Segal Consulting Segal Marco Advisors

public sector letter

Insights and Strategies

September 2018

DC Plan Cybersecurity

Protecting Participants' Data — and the Plan — Requires a Multifaceted Strategy

Data breaches — improper disclosures of individuals' private information — are, unfortunately, increasingly common. Protecting defined contribution (DC) plan data is a high priority for sponsors — not only because participants expect it, but also because data breaches are expensive to manage and may undermine participants' confidence in the plan. The average cost of a data breach in the public sector was $110 for each lost or stolen record.[1] The potential damage to the reputation of state, county or local jurisdictions that experience a breach is more difficult to quantify.

Fortunately, there are steps DC plan sponsors can take to manage cybersecurity risk.

Potential Vulnerabilities for DC Plans

Thankfully, to date, few state and local government DC plans and recordkeepers have experienced data breaches perpetrated by cybercriminals. Nevertheless DC plan sponsors should be increasingly vigilant, because the personally identifiable information (PII)[2] they safeguard is a tempting target.

For DC plans, business process failures are a more likely source of data breaches. Such failures can occur when plan sponsors exchange PII with the DC plan recordkeeper(s) and other DC plan service providers. Each transmission of data between the DC plan sponsor and recordkeeper(s) or service providers creates risk.

[1] Source: *2017 Cost of Data Breach Study: United States*. IBM Security and Ponemon Institute (2017): 4. The majority of data-breach incidents studied in this report happened in 2015. The average per capita cost of a U.S. data breach in all industries was $225. (The Ponemon Institute is a research organization that focuses on privacy, data protection and information security.)

[2] PII includes Social Security numbers, birthdates, addresses (home and email), compensation information, DC account balances and bank account information.

In fact, while just over half of data breaches (52 percent) are the result of malicious or criminal attacks by hackers, the other 48 percent are related to negligence and system failures.[3] Data breaches associated with negligence may involve information included in misdirected emails, mishandled paper records or on lost devices, such as laptops, smartphones or removable drives. Breaches related to system failures may result from information technology risk events, such as computer malfunctions. They may also be attributable to failed business processes, including human errors that result in the accidental distribution of personal data via a mass email, in website postings or printed material.

A Multifaceted Strategy for Managing the Risk

DC plan sponsors share responsibility for data security with recordkeepers and all stakeholders. For that reason, all parties should play a role in managing cybersecurity risk.

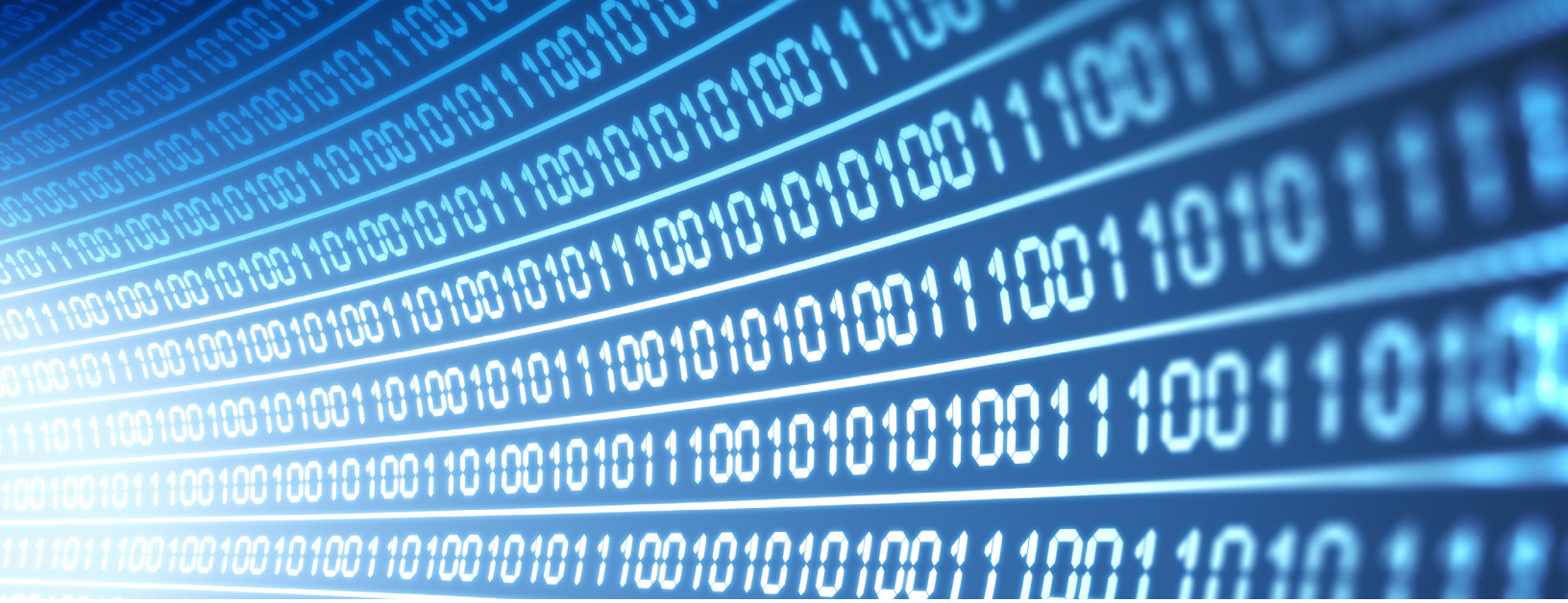
Aspects of a multifaceted strategy for managing cybersecurity risk include the following:

