The data risks of SMBs

Last year, 60 percent of all targeted cyberattacks struck small- to medium-sized businesses, most of which admit they are woefully unprepared for warding off breaches.

ebook
An SC Magazine publication

Sponsored by
Symantec. | Website Security Solutions

SMBs

Easy target

Experts suggest immediate tactics budget-conscious organizations can implement to minimize exposure. Larry Jaffee reports.

It's generally accepted that small-to-medium sized businesses (SMB) drive the nation's economy, create more new jobs than the Fortune 500, and account for about 50 percent of the Gross Domestic Product. Yet only about 50 percent of startups make it past year five, and while they're bootstrapping their way by cutting corners, it's unlikely IT security is a major priority.

It's not surprising then to learn 61 percent of small businesses reported last year they were victims of cyber attacks within the past 12 months, according to the National Small Business Association. And separately Symantec reported 60 percent of all targeted attacks in 2014 struck SMBs.

Despite a steady stream of news headlines about major corporate network hacks, and the negative publicity, brand damage and hit to the bottom line, SMBs are slow to adapt preventative measures, or are incapable to do so with their existing financial and personnel capabilities.

OUR EXPERTS: Data risk SMBs

James Chappell, CTO, Digital Shadows
Derek Gabbard, CEO, FourV Systems
Tom Gorup, security operations manager, Rook Security
Paul Henry, IT security consultant, Blancco Technology Group
Paco Hope, software security consultant, Cigital
Amandeep Lamba, director, cybersecurity and privacy, PwC
Jonathan Niednagel, CEO, Datum Security
John Prisco, president & CEO, Triumfant
Feris Rifai, founder & CEO, Bay Dynamics
Jacob Williams, chief scientist, CSRgroup

"These organizations often have fewer resources to invest in security, and many are still not adopting basic best practices like blocking executable files and screensaver email attachments," stated Symantec's 2015 Internet Security Threat Report. "This puts not only the businesses, but also their business partners, at higher risk."

SMBs that service large companies need to shore up potential IT security weaknesses if they want to keep those key customers so critical to the lifeblood of their business.

Consider what happened to Target, whose major breach in November 2014 resulted from attackers gaining network credentials from a Sharpsburg, Penn.-based, third-party vendor. Just how Fazio Mechanical Services, which specializes in air conditioning/heating/ventilation services, first became compromised is still not publicly known, and the federal investigation continues.

Fazio Mechanical's "data connection with Target was exclusively for electronic billing, contract submission and project management," according to the vendor, which clarified that it does not perform remote monitoring of or control heating, cooling and refrigeration systems for Target. The retailer is the only customer for whom Fazio Mechanical manages electronic billing, contract submission and project management on a remote basis.

On Feb. 6, 2015, Fazio Mechanical issued the following statement: "Our IT system and security measures are in full compliance with industry practices. Like Target, we are victims of a sophisticated cyber-attack operation. We are fully cooperating with the Secret Service and Target to identify the possible cause of the breach and to help create proactive initiatives that will further enhance the security of client/vendor connections making them less vulnerable to future breaches."

77%

of employees leave their computers unattended.

– Trend Micro, Ponemon Institute

Biggest data risks

So what is the biggest data loss risk for SMBs? Organization complacency, if you ask Amandeep Lamba, director of cybersecurity and privacy for PwC. "While many SMBs are taking steps to ensure that their processes work to meet their organization's functional requirements, security requirements are often left by the wayside," he says.

Furthermore, such SMBs suffer from a mindset that leads them to believe that they are not targets for potential data loss incidents, and this mindset impacts their basic security hygiene – patching, vulnerability management, data backups, and other basic components of a data security plan.

Amandeep Lamba, director of cybersecurity and privacy, PwC

Lamba cites TrendMicro data that found 65 percent of SMBs said that, in general, their organizations' sensitive or confidential business information is not encrypted or safeguarded by data-loss protection (DLP) technologies."

Malware delivered through social engineering is another huge risk, points out Tom Gorup, security operations manager for Indianapolis, Ind.-based Rook Security.

"Everyone is busy growing the company and emails are flying back and forth," Gorup describes of a typical SMB startup. "It would be quite easy to slip in a malicious PDF posed as a market

Immediate steps to take

Here are a handful of actions SMBs can take to protect themselves from a cyber attack, advises James Chappell, CTO of Digital Shadows:

Ensure software is patched and up to date at all times.

Develop and enforce some basic "rules of the road" for security, such as passwords, email and Web browsing.

If the business is reliant on a website or an online technology, it's worth investing in getting this tested by a certified professional penetration testing firm at least annually, but ideally more frequently. It will seem like a bigger expense, but it pays dividends if this is the core of your business.

