PROTECT YOUR MEMBERS

Data Security Best Practices for Benefits Administrators

basys
everyone benefits

Managing expectations

Fiduciary responsibility in the age of data breaches.

Ensure secure infrastructure

Basic building blocks of secure infrastructure.

Inquire about third-party security

Is your vendor SOC 2 certified?

Stay current with regulations and compliance

Failure to comply can be costly.

‹

Managing Expectations

Building Best Practices

Managing Expectations

Your Responsibility in the Age of Data Breaches

RECENT HEADLINES

Anthem Hacking Points to Security Vulnerability of Health Care Industry

— *The New York Times, February 5, 2015*

Health Insurer Anthem Didn't Encrypt Data in Theft

— *The Wall Street Journal, February 5, 2015*

Anthem Data Breach Cost Likely to Smash $100 Million Barrier: The company's cyber insurance policy is likely to be exhausted following the theft of up to 80 million records.

— *Zero Day, February 12, 2015*

Feds Warned Premera About Security Flaws Before Breach

— *The Seattle Times, March 18, 2015*

Up to 1.1 Million Customers Could be Affected in Data Breach at Insurer CareFirst

— *The New York Times, May 20, 2015*

4.5 Million UCLA Health Patients' Data Compromised In Cyber Attack

— *Forbes, July 17, 2015*

Responsibile benefits administration is rewarding, but not always easy.

From a Taft-Hartley perspective, regulatory demands have only grown — with ERISA in 1974, and then with the PPA in 2006, and then with HIPAA, CCA and a whole lot of other compliance concerns along the way.

So while benefits administration has never been easy, it is getting harder than many could have foreseen a generation ago. It's one thing to exercise prudence. It's another to find yourself battling an invisible realm of criminals bent on constantly trying to pry their way into your computers — and into your members' personal information.

Just looking at the headlines, any administrator or trustee could be forgiven for wondering: *What have I signed up for?*

While these headlines reflect just a portion of what has happened in the realm of healthcare, similar headlines have chronicled data breaches and other forms of cyberattacks across the spectrum of American organizations, from Harvard to Target to the IRS.

Health Insurers Become Prime Targets for Hackers

> *"...the Anthem hack relied on malware and tools that have been used almost exclusively by Chinese cyberspies, investigators said."*
>
> — *The Wall Street Journal*

Read beyond the headlines, and you may feel even more overwhelmed, as it appears they are being asked to battle not just criminals, but other countries. *The Wall Street Journal* coverage of the Anthem data breach reported, "Although the investigation remains in its early stages, the Anthem hack relied on malware and tools that have been used almost exclusively by Chinese cyberspies, investigators said."[1]

Health insurers are seen as prime targets for hackers because they maintain a wealth of personal information on consumers, including medical claims records and information about credit card and bank accounts.

Unfortunately, the attack on healthcare data seems to be only getting worse.

"We are seeing a shift in the causes of data breaches in the healthcare industry, with a significant increase in criminal attacks," Dr. Larry Ponemon of the Ponemon Institute, which studies breaches in healthcare, recently wrote.[2] "While employee negligence and lost/stolen devices continue to be primary causes of data breaches, criminal attacks are now the number-one cause."

Healthcare Data Breaches are the Most Frequent & Most Expensive

If it seems there are a lot of stories about healthcare data breaches, it isn't just because the media finds it so egregious that a hacker would go pawing through medical records. It's because healthcare data is the number one target of hackers — many of whom are believedto be foreign-sponsored cybercrime groups.

[1] "Health Insurer Anthem Didn't Encrypt Data in Theft" The Wall Street Journal, February 5, 2015

[2] "Study Reveals Five-Year Data Breach and Security Trends of Growing $6 Billion Epidemic That Puts Millions of Patients and Their Information at Risk" – Ponemon Institute, May 7, 2015

"Relatively small breaches can incur significant first-party costs for legal guidance, forensic investigations, victim notification, credit monitoring, etc."

