RISETECH
PARTNERS



KEEPING SMALL BUSINESSES SAFE:

COMBATING CYBERCRIME ON A SMBS BUDGET

https://www.risetechpartners.com

KEEPING SMALL BUSINESSES SAFE:

COMBATING CYBERCRIME ON A SMBS BUDGET

WHAT HAPPENS ON MAIN STREET STAYS ON MAIN STREET

When hackers breach the security of corporations it makes headlines, yet there is rarely a mention when cybercrime hits small to medium sized businesses (SMBs). Very few people are even aware that today's cybercriminals are targeting SMBs, not just supersized global businesses.

According to Verizon's Data Breach Investigations Report, 71% of the data breaches investigated by the company's forensic analysis unit targeted small businesses with fewer than 100 employees. Of that group, businesses with less than 10 employees were the most frequently attacked.

EVERYONE IS A VICTIM WHEN IT COMES TO CYBERCRIME

The loss and exposure of confidential data from a cyber attack is costly to both the people victimized and the businesses whose data was compromised.

For the victim, hackers typically retrieve personal information, bank account, credit card and social security numbers, resulting in identity fraud. The stress and time involved to reclaim their identity and get their financial house back in order is beyond measure.

For businesses, there are 47 state-specific DBN (Data Breach Notification) laws in effect in the United States. Adding to the complexity and costs of this process is the fact that laws and compliance obligations vary from state to state. A breach of customer data in Pennsylvania will

have different breach notification and followup requirements than a breach involving a customer in Massachusetts. This means firms servicing customers and clients from more than one state are responsible for these duplicative legal, regulatory and compliance burdens.

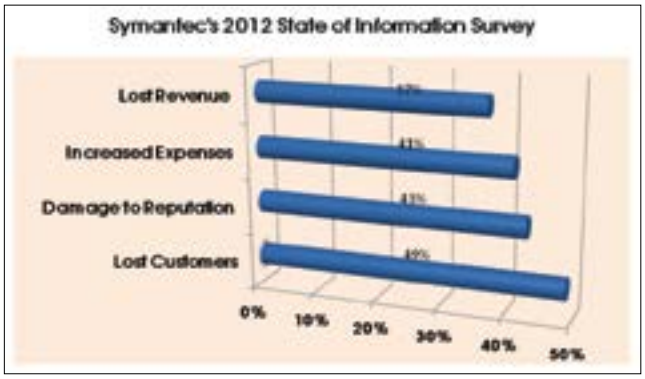
CYBERCRIME COMES AT A HIGH PRICE FOR SMBS

According to research compiled by the Ponemon Institute in their 2nd Annual Cost of Cyber Crime Study, the average cost per breached record in the U.S. is anywhere between $150 to $200. This amount factors in the costs of the investigation and notification process, fixing the issue that led to the breach, possible liability and litigation costs, lost business, and the time and effort that go into damage control. In many cases, a damaged reputation may prove to be irreparable. Nearly two-thirds of victimized companies are out of business within six months of a significant cyber attack, making cybercrime the death knell for many SMBs. This is because the consequences of cybercrime extend well beyond the actual incident and have long-lasting implications.

Small businesses obviously don't have the same financial footing to rebound and carry on with business as usual in the way organizations like Target, Amazon, Apple, or Citibank can.

Symantec's research found that customers affected by security breaches are generally less forgiving of smaller businesses, especially smaller online retailers, than larger companies. SMBs are contending not only with lost revenue and expenses, but also the possibility of never regaining the trust of customers, clients and business partners.

Symantec's State of Information Survey found that nearly half of all SMBs admitted to a data breach damaging their reputation and driving customers away.



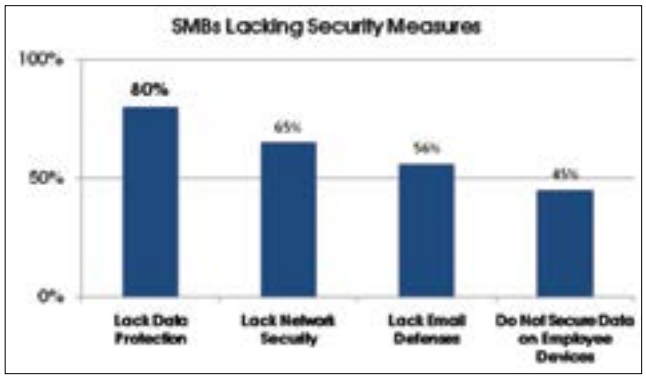
The trend of cybercriminals preying on smaller businesses doesn't seem to be waning. According to Symantec, the number of cybercrime attacks targeting firms with fewer than 250 employees jumped from 18 percent to 31 percent in just a year.

