SiteLock™

Security for Small Business

Key Website Security Facts to Know

A SiteLock Whitepaper

Contrary to what you may have read or heard, crime does indeed pay. And the numbers show that cybercrime pays best of all. According to the FBI Internet Crime Report for the year 2010, more than 300,000 people were victimized over the Internet, netting cyber crooks $1.1 billion in the U.S. alone.[i] On the other hand, these more than 300,000 complaints resulted in just 1,420 criminal cases that produced a paltry six convictions. You can do the math.

Sure beats robbing a bank at gunpoint.

The numbers cited above actually belie a trend indicating the security industry is making substantial progress in the fight against internet-related crime. Exhibit "A" is Verizon's respected and widely read *Data Breach Investigations Report* (DBIR), prepared with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit. For the third year in a row this report showed a huge drop in the number of records compromised. From 361 million records in 2008 to 144 million in 2009 to just 4 million in 2010.[ii]

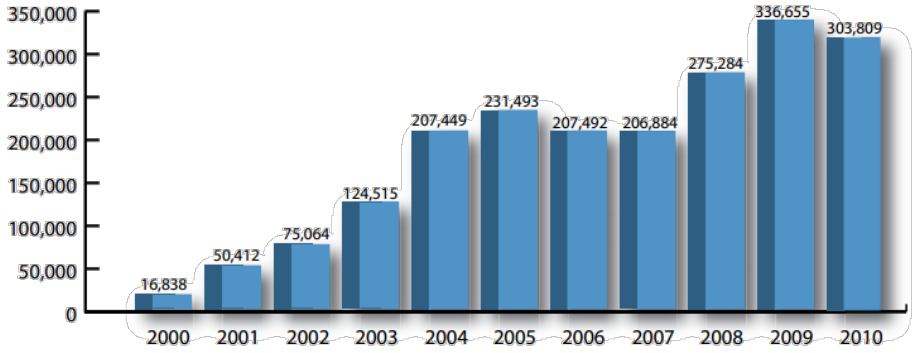
THE CYNIC'S PERSPECTIVE

But the DBIR dismisses the idea of such dramatic industry progress in such a short timeframe. It states that "cynics might argue cybercriminals were just as active and successful in 2010, yet the breaches were never discovered." Additionally, the report notes that while the number of compromised records fell dramatically, the number of "investigated incidents" was at an all-time high.

The DBIR goes on to explain what is mainly behind the improving numbers. Its authors reason that the recent prosecution and imprisonment of a handful of cybercrime kingpins – men collectively tied to many of the largest data heists in recent history – has had a positive effect. The result of which has deterred the criminal community's "B List" from going after big, high-profile scores.

After all, it's hard to live the good life when you're behind bars.

Yearly Comparison of Complaints Received via the Internet Crime Complaint Center



INDICATIONS ARE THAT THE CRIMINAL ELEMENT HAS SHIFTED ITS FOCUS TO SMALL BUSINESS.

Small to mid-size businesses (SMBs) make up 97 to 99 percent of all the businesses in the world. As the driving force of the global economy SMBs have valuable financial, intellectual and information assets. At the same time, according to the 2007 National Federation of Independent Business (NFIB) and VISA USA survey of small businesses –

- **57%** do not see securing customer data as something that requires formal planning
- **39%** say they rely on common sense to keep data safe
- **61%** have never sought out information about how to properly handle and store customer information. [iii]

The findings of the NFIB and VISA USA survey are confirmed by data in the Verizon DBIR showing that:

- **92%** of data breaches stemmed from external agents
- **92%** of attacks were not highly difficult
- ***96%*** *of breaches were avoidable through simple or intermediate controls*

Probably the most telling DBIR numbers that speak to the vulnerability of small businesses and shifting criminal focus are these: Of the 759 data breaches reported on, 482 of them – nearly 64% – involved organizations with between 1 and 100 employees.

Given the state of the market and actual results revealed above it's easy to see why SMBs – and their websites and customers – make such rich and vulnerable targets for data breaches and cybercrime.