AVERAGE COST PER-RECORD BREACHED

$956

CYBER CLAIMS FILED IN 2013

117

Healthcare was the sector reporting the most data breaches, followed closely by financial services, with the retail and professional services sectors tied for third, according to a study[3] of cyber liability insurance claims published by NetDiligence, a cyber risk assessment and data breach services company. The study was based upon 117 cyber claims filed in 2013, which NetDiligence notes only represents "5 to 10% of the total number of cyber claims handled by all markets" for the year.

The NetDiligence study found that when adding the costs for computer specialists to investigate and remediate the breach, the cost of attorneys, and the cost of notifying victims, paying for credit monitoring, and other expenses, the average cost-per-record for a breach was $956.

The cost can be far higher — especially for healthcare organizations.

"There continues to be no meaningful correlation between the number of records exposed and the total payout for the claim," the NetDiligence study found. "For example, in one incident in this year's dataset, only 80 [records] were lost. However, the legal defense and settlement costs were quite high, resulting in a cost-per-record of more than $11,000."

The study notes: "We think this is especially true in the Healthcare sector, where enforcement by State Attorneys General has been aggressive. Relatively small breaches can incur significant first-party costs for legal guidance, forensic investigations, victim notification, credit monitoring, etc."

[3] NetDiligence 2014 Cyber Claims Study

Building Best Practices

Protecting Your Members' Data

To help Taft-Hartley trustees and administrators carry out their critically important work, we've put together some best practices to help ensure assets — including PII (Personally Identifiable Information) and PHI (Protected Health Information) — remain protected, and that your organization doesn't end up in the headlines for the wrong reasons. The good news is that you usually aren't expected to walk into the server room and check for malware and viruses. But from a fiduciary standpoint, you do need to ensure that someone with the qualifications to do so is doing all of that and more.

Best Practices To Protect Your Members

- Ensure infrastructure is secure
- Check application security & maintenance
- Audit for services and applications
- Keep data secure
- Inquire about third-party party security
- Educate users
- Keep up with BYOD (Bring Your Own Device) policies
- Require audit trails
- Institute correspondence tracking
- Stay current with regulations and compliance
- Consider a hosted solution or other strong partner

Ensure Infrastructure is Secure

Because benefits tend to include healthcare coverage and retirement options, Taft-Hartley plans collect a wealth of data that could appeal to cyber criminals. As noted above, healthcare was the sector reporting the most data breaches, followed closely by financial services. So whether you are involved in providing health insurance services, pension plans, or a number of related services, you must assume that your organization is either already under attack, or soon could be.

While typically you may entrust other capable parties with the responsibility of protecting IT resources and data, the fiduciary responsibility is so great that it is helpful for trustees and administrators to have a foundation of knowledge and resources to help gauge the protection an employee or third-party vendor is providing.

NIST Cybersecurity Guidelines

Every benefits provider would do well to download and study a copy of the National Institute of Standards and Technology (NIST) report[4] *Framework for Improving Critical Infrastructure Cybersecurity.* The NIST report notes, "Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact." The key phrase in the above is that risk management is *an ongoing process*.

This excellent 40-page document is of special value because the NIST Framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization.

NIST Cybersecurity Guidelines

Click to view or download

[4] Framework for Improving Critical Infrastructure Cybersecurity, published by the National Institute of Standards and Technology, Feb. 12, 2014

"The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement," the report notes. "Utilizing the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment."

Trustees in particular should be aware of the NIST cybersecurity guidelines — and ensure their organization's IT managers are actively aware of the guidelines — because of the potential liability issues involved in ignoring the guidelines. In addition to financial liability, Taft-Hartley trustees usually are very focused on the specific effects a plan's administration has on the members they serve.

"In the Taft-Hartley community, trustees know their 'customers' are hard-working union members counting on the fund office to administer their benefits and, by extension, to protect their personal information from criminals and thieves," says Ron Rock, VP of Technology for basys, a long-time provider of benefits administration software for self-administered Taft-Hartley fund offices and TPA's. "Hackers don't just steal data, they also threaten the bond of trust members have with the fund office."

It isn't enough just to know that systems, including such basics as noted above, are in place. You need to know that the systems are being actively monitored, tested, maintained, and upgraded.

