BENEFIT PLANS AND CYBERSECURITY THREATS:

Controls Outweigh Technology

by | **Hormazd Dalal**

While technology is an important part of guarding employee benefit plans against cyberthreats, limiting access to information and having security protocols in place are key to protecting plan data.

The risk of cyberattack strikes fear into organizations around the world, with hackings of large public companies, large hospital systems, national elections, political entities and individuals continually making headlines. The apprehension of these organizations is justified. In fact, IBM found in a recent study that the global average cost of a data breach is nearly $4 million[1]—Its chief executive officer once was quoted saying, "Cybercrime is the greatest threat to every company in the world."[2]

Safeguarding private information, products and protocols has always been a priority for organizations. This is especially true in regard to protecting benefit plan information, since it includes an abundance of sensitive data such as Social Security numbers, addresses, financial information and more.

For decades, operations and security were viewed as separate business components. However, the prevalence of these cyberattacks, coupled with the realization that no entity is immune from a cyberbreach, means that chief operating officers and other high-level professionals no longer can keep the two separate.

Many plan sponsors and third-party administrators (TPAs) have long believed the key to mitigating cybersecurity risks was to invest in technology such as firewalls. In reality, this is only a piece of the puzzle when it comes to data protection. Controlling access to this information and putting protocols into place are far more important than technology alone.

Cybercriminals Look for Open Windows

Unfortunately, it is next to impossible to ensure complete security of data if trained hackers set their minds to infiltrating a system. Even our own intelligence agencies, including the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA), have fallen prey to infiltration. The good news for the majority of plan sponsors and administrators is that few will ever face a targeted, malicious attack. Most cybercrimes equate to casual theft, meaning they are crimes of opportunity—A victim has left a door unlocked or a window open, allowing thieves to come on in and take what they want.[3]

This is known as *phishing*—Cybercriminals cast a broad net looking for easy access to sensitive information that they can use for their own agenda, either to sell, exploit or use as leverage to extort money for its safe return.

The upside here is that with the right protections and protocols in place, plan sponsors and TPAs can lock the doors and ensure only the parties who should have access to the data have the keys.

Laws and Regulations Struggle to Keep Up With Technology

Legal protections have long been in place to regulate benefit plans and the sensitive data they contain. However, laws governing Internet transactions do not keep up with the changing pace of technology.

For example, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 was the first law to tackle the shielding of portable protected health information (PHI). It could not have anticipated how much business would be conducted online and the extent to which criminals would attempt to exploit those online operations.

The topic of cybersecurity may seem daunting, but protecting against cyberthreats goes hand in glove with the controls, policies and procedures benefit plan administrators are already familiar with.

Audits and Controls for Third-Party Service Providers

One way companies can protect sensitive data such as benefits-related information is by using third-party service providers that have undergone audits evaluating the effectiveness of their controls and procedures.

The American Institute of Certified Public Accountants (AICPA) has created standardized reports and guidelines to help third parties involved in the management of money to ensure their controls thwart fraud and protect sensitive data—preventing everything from embezzlement to breaches.

learn more

Education

Fraud Prevention Institute for Employee Benefit Plans
July 16-17, Boston, Massachusetts
Visit *www.ifebp.org/fraudprevention* for more details.
Managing Cybersecurity Risks in Benefit Plan Administration
Visit *www.ifebp.org/webcasts* for more information.

Service providers such as TPAs with years of experience managing funds can hire an unbiased accountant certified through AICPA to audit their systems and controls. The auditor measures the effectiveness of current operations, informs the company of any voids or shortcomings and offers solutions to remedy the situation.

This includes evaluating controls related to the management of funds (e.g., the person responsible for bookkeeping must not be the same individual who issues checks) to those affecting cybersecurity (e.g., only those who need access to sensitive data such as Social Security numbers to perform their job duties can access this information on the company's server).

Statement on Standards for Attestation Engagements (SSAE) 18 is the most current standard used by service organizations. This replaced the SSAE 16 and its predecessor, the long-used Statement on Auditing Standards (SAS) 70.

Ultimately, when service organizations can prove to an auditor they have met or exceeded all defined standards, they receive an official certification as evidence. In accordance with SSAE 18 standards, service organizations must comply with System and Organization Controls (SOC) 2 reports and examinations. An organization becomes SOC-certified upon completing the examination.

The initial audit, report and examination can take more than three years to complete and cost north of $50,000. This is why the program is only intended for companies managing a certain level of funds and that have had controls in place for multiple years. It is important that service organizations do not to view the SOC certification program as a one-time need; rather, they should hire a certified CPA to conduct the audits and exam annually.

As a result of completing the reports and certification, service organizations can provide their clients with proof they are abiding by best practices and fulfilling their duties, both from an ethical and fiduciary standpoint. Benefit plans can view the need for such reports much like the need for CEOs of publicly traded companies to report their financials and business practices to shareholders.

Beyond SOC: Everyone Plays a Role in Thwarting Cyberattacks

The importance of having proper protocols and procedures in place cannot be stressed enough. Imagine someone invested a significant amount of time and money into purchasing a new safe but somehow allowed the keys to get into the hands of unauthorized personnel, providing unfettered, front-door access that circumvented the protections that were just installed. When it comes to cybersecurity, technology alone will not protect a plan—Protocols are crucial.

takeaways

- Investing in technology such as firewalls is just one part of a cybersecurity strategy. Data protection protocols and controlling access to information also are important.
- One strategy for ensuring data security is to use third-party service providers that have undergone audits of their systems and controls.
- Benefit plans can use the same standards as a guide to evaluate their own data security policies and procedures.
- Procedures to evaluate include remote connectivity, identity management, disaster recovery and notification.
- Taft-Hartley plans are no more at risk of a data breach than other types of benefit plans; however, more entities have a hand in benefits matters compared with single employer plans. Trustees should make sure that access to sensitive data is restricted.