Make sure that the administration of the IT systems is appropriately controlled. If the SMB doesn't have an IT supplier, some cloud services offer some strong security offerings. Both Google and Microsoft cloud products have some great features baked in such as two-factor authentication. Use these features and make the most of what is offered by your IT suppliers. Not all cloud services are born the same so if you don't know about the security of your current suppliers, get them checked out independently.

Back up and test the backups. Lots of small businesses this year have suffered from things such a crypto locker and other infections. If the data is backed up, you can recover well from these sorts of attacks.

If you operate retail systems, make sure that you get advice about the security of the suppliers' systems. Get the EPOS checked out by an independent reputable security company. There are numerous opportunistic attacks targeting these types of systems. Ask your key supplier what they are doing to protect against these types of attacks. Additionally, organizations like SANS produce guidance for securing small to medium enterprises.

80%

of organizations believe managing and monitoring end-user privileges and entitlements is the most important security measure against data breaches.

– Trend Micro, Ponemon Institute

study or financial report from a competitor. Without the proper people, processes, and tools in place, this could easily turn into a company-wide compromise."

Hence, education and awareness programs may be an investment of employee time, "but can be cheap in real dollars," says Gorup, who suggests monetary rewards for employees who identify phishing attacks and security issues that affect your organization. "It's a great way to extend your potentially limited security resources to a more guerrilla force," he adds.

The point of hire is the perfect time to let new employees know what is expected in terms of IT security. Such education can be couched in marketing terms, notes Gorup, such as "Secure yourself, secure your family," to ward off the dangers of social engineering and inadvertently divulging company information that can leave open a backdoor.

Tom Gorup, security operations manager, Rook Security

"Click an [unsolicited] email and you can give up your [company] credentials," he adds, which is why IT and HR need to work together to mitigate phishing risks. "HR speaks the language of the user. IT really doesn't know how to talk to people," says Gorup. The bottom line: "A company shouldn't tolerate that its employees are too busy to follow process."

Doing any kind of business on the Internet is risky enough, points out Paul Henry, IT security consultant with Blancco Technology Group, headquartered in Alpharetta, Ga. Henry is troubled by security holes that emerge from an attacker bypassing the gateway with spear phishing, a USB thumb drive or drive-by-malware that can easily move laterally across the inside of the network completely unchecked.

"This is why environments have already been compromised for up to two years, on

SMB concern

There are at least five data security threats that should concern every SMB:

1. Employee negligence puts an organization at risk. 77 percent of employees leave their computers unattended
2. SMBs aren't protected enough. 65 percent of SMBs said that, in general, their organizations' sensitive or confidential business information is not encrypted or safeguarded by DLP technologies.
3. Employee mobility may prove disastrous. 56 percent of employees very frequently or frequently stored sensitive data on their laptops, smartphones, tablets, and other mobile devices.
4. SMBs fail to routinely back up data. 62 percent of SMBs do not routinely back up data, and about a third of U.S. companies had no backup and disaster recovery strategies in place, citing lack of budget and resources as primary reasons.
5. SMBs do not enforce data security policies. 80 percent of organizations, regardless of size, believe managing and monitoring end-user privileges and entitlements is the most important security measure against data breaches.

Source: Trend Micro, Ponemon Institute

62%

of SMBs do not routinely back up data.

– Trend Micro, Ponemon Institute

average, before they've ever been detected," says Henry, who advises SMBs to properly instrument the network behind the firewall and hunt down the intruders. "So if malware was propagating from one desktop to another, do you have your network instrumented to see that behavior?" Henry asks.

> "...the types of credit cards, goods and personal information flowing through their business would be very attractive to a fraudster."
>
> *– James Chappell, CTO and co-founder, Digital Shadows*

The patchwork nature of computer systems that organizations rely on is another major risk, according to Paco Hope, software security consultant with Cigital, an application and software security consultancy headquartered in Dulles, Va.

"[The systems] tend to grow organically, so [companies] acquire, build, and integrate software from lots of different sources," Hope explains. "Obviously there will be security mismatches and security gaps where unrelated products and services interface with each other."

He notes SMBs often don't build much of their own software, except perhaps programs for their core competency. "So the security of an SMB's own software and its software ecosystem is more dependent on applying security across disparate products that have disparate capabilities. Often some insecure, lowest common denominator is used because it is the technique that works, not because it offers the best security," Hope adds.

Paco Hope, software security consultant, Cigital

Standardization and the proliferation of protocols and platforms is a double-edged sword for SMBs, he notes. "Attackers know how to exploit standard platforms and protocols and they automate the attacks. So the SMB that modernizes and leverages well-known technology will be more competitive – getting more done with less. But that same modernization will make them easier prey to attackers, unless they assiduously apply security best practices on every platform they integrate."