WHY CYBERCRIMINALS ARE ZEROING IN ON SMALL BUSINESSES

Large corporations have the resources to invest heavily in the most sophisticated security strategies and successfully stop most cybercrime attempts. A typical large enterprise may have over twenty inhouse IT dedicated employees ensuring that every device connecting to their network is adequately protected.

In comparison, SMBs have neither the money nor the manpower of large enterprises and can't afford the same level of security. Very few SMBs have fulltime IT dedicated personnel on hand to run routine security checks. Even those who do have in-house IT support often find that their internal resources are too bogged down with other tasks to properly address security upkeep.

A joint survey of 1000 SMBs conducted by McAfee Internet Security and Office Depot further confirms how lax many SMBs are when it comes to protecting their data.



Not only have SMBs become easy prey for cybercriminals, but their sheer abundance also makes them an alluring target. There are roughly 23 million SMBs in the United States alone. Half of that figure is comprised of home-based businesses. Even in a struggling economy, it's projected that there are still an estimated 500,000 startups launching every month with only a handful of employees.

SMBS ARE NOT "TOO SMALL TO MATTER"

Since most cybercrimes affecting smaller businesses go unreported by the media, there is no sense of urgency by SMBs to prepare for cyber attacks. Too many SMBs mistakenly view their operations and data as trivial to hackers. They feel that large online retailers, global banks, and government entities are much more attractive targets for hackers.

The goals and methods of cyber attackers are evolving and will continue to evolve. The era of one "big heist" for hackers is over. Cybercriminals today often prefer to infiltrate the data of many small businesses at once, stealing from victims in tiny increments over time so as to not set off an immediate alarm. This method takes advantage of those SMBs who are especially lax with their security processes and may not even realize there has been a security breach for days or sometimes even weeks.

SMBs must end the "It will never happen to us" mindset. For instance, political "hactivists" have been responsible for a number of high-profile Denial-of-Service (DDoS) attacks in recent years. The goal of a hactivist is to disrupt the status quo and wreck havoc on the technology infrastructure of larger corporations and government entities. It's a form of cyber anarchy: A "stick it to the man" philosophy spearheaded by groups like 4chan, Anonymous, LulzSec, and AntiSec.

An owner or Chief Information Office (CIO) at a SMB may read of these high publicized attacks in the press and not think anything of it. They aren't Sony, Apple, or the Department of Defense, so why would a hactivist target their data? But it's estimated that there are on average 1.29 DDoS attacks throughout the world every two minutes and such activity is much broader in scope than the press may lead us to believe.

SMBS- THE ACCESS RAMP TO BIGGER & BETTER DATA

One reason small businesses are more vulnerable is they're often the inroad to larger better-protected entities. They are often sub-contracted as a vendor, supplier, or service provider to a larger organization. This makes SMBs an attractive entry point for raiding the data of a larger company. Since larger enterprises have more sophisticated security processes in place to thwart cyber attacks, SMBs often unknowingly become a Trojan horse used by hackers to gain

backdoor access to a bigger company's data. There is malware specifically designed to use a SMBs website as a means to crack the database of a larger business partner.

For this reason, many potential clients or business partners may ask for specifics on how their data will be safeguarded before they sign an agreement. Some may require an independent security audit be conducted. They may also ask SMBs to fill out a legally binding questionnaire pertaining to their security practices.

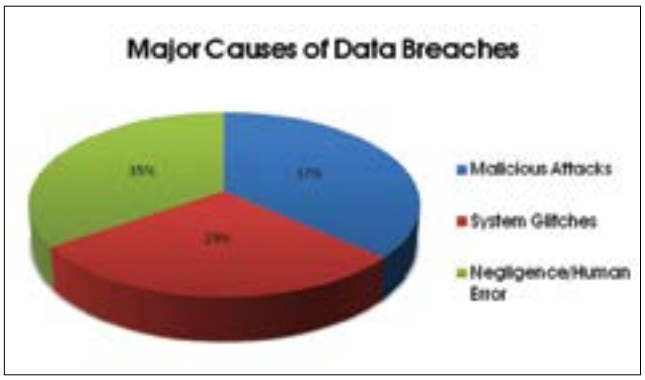
Moving forward, a SMB that is unable to prove they're on top of their infrastructure's security will likely lose out on potentially significant deals and business relationships. More large enterprises are being careful to vet any business partners they're entrusting their data to.

