the TCBN
TRAVERSE CITY BUSINESS NEWS
DECEMBER 2013 • VOLUME 19 • NUMBER 6

IT SECURITY 101 FOR BUSINESS

BY THERESA BLACKBIRD

Protecting your organization against information technology security risks is becoming increasingly important in today’s business climate. Instances of malware and cyber intrusion are more sophisticated and widespread than ever before.

You only need to look to the media to find examples. Corporate giants like Visa, JCPenney, and NASDAQ have all fallen prey to cybercrime. The cost of these crimes can be staggering: Five hackers were indicted this summer for stealing more than $300 million and 160 million credit card numbers.

Too small to fall prey to cybercrime? Think again.

Big businesses aren’t the only victims of cybercrime. These attacks are indiscriminate and can affect anyone. Smaller companies can be easy pickings as they don’t have the resources of larger companies. They typically lack the monitoring, forensics tools, logging capabilities, penetration testing, and other warning systems that would alert them to security breaches.

No matter the size of the company, most have financial data, bank accounts, and employees with social security numbers. Even if you store this information off of your network, an attacker can still find a way to gain access to a human resources or accounting computer. Hackers also know that many smaller companies do business with larger organizations, and can use your company as a stepping-stone to access more lucrative businesses’ networks and steal from them.

In fact, 31 percent of all targeted attacks are aimed at businesses with fewer than 250 employees, according to Symantec’s 2013 Internet Security Threat Report.

The first steps to improving IT security

The good news is it’s not too late. There are steps that you can take to help protect your company, employees, and data. Passwords are a great starting point.

- **Use strong passwords**. Require employees to use passwords with an industry standard complexity pattern of at least eight characters with a combination of upper and lowercase letters, numbers, and symbols.

- **Update passwords.** Require periodic password changes and don't allow users to recycle old passwords.

- **Enforce system time outs.** If a workstation or laptop is left unattended for more than a few minutes, it should automatically lock and require a password to login.

- **Recognize phishing.** Phishing is an email or instant message that directs you to enter details (username, password, credit card numbers, or banking information) on a fake web site that looks almost identical to the legitimate one.

- **Keep antivirus software current.** Over 101 new vulnerabilities were reported on a weekly basis last year. Protect against malware by ensuring all devices have up-to-date antivirus software.

- **Invest in a firewall.** This hardware or software solution helps prevent unauthorized access to your network.

Keeping a close guard on passwords is important. Recently, a hacker group boasted obtaining a spreadsheet of user names and passwords from a California telecom company. They input these credentials into Google and found corresponding Gmail accounts. From these email accounts, they identified online banking accounts and applied these same credentials again to steal funds.

The Traverse City Business News is published by Eyes Only Media LLC
(231) 929-7919 • 109 S. Union St., Suite 305 • Traverse City, MI 49684

The moral of this story is twofold – don’t use the same username and password for all of your online accounts and know who has your passwords and how they are protecting them.

IT security for mobile devices

With the proliferation of mobile devices and remote access applications, companies are facing a new level of potential IT security threats. Laptops, tablets, and especially smartphones can provide a door to your company’s network and data. Here are some steps that you can implement for greater mobile protection:

- **Secure connection.** Require a virtual private network (VPN) for remote access to your network.
- **Secure mobile devices.** Similar to workstations; enforce device time outs and lockdowns with a strong security code to unlock mobile devices.
- **Encryption.** Encrypt data on all mobile devices (tablets, laptops, smartphones, etc.)
- **BYOD (bring your own device) policy.** Control the types of devices staff can use for business purposes and how these devices connect to the network.

IT security – an ongoing responsibility

Just because you’ve taken steps to protect your data does not mean you can rest easy. Cybercrime is big business – attracting highly skilled and technically knowledgeable individuals worldwide. These criminals are on the cutting edge and constantly developing new scams and schemes to take advantage of the unwary.

It’s best to be proactive. Always assume you could be a target, work to understand the active threats, and know what data is vitally important to your organization and where it resides. Involve your staff in the process and take precautions, such as:

- Educate employees about the latest threats.
- Back up your data.
- Create and test disaster recovery plans.

Remember, nothing is 100 percent secure. IT security acts as deterrent. Measures like these will hopefully keep cyber criminals at bay long enough for them to consider moving to an easier target. You can also work with an IT services provider that can analyze your IT infrastructure to determine potential weaknesses, and build additional layers of security to protect your business.

Theresa Blackbird is a security engineer at Safety Net, Inc., a local IT services firm. A Certified Information Systems Security Professional, she has extensive experience in IT security working for the U.S. government and private sector. To learn more about IT security, watch this webinar: safetynet-inc.com/ITsecuritywebinar/.

Symantec’s Report Shows Big Cybercrime Increases

The following are the key findings from Symantec’s 2013 Internet Security Threat Report.

- There has been a 42 percent increase in targeted attacks in 2012.
- 31 percent of all targeted attacks aimed at businesses with less than 250 employees.
- One waterhole attack infected 500 organizations in a single day.
- 14 zero-day vulnerabilities were reported. A zero-day vulnerability is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known.
- 32 percent of all mobile threats steal information.
- A single threat infected 600,000 Macs in 2012.
- Spam volume continued to decrease, with 69 percent of all email being spam.
- The number of phishing sites spoofing social networking sites increased 125 percent.
- Web-based attacks increased 30 percent.
- 5,291 new vulnerabilities were discovered in 2012; 415 of them on mobile operating systems.