- **Create an Information Security Policy and an Incident-Response Plan (or Update Existing Ones)** — The information security policy should address what information is covered, how it is stored (electronically or on paper) and whether it is stored internally or externally. It should also describe how to protect that sensitive information. The incident-response plan should outline steps to be taken in the event of a breach as well as each party's roles and responsibilities. In addition, the incident-response plan should include steps to document breach events, resolutions and outcomes.

- **Minimize Requests for and Use of PII** — Consider how much PII must be collected in plan enrollment forms or included on participants' printed account statements. Social Security numbers, in particular, are a target for cybercriminals who use them for identity theft.

- **Train Staff Regularly** — All employees, particularly those that handle PII, should be trained on how to protect data and systems. That training should cover applicable laws and regulations and other requirements. It is also important to educate staff about procedures designed to avoid breaches associated with negligence and system failure

[3] Source: *2017 Cost of Data Breach Study: United States*. IBM Security and Ponemon Institute (2017): 4.



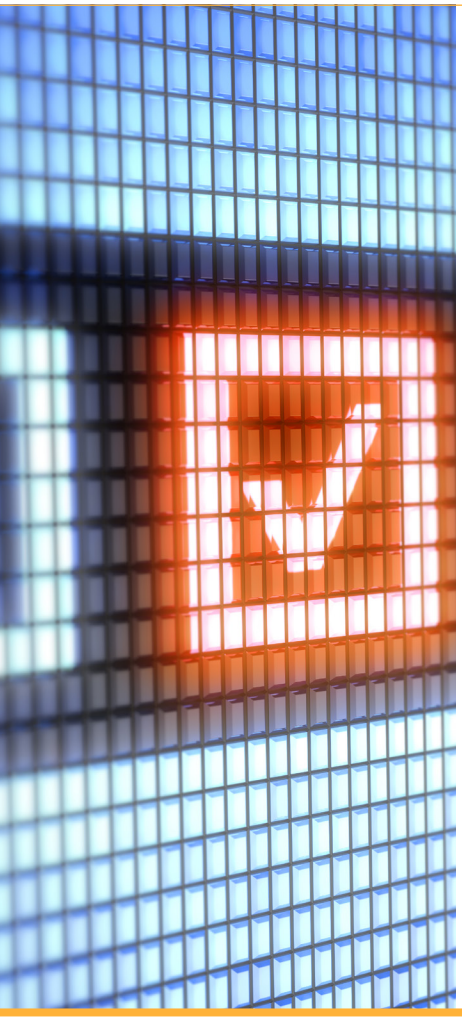
related to human errors. For example, if the passwords of HR staff, the recordkeeper's staff or plan participants are easy to guess because they are insufficiently complex, they can be a point of entry for cybercriminals. At a minimum, giving staff and participants guidelines for creating strong passwords, as well as tips for remembering them, is helpful.

