

Your Plan Will Face a Cyberattack. Here's How to Prepare.

While hacking is nothing new, the pace of large-scale cyberattacks has accelerated significantly in recent years, most notably the Equifax hack, which exposed the private information of a majority of Americans. More worrisome for many plan sponsors, the focus of cyberattacks in the defined contribution (DC) world has shifted from hardened targets like recordkeepers and custodians to plan sponsors, which often lack the extensive cybersecurity defenses of their vendors.

One of the most difficult challenges for plan sponsors is determining where to start in their efforts to defend against increasingly sophisticated cyberattacks. This article is designed to assist plan sponsors with formulating and executing their strategy to protect their information and their assets.

Putting the Pieces Together

To assemble the pieces of the cybersecurity puzzle, plan sponsors need to understand the scope and scale of the cybersecurity threat. Sponsors and DC plan vendors administer large asset pools and retain personally identifiable information for participants and beneficiaries, such as names, addresses, birthdates, bank account information, and Social Security numbers, which creates risk for all these parties. Plan sponsors

should seek to address cybersecurity at an organizational level and with the third parties that receive personal data (e.g., recordkeeper, trustee, investment advice provider).

Cybersecurity refers to techniques designed to protect the integrity of data, software, and networks from unauthorized access or damage. Cyberthreats can take many forms and involve a wide variety of malicious actors (**Exhibit 1**). And the cyber threat landscape continues to evolve, driven in part by the ever-changing security requirements that accompany developing technologies. These include the trend of employees using their personal gadgets at work (known as BYOD or “bring your own device”), and the rise in connected devices—like Amazon’s Echo speakers—commonly referred to as the “Internet of Things” (IoT). In addition, the increased adoption of cloud-based applications and data storage extends the need for cybersecurity protections beyond the traditional data center.

Cyber-risk is more than a technology concern; it is a people issue as well. For example, the 2017 WannaCry attack affected more than 230,000 computers—and it was facilitated by employees clicking infected emails, an insidious hacking technique known as “phishing.”

Regulations and Cybersecurity

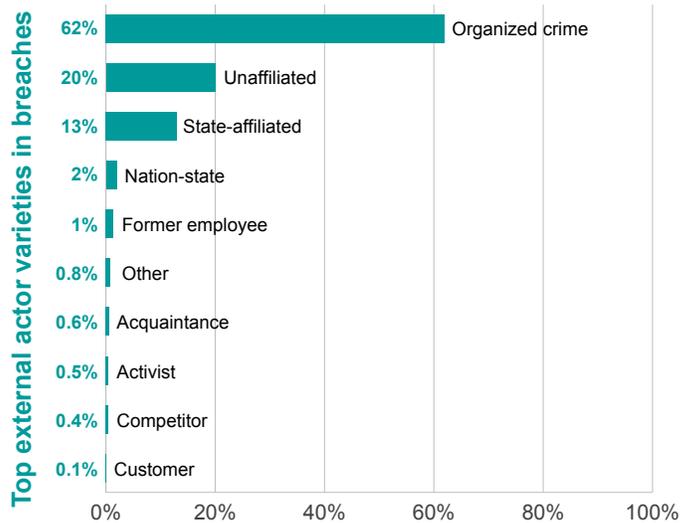
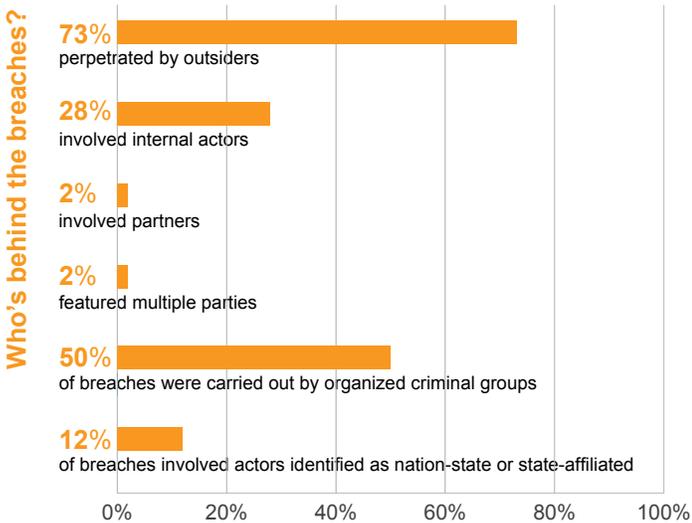
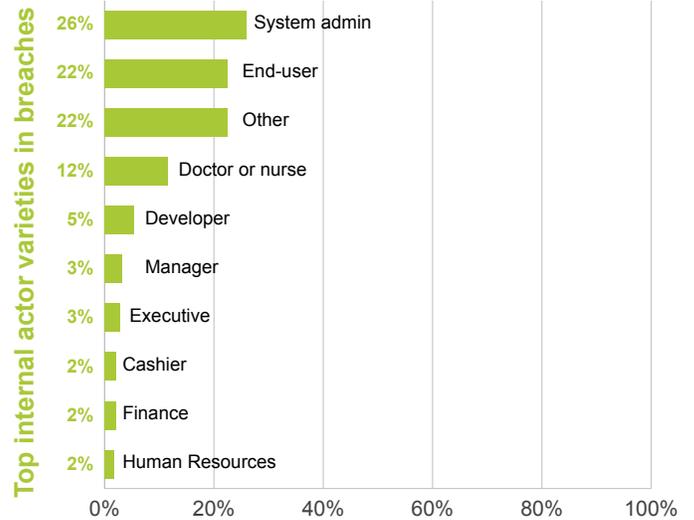
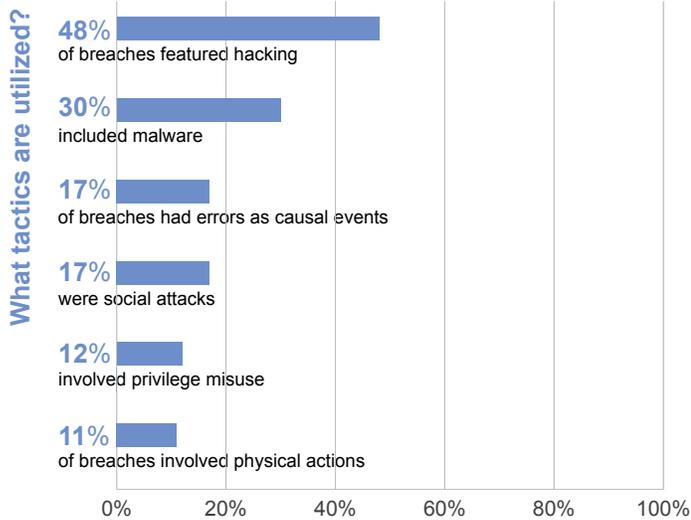
Fiduciary Obligations

