BALBOA
CAPITAL

Cybersecurity: What Every Small Business Owner Needs To Know

Don’t Let Your Company’s Sensitive Information Become Compromised

Whitepaper Brought to You By Balboa Capital

Over the past several years, there have been many high-profile security breaches involving some of the largest retailers, technology companies, health insurance companies and entertainment companies in the United States. Hundreds of millions of records were compromised without warning. If cybercriminals can break into large corporations' websites, there is no telling what damage they can do to small businesses like yours.

Imagine coming to work and finding out that your company's website or network was attacked or shut down by cybercriminals or a computer virus. It would turn your business upside down and result in decreased productivity, lost revenues and frustrated customers and vendors. Instead of focusing on the day-to-day responsibilities of running your business, you will be dealing with information technology experts to diagnose the problem, add the necessary security measures, and get your website up and running as soon as possible.

A worst-case scenario would be to have your company's highly sensitive information, or personal information about your customers, compromised by hackers. No matter how you look at it, there is a high price to pay for not protecting your company's website and network.

This Balboa Capital whitepaper features some helpful tips to help small businesses and equipment vendors keep hackers and viruses away from their websites and internal networks.

Become Familiar With Cyber Threats

In today's world, business owners and equipment vendors can't just relax and hope their websites and internal networks don't get hacked. Cybercriminals work around the clock throughout the world looking for vulnerable targets. The first step in bolstering a company's online security efforts is to understand the various cyber threats that are out there. This helps determine the risks that a website and/or internal network might be facing.

What You Need To Know

It goes without saying that running a business involves a large number of responsibilities and day-to-day tasks that can leave you with minimal time to devote to cybersecurity knowledge and protocols. But it is very important to become familiar with the malicious tactics that are being used to hack into websites and internal networks. Doing so can help you identify potential problems and correct them to protect your business, your employees and your customers.

You can start by having your information technology (IT) manager, or outside IT resource, provide you with an overview of common cyber threats and how they are carried out. This should be followed by a comprehensive assessment of your company's website, internal network, firewall, software systems and email communication program, to name a few.

Common Types of Cyber Attacks

Trojans - A type of malware that tricks users into clicking something (e.g., software update) that loads viruses onto their computers.

Malware - computer code that is designed to steal private information and/or destroy computers and servers.

Spyware - a form of malware that spies on users and records their keystrokes to access information.

Worms - viruses that can attack either a single computer or an entire network of computers.

Phishing - fake emails that are used to steal usernames, passwords, credit card information and more.

Establish Basic Security Protocols

Numerous studies indicate that over half of all privacy breaches are caused by insiders, the majority of whom simply made mistakes. When your employees are knowledgeable of security risks, they will be less likely to do something that puts your company's information at risk. An online security training session that is conducted by your IT manager, or outside IT resource, is a great way to educate your employees. You should also establish security protocols and communicate them to your employees so they are fully aware of the penalties for violating business rules and policies.

Prevent Internal Security Breaches

In a perfect business world, you wouldn't have to worry about your employees stealing intellectual property such as forms, documents, customer/client lists, and personal and financial information. Unfortunately, you need to be very proactive and protect your company from insider theft. According to an Identity Theft Resource Center (ITRC) study conducted last year, approximately 11.7% of security breaches were performed by malicious insiders. Preventing inside data theft is a difficult task, particularly if your employees use personal devices (smartphones, tablets and laptops) and portable storage devices. Without the right security tools in place, a malicious employee can access your company's vital information and transfer it to a USB drive in a matter of minutes.

Steps to Take

There are several strategies you can employ to stop an insider data breach before it happens. One of the most widely used solutions is data loss prevention (DLP) software, which prevents your employees from transferring critical information outside of your company's network. Another strategy to consider is limiting access to certain websites and technologies. Install software to block websites that offer file sharing, and format all of your computers' thumb drives and CD/DVD drives to prevent data from being illegally transferred. Lastly, there are numerous programs available that monitor your employees' Internet, email, printer and scanner usage. This will prove invaluable to your human resources manager should you need to "replay" an internal breach.

Use Firewalls To Help Keep Hackers Away

Hardware Firewalls

Today's state-of-the-art firewall systems are filled with robust security features and available as both hardware and software applications. Hardware-based firewalls have different levels of protection and are configured to provide optimum protection to every computer on your network. A hardware firewall's primary responsibility is to prevent hackers and malicious traffic from getting into your company's internal network. Hardware firewalls can also be used to "block" certain internal departments from each other. For example, the information that a company's human resources department accesses should be safeguarded from its sales team.

Software Firewalls

Software firewalls secure all of the computers at your company, and are especially beneficial if you conduct business offsite or at home. Some operating systems offer free basic software firewalls, but the protection they provide is minimal. Investing in a more powerful software firewall system provides a digital barrier between your company's network and malicious traffic.

Combine Forces for Maximum Security

When used together, hardware and software firewalls can provide your business with a higher level of protection from hackers. Because the installation and configuration of hardware and software firewalls is a complex and involved process, these tasks are best suited for information technology professionals. Once you have installed your firewall, it will need to be regularly monitored by an IT professional to make sure it is working properly and that no security breaches are occurring. Additionally, an IT professional is your best resource for downloading patches, updates and other security enhancements as they become available, as well as providing support for email, voice over IP (VoIP) and virtual private networks (VPNs).

