Survey: Small Business Security

A look at small business security perceptions and habits at each phase of business growth.

www.csid.com

CSID®

SUMMARY

Many small to medium-sized businesses (SMBs) are not taking measures to protect against security risks, and cyber criminals are starting to take notice. In fact, the number of attacks against SMBs nearly doubled from 18 percent in 2011 to 31 percent in 2013. Why the increased attention on smaller sized businesses? According to CSID's 2014 SMB survey, 31 percent of small businesses are not taking any active measures to protect against security threats.

To combat the increasing number of SMB data breach cases, business owners must first understand what kinds of risks they face at each step of growth in their business. Security risks shift, depending on the stage the business is in. This paper and corresponding survey results will explore the security risks businesses face during the different stages of its growth, how small business owners are currently addressing these risks, and what businesses can do to mitigate these risks.

THE BEGINNING: YOUR BUSINESS IS AN EXTENSION OF YOURSELF

When a business is first established, its information is tied back to the business owner – or owners. This individual must file and register the business, create a new business account with personal money or funds borrowed against their credit, and develop a website. These activities result in a lot of personal information becoming publicly available online and easily obtained by criminals. Since new business owners likely have money and a good line of credit, cyber criminals target these individuals to fraudulently obtain credit in the company's name until the business' credit is ruined. In CSID's 2014 SMB survey, we found that new business owners tend not to keep a close watch on their business credit. While the majority of small business decision makers (73%) are aware that their small business has a credit report, only 26 percent know their small business credit score. Nearly half (44%) never check their small business credit score at all. This leaves small businesses at risk for undetected fraudulent activity.

Criminals may also compromise new business websites, as security measures are oftentimes not yet in place. This low barrier of entry to tap a new business website gives cyber criminals an opportunity to intercept sensitive data like credit card numbers and customer's personal information.

BUSINESS GROWTH: RISK EXTENDS TO EMPLOYEES, VENDORS AND CUSTOMERS

As a business grows, cyber threats and risks shift. Instead of targeting one individual tied to the business, cyber criminals have several entry points to access vital company data including vendors and employees. Businesses also have more valuable information on hand such as customer and employee data the business has collected.

Our 2014 survey found that as a business grows, so does their concern over security risks caused by employees and vendors. Only 20 percent of businesses that had one to nine employees were worried about compromised employee credentials, compared to 30 percent of businesses with 20 to 99 employees. Similarly, 25 percent of businesses with one to nine employees were worried about security weaknesses with third party vendors. This number jumps to 40 percent for businesses with 20 to 99 employees.

This focus on employee and vendor security is not misplaced. IBM found in its 2013 Cyber Security Intelligence Index report that humans can account for roughly 80 percent of company breaches. Activities like employee social media use, lost devices with sensitive information, reuse of employee credentials on multiple sites, and inadvertently downloading malware – all can lead to a security breach and data loss.

> *As a business grows, cyber threats and risks shift.*

DOWNFALLS OF AN UNPROTECTED SMB

The immense cost of a data breach can be difficult to bounce back from. When a breach takes place, not only is there substantial financial cost – fraud cost totaled $18 billion dollars in the US in 2013 – but also the hard and overhead costs related to customer support, and the reputation cost of a damaged brand can often times be irreversible.

This report outlines CSID's survey results, provides a more detailed look into how small business owners feel about cyber security and details what actions they are taking to protect against these threats as a business grows. This report also presents recommendations on how SMBs can protect against cyber security threats.

SURVEY HIGHLIGHTS

43% of small businesses say their business credit score is important to the well-being of their business, but only 26 percent even know their score.

41% of small business decision makers are concerned with the security threats and risks that come with human error.

32% of small businesses consider employee social media use to be a security risk for their business.

40% of small businesses work with third party vendors to help with security.