Basic Building Blocks of Secure Infrastructure

Firewall

A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted.

Public Key Infrastructure

PKI is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

Virtual Private Networks

A VPN extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and thus are benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.

Antivirus & Malware Checking

Antivirus and malware software is designed to prevent, detect, and remove malicious software. Some products also include protection from other computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, Advanced Persistent Threat (APT), botnets, and Distributed Denial of Service (DDoS) attacks.

Encryption

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. While encryption doesn't prevent interception, it denies the message content to the interceptor. Encryption can be used to protect data "at rest," such as PII or PHI information stored on computers and storage devices. Encryption can also be used to protect data in transit — for example when transferring data via networks, including the Internet, mobile telephones, and across other wireless devices.

Intrusion Detection System

An IDS is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Some IDS systems focus on external attacks, while others focus on internal. Some systems may attempt to stop an intrusion attempt, though most are primarily focused on identifying possible incidents, logging information about them, and reporting attempts.

Check Application Security & Maintenance

The key phrase in the above is that risk management is an ongoing process, which means that trustee concern should be ongoing as well.

In the same way that you should take an active interest in ensuring that your infrastructure is secure and continuously protected, you should also look at application security. Small organizations may have one-off homegrown applications, or old legacy systems, that were created back when security was less of a concern.

Even modern applications can be problematic unless they were specifically designed, built, and tested to provide a secure foundation. Applications should be built to be secure. And they should also be put through annual security tests.

Security is always an ongoing concern, which is why software (and operating system) maintenance is crucially important. Across the globe a cat-and-mouse game is played as very motivated criminals seek out weak points to attack within applications and operating systems.

Responsible software publishers respond by regularly issuing maintenance updates and security patches to block whatever attack surface has been identified. This means that every organization needs to have staff dedicated to ensuring that all applications and operating systems are maintained with the latest software updates. Note that we aren't just talking about enterprise business applications. Attacks can come from anywhere. Popular targets include browsers, Java apps, and commonly used tools such as Adobe Flash and Reader.

By the way: one of the great value propositions for hosted environments is that, with the right vendor, the host exercises responsibility for updating and patching systems — though you will want to have completely spelled out and understood exactly what is, and potentially isn't, covered by the service.

Audit for Services and Applications

It is important to know what is running on your network. A good way to find out is to perform an audit of services and applications. The goal is to reduce the attack surface hackers can target by ensuring you have your operating system locked down so that you are only making use of services that are needed. The same with applications. An audit also helps you stay alert to all systems that need to be maintained and patched.

The importance of this was underscored in the wake of the Premera data breach. An article in the *Seattle Times*[5] recounted a routine technology audit that the U.S. Office of Personnel Management conducted of Premera infrastructure prior to the breach. The audit was carried out because Premera is one of the insurance carriers that participates in the Federal Employees Health Benefits Program.

"The auditors found that several servers contained software applications so old that they were no longer supported by the vendor and had known security problems, that servers contained 'insecure configurations' that could grant hackers access to sensitive information, and that Premera needed better physical controls to prevent unauthorized access to its data center," the *Seattle Times* reported.

Attacks can come from anywhere. Popular targets include browsers, Java apps, and commonly used tools such as Adobe Flash and Reader.

Keep Data Secure

Maintaining data security, especially PII and PHI, has to always be a top concern. Organizations should consider using encryption while storing data on their systems, as well as when transferring data across a network.

Data must be secured from an operational standpoint, too. Data centers — whether on premises or in a hosted environment — should be physically secured using industry best practices. Organizations should have their own data centers independently audited for Standard Operating Controls (SOC) Type 2 compliance. When using a hosted environment, you should require SOC Type 2 compliance there as well.

[5] "Feds Warned Premera About Security Flaws Before Breach," the *Seattle Times*, April 2, 2015

While working with data, IT and other authorized personnel should have a secret code that must be entered during sign on. Group policy can be used to provide granular needs-based access control, and software should support multiple levels of authorization.