- The selection and monitoring of service providers is a fiduciary act
- The decision makers must act prudently and solely in the interest of the plan participants and beneficiaries
- Plan fiduciaries are liable for failing to prudently select and monitor service providers
- This may include prudence in selecting and monitoring service providers to ensure they maintain adequate cybersecurity practices and protocols

ERISA and electronic distribution of plan information

- If plan notices are disseminated electronically, the plan sponsor (and not the service provider) is required to protect the confidentiality of personal data
- Similarly, plan sponsors are required to take measures to ensure websites with plan information are secured to protect the confidentiality of personal information

Exhibit 1: The Cybersecurity Threat Matrix



Source: Verizon 2018 Data Breach Investigations Report. Multiple responses were allowed.

One of the key challenges for plan sponsors is that there is no central governing law or self-regulatory organization over cybersecurity in retirement plans, as there is with group health plans (e.g., the Health Insurance Portability and Accountability Act, or HIPAA). However, plan sponsors are subject to the best interest clauses of ERISA, as well as the data privacy requirements for electronic notices. In contrast to the limited federal guidance, several states impose a duty on employers to protect the privacy of employees' Social Security numbers and/or notify employees promptly of any security breaches. Since these laws regulate the employer, rather than the plan sponsor, they likely would not be preempted by ERISA. And finally, the personal data of U.S. citizens working overseas or foreign citizens working in the U.S. may be subject to the data privacy laws of their country of origin or the country in which they reside (e.g., the EU-U.S. Privacy Shield requirements).

Building a Framework for the Threat

Organizations and governments typically have taken a reactive approach to cyberthreats, addressing them after an incident. This has generally meant they cobble together a series of new individual security technologies and protocols following a breach. Not only is this method expensive and complex, it is also largely ineffective.

A cybersecurity framework (CSF) provides guidance for how organizations can assess and improve their ability to prevent, detect, and respond to cyberattacks. There are a variety of frameworks that plan sponsors and recordkeeping vendors can use to manage their risk, which typically incorporate some or all of the following steps:

- **Risk Assessment:** understanding the cybersecurity risk to the organization broadly (including mission, functions, image, or reputation)
Example: Personal data held by human resources should be included in organizational threat assessments.