- **Assess the IT Environment** — Data loss can also occur because of outdated technology. The existing IT environment, including infrastructure, networks, hardware, software, security and IT support services should be evaluated periodically. While many state and local governments use older technology for payroll and HR administration, much of it highly customized, and while it is prudent to regularly evaluate these applications to determine if they need to be updated or replaced, it is essential that the assessment takes a longer view. In addition to software applications, an assessment of the IT environment should include, but not be limited to, hardware components (*i.e.*, workstations, laptops and removable media), operating systems, virtual components, backup methodologies, email transmissions, remote connections, portals, patching policies, malicious software protection and cloud-hosted services.

- **Mandate Use of Encryption for Data-at-Rest and Data-in-Motion** — The expanding use of portable technology (*e.g.*, laptops, flash drives, removable or external drives and mobile devices) to store plan data introduces new data risks. These devices are frequently lost or misplaced and potentially contain thousands of records. Consequently, encryption should be required for all portable devices to make any information on them unusable, unreadable or indecipherable to unauthorized individuals. Encryption should also be applied to plan data exchanged with other entities, such as email transmissions or accessing plan data through remote connections.

- **Assess Recordkeepers' Technology** — DC plan sponsors delegate significant responsibility for management of data security risks to their recordkeepers. DC plans depend on their recordkeepers to protect their DC plan data by using the latest technology, including hardware and software. For example, the latest fingerprint-identification technology can replace passwords. Ask for copies of recordkeepers' latest security assessments and actions taken to mitigate any deficiencies.

- **Review Recordkeepers' Security Procedures** — Sponsors should ask their DC plan recordkeepers if they follow the Association of International Certified Professional Accountants' System and Organization Controls for Cybersecurity, which is one measure of a recordkeeper's commitment to protecting participants' PII.[4] DC plan sponsors should request copies of all assessments and also ask recordkeepers if they plan to follow the SPARK Institute's newly created Cyber Security process, which is described in the text box below. Lastly, of course, many states have regulations regarding personal data security, and plan sponsors should expect their recordkeepers to meet any standards that apply to them.
- **Set Up and Regularly Review System Activity Logs** — System activity logs, which are generated in order to identify suspicious activity, can be one of the first lines of defense against cybercriminals provided they are properly used. Many organizations forget to establish a process to review the logs and follow up on any suspicious activity. Activity logs are only beneficial if they are acted on and are regularly reviewed.



Common Criteria Certification: The SPARK Institute's Bright Idea

The SPARK Institute established an Industry Data Security Oversight Board to create and oversee the uniform data-management standards for the DC plan marketplace. The results were Common Criteria Certification guidelines to ensure service providers offer a baseline level of security. These guidelines consist of 16 identified critical data security areas of focus:

1. Risk Assessment and Treatment
2. Security Policy
3. Organizational Security
4. Asset Management
5. Human Resource Security
6. Physical and Environmental Security
7. Communications and Operations Management
8. Access Control
9. Information Systems Acquisition Development
10. Incident and Event Communications Management
11. Business Resiliency
12. Compliance
13. Mobile
14. Encryption
15. Supplier Risk
16. Cloud Security

SPARK's Common Certification Criteria's guidelines can be used to evaluate the security of technology and systems. These guidelines also apply to a service provider's subcontractors that handle confidential data.

Source: Industry Best Practice Data Security Reporting, The SPARK Institute, Inc. (September 20, 2017): 5-7.

[4] Information about the System and Organization Controls for Cybersecurity is available on the AICPA's website.

First-Party Breach Costs Typically Covered by Cyber Liability Insurance

Cyber liability insurance generally covers these first-party breach costs:

- Legally required notification expenses,* including mailings to inform participants of the breach;
- Free credit monitoring for each plan participant affected;
- Identity-protection services;
- Forensic investigative costs to identify what information was taken, to determine what network damages occurred, how to respond to restore data and attempt to prevent future similar breaches from occurring;
- Services by attorneys who specialize in privacy compliance; and
- Communication and public relations services that may include call centers to help manage the deluge of calls that tends to follow breach notification.

