BURR FORMAN LLP

Birmingham Business Journal: Cybersecurity Table of Experts

Articles / Publications
04.01.2016

In an article published by the Birmingham Business Journal in the April 1 print edition, India Vincent provides her insight into a series of questions related to cybersecurity, including what are some best practices to help monitor for and identify breaches.

Vincent explains, "Even the most sophisticated companies often don't know about a breach until they are notified by a third party such as law enforcement. While it is impossible to be sure you will identify all suspicious activity proactively, some key things to watch for are computers within your system that are behaving abnormally, users identifying suspicious emails or unusual network traffic."

Full article is available in the April 1 edition of the *Birmingham Business Journal*. India's portion of the discussion is featured below. You can see the full discussion here.

Table of Experts Series: Insights into Cybersecurity - India E. Vincent

Q: A number of large retailers have been impacted by data breaches in recent years. How serious is the risk for small businesses? Data breaches are a serious risk for all sizes of businesses because any business can have data that a hacker will find valuable. Small businesses can be more attractive targets for a hacker because they have less security, even though they may not have as much data. If the data they do have has value to the hacker, they are a target. Research shows that a high percentage of small to medium size businesses have suffered cyber-intrusions, but they either went undetected or unreported.

RELATED PROFESSIONALS

India E. Vincent, CIPP/US, CIPM

RELATED CAPABILITIES

Cybersecurity & Data Privacy

Birmingham Business Journal: Cybersecurity Table of Experts

Q: What can my business do to reduce the likelihood of a cyber-attack? Given the current cyber landscape, it is not unreasonable to think that all companies will be victims of an attack at some point, regardless of the steps they take. The objective, then, is to take steps to minimize the impact such an attack would have on your customers and your business. At a high level, the most important thing for all businesses to do is to understand at least the general nature of the threat and to make informed judgments about what data to secure and how to secure it. It is not reasonable to expect small businesses to be able to undertake all the security measures a large, international company would. But at the same time, if the small business has particularly sensitive data, it will be expected to spend additional resources to protect that data. Understanding the type of attack most likely to be used on the business (phishing, DDOS, Advanced Persistent Threats, just as examples) can help determine the best course of action to protect the data.

Q: What are the key ingredients for a strong small business cyber-security plan? First, identify the data the business has that a hacker would find valuable. Is it customers' personal data, trade secrets, the company's financial information? Then retain only the data required for business purposes. If the data is not in your system, it can't be stolen during a breach. Use up-to-date operating systems and software and keep them updated and patched in a timely fashion. Use intrusion protection devices, including virus and malware protection, firewalls, and encryption if appropriate, and keep them up to date. Use complex passwords and maintain passwords in the appropriate manner. Passwords should not be on notepads under a keyboard, left with an administrative assistant or on a document on your computer. And train employees to understand and spot risks. Despite all the technological threats, a very high percentage of breaches continue to have a human act that makes them possible, such as clicking on a link in a suspicious email or downloading software from a questionable website. Even with training, employees will always be one of the biggest risks.

Q: Are there any laws or regulations I need to be aware of when it comes to protecting my customers' secure information? There is no single law or regulation that governs all these issues throughout the United States. So depending on your state, your industry and the scope of your business, you may have several different privacy and data security laws or regulations that you need to follow. Identifying these and staying up to date on their requirements is a key step in protecting your business. Your cyber counsel can help you identify these laws and regulations and conduct a risk assessment to see whether your current systems and policies are in compliance.

Q: What types of services are out there to help my company prevent or respond to a cyber-security threat or data breach? There are vendors for all areas of this industry. Some examples are: penetration or vulnerability testing to assess your systems; development of IT security plans and incident response plans; employee education and training; and data storage, back-up, business continuity etc. These services allow you to outsource many of the activities that give rise to risk, making the contracts you have with these vendors very important because they will determine who is responsible in the event of an incident. Basically, you could contract out almost all the actions that need to be taken to secure your data, and some of those services make a lot of sense for any business, but particularly for small businesses. However, even if responsibility for maintaining the system and financial responsibility for a breach can be delegated through a contract, there can be brand and reputation damage to your business as the result of

a breach - even if the vendor's systems were the ones breached - and sometimes it is impossible to recover from that damage.