For instance, assume for the moment you're not one of the "good guys" and that you have the moral ambivalence and necessary skills to rake in a huge income that affords you a lavish lifestyle. Given the facts and figures we've just presented would you rather go after the lucrative but much more heavily fortified vaults of the Global 1000 or the abundant orchards and low-hanging fruit (pardon us for mixing our metaphors) of the SMBs?

We thought so.

REAL WORLD EXAMPLES, AND CONSEQUENCES, OF LAX WEBSITE SECURITY

- In June of 2011 attorney Matt Passen of Passen Law Group, a two-man personal injury practice, clicked to the homepage of his website. Instead of its usual appearance he saw a series of letters and numbers that made no sense to him. Soon thereafter he received notification from Google that his website was infected and that the search giant had blocked access to it.

  After a couple of thousand dollars in expenditures, two failed fixes and an indeterminate number of lost business opportunities Passen's website was finally clean, secure and back in Google's good graces. [iv]

- In 2006 and 2007, Burger Me LLC in Bellingham, Wash. had its computerized cash register hacked and the cybercrooks made substantial fraudulent charges on the credit cards of Burger Me's customers. This led to the credit card company shutting down Burger Me's account and putting a hold on thousands of dollars of payments owed to it.

  By late 2008, the owner, Rich Griffith, no longer able to accept credit cards and burdened with debt from the hack – $12,000 for investigation and remediation costs alone – was forced to shut down his business.[v]

- Victor Tella had his e-commerce website infected with malware in 2010. So he subscribed to a site protection service offered through his hosting company. The service removed the malware and secured his website. So he thought. Ninety days later his site was hacked again.

  Victor contacted his hosting company but it had no clue about the most recent attack. (NOTE: Website security software and services can vary widely in their effectiveness.) After having to temporarily shut down his business and experiencing considerable stress, Tella engaged a new website security company and his site has been secure and malware free ever since.[vi]

- In March of 2011 copywriter and marketing consultant Ernest Nicastro was alarmed when he received an email from Google stating that it had blacklisted his website. After several days of lost productivity and client projects on hold while trying to resolve the issue himself, he contacted a security consultant. The consultant removed the malware and secured Nicastro's website, explaining that his failure to keep current on his Wordpress updates had left his site vulnerable to infection.[vii]

Unfortunately, there's money to be made, and taken from small businesses, in these and similar attacks.

A 2007 research report by the Yankee Group entitled *Trust Marks: What's Behind the Label Counts,* states that among SMBs reporting incidents, 30% pegged the financial loss due to the breach at more than $500,000.

IF YOUR WEBSITE IS ATTACKED… "IT'S NOT PERSONAL. IT'S BUSINESS."

The first fact you need to know is that if your website is attacked the overwhelming (92% according to the DBIR) odds are that – to quote Michael in *The Godfather* – "It's not personal, it's business." That's because the attacks are usually powered by spider-like automation technology that crawls the web looking for website vulnerabilities. When a vulnerability is found, it is exploited.

This is what happens in many instances of website infection. A spider crawls a site, finds an opening and lets itself in. It's analogous to a burglar trolling your neighborhood and testing the front door of every home. The homes with unlocked doors are the ones he robs. Today, this prevalent and widely used attack technology is responsible for the distribution of most malware. To give you an idea of how prevalent and widely used it is consider the following:

> According to one report IBM's X-Force security division monitored and blocked fewer than 10,000 such attacks per month in early 2008. By mid-2009 it was blocking more than 500,000 per month.[viii]

To that we say, good for IBM and its clients. But venture to add that most small businesses can't afford a monthly security contract or the resources necessary to implement a solution with IBM.

THE TOP TWO HACKS THAT ACCOUNT FOR MOST WEBSITE ATTACKS

Security industry research, incident reports and investigations, and our own experience show that two specific hacks account for the majority of all attacks:

1. **Cross-Site Scripting (XSS)** – XSS, often used for spam or phishing attempts and web browser exploits, makes it easy for hackers to distribute attacks on a wide scale. In XSS the attacker, disguised as a trustworthy source, inserts malicious coding into a link. Clicking on the link causes embedded programming to be submitted as part of the client's Web request. This programming can then execute on the user's computer, enabling the attacker to steal information.