Customized security required

Identifying which assets are the most important for any particular business is critical in designing a data protection program. If it's a transaction-based company obviously the customers' credit-card numbers, for example, are the family jewels. But any personally identifiable information (PII), or proprietary intellectual property that makes a firm unique, could be valuable to attacker and should be considered to assess the risk.

"Each business is different based on their industry and what kinds of information they create, store, and/or process," says Derek Gabbard, CEO of FourV Systems, a newly formed data analytics firm, based in Baltimore, Md. FourV's parent company is SRC Inc., a research and development firm specializing in the intelligence and defense needs of government agencies. The size of the company shouldn't give SMBs a false sense of security, he adds.

It does not necessarily matter how many accounts an SMB has, for example, but who these accounts are, agrees James Chappell, CTO and co-founder of Digital Shadows, a San Francisco-based company with anomaly-detection technology. He cites a luxury boutique hotel that charges premium prices. "They may have few records, but the types of credit cards, goods and personal information flowing through their business

56% *of employees very frequently or frequently stored sensitive data on their laptops, smartphones, tablets and other mobile devices.*

– Trend Micro, Ponemon Institute

Government help for SMBs

The Department of Homeland Security, in conjunction with the Federal Communications Commission (FCC), has developed a tool known as the "FCC Small Biz Cyber Planner," which allows small businesses to create customized cybersecurity plans via an online portal.

The tool, notes Amandeep Lamba, director of cybersecurity and privacy for PwC, allows businesses to choose aspects of cybersecurity that they believe apply to their organization and quickly generate a plan that can help SMBs get off on the right foot with the planning of a well-defined security strategy.

The FCC also suggests the following tips for the budget conscious SMB:

- Train employees in security principles.
- Protect information, computers and networks from viruses, spyware and other malicious code.
- Provide firewall security for your Internet connection.
- Download and install software updates for your operating systems and applications as they become available.
- Make backup copies of important business data and information.
- Control physical access to your computers and network components.
- Secure your Wi-Fi networks.
- Require individual user accounts for each employee.
- Limit employee access to data and information, and limit authority to install software.

Source: Federal Communications Commission

would be very attractive to a fraudster," Chappell says.

Feris Rifai, founder and CEO of Bay Dynamics, a New York, NY-based firm specializing in threat detection, notes: "Hackers follow the least path of resistance. If that means getting into the mom-and-pop shop that does transaction processing for a regional bank, then so be it. Hackers do not discriminate based on size. They will leverage any means necessary, even if unorthodox, so long as it pushes the ball forward."

> "To think that a company isn't attractive because they're 'small' is just naive on the part of that company."
>
> – *Jonathan Niednagel, CEO, Datum Security*

Jonathan Niednagel, CEO of Los Angeles-based Datum Security, which specializes in advising SMBs in measuring and managing their security profile, agrees: "To think that a company isn't attractive because they're 'small' is just naive on the part of that company."

Most small companies are not hacked because of the data that they possess, , Niednagel points out, but rather the access that they provide to larger companies. "A small company with minimal cyber defenses represents an easy jumping-off point for hackers to get behind the real target's first line of defenses because they look like a trusted partner."

That's why intruders, who can be very patient, often go undetected for months or years. However, even basic security improvements by an SMB can reduce the probability of a breach by 86 percent, studies have shown, according to Niednagel. It's the difference in convincing an attacker that it's not worth their while.

SMBs often rely on cloud-based backup, but such vendors are cognizant of their absolute need to take all precautions in protecting customer data, which at the very least should be encrypted.

65%

of SMBs said their organizations' sensitive or confidential business information is not encrypted or safeguarded by DLP technologies.

– Trend Micro, Ponemon Institute

Protection on a budget

It behooves small- to medium-sized enterprise (SME) grappling with small security budgets to identify steps that can be taken to mitigate the threat of an attack.

Examining a potential compromise in advance is important because recommended security controls must be within financial reach (measured both in capital and human costs), advises Jacob Miller, in a white paper published by the SANS Institute (http://tinyurl.com/p7eznc6).

Miller, chief scientist at CSRgroup computer security consultants, recommends that SMEs prepare for intrusions by implementing the following controls:

- Device inventory
- Software inventory and vulnerability assessment
- Log aggregation and review and event correlation, possibly using a security information and event management (SIEM) system
- Host-based intrusion detection systems (HIDS)
- Threat intelligence

Each SMB has to identify for themselves which assets they have that are the most valuable to them and which assets they have that are of the most value to someone else, points out Gabbard. "SMBs sometimes are stepping stones to the real targets of interest," he says, citing the Target breach.

