish strong security policies, procedures, guidelines, and standards that meet the following criteria:

- Approval by senior leadership.
- Review at least annually with updates as needed.
- Terms are effectively explained to users.
- Review by an independent third party auditor who confirms compliance.
- Documentation of the particular framework(s) used to assess the security of its systems and practices.

- Ensure proper patch management and data access management processes are in place
- Understand the risks posed by all of your vendors and third-party service providers; mitigate those risks that pose the greatest threat to your key assets
- Conduct cyber awareness trainings for employees to supplement technological protective measures
- Enable Multi-Factor Authentication for all users
- Proactively monitor logs for the early detection of threats

Incident Response

Morgan Lewis

FTI CONSULTING

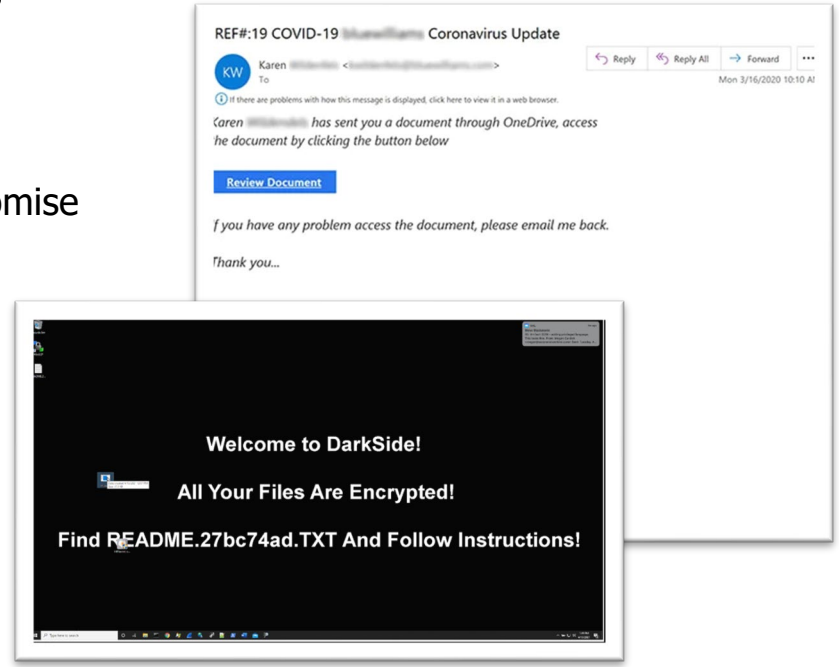
Cyber Risks & Threats

What's at Risk?

- Assets, Money
- Personally Identifiable Information
- Corporate Reputation
- Stakeholder Trust

Common Threats Facing Plan Sponsors or Service Providers

- Data Breach
- Phishing
- Business Email Compromise
- Ransomware
- Insider Threat



Incident Response Planning

Key Components

- Set criteria for when the plan should be activated
- Clearly define roles and responsibilities within an organization
- Outline internal and external information flows and processes
- Create contingency plans if certain resources are unavailable
- Identify external partners who can help in certain scenarios
- Understand applicable notification requirements
- Test your plan using realistic scenarios
- Continuously update your plan with lessons learned or to reflect changes in your organization

Who's Involved

- Board Members
- C-suite
- Senior Management
- General Counsel
- Technical Terms
- Communications, Media & Public Affairs Teams

DOL Cybersecurity Enforcement Initiative

Morgan Lewis

FTI CONSULTING

DOL Investigations

- Within weeks of issuing its cybersecurity guidance, the DOL began opening investigations into the cybersecurity practices of ERISA plan fiduciaries.
- These investigations often involved comprehensive information requests that were even more extensive than what is summarized in the guidance.
- The DOL has informally signaled that these investigations are here to stay and that cybersecurity issues will be addressed in the vast majority of investigations.

Proactive Steps to Mitigating Audit Risk

- Given the level of DOL activity in this space, plan fiduciaries may wish to prepare for a DOL investigation into their approach to cybersecurity as an inevitability.
- Plan fiduciaries may wish to take significant steps in response to this guidance (e.g., hiring a third-party vendor to assist, preparing and adopting a cybersecurity policy statement, issuing a cybersecurity questionnaire to vendors, evaluating the terms of their vendor agreements).
- Properly documenting these steps could benefit the plan and its fiduciaries by creating a record of the steps that the plan fiduciary took to mitigate the plan's exposure to cybersecurity events and to facilitate compliance with the DOL guidance.

THANK YOU