Combating Small Business Security Threats: How SMBs Can Fight Cybercrime

“The fact is that cybercriminals are now focusing their attention on small and mid-sized businesses because they are typically easier targets than large, multinational corporations”

– Martin Ward
McAfee

When hackers breach the defenses of huge organizations like Amazon, Apple or Citibank, it makes the news. When the same cybercrime exploits hit small and medium businesses (SMBs), it rarely rates a mention, but that doesn’t mean small businesses don’t get hacked, or that the impact on these SMBs is small.

In fact, quite the opposite. Nearly 72 percent of data breaches investigated by Verizon Communications’ forensic analysis unit in 20111 were at companies with less than 100 employees. And the trend of targeting SMBs is only increasing: The number of daily targeted attacks specifically aimed at small and midsize businesses more than doubled in the first six months of 2012². The financial impact of these incursions is enormous: reports estimate the cost of global cybercrime at $114 billion annually; significantly more than the annual global market for marijuana, cocaine and heroin combined³.

Small and medium businesses are in the cybercrime crosshairs largely because many SMBs lack the time, budget and expertise to coordinate an effective security solution and are easy targets to cybercriminals. They are also a much easier target for cybercriminals than a large multinational corporation, in part because many have a simplified notion of their network security risk: If all the computers are running up-to-date antivirus software, what could go wrong?

Well, plenty.

This white paper examines the rising security threat that puts small and medium businesses at risk, and in light of these threats, evaluates important security considerations that SMBs should be aware of. The white paper concludes with a discussion of a layered approach to security protections, and the tools and technologies that SMBs should consider when building defenses against cyber attacks.

SMBs: Cybercrime Targets or Peripheral Victims?
Some small business owners may take comfort in the illusion that their operations are too inconsequential to attract attention from international cybercriminals, who instead target global banks, Internet retailers, or government entities to harvest their databases of credit card numbers, client passwords, and account information.

But as security protections used by major corporations and governments grow in power and sophistication, small businesses increasingly find themselves in the bull’s-eye.

In fact, some cybercriminals may prefer to target small businesses, particularly in instances when SMBs deliver services and products to larger corporations and government agencies. A small business with lax security controls can serve as a backdoor into the data banks of an otherwise well protected enterprise.

Even a less high-profile business can find itself a target—dry cleaners and neighborhood restaurants are high-volume businesses with many credit and debit card transactions to mine. Gaining access to a small business store of customer email addresses can also be a goal. Know-
ing where individuals shop or bank can be extremely valuable ammunition for email phishing exploits, as botnets can blast out sophisticated email messages that are branded by the company they are stolen from and personalized with knowledge of the individual’s retail shopping habits, all the better to spoof the recipient into providing personal information.

Most SMB owners or managers are busy running their businesses, without a lot of time to dedicate to fine-tuning their security configurations; or to installing the latest updates; or considering if they have enough, or the right kind, of security protections for the scope of their operations. The result: To a professional hacker, SMBs are low-hanging fruit. Many small businesses believe they are fully protected while in fact they are much more exposed to attack than a larger enterprise with dedicated security management.

Best Practices to Boost SMB Security

Cybercriminals use extremely sophisticated technologies in their attempts to breach security defenses. Yet some of the strongest protections against hackers can be low-tech, common sense actions that seal up vulnerabilities at little or no cost.

• **Update software.** Make sure both software updates and antivirus programs are current. Malware is constantly evolving to take advantage of vulnerabilities in software, and so are patches and fixes that repair the weakness. But these do no good if updates aren’t applied.

• **Educate employees.** Make sure that employees are educated to never open unknown attachments in emails or click on unknown links. Web- and email-based threats are growing very quickly – in the first half of 2012, web-based malware infections grew 400 percent over 2011, and email-based attacks grew 56 percent from the first to the second quarter of 2012. While a web security solution should be now near mandatory for SMBs, preventing behaviors that put systems at risk remain very important.

• **Be careful of social media.** Sites like Facebook can be important marketing channels for SMBs. But be careful. Malicious code is increasingly injected into social networking sites, including harmless-looking links, advertisements and game apps. On Twitter, shortened URLs make it impossible to recognize if links are legitimate; retweeting the links helps spread the infection.

• **Employ stringent password policies.** For workers within a small business with access to financial or personal data, be sure to use different passwords to access these accounts and programs than are used for more general login purposes. Require that employees change passwords on a regular basis, using a mix of alpha and numeric characters that do not resemble words, so that exposure from any password theft is time-limited.

• **Limit access to financial data.** Minimize the number of people who have access to sensitive financial or personal content—the fewer the number of people who have log-in credentials to this data, the harder it is to hack in.

• **Be wary of downloaded apps.** Be alert when buying and installing applications from online app stores. If these apps will run on the business networks or smartphones, be certain the app store is reputable and has sufficient security protection in place. Downloadable apps infected with malware have become a major source for network infiltration.

Evaluating the SMB Digital Footprint

Computing networks at most small and medium businesses are much more complex than they were just five years ago. However, in many cases, internal security protections at SMBs have not evolved to keep up with these changes.

SMBs need to look at the full digital footprint of their business and follow the internal path of data or sensitive information. Is business data moving onto mobile devices? Are employees using private tablet computers to access internal business websites? Is financial or personal data being moved onto the cloud?

If the answer to any of these questions is yes, then antivirus software is of only very limited efficacy in keeping data and networks safe.

Most small businesses today employ three distinct computing infrastructures: tradi-
tional on-premises networks; smartphone and mobile networks within the business environment; and cloud services. Each of these must be accounted for in a comprehensive security strategy to ensure that the SMB has edge-to-edge protection.