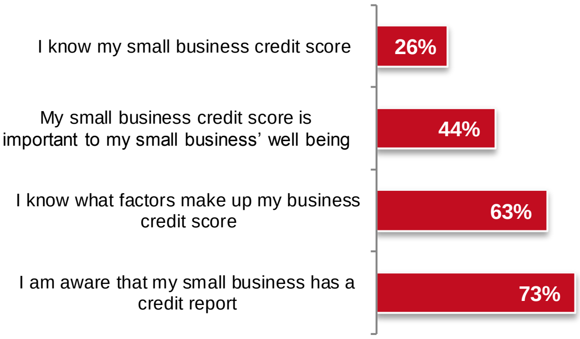
22% of small businesses plan to increase cybersecurity measures this year, up from 15 percent the year prior.

FINDINGS & CHARTS

WHILE MOST SMALL BUSINESSES KNOW THEIR BUSINESS CREDIT SCORE IS IMPORTANT, THEY DON'T TAKE THE INITIATIVE TO MONITOR IT.

The majority of small business decision makers (73%) are aware that their small business has a credit report, and 43% say that this credit score is important to their small business' well being, but only about a quarter (26%) know their small business credit score.

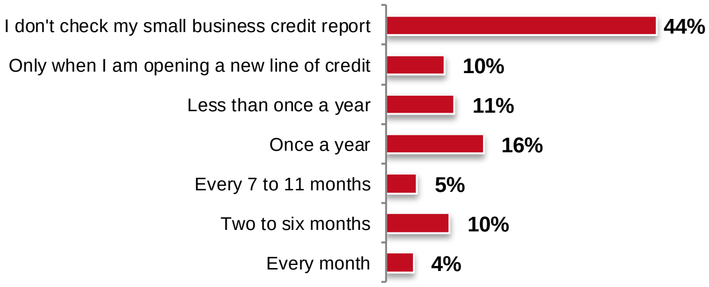
WHAT SMBS KNOW ABOUT BUSINESS CREDIT SCORES



SMALL BUSINESS DECISION MAKERS DO NOT CHECK THEIR SMALL BUSINESS CREDIT SCORE.

Almost half of small business decision makers (44%) say they never check their small business credit score, and only a third (31%) check it at least once annually.

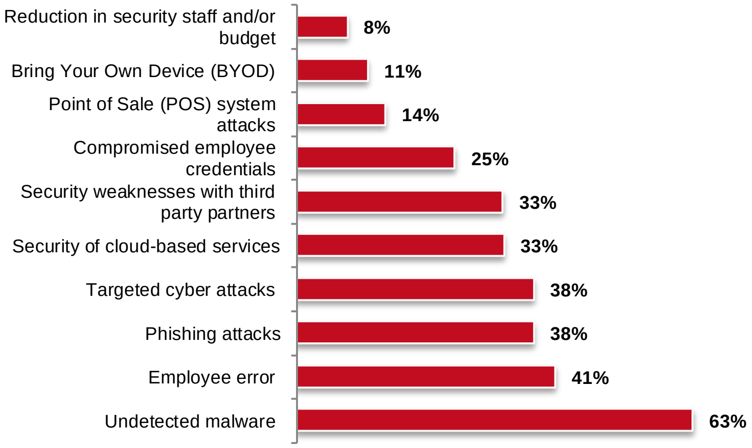
HOW FREQUENTLY SMBS CHECK THEIR BUSINESS CREDIT SCORES



SMALL BUSINESSES ARE MOST CONCERNED WITH MALWARE AND EMPLOYEE ERROR.

Two thirds (62%) of small businesses agree that they are concerned with the threat of malware attacks and 41% of small businesses consider employee error a major concern when it comes to their business' security.