- **Governance:** creating policies and procedures to manage and monitor the operational, legal, and other risk components
Example: Establish a chief security officer and create a framework for reporting cyberthreats.
- **Information Protection Processes and Procedures:** developing policies that address the purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities
Example: Draft documentation detailing the notification process and timing in the event of a data security incident.
- **Awareness and Training:** plan sponsor staff and third-party partners undergo cybersecurity awareness education and are adequately trained to perform their role within the CSF
Example: Hold annual training on common cybersecurity threats and the appropriate responses.
- **Access Control:** establishing protocols for, and limits on, who can access data
Example: Limit access to employee data to only the parties with a legitimate business need.
- **Data Security:** managing plan information and participant data to protect the confidentiality, integrity, and availability of information
Example: Use VPN technology to encrypt external access to an organization's systems.
- **Protective Technology:** managing software solutions to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements
Example: Require virus scans on a regular basis.
- **Maintenance:** performing system upkeep consistent with policies and procedures
Example: Promptly patch software to eliminate identified security weaknesses.

Navigating the ‘Certification Alphabet’

Various bodies have attempted to create consistent CSFs that organizations can use to manage risk. The myriad of CSF structures seek to solve different problems, and it is important for plan sponsors to understand the various benefits and limitations of each structure:

	Detailed Description of Purpose	Shorthand	Certification
ISO 9001	Specifies requirements for demonstrating an effective quality-management system that meets customer and regulatory requirements	Monitors quality management	Yes – ISO 9001:2015 The previous version, ISO 9001:2008, will expire Sept. 14, 2018
ISO 27001	Establishes standards for implementing and maintaining an effective information-security management system	Rules for cyberdefenses	Yes – ISO 27001:2013 The previous version, ISO 27001:2005, is no longer in use
ISO 27002	Provides supporting documents to ISO 27001, giving guidance and advice on implementation	Guidance for a cybersecurity plan	No – a company cannot be certified as ISO 27002-compliant; it is only a guidance document.
NIST CSF	Sets basic guidelines to identify, implement, and improve cybersecurity practices, and to create a common language to communicate those practices; its brevity makes it incompatible with common compliance requirements, such as HIPAA	Simplified standardized guidelines for cybersecurity	No
ISACA COBIT	Establishes high-level information technology (IT) management and IT governance, focusing on improving the overall business orientation through IT controls and metrics. COBIT also provides a set of recommended best practices for the governance and the control process of information systems and technology with the aim of aligning IT with the business.	Focuses on cybersecurity philosophies and management at an organizational level	No
HITRUST CSF	Establishes controls for health care organizations that follow a risk-based approach, offering multiple levels of implementation requirements determined by specific risk thresholds. It includes, harmonizes, and cross-references globally recognized standards, regulations, and business requirements, including ISO, NIST, PCI, HIPAA, and state laws.	Provides a prescriptive framework for the more stringent security requirements of the health care industry	Yes

The Framework Is Just the Start

There is no enforcement agency or mechanism to ensure ongoing CSF adherence. An organization may self-report compliance with any of the CSFs described above. However, that does not mean its CSF has been reviewed and certified by an independent auditor. Additionally, plan sponsors should be aware of what processes are included in the scope of the audit and to what extent these are assessed to confirm the process has been implemented and is operating effectively, because management determines the scope of the audit for certification purposes and may limit it to, for example, a single business unit or location. The certifications do not necessarily mean the remainder of the organization has an adequate approach to cybersecurity. Plan sponsors should be aware that certification is not the end of the process—ensuring strong cybersecurity controls is an ongoing effort.

Hacks Happen—Plan Accordingly

Let's start by getting the unrealistic goal of "don't get compromised" out of the way. The average American's personal data has been compromised multiple times—including usernames and passwords that could be recycled across multiple applications, like a retirement portal or company intranet. In defense, plan sponsors should seek to address:

- What is their internal risk?
- Where does their data go and how is it transmitted and stored (e.g., to third parties, or maintained on a server or in the cloud)?
- Have they conducted appropriate due diligence on their vendors, and the partners that those vendors may share data with?
- How does the organization define a "breach"?
- How do their vendors define a "breach," and what triggers disclosure?
- How do they monitor their internal processes and procedures and their external partners on an ongoing basis?
- Do contracts and agreements cover indemnification, notification procedures (i.e., does the vendor have to notify

the sponsor when it discovers a breach, or only after the breach has been contained), and remediation?

- What is their process for when they experience a breach?

Getting Covered for the Threat

Cyberinsurance is a policy used to protect against risks relating to information technology infrastructure and activities. Risks of this nature are typically excluded from traditional commercial general liability policies or at least are not specifically defined. Coverage provided by cyberinsurance policies may include first-party coverage against losses such as extortion, theft, hacking, data destruction, and other attacks. The coverage may also indemnify companies for losses to others caused by errors and omissions, failure to safeguard data, or defamation. The scope of cybersecurity insurance policies varies widely and requires a careful review to ensure the policy addresses key risks. One important cybersecurity risk that often goes unexplored is protecting the private data of participants in an employee benefit plan.