Install Antivirus and Antispyware Software

Many small business owners and equipment vendors think a firewall is all that is needed to provide lock and key protection for their company's important information. However, a firewall is just one piece of the online security puzzle. Antivirus and antispyware software with built-in security applications can help protect every computer at your business, even those that are used away from the office. There are a large number of antivirus and antispyware software packages available, and most of them offer automatic update features that you can set to run whenever you want. You might want to update your software at night so that nothing interferes with you and your employees' daily tasks.

The Risks are Serious

Don't let your company or equipment vendor business become susceptible to a computer virus or spyware attack. Should either of these problems occur, a number of serious problems could decrease your company's productivity and, even worse, have a negative effect on your bottom line. Viruses and spyware can infect your network, disrupt your Internet service, and damage your computers and software. The more advanced spyware programs can track the keystrokes and mouse clicks that you and your employees make and write them to files, a blatant violation of business and personal privacy.

24/7/365 Protection

Antivirus and antispyware programs run at all times and check for viruses, malware, Trojans, worms and other types of corrupted data that can harm your company's network and computers. Viruses and spyware can be embedded in documents, videos, emails, website links and advertisements, to name just a few. As long as there are hackers committing digital crimes, there will be a need for small businesses and equipment vendors to use antivirus and antispyware software.

Make Sure Your Website Is Secure

If you are a small business owner or equipment vendor, you might assume that your company is too small to be noticed by hackers. But did you know that hackers all over the world develop automated web-based programs to find vulnerable websites? Without warning, hackers can wreak havoc on your website… unless you are proactive with your online security measures. Securing your website now can help thwart attacks before they occur.

Provide a Safe Online Shopping Experience

Your website receives traffic every day from existing customers and prospects who are interested in the products and/or services that you offer. If your website handles online transactions, it needs to provide your customers with iron-clad protection from identity theft. Today's hackers are finding ways to steal identities and credit card information like never before.

How to Secure Your Website

The industry standard for securing websites is the Hypertext Transport Protocol Secure setting (HTTPS). When filling out forms and/or making purchases online, the web page(s) that are being used switch from HTTP to HTTPS. The HTTPS setting provides users with maximum security; it encrypts their personal and financial information and ensures that it will be transported through the Internet safely.

Online certification authorities such as Symantec, Verisign and GlobalSign issue HTTPS certifications to companies of all sizes, and in all industries. In order to receive a digital certificate, your website needs to meet stringent requirements set forth by the certification authority. Finally, adding an online certification logo to your website lets people know that it is a trusted place to interact and conduct business.

Regularly Backup Your Data And Your Website

If you are like most small business owners and equipment vendors, you put quite a bit of time, effort and financial resources into your website. So, doesn't it make sense to protect your investment with regularly scheduled backups? A hard drive failure, malware attack or problem with your web hosting company's servers can present you with a digital catastrophe if you end up losing portions – or all – of your website's content.

Better Safe Than Sorry

Prevention is the best medicine when it comes to preventing lost website data and content. Periodic website backups ensure that you will always have access to your web content should an unexpected problem occur. Your web hosting company maintains a complete copy of your website on a server network, but check to see if they offer managed backup services.

Consider a Move to the Cloud

You can give your website extra layers of protection by backing it up on your own secure servers and to a cloud-based server. Cloud storage will enable you to do a full website restoration quickly if your office and server gets damaged by a fire, flood, earthquake or other natural disaster. Backing up your website is a relatively simple task that can be managed by your IT professional.

Have a Post-Hack and Post-Breach Plan

If your website and/or network ever get hacked, or if your company suffers an internal breach, you need to move swiftly to get the problem resolved. After you have an IT professional get your website and network restored, have them update your website software, plugins, extensions and other related tools, and run a complete backup of your website. Next, change your password for all important access points (e.g., FTP, SSH, and cPanel), along with your database and administrator accounts.

You should also have an IT expert run a virus scan on every computer, laptop and tablet in your office. Lastly, it is also a good idea to have your employees change all of their computer login passwords and email passwords.

Inform Your Customers

If your website is hacked and knocked offline, your customers will become frustrated. Plus, potential customers who find your site via organic search, referral traffic, or social networks will probably not come back if they see an error message or a blank screen. If your website will be offline for a considerable amount of time, be proactive and protect your brand. Have an IT professional place a temporary landing page on your website that tells users when you anticipate being back online, and that you are extremely sorry for the inconvenience. You can also post this message on the various social networks that your company or equipment dealer business uses.

Summary

Your website represents the brand of your company or equipment vendor business. It is an important part of the marketing mix because it can help you increase brand awareness and generate new business without the large budgets that are commonly associated with traditional advertising efforts.

So, your website needs to provide a great first impression, and deliver on your customers' expectations every time they visit. If your website is well-designed and user-friendly but isn't safe and secure, your online relationships will be jeopardized. Invest in the tools, hardware and software that can protect your website and network infrastructure from hackers, viruses, and other malicious activities.

About Balboa Capital

Balboa Capital is a technology-driven financing company that provides business owners with fast, hassle-free solutions to fuel their growth and success. The company specializes in small business loans, equipment financing, commercial financing, equipment vendor financing, and franchise financing.

Balboa Capital developed an intuitive online platform that simplifies the entire financing process. Calculators provide instant estimates, applications can be completed and submitted in a matter of minutes, and sophisticated credit scoring technology provides instant decisions Visit http://www.balboacapital.com to learn more.

BALBOA CAPITAL