   Most successful XSS hacks occur because web applications that generate pages dynamically, fail to validate user input and to ensure that pages generated are properly encoded. To protect against XSS, we recommend that all Web applications include appropriate security mechanisms and validate input as a matter of course.

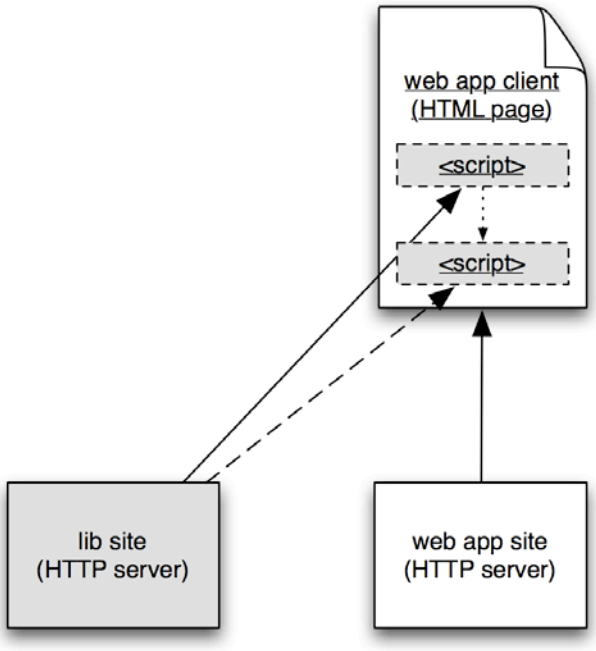
2. **SQL Injection (SQLi**) – In SQLi, the attacker injects Structured Query Language (SQL) code into a web form to gain access to resources or make changes to data. SQLi can be used to overwrite a database and redirect visitors to a malicious site, take control of a website, or for massive database theft. With the advent and rapid proliferation of automated SQLi programs both the likelihood and potential damage of a successful attack has increased enormously. Plus, the fact that SQLi attacks the Web application, which is the business owner's responsibility, and not the Web server, managed by the hosting provider, puts the site at even greater risk.

   If an attacker can find just one SQLi vulnerability in an application, state HP's researchers, "there's a very good chance they can compromise it completely." [ix]

In Hewlett-Packard's *2011 Mid-Year Top Cyber Security Risks Report*, results from analysis and testing of 236 unique applications showed that a full 69% of them contained at least one SQLi flaw.

In time, the prevalence of these attack modes may diminish. Yet, it is likely that others will replace them and we will see the continued proliferation of even more proficient and harmful attack methods. For supporting evidence we offer this from Microsoft's February, 2012 Security Intelligence Report, The Evolution of Malware and the Threat Landscape – a 10-Year review:

> "At the end of 2001, approximately 60,000 forms of malware or threats were known to exist...Over the last decade, the proliferation of malware has become an online crime story. Today, estimates of the number of known computer threats…range into the millions. "[x]



ACTIONS TO TAKE TO KEEP YOUR BUSINESS AND ITS WEBSITE FROM BECOMING A VICTIM

As has been the case for ages, small businesses operate in a world that is full of opportunity and rewards and at the same time fraught with challenges and risks. Today our "connectedness" plays a huge role in both. Opportunity, for many businesses, exists throughout the world; and if a business has a website – as most do – there exists also a financial risk that can emanate from any corner of the world.

So in concluding this white paper we offer you key tips about how to lock out the bad guys – wherever they may be – and substantially lessen the financial risk to your business. We'll start with seven recommendations from StopBadware, a SiteLock strategic alliance partner and standalone nonprofit organization that began as a project of the Berkman Center for Internet & Society at Harvard University.