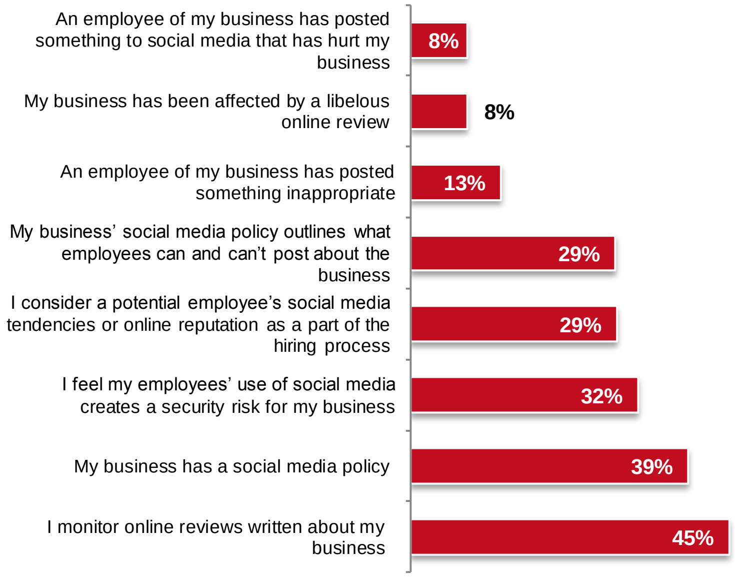
WHICH SECURITY THREATS ARE OF MOST CONCERN TO SMBS



SMALL BUSINESSES ARE AWARE THAT SOCIAL MEDIA CAN HARM THEIR BUSINESS' REPUTATION & SECURITY.

About a third of small businesses (32%) consider employee's social media use to be a security risk for their business and take active measures to mitigate that risk, including establishing social media policies (39%) and considering potential employees' social media tendencies as a part of the hiring process (29%).

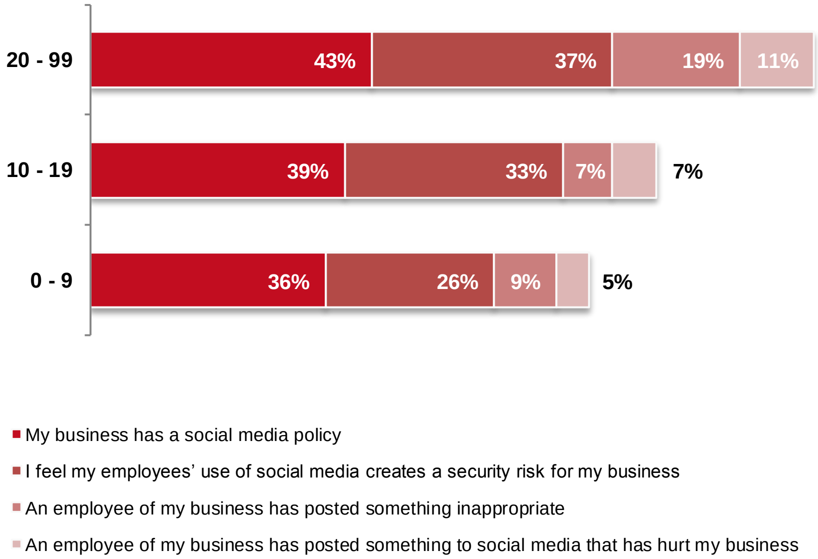
HOW SMALL BUSINESSES PERCEIVE SOCIAL MEDIA AS IT RELATES TO BUSINESS SECURITY & REPUTATION



AS SMALL BUSINESSES GROW, EMPLOYEE SOCIAL MEDIA USE BECOMES MORE OF A CONCERN AND RISK TO THE BUSINESS' SECURITY AND REPUTATION.

Our research shows that 19% of small business with 20-99 employees have had an employee post something inappropriate, compared to 9% of businesses with less than 10 employees. Eleven percent of businesses with 20-99 employees have had an employee post something on social media that has hurt their business, compared to only 5% of businesses with less than 10 employees.

