siekmanncо
Retirement and Employee Benefits
empowered by GBQ

Protecting Your Employee Benefits Plans from Cybersecurity Threats

September 14, 2021

Presenters

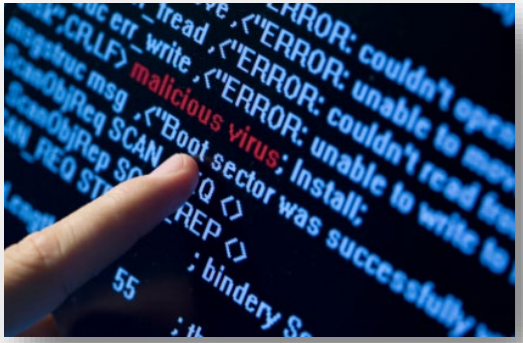
Aaron Siekmann,
CRPS® AIF®
President
The Siekmann Company
(614) 873-5200
aaron@siekmannco.com

Doug Davidson,
CISA
Director of Information Technology Services
GBQ
(614) 947-5340
ddavidson@gbq.com

Agenda

- Top Causes for Loss
- DOL Guidance on Retirement Plan Cyber Security
- Cyber Security Program Best Practices
- Tips for Hiring Service Providers
- Online Security Best Practices for your Plan Participants

Cyber Top Causes of Loss



RANSOMWARE
When your information is held hostage, can you recover?

SOCIAL ENGINEERING
Being tricked into paying money to a fraudster

THIRD PARTY VENDORS
Cyber attacks on Cloud/IT Provider/Credit Card Processors impacting our insured

EMPLOYEES
Click on phishing emails

DOL Guidance on Retirement Plan Cyber Security

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

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

Where do we start?

Risk Assessment

- Conduct prudent annual risk assessments.

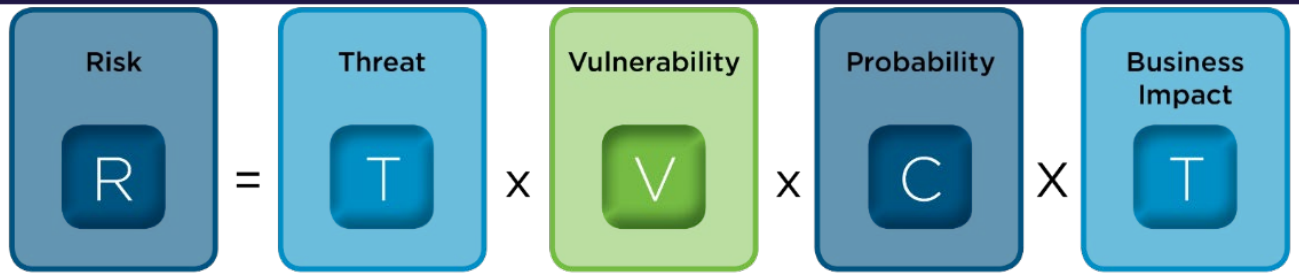
Improve or Remediate Findings

- Have a formal, well documented cybersecurity program.
- 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.
- Clearly define and assign information security roles and responsibilities.
- Have strong access control procedures.
- Conduct periodic cybersecurity awareness training.
- Implement and manage a secure system development life cycle (SDLC) program.
- Encrypt sensitive data, stored and in transit.
- Implement strong technical controls in accordance with best security practices.
- Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
- Appropriately respond to any past cybersecurity incidents

Test, Manage, Assure (Audit)

- Have a reliable annual third party audit of security controls.

