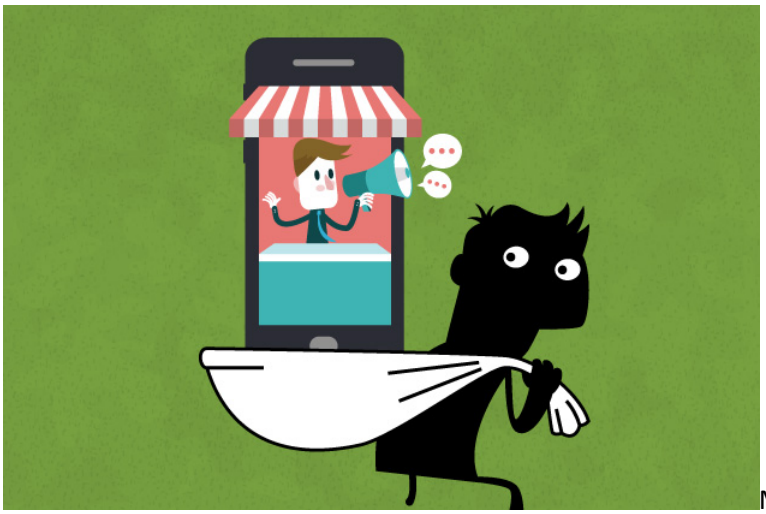
The Small Business Cybersecurity Blindspot

by Richard Thompson | June 1, 2014 at 6:02 am



Many believe that large corporations are more likely to be at risk from cyberattacks and IT system compromises than small or medium enterprises. The data from bigger businesses is more desirable simply because of the scale of operations, they reason.

But this assumption is wrong. In fact, the data that small businesses have is of great value to cybercriminals, and small businesses may actually be at greater risk to cybersecurity threats than their larger counterparts.

The Verizon 2012 Data Breach Investigation Security Report found that 67% of cybersecurity compromises in 2011 happened in organizations with just 11 to 100 employees. This is because all information is valuable, whether it is held by big businesses or small start-ups. Hackers can profit from any kind of data, especially if it can be used in combination with other data that may have been obtained from similarly sized businesses.

Opportunism further motivates cybercriminals to target small businesses. These hackers are not the geniuses portrayed in Hollywood films-you do not have to be particularly skilled to hack into a system unless it is well defended. Though large organizations are by no means immune to cybersecurity breaches, they are generally more likely to have strong policies in place to regulate online activity and reduce the likelihood of cyberattack. That means it is simply easier for cybercriminals to get their hands on data from small companies than it is to break into a big corporation.

What Are Small Businesses Doing Wrong?

The underlying problem is a matter of perception. Small business owners are either largely unaware of the risk presented by poor cybersecurity, or they say they understand that good cybersecurity practices are important to their business but just assume that they are safe.

According to the National Cyber Security Alliance/Symantec Small Business Study, 73% of small businesses say a safe and trusted internet is critical to their success, yet most do not have an internet security policy. A full 87% do not have a formal policy and 69% are without even a basic informal internet security policy.

As a result, employees receive no guidance as to how they should behave online. They are not trained to identify and avoid online threats such as phishing scams, unsecured websites or signals that a computer may be infected with malware. They are not given guidance on choosing safe passwords and changing them regularly, and they are not given formal instructions on how to update anti-virus software, or even how to inform the proper personnel if the software on their system expires.

That means employers are relying on the experiential knowledge and common sense of employees. But depending on background and, often, age, employees will have vastly different levels of familiarity with good cybersecurity practices. Most small businesses blindly rely on this eclectic mix to stay safe. Unfortunately, it only requires one careless individual to disregard safe practices and become the chink in the armor that brings the whole business down.

Personal Problems

Many employees of small businesses are also not given any guidance on using personal accounts. Again, just one individual using a personal email for work purposes can put the company at risk. Personal emails are outside the control of the business-there is no backup, no governance and no security that the company has any power to influence. Instead, files or emails relating to the business rely on third-party terms and conditions. You might think that Gmail, for instance, is going to be reliable, but remember that Google is currently in a legal battle to retain the right to scan the contents of users' emails and share this content with the NSA. If employees are using Gmail to send confidential client information, they could jeopardize the security of those clients.

It can also be a problem if an employee uses personal email to sign up for anything on the company's behalf. Technically, the owner of the email account owns anything related to it. Should an employee leave the company or become uncooperative, the company may have no legal right to that asset. For example, if an employee sets up a Twitter account for his or her company using a personal email address, the employee technically owns the account. This could put the company in a very sticky situation down the line.

About 75% of small businesses do not have a social media policy and, for many of those that do, the policies are not broad enough. These policies need to go beyond limiting the amount of time that can be spent on social media. Take the example of the employee who used a personal email to set up the company Twitter account. Someone hacking into the employee's email account could then gain access to the company's Twitter page and cause a lot of damage.

Social media is also vulnerable to viruses and malware since it relies so heavily on user-generated content. If an employee's friend posts a link to a malicious website on Facebook and the employee clicks on it, the computer on the company's network could easily become infected.

Firesheep, for example, was a piece of malware created to highlight the security risks of sites like Facebook and Twitter, which encrypt the login process but not the cookies that are created during the process. This malware allowed anyone to capture login details without permission. It highlighted massive security flaws in networks that billions of people use every day. The add-on is still available for anyone to download and exploit.

Small businesses are not formalizing security policies because they simply do not accept the risks posed. Despite the lack of formal protocols, 86% of small businesses are satisfied with the amount of security they provide to protect customer or employee data. Only 6% said they were somewhat or very unsatisfied.

Business owners need to understand that a security breach could be extremely serious. Many small businesses actually close after a data breach-in the United Kingdom, poor cybersecurity practices cost a business an average of up to £4,000 a year (about $6,650).

But many do not understand this. Nearly half said that, if their business suffered a data breach, the occurrence would be an isolated incident and would have no impact. It is exactly this attitude that perpetuates the seriousness of the risk. As long as small businesses believe they are not at risk, they will do less to protect themselves, thereby increasing the risk of a breach.

One way to help ensure that a company is protected is to obtain an ISO 27001 accreditation. This means that employees within a company have specialized training on to how to treat data security and that the company has the proper operations in place to ensure safe handling of information.

Companies should also consider cyberliability insurance, which can protect their intellectual property from data breaches, privacy concerns and network security failures. Unlike larger companies, small businesses often do not have the capacity to recover from a costly data breach. By understanding their cybersecurity risk and taking specific steps to reduce or mitigate it, however, small businesses can avoid big problems in the future.

Source: http://www.rmmagazine.com/2014/06/01/the-small-business-cybersecurity-blindspot/