INFORMATION SECURITY

Are You Really Protecting Your Information Assets?

David Barton

Ongoing hacks and breaches of security lead businesses to continually question just how well protected their information really is. The unintentional—and often intentional—disclosure of personal and proprietary information is a real threat to most businesses. As technology evolves and new threats and challenges are created, it is becoming increasingly difficult for organizations to maintain adequate security levels.

It wasn't too long ago that a company could protect its information and data by making sure there was a firewall and anti-virus software installed between their local area network and the Internet. Those days are long gone. We now live in a hyper-connected world, rife with new technologies and the new threats that accompany them.

On top of the more traditional security challenges an organization faces, elements such as bring your own devices (BYOD)—allowing employees to use their own devices for work—and the cloud introduce new layers of complexity and risk. The good news is that there are many actions PEOs can take to help protect data, ranging from relatively simple to highly sophisticated. At a minimum, there are several leading practices that all PEOs should take to protect themselves and their clients.

Understand the Environment: BYOD

Companies struggle with employees using their own technological devices at work, trying to manage security and work output expectations. As the BYOD trend continues to grow, so do the challenges associated with it. Gartner research reports that 38 percent of companies expect to stop providing devices to workers altogether by 2016.[1]

PEOs need to put in place a BYOD policy and be sure all employees understand and comply with it. At a minimum, companies should require each employee to enter a password to access his or her device.

Personal devices can include laptops, tablets, and smart phones. Because they're all portable, they are easily lost or stolen and pose a significant risk to the information security of the organization.

In the event of a lost or stolen device, there are applications to wipe data off them remotely, and that practice is increasingly common these days. However, these tools should not be used on personal devices without permission, so a strong BYOD policy is a required first step.

Decide if the Cloud is the Right Choice

Research indicates that more than half of all U.S. businesses are now using cloud computing.[2] Advantages include potential cost savings, ease of use, flexibility, and in some cases, better security. But is it really safe? What risks does the cloud pose? Cloud providers generally have security included as part of their service, and it's often less expensive and better than the security that can be provided in a private computing environment.

The biggest change PEOs will see with cloud computing is the loss of control over their own data. The cloud is relatively new and the industry lacks broadly accepted standards for secure access and data handling. Understanding contracts and service level agreements (SLAs) will minimize the impact of this shift in control and maximize security. A contract with a cloud provider should address how the vendor manages sensitive data such as Social Security numbers. The contract should include minimum security and infrastructure practices, require that security prac-

[1] "Bring Your Own Device: The Facts and the Future," April 11, 2013, by analyst David A. Willis.

[2] *www.forbes.com/sites/reuvencohen/2013/04/16/the-cloud-hits-the-mainstream-more-than-half-of-u-s-businesses-now-use-cloud-computing.*

Reproduced with permission of the National Association of Professional Employer Organizations

tices be regularly updated, and include provisions for third-party audits to confirm compliance.

Create an Information Security Policy

The best first step that any business can take towards information security is to develop a comprehensive set of formal information security policies for the organization and make sure all employees and stakeholders (i.e., contractors, service organizations, etc.) understand them.

It is critical that employees know what is expected of them. Policies are the best and least expensive way to ensure that everyone is on the same page about what is allowed and what is forbidden when it comes to maintaining the three key attributes of information: confidentiality, integrity, and availability.

For example, be sure to include specific policies related to social media and BYOD. An effective information security policy clearly communicates what is acceptable, clearly assigns responsibility, and defines the consequences of noncompliance.

Train Employees Well and Often

People are the weakest link in the security chain. For example, if a staff member has been told that the client "has to have this spreadsheet by 5 p.m.," but the corporate email system won't allow the attachment because it is too large, he may use his personal email that has no size restrictions on attachments, place the spreadsheet out on Google docs to share it, or use a USB flash drive. All of these methods are insecure and may be in direct violation of the security policies (if they exist).

Without frequent training about *why* the policies exist and the risks associated with violating them, employees are not motivated to think about the security risks and consequences. Security policies have to be constantly reinforced with training and real-world examples to be effective.

Encrypt Data

A critically important step for PEOs to take is encrypting data that is sent to and from customers. In general, businesses and their employees trust email more than they should. Hours, pay rates, Social Security numbers, and additional confidential data are shared all too frequently via email, often insecurely. Small PEO businesses in particular are using email more than they should for the transfer of personally identifiable information (PII). There are numerous email encryption products on the market that can help prevent sending PII via unencrypted email.

If storing or maintaining PII in the cloud, it is strongly recommended that the data be encrypted both in-transit and at-rest, meaning stored in an encrypted form. While this does add to the overhead, it provides a reasonable assurance that the data will not be compromised.

Obtain Third-Party Assurance

Customers want to know that their vendor has a strong system of internal controls to ensure confidentiality, integrity, and availability of their data. The standard mechanism for providing that assurance today is the SSAE 16 (SOC 1) report (*www.aicpa.org/soc*). A CPA performs an SSAE 16 attestation and the resulting report provides a detailed description of the controls in place at a service organization like a PEO. The SSAE 16 report also summarizes the testing of the controls to ensure they are working as management intended.

Stay on Top of Information Security Trends

Just as there are new threats to information security each day, so are there new processes and technologies to deal with them. It is imperative that an organization be aware of new risks and new methods and tools to address them. Each organization should have a designated person responsible for information security, and that person should devote time each week to exploring new threats and new controls.

Information security is an ever-evolving process. Each new technology that emerges brings the promise of increased productivity and efficiency, but also new security risks that must be addressed to fulfill those promises.

As stewards of a customer's data, the PEO needs to ensure it has taken the necessary steps to minimize the possibility of a data breach. By focusing on the leading practices presented here, a company can be ahead of the curve when it comes to providing a secure environment for its customers and rest assured that its information will remain its most important asset.●

David Barton is a principal at UHY LLP, based in Sterling Heights, Michigan, and leads the Internal Audit, Risk, and Compliance practice.