BPX Digital 4000

By BridgePact

Cybersecurity Report

IS YOUR BUSINESS A TARGET?

MILLIONS OF US SMALL BUSINESSES AT RISK FOR CYBERATTACKS

By: Michael Nelson, CEO
BridgePact International

Many large corporations spend hundreds of thousands, or even millions of dollars on cybersecurity annually. But when it comes to small businesses (SBMs), many owners simply aren't spending enough – or even dialed into – the potentially devastating impact that just one cyberattack can have on the bottom line.

THE SURVEY RESULTS ARE IN

Last year, over 2000 small business owners from a wide variety of industries participated in the CNBC / SurveyMonkey Small Business Survey (by Chris Morris, special to CNBC.com).

Only two percent of the participants said they view the threat of a cyberattack as the most critical issue they're faced with in business. From the survey results, taxes and the high cost of employee health care took the top two areas of concern for business owners.

With the rapid increase in cyberattacks, online security experts say that very lack of focus on cybersecurity makes small business owners much more vulnerable now than they realize.

TOP 3 MYTHS ABOUT CYBERSECURITY

1. I don't have an e-commerce site so I am not vulnerable
2. My current IT person has me covered
3. Why would anyone try to hack my business; I'm just a small business owner

Last year, 43% of small businesses owners (1000 employees or less) were targets of cyberattacks. And of those hacked, over 40% were out of businesses within six months. Why? Two reasons:

1. The high cost of cyber repair.
2. Companies who had their websites used for criminal activity (see cross-site scripting below) by hackers, in many cases were closed while they were being investigated.

CYBERFACT #1: Cyberattacks cost companies an average of $700k to $1 Million or more per attack to repair hacker damage

When it comes to small business owners, it is ***mission critical*** that they realize just how vulnerable their business really is.

“It’s because you're the little guy that you're of interest," says Hemu Nigam, founder of US-based SSP Blue, an internet security consultant company. “Hackers love small businesses,” said Nigam. “They haven’t had the resources to put in high-end cybersecurity protection and they may not be consciously aware they are a target."

How big a deal is cybersecurity to small businesses? According to the 2017 State of SMB Cybersecurity Report, the Senate introduced the Main Street Cybersecurity Act, which would create a voluntary cybersecurity framework for small businesses. (The act has been locked in the Committee on Commerce, Science and Transportation since April, with no apparent movement).

CYBERFACT #2: Hackers want people’s personal data and credit card information and backdoor access to websites to commit fraud

Hackers are very dangerous and their goals vary. Many businesses in all industries are hit with a malware attack, and then initially do nothing to respond to the attack. But this can transform a company's systems into "zombie computers," which can be used unwittingly in a larger attack. Some hackers use security lapses in small businesses as backdoor entries into larger partner companies. Hackers will hold data for ransom and force the business owner to pay to retrieve it.

"What they're doing when they attack is freezing the company's assets, encrypting them and saying, ‘Give us $300 to $400 to get it back,’" says Nigam. "Most small businesses will pay that because they never backed it up properly."

More recently, hackers are using accessed servers as an email relay for spam, or to setup a temporary web server for more criminal activity.

One way to add a layer of protection is to contract an outside firm to either transfer or build a WordPress website, instead of using a do-it-yourself website platform or developers working from home without cybersecurity platforms. Companies that have built out cybersecurity platforms have more advanced security systems that can weed out many phishing attacks and malware.

The biggest security risks for small businesses can be born from boredom. Small-business owners who check their personal email or social media sites or favorite websites from their work computers put their company's data at extra risk. And with storage space costing less, companies that keep their data local (vs. with a cloud-based service) often have a lot more information for hackers to mine.

Finally, while several prominent large corporations have withstood major hacking incidents, the story doesn't always end as well for small businesses. When customer data or credit card information is stolen, it can break the circle of trust which often drives your customers to the competition. Beyond that, the financial costs of recovery are often beyond what a small business owner can handle.

BUSINESS AND WEBSITE VULNERABILITY (TOP 9)

You may not think your website has anything worth being hacked for, but websites can be compromised at any time. Hacking is regularly performed by automated scripts written to scour the Internet in an attempt to exploit known website security issues in software. Again, the majority of website security breaches and cyberattacks are not always about stealing your data or defacing your website. The focus is on attempts to use your server as an email relay for spam, or to setup a temporary web server, for the sole purpose of creating criminal activity.

The following 9 areas of vulnerability are just the tip of the iceberg:

1. Software Not Up-to-Date

It may seem obvious, but ensuring that all software up-to-date on your website is vital to keep your site secure. This applies to both the server operating system and any software you may be running on your website such as a CMS or forum. When website security holes are found in software, hackers are quick to attempt to abuse them.