While the SOC program is a good way to spot and respond to cybersecurity risks, it is intended only for established service organizations. However, any organization can use the SOC program as a guide. Putting simple day-to-day policies and protocols in place can effectively shield benefit plan data from the reach of cybercriminals.

The following is a look at the areas that benefit plans should examine when evaluating security risks, along with the steps to follow in each area. Each of these steps is tested for in the SOC examination process.

Organization

- Ensure employees, contractors, temporary staff and third-party service providers are subject to data confidentiality agreements.
- Have appropriate cybersecurity insurance coverage and keep copies of the policy readily available.

Personnel

- Provide information technology (IT) administrators with new-hire documentation, the hardware and soft-

ware requirements of those employees and what security level they will be assigned.
- Allow personnel access only to information that is pertinent to their work. Everyone should be denied access until explicitly permitted into specific areas of activity.
- Conduct exit interviews when employees leave, and recover company property, laptops, cellphones and all other means of connection/access to company information.

Network

- Install a security appliance such as a firewall, ensuring it is configured to deny all services unless explicitly permitted.
- Update this security technology regularly—Maintaining an active subscription with the firewall manufacturer is important.

Remote Connectivity

- Restrict remote access to network resources unless explicitly permitted. This means that instead of allowing employees to access the network remotely unless specifically prohibited, organizations should have a control automatically prohibiting access unless an individual is added to a list of specifically authorized users. The rule should apply to any employee or contractor working off site, whether on a company laptop or personal device.
- IT administrators must be able to revoke those permissions immediately.
  —Remote connections should disconnect after a specified time-out period.

Data Security and Backup

- Store company data on redundant hard drives and in permission-restricted file structures.
- Perform backups regularly, and periodically restore them to check for integrity.
- Regularly move/upload backups to an off-site location.
- Encrypt all sensitive account information when transmitted outside of the organization.

System Security

- Ensure all servers and desktop systems are running on supported operating systems to avoid issues with updates and security patches
- Maintain active subscriptions to antivirus software.
- Guarantee that companywide e-mail is filtered for viruses, spam, malware and other threats.
- If there are file transfer protocol (FTP) transactions, the plan must maintain a mechanism to monitor inbound and outbound file transfers for threats.

Identity Management

- Take active steps to prudently manage user accounts and passwords—Ideally, there will be a central directory for user authentication and permission assignments.
- Ensure passwords are unique to each log-in identification/employee, are sufficiently complex, expire frequently and are prohibited from being reused in a set time period.
- Have safeguards in place to lock accounts after a number of failed attempts, and log users out after a certain amount of time has elapsed.
- Implement a process for elevating user permissions when more access is needed.
- Train personnel on how to spot a potential phishing scam, what to do in the event of suspect activity and whom to notify.

Disaster Recovery and Physical Management

- Maintain a formal disaster recovery plan.
- Significantly restrict physical access to servers and networking equipment.
- If feasible, introduce closed-circuit television cameras and other detection devices—Their presence alone will often act as an effective deterrent for mischief.

Notification

- Put a plan in place to notify designated contacts in the event of a breach—This is vital. The notification process should include the circumstance and severity of the breach, as well as what efforts have been made to correct/mitigate the damage. (When formulating the plan, start by reviewing the breach notification guidelines provided in HIPAA protocols.)

Cybersecurity Considerations for Taft-Hartley Plans

While trustees of Taft-Hartley benefit plans often are responsible for considerable amounts of data, these plans are at

no more risk of breach than any other plan sponsor. The same cybersecurity strategies above apply to them.

Unions, like any large private employer, are responsible for holding a significant amount of information about members, which increases the importance of having top-notch cybersecurity measures in place. It is critical they look after controls, implement password protections and encrypt data.

The primary difference between multiemployer plans and plans sponsored by a single employer is the number of people involved in benefits-related processes. Due to the nature of Taft-Hartley plans and collective bargaining, there are significantly more entities with a hand in benefits matters when it comes to these plans—This includes employers/management trustees, union trustees, attorneys, actuaries, benefits administrators and more. For this reason, restricted access should be top of mind. Trustees should carefully consider who should and should not have access to sensitive data, such as Social Security numbers. The only parties who should have access to this information are those involved in monetary transactions—no one else. In addition, with the multiple parties handling the data, best efforts should be made to redact information that is not pertinent when sending it to another party.

The majority of parties involved in a fund do not need access to the identifying information of plan participants. The only ones who truly need this information are the employer, the TPA and the union—those with direct control over the money.

Conclusion

In addressing the topic of cyberthreats, it is important to avoid wholesale panic and have a logical application of steps in place that is within one's control. There is so much yet to understand about the threats, the rapid way in which those threats change and how to stay abreast of the developments. The steady barrage of sensational documentation regarding one high-profile security breach after another doesn't provide comfort. However, plan sponsors can thwart most cybersecurity attacks by astutely following common-sense measures, implementing known methods and preventions, and voraciously updating their security environment.

Endnotes

1. See http://fortune.com/2016/06/15/data-breach-cost-study-ibm/.
2. See www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#6c75510973f0.
3. See www.securityweek.com/cyber-threat-intelligence-shows-majority-cybercrime-not-sophisticated.

bio

Hormazd Dalal is chief financial officer at Benefit Programs Administration (BPA), a Los Angeles, California–based, technology-driven third-party administrator for Taft-Hartley and other benefit plans. Dalal holds a bachelor's degree from the University of Southern California Marshall School of Business.

benefits MAGAZINE