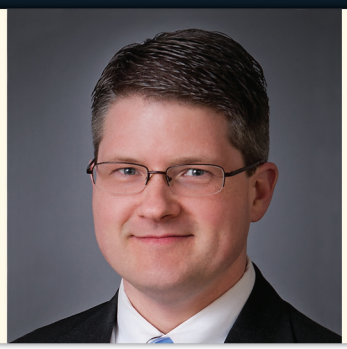
VIEWS & VISIONS

A publication of Bowles Rice LLP

Summer 2015



Security is Everyone's Business

Brian M. Peterson, Partner
Bowles Rice LLP

Brian Peterson is a partner in the Martinsburg, West Virginia office of Bowles Rice and practices in the areas of employment law, civil rights defense, and state and local government defense. He also serves as chair of the Bowles Rice Technology Department.

Brian counsels and advises clients in wage and hour matters, workplace harassment investigations, development of handbooks and policy manuals, hiring and discharge of employees, drafting and litigation of employment contracts, including restrictive covenants, wrongful discharge claims, workers' compensation matters, compliance with state and federal employment laws, and unemployment benefits claims.

He defends employers against claims under the Family and Medical Leave Act (FMLA), Age Discrimination In Employment Act (ADEA), Americans with Disabilities Act (ADA), Fair Labor Standards Act (FLSA), the West Virginia Wage Payment and Collection Act, Title VII of the Civil Rights Act of 1964, and the West Virginia Human Rights Act, including claims of discrimination, harassment and retaliation.

Brian earned his law degree from West Virginia University College of Law in 1998, where he served as editor-in-chief of the *West Virginia Journal of Law and Technology*. He is admitted to practice in both Virginia and West Virginia.

How would your employees respond if they were asked, *"Who is responsible for information security in your company?"*

Historically, the IT department has been assigned responsibility for data security and privacy in most companies. But a recent stream of high-profile data breaches, along with tightening regulations and laws, have caused customers and clients to demand more stringent security controls from their business partners and vendors. While some breaches are initiated by remote computer access, many can be prevented by better-trained, more vigilant employees.

Every organization possesses valuable and sensitive data, whether it's pricing or product information, business strategies, personnel records or customers' credit card numbers. This data must be protected, wherever it resides, with appropriate controls. Security is everyone's business because it affects every person in the organization. To gain access to valuable data, hackers need a foothold. Any employee, regardless of his or her position in the organization, can be targeted. Security should be on everyone's mind all the time. To accomplish that goal, your company needs an information security program.

Developing an Information Security Program

An information security program is comprised of written policies and procedures, employee training and continuous monitoring and auditing of security practices. Regardless of the size of your organization, a security program can be developed to suit your needs and inform your employees about the risks and responsibilities for keeping information secure.

Because the majority of a company's information is in electronic form, your first instinct may be to place full responsibility for the security program with IT. While IT will certainly play a large role, they should not be the only ones developing and running the program. From the outset, senior management must be involved. Support from the top is crucial to the success of the program.

Furthermore, IT simply cannot control all of the company's information. In most organizations, a lot of information remains in paper format. Your security program must address how the company will handle all of the information in all of its forms. How will you secure paper files? Do you lock file cabinets at the end of each day? Is your off-site file storage monitored? Is your record room flood proof? Are paper files exposed to sprinkler systems? An information security program will identify the most likely risks to your information and prescribe controls to mitigate those risks.

The Human Element

Human resources plays an important role in the program. When people leave your organization, what sorts of security risks can be presented? Are passwords being deactivated immediately? How are new hires being screened?

This particular risk was highlighted in the 2014 Home Depot security breach that exposed 56 million credit and debit card transactions due to lax security. The company's lead security engineer was convicted in May 2014 of sabotaging his former employer's computer network. His name is Ricky Joe Mitchell. He graduated from Capital High School in Charleston, West Virginia, in 1997. Had Home Depot screened Mitchell a little better, they would have found not only that he stood accused of hacking his former employer's network but also his 1996 personal web site, in which he posted the following description of himself with the title "The Story of RickDogg":

"I love to write and distribute Viruses. They intrigue me. I have taught myself how to program

in assembly, c- - and pascal. I also love to fix computers as well. I am considered smart at school although I am very lazy. I do not like the s--- they try to teach me so I get bored and try to liven things up a bit."

When he was a junior, Mitchell was expelled from school for planting 108 computer viruses to disk space assigned to another student on the Capital High School computer system. He then posted threats to students whom he blamed for reporting him. Home Depot's failure to screen this high-level security employee will, no doubt, figure prominently in lawsuits filed against the company by its customers.

In addition to Human Resources and IT, other employees in your company play a significant role in security. Facility managers help ensure physical security, such as locks on server room doors, fireproof file cabinets and installation of security cameras. Even your receptionist plays a role in ensuring that visitors are identified and only enter secure portions of the building with an escort.

The security program will have a number of facets. Among the most important is the documentation of your security practices and the collection of those policies into a comprehensive set of written information security policies and procedures. For service-based organizations, clients and customers are increasingly asking to see such documents as a condition of doing business.

Perhaps the most important part of the program is the training element. One of the most common ways a hacker gains access to your network is to be let in by one of your employees. Hackers use emails with fake links or innocent-looking attachments that transfer malicious code onto the employee's computer.

Hackers may call on the telephone posing as Tech Support to obtain passwords. They may drop free thumb drives in the parking lot that execute malicious code when they are inserted into a PC's USB port. It's much easier to trick a human being into allowing access than it is to hack into a computer system with no credentials. Once a hacker has a valid username and password, he can inflict all sorts of additional damage through lateral movement in your network. Training your employees to recognize threats and engage in safe computing practices is central to your company's security program.

Certification of Your Security Program

Once you establish your information security program, your company may benefit from taking the additional step of obtaining a recognized certification, such as ISO 27001 certification. ISO 27001 is a global standard published by the International Organization for Standardization (ISO) that describes how to manage information security in an organization. ISO 27001 can be implemented by any company, small or large, for-profit or non-profit, private or public.

ISO 27001 is a certifiable standard, which means companies can become certified by third-party auditors. The standard contains some absolute requirements, but allows flexibility for companies to prioritize and mitigate its biggest areas of risk. To obtain certification, a company must show a systematic and ongoing approach to managing sensitive information. Although certificates are nice to have, the greatest reward of becoming ISO certified is that your company will have an ongoing and properly functioning information security management program.

Your company's information assets are constantly expanding, and with them, your risk. Protecting your information is not optional – it is critical to the life of your business in the digital age. Good security training and practices will continue to help protect organizations from attackers who seek to exploit vulnerabilities and employees' trust in order to gain access to your valuable information. Developing an information security program will get everyone involved and make security everyone's business.