* All states have laws requiring private or governmental entities to notify individuals of security breaches involving PII. Many of these laws have standards of enforcement and compliance, including, but not limited to, new or increased fines and penalties, stringent self-audit requirements and new authority for state attorneys general to pursue civil actions on behalf of state residents who are adversely affected by these violations. To avoid fines and penalties due to a breach event, various legal requirements must be met. The National Conference of State Legislatures has a webpage that links to security breach notification laws.

Source: Segal Select Insurance Services, Inc., 2018

- **Maintain Adequate Levels of Cyber Liability Protection** — Cyber liability insurance is designed specifically to help protect against the financial consequences of improper disclosure of plan participants' private information. It can help mitigate the damages associated with a data breach, including administrative, technological and legal costs. Such policies are intended to cover an entity's first-party breach costs[5] (listed in the text box above), as well as to provide protection from third-party liabilities that might result from a breach event.[6] Some policies include limited regulatory proceeding coverage (coverage for lawsuits or investigations by federal, state or municipal regulators in relation to privacy laws) and extend the policy to cover certain fines and penalties that may also be assessed. Cyber liability insurance policies can also respond to cyber extortion threats, if that additional coverage is purchased. The policy provides access to a variety of pre-breach and post-breach services and industry experts to assist clients in navigating data incidents.

Although public sector plans are not subject to Employee Retirement Income Security Act (ERISA), when setting a strategy for managing the operational risk associated with cybersecurity, state and local governments may find it helpful to review a 2017 report on cybersecurity created by the 2016 ERISA Advisory Council for the Department of Labor. That report, Cybersecurity Considerations for Benefit Plans, includes this resource for plan sponsors as an appendix: "Employee Benefit Plans: Considerations for Managing Cybersecurity Risks."

By adhering to the multifaceted strategy described above, plan sponsors can manage cybersecurity risk.

[5] First-party breach costs are the costs associated with recovering from a data breach.

[6] Third-party liabilities are those claimed by individuals who allege that they have been harmed by the breach (for example, a participant who, through identity theft, might seek financial redress).

The ROI of Being Prepared to Protect Participants' Data

The risk of inadvertent disclosure of personal information is real — and so are the potential savings associated with your data-protection efforts. According to the Ponemon Institute:[7]

> Having an incident response plan and team in place, extensive use of encryption, employee training, BCM [Business Continuity Management] involvement and extensive use of data loss prevention technologies all reduce the cost of data breach by more than $9 per compromised record. [That is a reduction of nearly 9 percent of the average cost of a data breach in the public sector.]

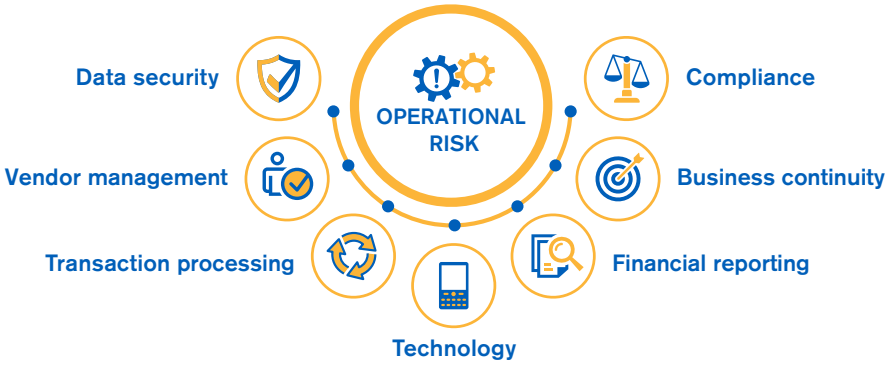
Not only will being prepared reduce the cost of the breach, it will enable you to:

- Address and resolve the breach;
- Respond swiftly to participant and/or press inquiries; and
- Help minimize the negative perceptions of the breach.

The bottom line is: Investing in managing the risks associated with DC plan data security pays off in multiple ways.

Managing Operational Risk — The Big Picture

This *Public Sector Letter* is the third in a series on managing operational risk in DC plans. Operational risk is the risk of direct or indirect loss resulting from external events or inadequate or failed internal processes, people and systems. For DC plans, operational risk encompasses potential losses attributable to failures across a range of functions, as illustrated below.