Prudent Annual Risk Assessment



A risk assessment should:

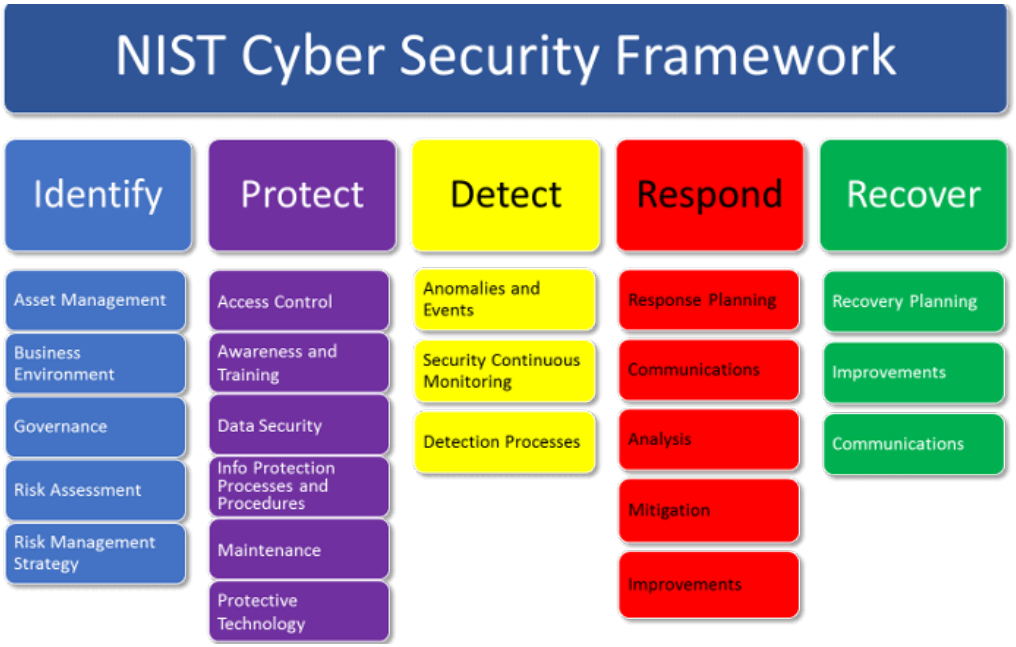
- Identify, assess, and document how identified cybersecurity risks or threats are evaluated and categorized.
- Establish criteria to evaluate the confidentiality, integrity, and availability of the information systems and nonpublic information, and document how existing controls address the identified risks.
- Describe how the cybersecurity program will mitigate or accept the risks identified.
- Facilitate the revision of controls resulting from changes in technology and emerging threats.
- Be kept current to account for changes to information systems, nonpublic information, or business operations.

A formal, well documented cybersecurity program …

Protect 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



Tips for Hiring Service Providers

01 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.

02 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.

03 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.

04 Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.

05 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).

06 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.

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

Cyber Security Guarantees

Many of the industry's top 401(k) Plan custodians offer Cyber Security guarantees for reimbursement of lost funds due to Cyber Security or Identity Theft attacks that were not due to negligence of the plan or its participants.

Common requirements include:

- Creating and maintaining strong and unique usernames and passwords
- Not sharing or storing your login information with the public or unsecure locations
- Practice safe internet usage and maintaining proper antivirus tools
- Prompt notification of suspicious activity and or breaches

CAUTION 1: Guarantee only as good as guarantor

CAUTION 2: As with cyber liability insurance, these requirements will likely change over time!

Online Security Tips

REGISTER, SET UP AND ROUTINELY MONITOR YOUR ONLINE ACCOUNT

USE STRONG AND UNIQUE PASSWORDS

USE MULTI-FACTOR AUTHENTICATION

KEEP PERSONAL CONTACT INFORMATION CURRENT

CLOSE OR DELETE UNUSED ACCOUNTS

BE WARY OF FREE WI-FI

BEWARE OF PHISHING ATTACKS

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

Key Takeaways

- Cybercrime is impacting benefit plans
- Government action is motivated by losses
- Build a security program that includes a risk assessment, a written plan, and key technologies
- Practice safe online behavior yourself
- Consider security in selecting the best retirement plan for your company

Questions?

Presenters

Aaron Siekmann,
CRPS® AIF®
President
The Siekmann Company
(614) 873-5200
aaron@siekmannco.com

Doug Davidson,
CISA
Director of Information Technology Services
GBQ
(614) 947-5340
ddavidson@gbq.com