nerd wallet
We do the homework for you.

FAQ: How do I protect my small business from cyber attacks?

by DIVYA on SEPTEMBER 27, 2012

The facts: small businesses underestimate their vulnerability

Last week brought about cyber attacks targeting several American banks. Although hackers often target large companies, small businesses are becoming increasingly vulnerable as well.

Small businesses tend to underestimate their vulnerability to cyber attacks because they underestimate their value to cyberthieves. They believe they are not worth the effort to hack, but small business owners often don't realize how little effort hacking a company with minimal security is to an experienced cyberthief.

The Symantec Threat Awareness Poll showed that small businesses tend to do too little to protect themselves from attacks:

- 50% of small business owners think they are too small to be a target for cyber attacks
- 61% of small businesses don't install antivirus software on all desktops
- 47% do not use security on mail servers
- 67% do not use any web-based security

Verizon Business ran an extensive study of cybersecurity breaches in 2011, with some surprising results on the tendencies of hackers to target small businesses:

- 72% of reported hacker breaches targeted business with 100 or less employees
- 79% of 2011 cyber attack victims were targets of opportunity

Although small businesses might think themselves small enough to fall under the radar of cyberthieves, the usually lax security measures implemented by small businesses make them an easy target for hackers. Most victims were not businesses with considerable assets or trade secrets, identified by thieves before a heavily planned attack; rather, most victims simply had weak cybersecurity that thieves exploited.

Hacking through employees

81% of breaches in 2011 used some form of hacking, and 69% used malware.

One common way for cyberthieves to break into company infrastructure is through hacking employees rather than management. Cyberthieves can send phishing emails to individual employees, and when these emails are opened on the company server, malicious software can steal company information.

Businesses should establish a clear company policy on what company information can be disclosed through social media, websites employees should not access at work, how to identify phishing emails, and how to preserve the security of mobile devices, particularly if they can log into a company server through their personal device.

NerdWallet's tips: how should you protect your business?

The FCC has a handy small business cybersecurity planning tool that allows small business owners to create a custom cybersecurity plan containing advice from experts on twelve subjects, including network security, mobile devices, facility security and policy development.

NerdWallet recommends that businesses take four initial steps to protect themselves:

1. Assess your security status. Where are all of your possible data breaches and security gaps?
2. Implement a firewall and antivirus software
3. Hold a training session for employees and relay to them the company policies on cybersecurity
4. Create administrative passwords that are difficult to guess, ideally ones comprised of a combination of numbers and letters

By implementing a comprehensive cybersecurity plan and educating employees on this plan, businesses can protect their assets.

Other Expert Opinions

- **Robert Siciliano, McAfee Online Security Expert, offers five tips for ensuring your company's cybersecurity**

  "1. Not all data is hacked. Exercise basic to advanced premise/physical security such as access control, security cameras and alarms.

  2. Limit the amount of data required from customers. If you don't really need a Social Security number then don't store it. If credit card information doesn't need to be stored then don't store it.

  3. Recognize that knowledge based authentication questions as password resets can bring down the house. Many of the answers can be found in social media sites.

4. Laptops are one of the biggest data breach points. Laptop data should be encrypted. Laptops should never be left in a car overnight or left in a hotel room or office alone or on a coffee table in a café unattended. Laptop tracking software that locates and wipes data is essential.

5. Train, train, train, train. Training on data security and what to do, and what not to do is priority number one. Clicking links in emails, downloading anything from the web or email, opening attachments in emails, have all been recent successful ways to infect a network."

- **Nathan Corbier, founder of Corbier and Associates, talks about employee devices**

"We do not allow anyone to plug unauthorized devices into our workstations or company laptops. That includes MP3 players, cell phones, USB keys, nothing. If someone does so, it immediately locks the PC up with a blue screen of death and sends an SMTP alarm. The only authorized USB devices we allow are Yubikeys and Iron Keys.

We require all android smart phones to be synced with our Google Apps Account, have password authentication enabled, and be encrypted."

- **Michelle Schenker, owner of Cover Story Media, speaks to the importance of changing passwords frequently**

"Change passwords frequently and always use complex and unique passwords for anything you are doing online. Passwords become harder to decode when they contain a wide variety of characters, generally it is best to incorporate numbers, letters, capital letters and symbols in your password. Passwords should be difficult to guess and it is important that they are changed regularly. It is suggested that you change your online passwords once every month in order to keep them dynamic and reduce the likelihood that someone will gain access to your personal information. "

- **Kyle Marks, founder Re-Tire IT, says to dispose of old technology securely**

"When an organization retires unwanted technology, it faces risks associated with data security and environmental compliance. Threats from trusted insiders and negligent vendors increase the challenge. Companies should be aware of the data security threats that come with updating IT."