- **On-premises networks.** Antivirus software is no longer sufficient to protect network infrastructures from cyber attack. New generations of malware can lodge beneath the level where operating software (OS) based antivirus protections can detect and eliminate them. McAfee detects 3,500 new rootkits daily, which are designed to subvert the OS and commandeer slave machines to steal data or act as mindless botnets remotely driven to attack other devices.

- **Mobile devices.** SMBs need to evaluate how smartphones and tablets are being used within the network infrastructure. Are mobile devices used to access business email? Are mobile phones used as Internet hotspots for credit card transactions? Are tablets used to access internal websites containing sensitive information? If access to internal websites is not secured or the data on these mobile devices is not encrypted, they constitute enormous security vulnerabilities.

- **The cloud.** SMBs are generally ahead of the crowd in taking advantage of cost-effective public cloud services. But businesses need to evaluate what they are using the cloud for—are they storing financial data remotely? If SMBs are uploading sensitive data to the cloud, then they need to determine the level of protection that this data demands and ensure that the cloud services provider meet these requirements. Ask what level of encryption is used to protect the perimeter of their cloud. Ask about physical security procedures that providers follow in their own environment: Who has access to the data center? At least every six months, SMBs need to take a look at their technology footprint and make sure that any new devices, services, or user scenarios are covered by a comprehensive edge-to-edge security strategy. If not, they need to expand their security solutions accordingly.

**What to Look for in New Security Solutions**

The bad news: Security threats are growing increasingly sophisticated. The good news: So are security technology defenses.

Antivirus is a fundamental defense for protecting SMBs against attack, but it is by no means sufficient on its own. For more complete protection against today’s security threat, SMBs must develop a layered approach to security, in which multiple forms of anti-malware protections are integrated for maximum protections. A layered security solution should ensure the following safeguards are in place.

- **Web protections.** Just visiting websites can be dangerous with web-based

---

**WHY SMALL AND MEDIUM BUSINESSES ARE AT RISK**

### Business Transactions

- **Only 38%** of SMBs personally examine monthly business transactions
- **38%** of SMBs exclusively use a personal account for their business

### Staff Concerns

- **Only 5%** conduct background checks on new hires
- **Just 3%** train employees on safe workplace Internet usage

### Internet Security

- **Only 18%** run antivirus software designed specifically for business
- **43%** take no Internet safety precautions at all
Combating Small Business Security Threats: How SMBs Can Fight Cybercrime

threats like phishing, social engineering, and drive-by websites seeking to corrupt infrastructures, steal identities, or enslave computers as part of "bot" networks. Web protection technologies are necessary to secure gateways to the Internet, restrict potentially harmful web traffic before it enters the network, and to filter incoming web content to ensure it is free from malware and exploits.

- **Email protections.** Email is another potential venue for delivery of malware and unwanted communications. Integrated email protection technologies can stop spam, phishing messages, and other email-based threats before they reach the network.

- **Data protections.** Sensitive and confidential data can reside in endpoint hard drives, in networked storage, or in the cloud. Dynamic data protection technologies provide multilayered protection for information no matter where it resides, and systematically block unauthorized access to critical data and prevent information leakage or theft.

- **Mobile protections.** Mobile Device Management (MDM) technologies secure mobile devices with encryption and password protections plus let administrators remotely strip data from devices if they are lost or stolen. MDM solutions can also be employed to manage and secure work-from-home scenarios and provide a blueprint for introducing employee-owned devices into the business network. Token-based network authentication, in which time-limited, randomly generated tokens are used in place of usernames and passwords for network access, are broadly available and affordable, and add another layer of security, particularly for off-premises workers.

These security features are available in integrated, all-in-one solutions from a variety of security software specialists, or can be procured as best-of-breed technologies from separate vendors. If deployed separately, be sure to have an MSP or security specialist integrate the systems; simply running them on top of each other can create vulnerabilities of its own.

**The future: Layered Security**

For SMBs, the security future isn’t just doom and gloom. There is good news—real progress is being made to reduce the threat of malware and other risks to computing security.

Security technology is moving away from reactive defenses such as antivirus software and toward more proactive, multi-layered protections that block malware intrusions before they enter the network. Rootkits and other malware that are designed to evade OS-based antivirus protections can be defeated with new hardware-based security solutions. These defenses operate at the firmware level and can detect and isolate rootkits before they activate.

Talk to your MSP or local security expert about the new generation of multi-layered security solutions specifically designed for SMBs, such as always-on, always-up-to-date cloud-based offerings, or edge-to-edge systems that can be customized to specific needs and environments. Real progress is being made in SMB security and it’s time to move forward.

**BROUGHT TO YOU BY**

This white paper is brought to you by McAfee and Intel, who are working together to develop comprehensive, cost-effective security solutions for small and medium businesses. If you’d like to learn more about protecting your data from theft and compromise, please visit www.intelhybridcloud.com/mcafee.html or www.mcafee.com/endpoint for more information.

Do it today, before your business becomes one of the statistics.

For more information on McAfee Endpoint Protection Suite, visit intelhybridcloud.com/mcafee.html

---

2. More than a third of global targeted attacks are aimed against small businesses
3. Study Calculates Cost of Global Cybercrime: $114 Billion Annually
4. Cracking the Code on Password Protection
5. Cyberattacks up 400% since 2011

**INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL’S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked “reserved” or “undefined.” Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel’s Web site at www.intel.com.

Copyright © 2012 Intel Corporation. All rights reserved. Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the United States and other countries. 

* Other names and brands may be claimed as the property of others.