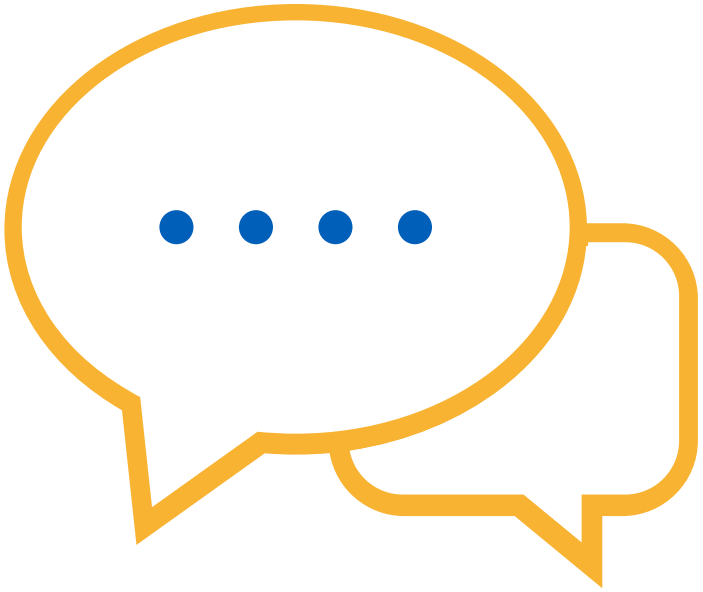


Risks associated with cyber threats, also known as data security risks, are a type of operational risk. Plan sponsors can manage data security risk through the steps and tools outlined in this publication.

Source: Segal Consulting, 2018

[7] Source: *2017 Cost of Data Breach Study: United States*. IBM Security and Ponemon Institute (2017): 11.

Questions? Contact Us.



For more information about managing operational risk or other risks DC plans face, contact your Segal benefits consultant and your Segal Marco Advisors investment consultant or the following experts:

Wendy Carter
202.833.6422
wcarter@segalco.com

Julian Regan
617.298.0967
jregan@segalmarco.com

Amy Timmons
303.601.8548
atimmons@segalco.com

Segal's consulting services for state and local governments that sponsor DC plans include the following:

- Plan design,
- Plan assessment studies,
- Participant communications,
- Compliance consulting,
- Vendor searches for recordkeepers and other service providers, and
- Administration and technology consulting.

Segal Marco Advisors, the SEC-registered member of The Segal Group, provides the following investment solutions for DC plan sponsors:

- Fiduciary oversight and training,
- Creation and ongoing review of investment policy statements,
- Ongoing monitoring and performance analysis,
- Investment menu design and evaluation,
- Selection of best-in-class investment managers, custodians and options,
- Oversight and monitoring of recordkeepers, and
- Benchmarking services (including fees and administrative services).

Segal Select Insurance Services, Inc., the member of The Segal Group that provides brokerage services for a wide range of insurance coverage, can help plan sponsors obtain cyber liability insurance, crime insurance and fiduciary liability insurance.

To receive future public sector publications, join The Segal Group's email list.

Segal Consulting Segal Marco Advisors

Our Services for the Public Sector

Public sector entities face tough decisions. We understand those challenges as well as options for meeting them. Having worked with hundreds of public sector clients for more than 50 years, Segal Consulting has insight into the spectrum of design characteristics and features of all types of compensation and benefit plans throughout all levels of government. We provide the following services:

- Health and welfare plan consulting for active and retiree coverage, including pharmacy benefit management;
- Defined benefit and defined contribution retirement plan consulting, including plan design and modeling;
- Compliance consulting;
- Benchmarking and design of total rewards that encompass financial and non-financial rewards;
- Participant communications, including personalized statements; and
- Administration and technology consulting.

Segal Select Insurance Services, Inc. provides brokerage services for a wide range of insurance coverage, including cyber liability insurance and fiduciary liability insurance.

Segal Marco Advisors provides investment solutions.

Follow Segal Consulting: Follow Segal Marco Advisors: