Ensure Your Organization's Confidential and Sensitive Data Is Protected

Protecting private, confidential and sensitive data and information is increasingly challenging.

As cybercriminals become more active, aggressive and creative in targeting organizations by exploiting weaknesses in technology and human psychology, ensuring a strong cybersecurity discipline has become increasingly difficult — especially with greater numbers of employees working from home.

How can you identify weaknesses in your cybersecurity administrative, technical, physical and logical controls? Regular, systematic and comprehensive cybersecurity risk assessments can help. Using these assessments to address any identified weaknesses can potentially help you avoid fines from regulatory agencies, expenses related to security incidents or actual data breaches (inadvertent or otherwise) and possible lawsuits from those who may have been harmed.

Perform regular cybersecurity risk assessments

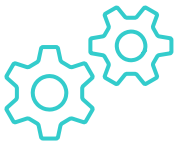
Cybersecurity risk assessments are detailed evaluations of your organization's cybersecurity discipline. The goal is to help you improve the security of private, confidential or sensitive and likely regulated data. This includes but is not limited to plan participants' data and information.

There are multiple types of cybersecurity risk assessments. Some are designed specifically to meet particular regulatory compliance obligations. Others are designed to provide organizations with a more comprehensive cybersecurity evaluation and are not tied to one regulatory perspective.

Regardless, these risk assessments can help identify vulnerabilities that could lead to a security incident or data breach.

Policies

Potential Compliance



Procedures

Technology

To keep pace with evolving threats, certain cybersecurity risk assessments should be performed annually. Examples include an annual assessment against the National Institutes of Standards and Technology (NIST) Cybersecurity Framework (CSF) or an assessment based on the 2021 DOL cybersecurity guidance.

Others, which may be associated with compliance obligations, are typically performed every one to three years. An example is an assessment that focuses on HIPAA security rules and the HITECH Act.

Segal

Seek assistance from those with IT and administrative expertise

Segal's Administration and Technology Consulting (ATC) Practice has conducted hundreds of cybersecurity risk assessments for clients and can help your organization improve its cybersecurity maturity. Our ATC consulting team, which includes nationally recognized subject matter experts, has in-depth, hands-on knowledge of employee benefit plans and technology.

Our core services include four types of cybersecurity risk assessments:

HIPAA-HITECH security assessment — The HIPAA Security Rule applies to electronic protected health information (ePHI) that is transmitted or stored electronically. Health plans must take actions to protect ePHI as required by the HIPAA Security Rule. Group health plans must perform regular HIPAA security assessments to ensure how they "...store, transmit, and protect, and eventually destroy ePHI..." follow the rule.

NIST CSF assessment — Some organizations may benefit from the rigorous and thorough NIST CSF assessments so they can improve their cybersecurity and data protection in a comprehensive manner. There are no fines associated with falling short of NIST standards since they are not required for plan sponsors; rather, this is a "best practices" framework.

DOL cybersecurity assessment — In 2021, the DOL issued non-regulatory guidance for benefit plans subject to ERISA on how to reduce cybersecurity risks, including "Cybersecurity Program Best Practices" and "Tips for Hiring a Service Provider with Strong Cybersecurity Practices." As fiduciaries, plan sponsors will want to ensure their current practices are in accord with the best practices identified by the DOL, as the DOL is expected to look to this published guidance if and when it investigates plans.

Third party risk management (TPRM) assessment — Successful TPRM enables better vendor selection, negotiation and cost savings. Good TPRM often translates to cost avoidance and achieves better management of contracts, improved third-party service levels, strong regulatory compliance and the prevention of business interruptions. Effective TPRM also significantly reduces the possibility of litigation, regulatory fines, rework, lost productivity and reputational damage.

Our cyber risk assessments include these components:

- Clarification interview sessions where we'll gather data and other information from your key stakeholders
- Review and analyze policies, procedures, manuals and evidence of work performed, such as reports and log files
- A report that identifies specific vulnerabilities and prioritizes risks by various categories and proposes next steps to strengthen your organization's cybersecurity discipline
- As part of the DOL cybersecurity assessment we will survey and gauge the cybersecurity risk associated with your third-party service providers. We'll give you individualized vendor and vendor group analysis and reporting

To learn more about ATC's cybersecurity risk assessments, please get in touch.

Contact

Michael Stoyanovich, CDPSE
Vice President & Senior Consultant
mstoyanovich@segalco.com
248.910.2637

Segal is a leading global employee benefit and HR consulting firm delivering trusted advice that improves lives. Visit segalco.com

Segal