If you contract with third parties for any of these services, you need to understand what your vendors are doing for you, what risks you are mitigating, and what risks you still bear.

Q: What are some of best practices to help monitor for and identify breaches? Even the most sophisticated companies often don't know about a breach until they are notified by a third party, such as law enforcement. While it is impossible to be sure you will identify all suspicious activity proactively, some key things to watch for are computers within your system that are behaving abnormally, users identifying suspicious emails, or unusual network traffic. Sometimes the first sign of an issue is a phone call from a user that has received an unusual email (and perhaps has already clicked on a link in that email or replied to the email). Other times, users may report that a computer or group of computers is operating particularly slowly or is generating unusual error messages or otherwise performing differently than usual. To the extent you have the ability to monitor traffic and activity on your network, review the logs. Signs of unusually high traffic in or out of the network, or traffic between parts of the system that don't typically communicate directly, can all be signs of malicious activity. It is important to investigate these types of occurrences, or if you have a vendor handling those issues for you, to make sure the vendor looks into the incidents.

Q: What are the key components to be included in a breach/incident response plan? First, specify the criteria that will be used to declare an incident or a breach, the individuals who are responsible for making that declaration, who will be informed of the declaration and how they will be notified. The incident response team should include an Incident Lead, a business decision maker, external legal counsel with expertise in data breach responses, external forensic specialists, and HR, and possibly law enforcement, an external PR firm or a data breach resolution provider. Each team member needs a copy of the incident response plan and contact information for all team members, in paper form, because you should not rely on communications via the compromised system. The response plan should include a checklist for the first 24 hours after declaring an incident or breach; a list of follow-up activities; a description of the hardware and software components of your system and expected data flows between these components; contact information for your identified third party vendors; and a list of customer/client notification requirements applicable to your business. In addition to responding to the breach, you need to identify who is going to focus on maintaining or restoring business operations, and what resources they will need to do so. Finally, make sure the incident response team practices implementing the plan in simulation exercises.

Q: What are some things businesses often overlook when developing a plan to protect their sensitive data? I agree about mobile devices. People generally don't think about the computing power typically available on a mobile device or the amount of data that can be compromised if such a device is lost, stolen or hacked. Because society tends to rely on mobile devices for convenience both personally and professionally, users often want to compromise security of these devices for convenience. Businesses should always make an assessment between the business risk and convenience of their users, but it is important that the choices about mobile device security be well considered and not driven by the latest

features available in technology. Possibilities to consider are password protection, two-factor authentication, encryption, ability to remote wipe a device, and lost device locator options.

Q: What are some good components of an emergency plan as it pertains to cyber security and protecting/backing up data? While it is technically possible to have systems that provide completely redundant, realtime business continuity, that is not cost effective for most businesses, particularly small to medium size businesses. Each business needs to consider the aspect of their business that would be critical to continued business operations in the event of a data incident, a natural disaster, or similar occurrence that makes the primary systems unavailable for some reason. The key is to identify those critical items, find ways to ensure they are available in a reasonable time through a secondary source, and to prioritize other systems and determine how you would go about retrieving that functionality and/or which vendors will handle this function for you.

Q: What options are available to train employees about the importance of cyber security? You can prepare basic training on your own with a little time on the Internet. The FTC, NIST and the SBA as well as several other sources all provide good materials for educating yourself and your employees about the risks for small businesses. For larger companies that have the resources, there are vendors who will conduct cyber awareness, planning and/or incident response training as well as provide follow-up assessments and testing. This is one area where there is no shortage of information, and any additional knowledge you can give your employees about how to avoid breaches can have a direct impact on your chances of catching an intrusion before there is any damage, or limiting the damage once an intrusion has occurred. In either case, your cyber legal counsel can assist in identifying training materials or providers and can often even provide the training assistance.