- **John S. Pitts, founder of Tekcetera, Inc., encourages the use of firewalls and VPNs**

"With the increasing number of computer hackers and identity theft victims, it is imperative that you provide your company with reliable protection by using firewalls. These can either be software-based or hardware-based and are used to help keep a network secure. Ultimately, firewalls analyze data packets and determine what information should be allowed through, based on a predetermined rule set.

Virtual Private Networks (VPNs) provide security through tunneling protocols and security procedures such as encryption. For example, a VPN could be used to securely connect the branch offices of an organization to a head office network through the public Internet."

- **Alfea Principe, Global Marketing Director for Electronics Recycling Services, reminds small business owners to recycle computers safely**

  "A common issue that financial and government issues are unaware of is the dangers associated with not recycling computers, cell phones, printers, fax machines, etc. correctly. If these electronics are not dismantled correctly and put in the wrong hands, this very sensitive and confidential data (credit card, banking information, social security numbers, etc.) can be extracted."

- **Michael Becce, MRB Public Relations, warns of keyloggers**

  "The real threat to small businesses is keyloggers. Keyloggers is a form of malware that tracks every keystroke you make on your keyboard and makes it available to hackers. Most people assume that anti-virus product will prevent keyloggers from getting on their systems, after all, it says so on the box. The reality is that the very best anti-virus products can detect less than 25% of known keyloggers. Many systems are already infected. Keyloggers track everything from your Windows log-in, bank forms, financial information, email, social media, even instant messaging. Every small business should assume that at least one person in the organization has been hit or will be. Many small businesses have been completely shut down already. To prevent it from stealing your keystrokes (and your data, secrets, money, etc.), use a keystroke encryption tool to encrypt each keystrokes as you make it so the keyloggers read fake data."

- **Sid Haas, VP of Business Development at LKCS, speaks to hiring a third party network security firm and holding trainings**

  "We hire a 3rd party independent network security firm to perform external vulnerability assessments on our servers and web sites every 6 months. These assessments identify specific security vulnerabilities based on the level of risk. We utilize the information in these assessment reports to mitigate as many vulnerabilities as possible — starting with any identified as high risk but also addressing items identified as medium and low risk.

  We've found that cybersecurity is as much about education and training than all of these other steps. We hold annual security training sessions with all employees and continually remind all of our employees about security issues, scams, and threats throughout the year via e-mail and small posters displayed throughout our facility."

- **Doug Landoll, Chief Strategist at Lantego LLC, encourages businesses to review their security regularly**

  "We review current administrative, physical, and technical controls, assists with filling out the security surveys, and gets the small business back into compliance. This involves physically inspecting the protection of systems and sensitive data storage, developing security policies, and
  locking down our systems.

  Small businesses are often targeted by hackers because they anticipate weak controls. The chance of your sensitive information being compromised could be very likely. For minimal effort basic controls can be put in place to not only bring you into compliance but also to protect your customers' sensitive information and increase their satisfaction with your service."

- **Mark J. Sexton, owner of Nevada Medical Security Technologies, talks about the importance of training staff**

  "When talking about cybersecurity for small businesses, the main objective is to create security awareness with the business owner and staff. You can't protect what you don't know about, so becoming informed on the nature of cyber crime, the methods the bad guys use to obtain either protected information or money/assets is key. Once people have a basic understanding of how thieves use technology to steal, then they can look at their own systems and processes and see if there are loopholes or pieces missing.

  Basic things like using complex passwords and changing them regularly, keeping systems and antivirus software up to date. Using a malware/spyware scanning application on their systems regularly. Educating the staff on appropriate use of technology and how phishing and social engineering attacks work, having policies about appropriate use of business computers and not allowing users to be full administrators of their systems constitute the low hanging fruit here. Administrative rights is a big one, if users can install software they can become a nexus for an attack or allow for key logger software and other such malicious software on to their systems and potentially on all systems in the business.

  In the end though it's all about knowledge and being informed. It is almost impossible to offset poor computing practices by employees and as a result training becomes key."