> "Anti-virus today is just reducing the noise level."
>
> – *John Prisco, president and CEO, Triumfant*

In general, organizations rely too heavily on anti-virus software to solve their security problems, believes John Prisco, president and CEO of Triumfant, a Rockville, MD-based malware and exploit detection firm. "Anti-virus today is just reducing the noise level. Typically, these software programs are only able to detect about 20 percent of attacks that are occurring and are limited to identifying known threats," he says.

John Prisco, president and CEO, Triumfant

Free anti-virus products from Avast, Microsoft Security Essentials, AVG, and Ad-Aware, Prisco believes, does as good a job as paid products. "Take the money that would have been spent on anti-virus per-computer per year and pay a managed-service provider (MSP), which might give the ability to have anomaly-based detection that could find zero days. Then you really get sophisticated (defensive technology) at a low cost."

A benefit of an anomaly-based detection scheme is that it comes with basic cyber hygiene, such as continuous patching, he notes. "That's a reasonable approach when you have a limited budget."

Prisco believes a large data risk involves employees, administrators and executives relying on simple passwords to protect their companies' information, including human resources, benefits and banking and financial records.

"These days, processors can cycle through a near-infinite amount of character combinations in no time, so a password is almost useless," Prisco says, advocating a must-do for all organizations:

29%

of IT pros at organizations with 250-499 employees are the least likely to strengthen server security.

– CloudEntr, "2015 State of SMB Cybersecurity."

For additional reading:

1. "2015 State of SMB Cybersecurity Survey," CloudEntr, 2015
   http://tinyurl.com/pa3wkgv
2. "Practical Threat Management and Incident Response for the Small- to Medium-Sized Enterprises," SANS Institute, 2014
   http://tinyurl.com/p7eznc6
3. "5 Data Security Risks Every Small Business Should Know About," Trend Micro, 2012
   http://tinyurl.com/qy8oqg4
4. "Easy Guide to Comprehensive IT Security Strategies for SMBs," CoSoSys, 2008
   http://tinyurl.com/noga9qt

two-factor authentication – a password plus an authentication code.

He explains the majority of security innovation is geared toward larger enterprise buyers that tend to be early adopters of advanced security technology. "This often means security solutions for downstream markets are antiquated, limited or are out of reach financially," Prisco points out.

Wake-up call

CloudEntr's 2015 report on SMB Cybersecurity, based on 438 responses, offered some sobering glimpse of how ill prepared collectively organizations are to ward off attacks amid the trend toward workplace usage of unsecure BYOD devices:

IT pros at organizations with less than 50 employees are the least likely to invest in security software tools (14 percent), and those at organizations with 250-499 employees are the least likely to strengthen server security (29 percent).

IT pros at smaller organizations are more concerned with hackers getting in through servers than those at larger organizations, which aligns with their plans to strengthen server security.

The report found that SMBs are relying more and more on web and cloud-based services to scale their businesses, reduce costs, enable mobility and increase employee satisfaction. However, respondents pegged employees to be the weakest link across all industries in security infrastructure as a result of attackers' social engineering tactics to abscond with data.

> "... downstream markets are antiquated."
>
> – *John Prisco, president and CEO, Triumfant*

If that's not enough incentive for your organization to heed the wakeup call, how about this scary thought? While banks generally cover individuals' fraudulent credit card charges, the same is not true for small businesses.

To sum up, Chappell sees SMBs as "almost permanently exposed to opportunistic threats by virtue of the unmanaged and secondary priority assigned to security. They are essentially low hanging fruit for attackers." ■

For more information about ebooks from SC Magazine, *please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

14%

of IT pros at organizations with less than 50 employees are the least likely to invest in security software tools.

– CloudEntr, "2015 State of SMB Cybersecurity."

Sponsor

Symantec. | Website Security Solutions

Symantec Website Security Solutions include industry-leading SSL, certificate management, vulnerability assessment and malware scanning. The Norton™ Secured Seal and Symantec Seal-in-Search assure your customers that they are safe from search, to browse, to buy.

For more information, please visit www.symantec.com

Masthead

EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com
ASSOCIATE EDITOR Teri Robinson
teri.robinson@haymarketmedia.com
SPECIAL PROJECTS EDITOR Stephen Lawton
stephen.lawton@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com
PRODUCTION MANAGER Krassi Varbanov
krassi.varbanov@haymarketmedia.com

SALES
VP, PUBLISHER David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
REGION SALES DIRECTOR Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*
WEST COAST SALES DIRECTOR Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*