Ultimately, cyberinsurance must be viewed as more than a commodity, and policy buyers should be careful to investigate both what is covered and what events trigger coverage. For example, it may seem obvious to a plan sponsor what constitutes a "breach" or an "event," but these terms are used differently by different insurers, and are terms of art. Until this market matures, it is essential to align the specific breadth of coverage—and associated contractual triggers—to the specific needs of each organization.

Conclusion

Cybersecurity is a constantly evolving, high-priority task for plan sponsors. We expect that continued evolution will need to occur in their defenses as knowledge-based authentication (e.g., mother's maiden name) weakens over time as more and more individuals' personal information is exposed to hackers and malicious actors.

Even so, every organization has the capacity to undertake some key steps to help secure their plans and participants' data. The challenge for many is deciding where to start. Understanding the scope of the cybersecurity risks and the "ecosystem" of a plan (i.e., recordkeepers, managers, and other vendors) can help frame the actions plan sponsors should take.

Callan recommends plan sponsors take these steps to address their cybersecurity vulnerabilities and prepare for an inevitable attack:

- Explore the appropriate cybersecurity framework options for your organization and make an informed choice
- Implement solutions, guidelines, and protocols for that cybersecurity framework
- Review the cyber protections in place at your vendor, and their vendors that may have access to plan participants' personally identifiable information
- Consider how data protection is covered in contracting, specifically assessing the indemnification, notification, and remedies outlined in the agreements
- Take inventory of what is covered or not covered by any cyberinsurance policy the organization has in force or is considering

Authors



Ben Taylor is a senior vice president and a defined contribution (DC) consultant in Callan's Fund Sponsor Consulting group based in the San Francisco office. Ben serves as a lead consultant to DC plans, and has a primary focus on public sector DC plans, ranging from 457(b) plans to single and multi-vendor 403(b)/401(a) and 401(k) plans. As a member of Callan's DC team, Ben also conducts specialized research for DC plans.



Jana Steele is a senior vice president and defined contribution consultant in Callan's Fund Sponsor Consulting group. Jana has more than 17 years of consulting experience on qualified and nonqualified retirement plans, including plan design, vendor management, vendor searches, fee benchmarking, data security analysis, and compliance support.

The **DC Observer** is a quarterly newsletter that offers Callan's observations and opinions on a variety of topics pertaining to the defined contribution industry. For defined contribution inquiries, please contact Jimmy Veneruso at 312.346.3536.

Editor – Stephen R. Trousdale

About Callan

Callan was founded as an employee-owned investment consulting firm in 1973. Ever since, we have empowered institutional clients with creative, customized investment solutions that are backed by proprietary research, exclusive data, and ongoing education. Today, Callan advises on more than \$2 trillion in total fund sponsor assets, which makes it among the largest independently owned investment consulting firms in the U.S. Callan uses a client-focused consulting model to serve pension and defined contribution plan sponsors, endowments, foundations, independent investment advisors, investment managers, and other asset owners. Callan has six offices throughout the U.S. For more information, please visit www.callan.com.

About the Callan Institute

The Callan Institute, established in 1980, is a source of continuing education for those in the institutional investment community. The Institute conducts conferences and workshops and provides published research, surveys and newsletters. The Institute strives to present the most timely and relevant research and education available so our clients and our associates stay abreast of important trends in the investments industry.

© 2018 Callan LLC

Certain information herein has been compiled by Callan and is based on information provided by a variety of sources believed to be reliable for which Callan has not necessarily verified the accuracy or completeness of or updated. This report is for informational purposes only and should not be construed as legal or tax advice on any matter. Any investment decision you make on the basis of this report is your sole responsibility. You should consult with legal and tax advisers before applying any of this information to your particular situation. Reference in this report to any product, service or entity should not be construed as a recommendation, approval, affiliation or endorsement of such product, service or entity by Callan. Past performance is no guarantee of future results. This report may consist of statements of opinion, which are made as of the date they are expressed and are not statements of fact. The Callan Institute (the "Institute") is, and will be, the sole owner and copyright holder of all material prepared or developed by the Institute. No party has the right to reproduce, revise, resell, disseminate externally, disseminate to subsidiaries or parents, or post on internal web sites any part of any material prepared or developed by the Institute, without the Institute's permission. Institute clients only have the right to utilize such material internally in their business.

Callan

Corporate Headquarters

600 Montgomery Street
Suite 800
San Francisco, CA 94111
800.227.3288
415.974.5060

www.callan.com

Regional Offices

Atlanta
800.522.9782

Chicago
800.999.3536

Denver
855.864.3377

New Jersey
800.274.5878

Portland
800.227.3288

 @CallanLLC

 Callan