SOCIUS

Cyber Risk Management:

How Do I Start?

By: Laura Zaroski, J.D., Socius Insurance Services

Hardly a day goes by without a news flash about another cyber breach. Since security breaches have become a daily occurrence, I sat down with Jeremy Henley at ID Experts to discuss the most common ways that companies are being breached and how companies can start to assess their cyber security risk profile.

Question; Jeremy, what are the most common ways that you are seeing small to mid-size companies being breached?

Answer: One of the common ways that companies are being breached by hackers is that the hackers exploit vulnerabilities in the company's security network. This includes the company's failure to update software or upgrade their systems, as well as the failure to have the appropriate checks and balances in place. Small to mid-sized businesses are particularly vulnerable as they often don't have the IT staff or budget to continually upgrade and update their systems as their organizations change and grow.

The second most common way companies are breached is through simple employee negligence. This would include a company's failure to train and educate their employees on basic cyber security. For example, the failure to educate employees on the risks of downloading private data onto a portable device that is not encrypted as well as the failure to educate employees as to how to identify Publishing scams that ask them to open suspect emails or attachments. Companies need to educate their employees about the dangers of connecting to unsecured Wi-Fi connections at the airport or Starbucks when they are doing work that includes logging into sensitive company systems. If someone is spoofing the airport Wi-Fi you are essentially sharing everything you are doing online with that attacker.

Question: Once clients realize the security risks they face in today's world, clients often ask where they should start with respect to updating their network security. Do you have any guidance for them?

Answer: I advise our clients to start by asking themselves three questions: 1) What data are we collecting? This is important as it will help them determine what regulations they may need to comply with (HIPAA /HITECH, PCI, and 47 State Breach Notification Laws, etc.), 2) How are they managing the data that they have? This includes examining what technology the company is using, if they are creating multiple layers to their security with firewalls and anti-virus and if they are creating policies and procedures and training their employees as to security safeguards, and 3) I would ask the company to examine who they are sharing the data with. Specifically, which vendors or clients have access to their systems and ask those vendors what security and privacy policies they have in place (if any)? You might consider requiring your vendors to provide proof of a security audit or insurance in the event they are the cause of a breach of info that you were trusted with.

Question: What role does cyber insurance play with your clients?

Answer: Cyber insurance has been invaluable to many of our clients as most cyber policies include pre-breach education tools, employee training information as well as sample security policies or an incident response plan. Some carriers also work with us to provide risk assessment and penetration testing so that weaknesses can be identified and corrected prior to a breach incident. In my experience, the most valuable part that Insurance plays is that the insured is able to fund an appropriate response in the wake of a breach. Clients that do not have cyber insurance usually do not have a budget set aside to deal with this unfortunate event, and after a breach do not have the funding to adequately fund the most appropriate response, therefore, limiting their ability to respond to the significant reputational, financial and legal ramifications that such an incident can cause to their organization.

ABOUT:

Jeremy Henley is the Director of breach services at ID Experts. ID Expert brings simplicity to the complex world of privacy incident response by providing a complete solution that focus on limiting the occurrence of a breach, preparing for the inevitable and then providing a one stop solution to breach response including forensics, crisis PR, printing and mailing, call center services and a variety of identity monitoring and protection. We thank Jeremy for his time. If you have further questions regarding cyber insurance, or risk management, Please contact your Socius Producer.