IT and HR: Managing your data securely


Sarah Sommers and Tony Rucci

Just this past month, I had a prospective client tell me that they lost a flash drive with employee information containing medical and personnel information. Nationwide, we have heard and read many stories of companies losing customer and employee information or that their IT systems were hacked, credit card and employee information stolen. Those threats are real for all businesses — small or large. What are you doing to prevent such attacks? Are you educating your employees on best practices to protect company information?

Let's begin by discovering what information you are keeping on each of your employees. That data is vital to every employee's livelihood; first and last name, Social Security number, banking information for direct deposit, insurance information ... the list goes on. This list is a thief's crown jewel! To protect employees, many companies are moving in the direction of storing that information electronically — some in Excel spreadsheets on the company server with limited access while others elect to access an Internet-based Human Resource Information System to store that data securely in the cloud. We can expect that the future of technology in human resources will be more Web-based so that all users, employees, managers and decision makers will have access to the data via multiple systems and platforms to make decisions promptly, independently and strategically.

In the information security industry, we use the terms "Personally Identifiable Information," also known as "PII," and "Insider Threat." PII has been around as an industry term for many years, and is information that can be used by itself or collectively with other information to positively identify an individual, or more importantly present themselves as that individual for nefarious purposes. Years ago, one would think nothing of providing a Social Security number publicly, and it was rarely protected to today's standards.

As an example, new military recruits were issued duffel bags at the reception station when they reported for basic training. To properly identify each new soldier's equipment, the supply sergeant would stencil the recruits' last and first name, middle initial and Social Security Number! Surprisingly, it was common practice in many companies beyond the military until recent years. Protecting your PII has never been more important than it is today with as much potential for exposure through digital means.

Here are some things you should consider regarding your PII and PII of others to which you may have access as part of your professional role. Implement a rigid policy regarding the release of PII. PII should only be released with the expressed approval and/or knowledge of the individual to which the information belongs. The Fourth Amendment protects our right to privacy, while Nevada's Security of Personal Information Law provides the enhanced guidance on the state's requirements to protect PII as well as the responsibilities and notification requirements should an individual's or organization's PII be exposed.

The Insider Threat can have a catastrophic impact on an organization, or multiple organizations, as you may have seen recently reported in the news with such cases as Eric Snowden and Bradley Manning. Insider threats can be intentional or unintentional. The intentional insider is extremely difficult to defend against, and it is often the most damaging to an organization. Unintentional insiders are somewhat easier to manage with a rigorous, proactive insider threats program, but all too often can cause just as much damage when situations are allowed to spiral out of control.

Today's economy has driven those who may have been exceptional employees to take drastic measures. The recent government shutdown and furloughs to follow are current examples of how low morale can bring out the worst in trusted employees during troubling times. Insiders have access to the crown jewels, which distinguish your company from your competitors. Trusted insiders in many cases have unfettered access to your proprietary information, contacts lists, trade secrets and corporate strategies. Participants in recent industry surveys reported that if they were fired tomorrow, they would definitely take corporate data with them to their next employer.

Bottom line: All companies have to deploy proper security measures to protect their company, employees and clients. Business owners need to facilitate that conversation regularly with their employees to ensure that each are following those best practices to protect the company and that proper measures are taken when an employee violates such practices. It is vital that all employees understand proper usage of their equipment and that the company has standards in place and guidelines when something goes array.

Rigorous systems administration of your organizations' computer network is paramount to your success. Successful configuration of your routers, firewalls and segmenting your networks in such a way that if one element (or division) of your network is compromised, it doesn't necessarily compromise everything. The question isn't necessarily if you will be compromised. The real question is, "When?" It's highly likely that your organization, irrespective of how small or large, already has some compromised machines on your network or the networks of those with whom you do business. While you may be able to manage your network efficiently and securely, you open yourself to potential threats through your business partners, who become those "trusted insiders" we mentioned earlier. The question then becomes this: How will you recover once you experience a data breach? Do you have a backup and recovery plan already established? Do you have concrete reporting procedures in place? Do you have compliance rules and regulations to abide by based on your industry space? (Think PCI & HIPAA as examples). What are your data breach notification requirements to your clients, shareholders and employees? When do you go public?

There are so many things to consider. All too often, it's an after-thought and knee-jerk reaction when you don't have a plan in place, a team to implement the plan or exercises to work out the kinks in your response plan. Hold critiques following every action or trainings to ensure that you are streamlining your processes as you work toward becoming an efficiently operating team that protects your crown Jewels. When you really think about it, aren't your *employees* your true crown jewels?

Take care of people, and they will take care of you.

Don't take care of people ... and they *will* take care of you!

Think about it.

Sarah Sommers is chief executive officer of Solutions At Work, a Reno-based human resources consulting firm. Contact her at 775-827-9675 or sarah@mysolutionsatwork.com. Tony Rucci is founder and owner of /Root Technology, a Reno-based professional IT security services practice. focused on secure network management, disaster recovery and security. Contact him at 775-391-0865 or Antonio.Rucci@RootTechnology.net.

QUOTE OF THE WEEK

"My parents taught me how to listen to everybody before I made up my own mind. When you listen, you learn. You absorb like a sponge — and your life becomes so much better than when you are just trying to be listened to all the time."

Steven Spielberg

northern nevada BusinessWeekly www.nnbw.com

GENERAL MANAGER
Rick Carpenter
(rcarpenter@nnbw.biz)

EDITOR
John Seelmeyer
(info@nnbw.biz)

BUSINESS MANAGER
Inga Smith
(ismith@nnbw.biz)

CIRCULATION AND DISTRIBUTION MANAGER
Keith Sampson
(ksampson@sierranevadamedia.com)

REPORTER
Duane Johnson
(djohnson@nnbw.biz)

REPORTER
Rob Sabo
(rsabo@nnbw.biz)

REPORTER
Anne Knowles
(aknowles@nnbw.biz)

SENIOR SALES EXECUTIVE
C. Eli Zeiter
(ezeiter@nnbw.biz)

CONTRIBUTIONS
If you have a news item you'd like to contribute to NNBW, a guest column you'd like to write or an ad you'd like to place, call 775-770-1173 or visit nnbw.com. We'll walk you through the process. We work diligently to be easy to work with.

HOW TO SUBSCRIBE
For subscription information, call 775-770-1173 or visit nnbw.com.