If you are using third-party software on your website such as a CMS or forum, you should ensure you are quick to apply any security patches. Most vendors have a mailing list or RSS feed detailing any website security issues. WordPress, Umbraco and many other CMSs notify you of available system updates when logging in.

2. SQL Injection

SQL injection attacks are when an attacker uses a web form field or URL parameter to gain access to or manipulate your database. When you use standard Transact SQL it is easy to unknowingly insert rogue code into your query that could be used to change tables, get information and delete data.

3. XSS

Cross-site scripting (XSS) attacks inject malicious JavaScript into your pages, which then runs in the browsers of your users, and can change page content, or steal information to send back to the attacker. For example, if you show comments on a page without validation, then an attacker might submit comments containing script tags and JavaScript, which could run in every other user's browser and steal their login cookie, allowing the attack to take control of the account of every user who viewed the comment.

Understand that if your business and web pages are being used by criminals on the dark web, the authorities more than likely will trace these crimes back to your website and your business first. While you may be completely innocent of the crimes that have been perpetrated, the big question is… can your business withstand being shut down for weeks or months while you are being investigated?

4. Error Messages

Businesses need to be careful about how much information they give away in their error messages. Provide only minimal errors to your users, to ensure they don't leak secrets present on your server (e.g. API keys or database passwords). Don't provide full exception details either, as these can make complex attacks like SQL injection far easier.

5. No Server-Side Validation and/or Form Validation

Validation should always be done both on the browser and server side. The browser can catch simple failures like mandatory fields that are empty and when you enter text into a number only field. These can however be bypassed, which can lead to malicious code or scripting code being inserted into the database or could cause undesirable results in your website.

06. Passwords

Everyone knows they should use complex passwords, but that doesn't mean they always do. It is crucial to use strong passwords to your server and website admin area, but equally also important to insist on good password practices for your users to protect the security of their accounts.

As much as users may not like it, enforcing password requirements such as a minimum of around eight characters, including an uppercase letter and number will help to protect their information. Passwords should always be stored as encrypted values, preferably using a one-way hashing algorithm such as SHA. Using this method means when you are authenticating users, you are only ever comparing encrypted values. For advanced protection, it may be a good idea to use a Salt. With cryptography, you can Salt passwords, using a new Salt per password, which adds extra website security.

7. File Uploads

Allowing users to upload files to your website can be a big website security risk, even if it's simply to change their avatar. The risk is that any file uploaded, however innocent it may look, could contain a script that when executed on your server completely opens up your website. If you have a file upload form then you need to treat all files with great suspicion.

8. HTTPS

HTTPS is a protocol used to provide security over the Internet. HTTPS guarantees to users that they're talking to the server they expect, and that nobody else can intercept or change the content they're seeing in transit.

If you have anything that your users might want private, it's highly advisable to use only HTTPS to deliver it. That of course means credit card and login pages (and the URLs they submit to) but typically, far more of your site too. A login form will often set a cookie for example, which is sent with every other request to your site that a logged in user makes, and is used to authenticate those requests. An attacker stealing this would be able to perfectly imitate a user and take over their login session. To defeat these kind of attacks, you almost always want to use HTTPS for your entire site.

Also, Google has announced that they will boost your website up in the search rankings (or de-list your website if you don't) if you use HTTPS, or de-list your site if you don't have the required security in place. This security adds additional SEO benefit too. Chrome and other browsers started the process of implementation in January 2017 for all websites on the Internet.

9. Website Security Tools

Once you think you have done all you can then it's time to test your website security. The most effective way of doing this is via the use of a digital tech company with cybersecurity platforms and security tools and monitoring.

BPX DIGITAL AI CYBERSECRUITY SOLUTIONS BY BRIDGEPACT

Since every business owner is at risk, there are two options to make it more difficult for hackers to attack your business:

- Hire a full-time cybersecurity expert employee ($175k per year average) or
- Partner with a digital technology and development team for a fraction of the cost of hiring just one part-time employee

BridgePact provides a FREE business assessment, which includes an API status report and a cybersecurity scan. Find out if your website is currently being targeted for an attack with ransomware and/or malware and most importantly, what you can do about it.

In addition to our full suite of BPX Digital 4000 and AI platform services, BridgePact provides ongoing cybersecurity hosting tools and monitoring for pennies on the dollar. Take the proactive, integrated approach and defer hackers from gaining control of your business.

Give us a call today for a FREE digital business assessment and cybersecurity scan. You'll be very glad you did.