EVALUATING CYBERSECURITY VULNERABILITIES

by | **Paul Catenacci**

As the persistence of cyber threats grows, organizations and their employee benefit plans are attractive targets. The author discusses proactive measures that plan sponsors and trustees can implement to support an effective cybersecurity program.

plans & trusts

education | research | information

Whether you've experienced the ill effects of a cyberthreat or been required to participate in training sessions, you have had to contemplate cybersecurity. For those of us who grew up when the internet was in its infancy, there might be a yearning for simpler times, when things like passwords were more of a nuisance rather than a core security practice.

Unfortunately, the simpler times are not returning. No matter how much we might want to, cybersecurity is a risk that we cannot ignore and must take proactive measures to address. While there is no silver bullet to vanquish a problem that neither knows nor respects borders, benefit plan sponsors and trustees can use several widely available cybersecurity models to create a cybersecurity monitoring program and to harden against cyberattacks. In addition, while developing and implementing a robust cybersecurity program benefits from the help of IT experts, even small benefit plans that cannot afford dedicated full-time IT staff can still use publicly available tools to set up a good program. This article will discuss at a high level some primary considerations for plans and trusts when implementing a cybersecurity program.

Step 1—Identifying What Your Plan Needs to Protect

Plan sponsors and trustees should evaluate the employee benefit plan's cyber vulnerabilities by assessing the data of interest to bad actors and determining its location. The operation of plans and trusts results in the generation of a great deal of data. The majority of plans rely on third-party administrators (TPAs) for plan administration. In such cases, the TPA represents the hub of the wheel with the various services providers (such as actuaries, accountants, lawyers, etc.) representing the spokes. Sensitive data is exchanged among all these entities, but the TPA serves as the custodian of the plan's records. Even in the less common instances where a plan is internally administered by employees of a fund or the plan sponsor, the central role and recordkeeping function of that office remains the same. Therefore, the TPA serves as an excellent starting point for identifying the data your plan possesses along with its destinations and storage methods as well as the entities with whom it is shared.

To kickstart the assessment of the plan's vulnerabilities, embark on an exercise to catalog the types of data your plan generates, identify its recipients, understand the methods and locations of data receipt and storage, and determine the entities with whom it is shared. If this information isn't readily available, start to obtain it by simply asking for it. Consider beginning a review of provider agreements and ask each vendor to identify the data it receives and how it is stored (e.g., the cloud, internal servers). Within your organization's office, if your plan is self-administered, identify where data is stored and how it is accessed (think laptops, mobile devices, servers and the cloud). Once plan sponsors have obtained the necessary information, create a chart or other tracking system that commits these results to a record you can maintain, monitor and update over time. This first step is one building block of a comprehensive program that aids your plan in identifying and assessing its cyber vulnerabilities.

Takeaways

- Plan sponsors should assess the data generated by their benefit plans and understand its location, recipients and methods of storage.
- A comprehensive review of provider agreements and internal data storage practices is recommended to identify vulnerabilities.
- Choosing a standard that aligns with the plan's needs and incorporating it into policy statements or by-laws forms the foundation for a cybersecurity monitoring program.
- Organizations should undergo a comprehensive review and consider software, hardware and insurance polices dedicated to cyberattacks.

Step 2—Setting a Standard

Once you have a handle on what information your benefit plan generates, who has it, and how it is being used and stored, you can start to work on assessing vulnerabilities against a standard set of security requirements and best practices. The Department of Labor (DOL) published a list of cybersecurity best practices for employee benefit plans in the United States. These best practices are mainly modeled on the cybersecurity framework created by the National Institute of Standards and Technology (NIST).[1] While the DOL best practices apply to U.S.-based plans, the NIST model is easily adaptable to any organization and is used in many countries worldwide. Of note, the Canadian government has promulgated its version of a framework similar to the NIST framework, ITSG-33.[2] Both focus on a continuous monitoring model and adopt various security practices universally applicable to any organization.

Consider integrating one of these frameworks as a foundational level of compliance for your plan's service providers and internal operations. Memorializing the chosen standard as a policy statement or by-law can serve as the foundation for implementing an ongoing cybersecurity monitoring program. Selecting the standard that best fits your plan is the responsibility of the body charged with plan governance. The standard will apply to not only your plan but also all the organizations providing services to your plan that receive sensitive data. Even if your plan does not employ full-time IT staff, working on this endeavor with an IT expert, even if only on a project basis, would be a prudent and productive use of plan assets.

With your data cataloged, its locations identified, its users and usage determined, a standard chosen, and a policy statement or by-law formulated, you are prepared to start implementing your cybersecurity program.

Step 3—Implementing a Cybersecurity Monitoring Program

Ideally, you can easily adapt your policy statement or by-law into a survey format and send it to plan service providers to confirm they meet or exceed these standards. The policy statement or by-law can also be used as a guidepost and a compliance checklist for the internal operations of your plan that will produce a record of awareness, vigilance and due diligence with respect to recognizing and managing cybersecurity risks.