TO STAY SECURE A GOOD DEFENSE IS THE BEST OFFENSE

SMBs must understand that the time has come to get serious with their security. Sadly, many small businesses have a false sense of security. In the McAfee/ Office Depot joint survey of 1000 SMBs, over 66% were confident in the security of their data and devices despite admitting to obvious flaws.

Cybercrime is only one cause of compromised data. There are 3 primary causes of breached security at businesses according to the Symantec Global Cost of a Data Breach study. Only 37% are attributed to malicious attacks. The remaining 64% are human error and technology errors.

Data breaches aren't always about bad people



doing bad things. Many are the result of good employees making mistakes or of technology failure. SMBs don't necessarily need a large budget or dozens of employees to adequately protect sensitive data. A secure environment is possible even on a SMBs budget. Here are a few steps to improving data and network security.

STEP 1
KNOW ALL DEVICES CONNECTING TO YOUR NETWORK

Keep a frequently updated list of every device that connects to your network. This inventory is especially important given today's BYOD (Bring-Your-Own-Device) workplace where employees can access your network through several different devices. Knowing what these devices are and ensuring they're all configured properly will optimize network security.

All it takes is a regularly scheduled review to add or remove any devices and affirm that every endpoint is secure. Much of this process can be inexpensively automated through a Mobile Device Monitoring (MDM) tool. A MDM tool will approve or quarantine any new device accessing the network, enforce encryption settings if sensitive information is stored on such a device, and remotely locate, lock, and wipe company data from lost or stolen devices.

STEP 2
EDUCATE & TRAIN EMPLOYEES

Every employee should participate in regular general awareness security training. This will not only reduce security breaches directly tied to employee error or negligence but also train employees to be on the defense against cybercrime. Employees are critical to your security success and the prevention of data breaches. Hackers commonly break into networks by taking advantage of unknowing employees. Phishing attacks – legitimate looking emails specifically crafted to mislead recipients into clicking a malicious link where they're asked to provide their username and password- are still successfully used by hackers to capture login credentials.

If a large company makes the news for a data breach tied to an infected email, be sure to share that news with employees with a warning. Come up with fun ways to teach employees how to identify spearphishing email attempts and better secure their systems and devices.

It is also important to have a security policy written for employees that clearly identifies the best practices for internal and remote workers. For example, password security is critical and passwords should be frequently updated to a combination of numbers, lower case letters and special characters that cannot be easily guessed. Security policy training should be integrated into any new employee orientation. This policy should be updated periodically. More important than anything, this security policy must be enforced to be effective.

STEP 3
PERFORM AN AUDIT OF SENSITIVE BUSINESS INFORMATION

If you want to keep your most sensitive business information secure, it's important to know exactly where it's stored. A detailed quarterly audit is recommended.

STEP 4
USE CLOUD AND MANAGED SERVICE PROVIDERS

Overall, the cloud is likely a more secure data solution for small business. Any conception that the cloud isn't safe is outdated. Most security breaches are the result of lost or stolen devices, printed documents falling into the wrong hands, and employee errors leading to unintended disclosures. It's fair to speculate that many of these breaches wouldn't have occurred had this information been stored in the cloud rather than computers, laptops, and vulnerable servers.

SMBs with limited budgets are actually enhancing their security by moving to the cloud. Since there is no way a SMB can match a large enterprise's internal services, moving services like emails, backups, and collaborative file sharing to the cloud not only reduces total-cost-ofownership, but gives access to top-level security to better defend against internal and external threats.

Meanwhile, a Managed Service Provider (MSP) can assume responsibility for security measures like the administering of complex security devices, technical controls like firewalls, patching, antivirus software updates, intrusion-detection and log analysis systems.

MSPs are also capable of generating a branded risk report for any potential client or business partner reviewing your security measures. This thirdparty manual assessment of your network security can instill confidence in prospective business partners by proving to them that any possible security risks or vulnerabilities will be properly managed and addressed.

RISE TECH PARTNERS

111 West Pleasant Street, Suite 101, Milwaukee, WI, 53212
Email: gherpel@risetechpartners.com
Phone: 414.276.3300