The Next Data Breach Could be Yours – Confronting Cyber Security Risks

By Kristina Brines, Esq., PHR, SHRM-CP & Kerin Stackpole, Esq., SPHR
Paul Frank + Collins P.C., Burlington, Vermont

Cyber security breaches are no longer only the concern of major retail businesses and government agencies. If you retain any information relating to the public, or if you have trade secrets and valuable business information that you don't want in the hands of the wrong party, you should be taking steps to protect your business from cyber security threats. All employers now should be thinking about how to protect their businesses through good employment practices and policies. How should you accomplish this? Engage all employees in the effort to secure your data, and make sure that employees have the knowledge and the tools to help you defend against cyber threats. Here are some tips for making sure that your business is not next in the headlines for a data breach.

Many of us think that as a small business, we are not likely to be targeted for a data breach. In fact, in 2012, 45% of breaches happened to businesses with less than 100 employees.[1] Data relating to credit card information, social security numbers, financial information, passwords, and other sensitive information are all fodder for those contemplating these kinds of attacks. Sensitive data is generally classified as Personally Identifiable Information (PII), Payment Card Information (PCI) and Private Health Information (PHI). Businesses in the sectors of healthcare, financial services, retail, technology, and professional services are at an increased risk.
The dangers associated with a cyber security breach are not only the time and resources involved in addressing them, but also loss of reputation and goodwill, loss of trade secrets, and potential lawsuits by your customers. You may also be at risk of violating state or federal laws regarding protection of sensitive information. For instance, in Vermont, an employer generally has 14 days to inform the Attorney General's office of a breach and 45 days to inform customers.

Who and what are causing these breaches? In a recent study, hackers accounted for 31% of reported breaches, Malware/Virus issues for 14%, and employee mistakes or intentional acts by employees for 11%.[2] There was insider involvement in 22% of the insurance claims submitted for breaches in 2015.[3] Beyond the obvious need for firewalls and other IT protection devices – your employees are a key element to defense. Prevention requires proper training of employees, creating a culture of accountability (so that employees know they need to be vigilant, and they are held accountable if they are not), solid policies and protocols, and continuing communication with employees about their role in helping to keep business information safe.

What steps should you take to prevent a breach?

- Don't collect data you don't need.

[1] 2013 Verizon Data Breach Investigations Report.
[2] Net Diligence 2015 Cyber Claims Study.
[3] *Id.*

- Only keep data as long as you need it, and know what you have.
- Limit access to information by your employees – only those who need access should have it.
- Establish clear policies and protocols for employees handling sensitive information, including: policies on securing the data; policies on how to prevent loss or theft of data; protocols for reporting suspected or actual breaches; consequences for failure to follow proper protocols.
- Train employees who handle sensitive information how to spot potential danger signs and how to prevent breaches.
- Require employees to lock their computer whenever they are away from their computer, and assign each employee a unique user name.
- Conduct periodic cyber security awareness trainings for your employees.
- Control portable data and employees' ability to use their own devices for work purposes.
- Consider using a third party vendor to handle sensitive data.
- Consider carrying cyber liability insurance.

What should you do if you are victim of a breach?

- Call legal counsel to assist with compliance measures. This will include notification of state and federal agencies and notification of consumers, and will help to minimize regulatory fines and litigation costs.
- Call your insurance carrier, if you have appropriate coverage.
- Investigate the cause of the breach (this may well involve hiring an outside vendor or making sure internal human resources and IT employees are properly trained to conduct such investigations).

An ounce of prevention is always worth a pound of cure, and your employees will play a big role in your prevention efforts if they are well trained and have safety and security top of mind. Plan, engage, train, hold people accountable, get some good insurance; and have counsel lined up to help if a breach happens.