For the internal workings of your plan, the process will largely depend on the level of self-administration. If your plan employs an in-house staff, you must conduct a comprehensive review of all software and hardware being used. This includes service providers you contract with, such as cloud providers, servers and IT organizations. Speaking of IT, if you are administering your plan internally and do not have full-time IT personnel on staff, consider contracting with an organization specializing in IT to help you, even on a periodic or project basis. IT experts can go a long way in ensuring your plan's cybersecurity by reviewing the plan's operations.

Your plan should also examine its insurance policies. Even if your organization outsources the majority of its operations and associated data storage, an essential requirement is a dedicated standalone policy specifically covering damages from cyberattacks. One of the main reasons to have a policy specific to your plan is that even if your service providers are well-insured, those policies protect all their clients—not just your plan—so having a policy specific to your plan ensures it has its umbrella to deploy in the event of a breach. Determining the appropriate amount of coverage to purchase is a decision specific to each plan; insurance brokers and IT experts can assist in selecting coverage levels and ensuring the completion of the application. As the saying goes, "the devil is in the details." Insurance policies are replete with landmines prospective insured individuals may inadvertently encounter if they do not provide accurate answers. Receiving expert assistance ensures that if you ever need to utilize your insurance policy, you won't be confronted with the unwelcome surprise of your insurer challenging or denying coverage due to an innocent mistake when completing the application. Cyber insurance also frequently comes with resources to help your plan. In addition to coverage, many cybersecurity carriers provide free resources to help your plan not only improve its security but also train staff on cybersecurity best practices.

Regarding third-party service providers, building a survey these providers will complete from your adopted policy statement or by-law is a practical way to ensure the providers are adhering to a standard that is set by your plan but also based on standard industry best practices. The survey can further inquire whether the providers obtain certifications, such as ISO-27001, or undergo a Service Organization and Control (SOC) audit. These high-level protocols may not be necessary or practical for every organization. However, numerous sizable organizations (including administrators, health care providers and cloud service providers) routinely acquire them. In such cases, your plan has the option to request a copy of the findings or the audit report.

When examining your plan's service provider, inquire whether the organization has experienced any compromises previously (and if so, what remedial measures it implemented), the contingency planning in place for ensuring uninterrupted operations during emergencies (encompassing all types, not just those related to cyberattacks), and whether the organization maintains cybersecurity insurance. The level of insurance will vary depending on the service provider. Larger entities, or those that receive significant amounts of sensitive information, are apt to carry more insurance, whereas lower risk organizations will likely have less. Plans should consult their providers and insurance brokers about market norms for different organizations when determining the appropriate amount of insurance to carry, as there is no hard and fast rule in this regard.

The survey responses can then be compiled annually for review by the plan's overseeing entity, with assistance from appropriate providers, to fulfill due diligence requirements. Ask service providers with identified deficiencies to demonstrate the corrective measures. Plans may also consider updating service contracts to require that the provider comply with the plan's selected baseline level of cybersecurity standards or state that they must adhere to all plan policies in general as a condition of being a service provider. Contractual acknowledgments of this nature can also fill a gap in the absence of any direct legal requirements imposed by governments to implement specific requirements.

Enhanced evaluations can complement annual surveys and the examination of the provided documentation. Some organizations may elect to bring in external IT consultants to conduct "field" style surveys, ensuring an independent verification of the organization's security posture. Whether or not to take this step requires each plan to consider the costs and benefits of such a review. These reviews can be costly and intrusive to the organization undergoing them. In Canada, there are jurisdictional privacy laws to take into account in cases where a breach occurs. Compliance with these laws (e.g., a possible requirement to provide credit monitoring to affected individuals) can be costly to plans. There can be legitimate objections to these reviews because of the risk of compromised security protocols or unauthorized access to client data and physical facilities. In addition, one must always consider the risks that arise from risk management.

Carefully consider where completed reports might ultimately be stored, who might access them, and how they could be utilized for the benefit or detriment of your plan. This consideration remains pertinent regardless of the chosen review type, whether it be a survey or "field" style assessment. This doesn't imply that your plan should avoid surveys or other review methods; instead, it serves as a reminder that managing risks should not occur in isolation. Fiduciaries are obligated to act only when well-informed about the costs and benefits associated with the contemplated action (or inaction). This principle remains the case when addressing the management of cybersecurity risks. The implementation of a robust cybersecurity program can be costly, but a breach can be even more expensive.

Data Security and Privacy Laws and Regulations

Another key element of your cybersecurity program is ensuring that you are complying with the applicable privacy laws that apply to your jurisdiction.

When considering Canadian jurisdictional privacy laws in the event of a cybersecurity breach, it's essential to understand the legal framework and obligations that apply. Canada has both federal and provincial privacy laws that may come into play, depending on the specific circumstances of the breach. Here are some key privacy laws and considerations to keep in mind.

Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA is Canada's federal privacy law that applies to the collection, use and disclosure of personal information by private sector organizations, unless a province has its own substantially similar legislation (e.g., Alberta and British Columbia have their own privacy laws). Key considerations under PIPEDA include the following:

- Notification—Organizations are required to notify affected individuals and report significant breaches to the Privacy Commissioner of Canada.
- Record-keeping—Organizations must maintain records of all data breaches, including details of the breach and remedial actions taken.

Provincial Privacy Laws

Several Canadian provinces have their own privacy legislation, such as the Personal Information Protection Act (PIPA) in Alberta and the Personal Information Protection Act (PIPA) in British Columbia. These laws have their own breach notification requirements and may differ from PIPEDA.

Data Security Standards

You should comply with industry-specific data security standards and best practices, such as the Payment Card Industry Data Security Standard (PCI DSS) for credit card data or the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

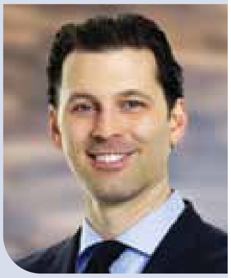
Other Considerations for Plans

These additional considerations can be categorized into the following general areas. Plans should be aware of best practices in the following domains.

- **Cybersecurity Incident Response Plan**—Develop and maintain a cybersecurity incident response plan that outlines the steps to be taken in the event of a breach. This plan should include procedures for assessing, containing and mitigating the breach as well as notifying affected parties.
- **Breach Notification**—Understand the specific breach notification requirements under both federal and provincial laws. Typically, organizations are required to notify affected individuals, relevant authorities and, in some cases, third-party organizations or credit reporting agencies.
- **Record-Keeping and Reporting**—Maintain detailed records of the breach, including the nature and scope of the incident, the data affected and the steps taken to address it. Reporting requirements may differ between federal and provincial laws.
- **Penalties and Liabilities**—Be aware of potential penalties and liabilities for noncompliance with privacy laws. Fines and legal actions can result from failing to meet breach notification requirements or adequately protect personal information.
- **Legal Counsel and Cybersecurity Experts**—Consult legal counsel with expertise in privacy and cybersecurity to ensure compliance with applicable laws and regulations. Engage cybersecurity experts to assess and strengthen your organization's security measures.
- **Public Relations and Reputation Management**—Develop a communication strategy to manage public relations and protect your organization's reputation in the aftermath of a breach.
- **Training and Awareness**—Ensure that your employees are trained on cybersecurity best practices and know how to recognize and report security incidents promptly.

It's important to note that privacy laws and regulations can change over time, so it's essential to stay up to date with the latest developments and seek legal advice to address specific breach incidents effectively and in compliance with the law.

BIO



Paul Catenacci is a senior partner at Novara Tesija Catenacci McDonald & Baas PLLC, where he leads the firm's employee benefits practice group. He focuses his practice on all areas of employee benefits law and the operation of fringe benefit plans under the Employee Retirement Income Security Act (ERISA) and the Internal Revenue Code (IRC). Catenacci's experience includes not only working with defined benefit and welfare plans, but also other benefit plans common to the multi-employer industry, such as defined contribution and 401(k) plans, apprenticeship and training trusts, supplemental unemployment plans and vacation funds. Prior to joining the firm, he was employed in a national security–related position where he held a top-secret/SCI-level security clearance.

Final Thoughts

There are diverse opinions on the optimal way to establish a robust cybersecurity program, but everyone concurs that disregarding this risk is perilous. Although it may appear daunting, adopting a methodical, step-by-step approach and leveraging an established model for cyber risk management eliminates the need to start from scratch.

In addition, lean on professionals, particularly if you outsource the building and implementation of your cybersecurity program. Ensure that the service contract contains a set of agreed-upon procedures, especially for any "field" surveys or reviews of provider survey responses that will result in an opinion or report with associated scoring. You want to know in advance not only what your plan is getting from the report but also what your plan is not getting. Consulting agreements frequently impose extensive restrictions on the provider's liability for the delivery. Opinions that your benefits plan may rely on, even seemingly trustworthy, can have enough limitations to render them practically worthless. Legal counsel will play a key role in clarifying what the third-party provider is expected to deliver, how delivery will occur and the permissible actions with the results as outlined in the contract. Dedicating time to the contracting process will also help avoid cost overruns and keep the process within the control of the contracted plan.

Finally, don't be surprised and don't despair if your labour produces some sour fruit. No one is perfect, and no organization is impervious to cyberattacks. If vulnerabilities are uncovered, create a plan to correct them, prioritize the highest risks first and then learn from the experience. In the realm of cybersecurity, you often discover that the most straightforward solutions yield the most substantial impact. Hardening your plan against cyberattacks is not a one-time process but an ever-evolving one that requires constant vigilance and attention. Most importantly, it requires a collaborative effort undertaken by everyone who works with and for your plan.

Endnotes:

1. https://www.nist.gov/cyberframework.
2. https://www.cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33.