> *"The auditors also found that several servers contained software applications so old that they were no longer supported by the vendor and had known security problems ..."*
>
> *—The Seattle TImes*

Inquire About Third-Party Security

Every security measure you expect from your own IT infrastructure should also be required of third-party vendors and other organizations with which you exchange data. The NetDiligence study found that 20% of the data breach claims it studied were attributable to interactions with third parties.

Educate Users

User education should be an ongoing effort. Users should be kept up to date on what's happening in the world of malware and phishing, as social engineering scams continue to be a major entry point for otherwise well-protected environments.

Sophisticated hackers often target some of the users you'd least expect to let down their guard on data security — your IT leadership.

"Your IT Director or Systems Administrator usually knows all the backdoors into and passwords for your system and may have set up some shortchuts he or she uses to work quickly," says Ron Rock of basys. Exceptionally crafty hackers devise phishing schemes and other tricks targeting your top IT staff, knowing they'll hit the jackpot if they get through that particular entry point. Constant vigilance is key."

Lost or stolen laptop computers have figured into many data breaches. Users who carry data on laptops, thumb drives, smartphones and other portable devices must be aware of and follow whatever policies you create for encrypting and otherwise protecting data — especially PII and PHI.

> *“It was surprising that the two largest payouts ($13.7 and $11.7 million) in this year’s dataset were to small-revenue organizations.”*
>
> *—NetDiligence*

Even relatively small data losses can create big problems — for the people you serve, as well as your organization — including legal and regulatory actions.

“It was surprising that the two largest payouts ($13.7 and $11.7 million) in this year’s dataset were to small-revenue organizations,” NetDiligence reported. “What drove the costs up on both of these claims were legal and regulatory actions. Interestingly, these two events had virtually nothing in common. In one, a healthcare provider lost a device with a relatively modest number of PHI records (approximately 25,000). In the other, a hacker stole almost 2.5 million PCI [Payment Card Industry] records from a retailer. Nevertheless, in both cases, legal/regulatory defense and settlements were in the millions of dollars.”

Employees — especially those who travel for business — should be educated on the need for using VPNs, and on security basics such as not inadvertently leaving behind documents, especially those containing PII or PHI data, in the temp drive of public machine.

Within the office, employees should be provided with secure shredders, and educated on the secure use of copiers and when to block out fields that contain PII or PHI data.

Keep Up with BYOD

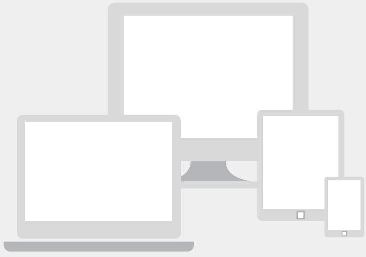
A sign of the times is the unstoppable tide with which the practice of employees working on their own devices has swept into the workplace. While many within the IT community fought the trend on security grounds, the ubiquity of smartphones and other mobile devices — especially with road warriors and others working in the field — simply proved too powerful.

Your IT group (or IT person) should work with users to know what is being used, and to insist that all devices are properly maintained with software updates and security patches. The need for this was underscored by a *Wall Street Journal* article[6] “BYOD Beware: Employees with Old Versions of Android May be at Risk,” which reported that Google would no longer patch security holes in some older versions of the Android operating system.

“As more employees begin to use Android devices at work, CIO’s will need to pay close attention to which versions of Android Google decides to stop patching,” the story noted. While this particular article was about Android, it serves as an alert for all organizations with policies allowing BYOD.

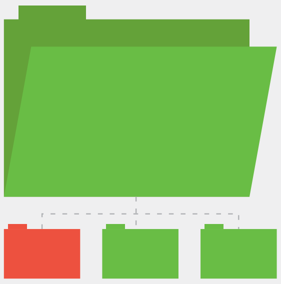
Mitigate BOYD Risk

The *Wall Street Journal* recently offered advice on how organizations can limit the security risks of employees using their own devices for work



Limit Usage of Devices in the Workplace

Limit the types of devices permitted to only those that allow for remote location and data deletion by the IT department. Most of today’s major brands either have this feature or support applications that provide this function.