ESSENTIAL TIPS TO PROTECT YOUR WEBSITE

1. Never store credentials, like your FTP password, on your local PC.
2. Use strong passwords and try to set up difficult-to-guess usernames (such as "av21Bx" instead of "Alex").
3. If you use FTP, consider switching to a more secure solution, like ssh/SCP/SFTP.
4. Make sure to check your website frequently for web application vulnerabilities and malicious code. Vigilance can protect your visitors.
5. Install only reputable plugins. Make a list of all third party plugins you use, and be sure to update them regularly. Both the software you use to run your website and all your plugins should be kept current!
6. Set appropriate file permissions on your web server.
7. Make sure you regularly scan your local PC with at least one, and preferably more than one, antivirus engine. Antivirus software for your PC won't detect website infections, but using an infected local machine can cause a website to become infected, so it's important to protect your PC, too![xi]

To these seven we add five essential operational tips:

8. Maintain clear, unambiguous and written company policy that spells out how and when employees can access the Internet.
9. Maintain clear, unambiguous and written company policy for employees who access the computer system from home or a mobile device.
10. Scan your website for vulnerabilities and malware!
11. Update all applications and plug-ins to latest stable version.
12. Leverage additional security features for third-party, open source applications you may be using such as WordPress, Joomla, osCommerce, or other content management, blogging, or e-commerce solutions.

WHY MANY SMBS ARE SEEKING OUTSIDE HELP TO FULLY SECURE THEIR WEBSITES.

Three main factors are causing many SMBs to seek outside help to secure their websites:

1. The proliferation and increasing sophistication of hacking technology
2. The risk of substantial financial loss, a crippled business and a damaged reputation
3. The lack of IT staff, staff expertise, or both.

We've covered the first two, and as a small business owner or executive you're probably familiar with the third factor. According to a 2008 survey by CDW, a leading provider of software, hardware and services to small business , only 9% of the small businesses (5 - 99 employees) surveyed had a full-time IT professional on staff.[xii]

According to another study of SMBs:

- **22%** have a total staff of 1-2 people
- **27%** have 3-9 people
- **58%** in the U.S. have fewer than 10 IT people on staff with the percentage for Canada and Germany coming in at 69% and 81%.[xiii]

Even those SMBs with larger, more experienced IT staffs often lack a dedicated or centralized security team. To combat this lack of staff and expertise, and the Web's criminal element, more SMBs are enlisting outside help in their security efforts.

Google "website security" and you'll find that you have a multitude of vendors to choose from. As pointed out earlier though, website security software and services can vary widely in their effectiveness. That said, here are five factors to keep in mind as you sift through your search results:

1. **Response time** – Once you receive the dreaded Google blacklist notification, every hour you go without a successful resolution can be costly to your business, to your business reputation and, depending on the situation, to your customers. A rapid and appropriate response is the key to preventing or minimizing financial loss, productivity and opportunity loss, downtime, damage to your business reputation and other negative consequences.

   Also, at such a critical and stressful time, you will want the reassurance that only a real-time conversation with a skilled security expert can give you. So make sure that this option is part of any security package you consider.

2. **Designed with the small business in mind** – As noted earlier, many small businesses have minimal to no IT staff, and even then that staff may be lacking in IT security expertise. So it's important that the solution be easy to use and the technology intuitive and easy to grasp.

3. **Scalability** – Depending on the stage of growth your business is in and the type of business you do the level of functionality and service you need varies widely. If you're a lawyer, an accountant, a medical practice, an insurance agency or some other services organization that doesn't transact online business a basic level of service or program that continuously scans your site for malware will probably suffice.

   On the other hand, if yours is a highly interactive e-commerce site that generates a substantial number of credit card orders every day you'll require a much more robust solution. Or maybe you've just launched your business with a basic website but your business plan calls for adding e-commerce capabilities by next year. In that case, you'll want a solution that can accommodate your plans for growth.

4. **Hosting environment** – Ideally, your security solution will function equally well in any hosting environment your website finds itself in. For example, many small businesses sites are hosted in a shared environment, so called because a number of sites will share space on the same server. It's less expensive, less headache and suits the customer fine.

   At any rate, the same equipment may serve 50, 500, 1,000 or a few thousand websites depending on the hardware and the host company. Now some security products are programmed to scan 30,000 – 40,000 times a day and that can cause problems. Case in point: If you get multiple sites on the same server with identical activity your hosting company may throttle down your site, making it slow to use. In some instances, your host may make you upgrade to a more expensive hosting plan or even shut your site down. Having an effective, but lightweight solution is of critical importance in these cases.

5. **Proactive, total solutions capabilities** – Malware is a dangerous and serious security problem that can hurt your website and your business. At SiteLock we get a lot of our business from small businesses that get malware on their site (we cleaned over 1,000 small business websites in 2011 alone), receive the dreaded Google email and come to us to get them off the blacklist. We do that. But it's only part of the security solution, not a fully functional security solution.

   What you want to look for as you sift through your Google search results is a solution provider that will not only help you fix your site when something goes wrong but also help you be proactive about security to keep things from going wrong in the first place.

In this white paper we've done our best in a relatively few pages to increase your awareness about a very serious threat to all businesses and especially small businesses. We have laid out the problems and tried to give you not only an overview of the solutions but point you in the direction of a few specific remedies. In this effort it is our sincere wish that we have pointed you in the right direction. Thank you for reading.

About SiteLock

Established in 2008, SiteLock has helped small businesses protect their websites and reputations through website security services and scanning. Founded on the principle that effective website security should no longer be an expensive and unattainable goal for small to midsized businesses, SiteLock offers the most affordable and complete website security solution available on the market, protecting against malware, spam, viruses and other vulnerabilities. SiteLock differentiates itself from all competitors by also offering on-demand expert services, maintenance plans, website design and hardening.

Using one of a kind technology developed by seasoned security and business veterans, SiteLock currently protects over 500,000 customers worldwide and scans over 2 million web pages daily for threats. SiteLock's 360-degree scanning provides the ultimate protection while still being light enough to not affect a server's performance, as many of SiteLock's customers are online merchants that rely on their website as their business storefront. These services, available to all SiteLock members, can fix identified issues and keep website owners up-to-date on newly developing threats. Each subscription to the service includes SiteLock's Trust Seal, which is proven to increase sales and conversions by more than 10%. SiteLock is headquartered in Jacksonville, Florida and has offices in Scottsdale, Arizona.

Contact SiteLock
Website: www.sitelock.com
E-Mail: support@sitelock.com
Toll Free: 877-257-9263
International: 415-390-2500

SiteLock™
Security for Small Business

Sources

[i] *Internet Crime Complaint Center, 2010 Internet Crime Report,* *http://www.ic3.gov/media/annualreport/2010_ic3report.pdf*

[ii] *Data Breach Investigations Report,* *http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf*

[iii] *Small Businesses Recognize Importance of Data Security, but Lack Formal Plan for Addressing, New Survey Shows* *http://corporate.visa.com/newsroom/press-releases/press687.jsp*

[iv] *New cyberattacks target small businesses, USA Today, 7/4/2011,* *http://www.usatoday.com/tech/news/2011-07-04-small-business-cyber-attackss_n.htm*

[v] *Hackers Shift Attacks to Small Firms, Wall Street Journal, wsj.com, July 21, 201,* *http://online.wsj.com/article/SB10001424052702304567604576454173706460768.html*

[vi] *Sitelock.com website, Testimonial,* *http://www.sitelock.com/company-testimonials.php*

[vii] *Interview with Mr. Nicastro.*

[viii] *New cyberattacks target small businesses,* USA Today, *7/4/2011,* *http://www.usatoday.com/tech/news/2011-07-04-small-business-cyber-attackss_n.htm*

[ix] *The 2011 Mid-Year Top Cyber Security Risks Report,* *http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-7045ENW.pdf*

[x] *The Evolution of Malware and the Threat Landscape – a 10-Year review, February 2012,* *http://www.microsoft.com/security/sir/story/default.aspx#!10year*

[xi] *5 reasons why websites are hacked and blacklisted, February 21, 2012 StopBadware Blog,* *http://blog.stopbadware.org/2012/02/21/5-reasons-why-websites-are-hacked-and-blacklisted/*

[xii] *2008 CDW Small Business Driver's Seat™ Report, April 29, 2008.* *http://webobjects.cdw.com/webobjects/media/pdf/2008-CDW-Small-Business-Drivers-Seat-Report.pdf*

[xiii] *Webroot State of Internet Security: Protecting Medium & Small Businesses* *http://www.webroot.com/pdf/StateofInternetSecurity_SMB1007.pdf*