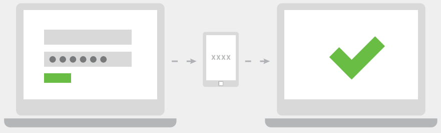


Limit Access to Corporate Information

Limit access to corporate information based on the type of device and employee need. For example, allow employees to access only email via their smartphone. If certain employees require remote access to the company server, allow such access only through a secure VPN connection.

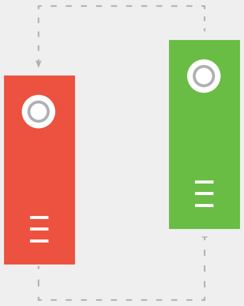
[6] “BYOD Beware: Employees with Old Versions of Android May be at Risk,” The Wall Street Journal, Jan. 26, 2015

Mitigate BOYD Risk (Cont.)



Monitor Corporate Files

If employees are allowed to access the company database, ensure that corporate files can only be saved to the company server, not downloaded to the remote device used to access such files.



Two-Factor Authentication

Require two-factor authentication to remotely access the company server. This includes something you know (e.g., a PIN) and something you have (e.g., a security token).

End-user Agreements

Require that each employee who participates in the BYOD program sign an end-user agreement that clearly identifies the employee's obligations, grants the company certain rights with respect to the device so that data can be removed if necessary, addresses reimbursement for data charges, and specifies how to handle data loss.

Require Audit Trails

Be sure your enterprise software system supports audit trails — a log of precisely who touched data, when it was touched, and what changes were made. The NetDiligence study found that of the 111 breach events in its dataset, 32% were attributable to insiders. While 58% of insider breach events were unintentional, caused primarily by staff mistakes, the rest were malicious in nature, caused or abetted by rogue employees.

In such cases an audit log can be extremely helpful. Unfortunately, healthcare seems to have more rogue incidents than other sectors, making audit logs all the more important.

Institute Correspondence Tracking

Organizations should also have an application that supports correspondence tracking — a method for recording all interactions between plan participants, their dependents, employers, health claim providers, agents, and plan administrative personnel. Tracking might include phone conversations, face-to-face discussions, and incoming and outgoing mail. Correspondence tracking should also provide the ability to record the receipt of specific required information or documents (as in pension application tracking).

Stay Current with Regulations and Compliance

Ensure that personnel and practices are in place to consistently monitor for, and react to, changes in whatever regulatory and compliance environment they operate in. Organizations do well to prepare far in advance to ensure they are prepared for the evolution of regulatory requirements like HIPAA 5010, ICD-10 Procedure Coding System (PCS) code sets, and new mandates from the Department of Labor and the IRS.

Consider a Hosted Solution or Other Strong Partner

Faced with the challenge of creating and maintaining a secure environment, and the constant monitoring and security patches, as well as the need to remain current with all applicable regulations and compliance requirements. Taft-Hartley organizations should strongly consider working with an established hosted solution. In cases where the organization desires to (or is required to) operate an on-premises solution, finding a strong partner for your enterprise business applications can be a great advantage.

Today, the cost of owning and managing in-house IT infrastructure can be daunting. Hosting through a reputable partner offers peace of mind on data security and regulatory compliance, and can save your organization thousands of dollars it would cost to continually acquire, monitor and maintain new servers and other hardware. But when considering hosted solutions, it is important to find a partner that understands the complexities involved with high availability secure application hosting. Whether seeking a hosted solution or an on-premises deployment, Taft-Hartley organizations should seek a software vendor whose solutions are geared specifically toward organizations that value information safeguards, data protection, and redundancy.

About Basys

Since 1977, basys has specialized in benefits administration software for the Taft-Hartley community, providing integrated technology solutions that help trust fund offices, national multiemployer plans and third party administrators accurately and efficiently serve millions of members across the US and Canada. Basys software suites, web-based portals and hosting services deliver cost-effective and reliable health and benefits processing, fund office administration, reporting and member services on a platform built for data security, regulatory compliance and a lower total cost of ownership. Basys is state-of-the-industry technology driven by decades of commitment to benefit American workers.

For more information, please call us at 410-850-4900, or visit our website www.basys.com.