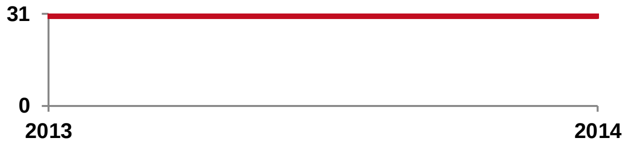
SIZE OF SMALL BUSINESS (NUMBER OF EMPLOYEES) VS THE BUSINESS' PERCEPTION OF SOCIAL MEDIA & SECURITY



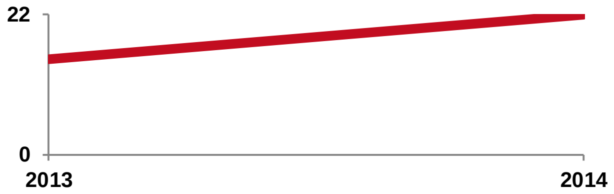
DESPITE SEEMINGLY STATIC ACTIONS YEAR OVER YEAR, AN INCREASING NUMBER OF SMALL BUSINESSES PLAN TO DEDICATE MORE BUDGET TO SECURITY.

While a third (31%) of small businesses are currently not doing anything to protect against security threats - the same percent as found in our 2013 SMB survey - more small businesses (22%) have plans to increase their security budget in 2014 than they did in 2013 (15%).

PERCENT OF SMBS WHO ARE NOT DOING ANYTHING TO PROTECT AGAINST SECURITY THREATS, 2013 VS 2014



PERCENT OF SMBS WHO HAVE PLANS TO INCREASE SECURITY BUDGETS, 2013 VS 2014



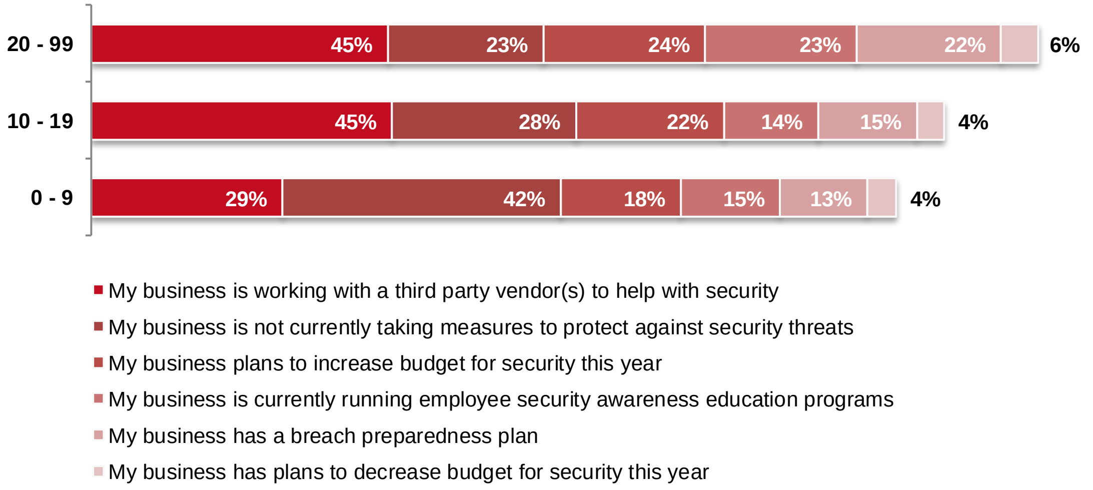
MICRO-SIZED SMALL BUSINESSES ARE FAR LESS LIKELY TO PROTECT AGAINST SECURITY RISKS THAN SLIGHTLY LARGER BUSINESSES.

Only 29% of small businesses with less than 10 employees say that they are taking any measures, compared to 45% of businesses with 10-19 employees and 45% of those with 20 to 99. employees.

IN GENERAL, AS SMALL BUSINESSES GROW THEY ARE MORE LIKELY TO TAKE MEASURES TO PROTECT THEIR BUSINESS AGAINST SECURITY RISKS.

For instance, 22% of businesses with 20 to 99 employees have a breach preparedness plan, compared to 15% of those with 10 to 19 employees and 13% of those with less than 10 employees.

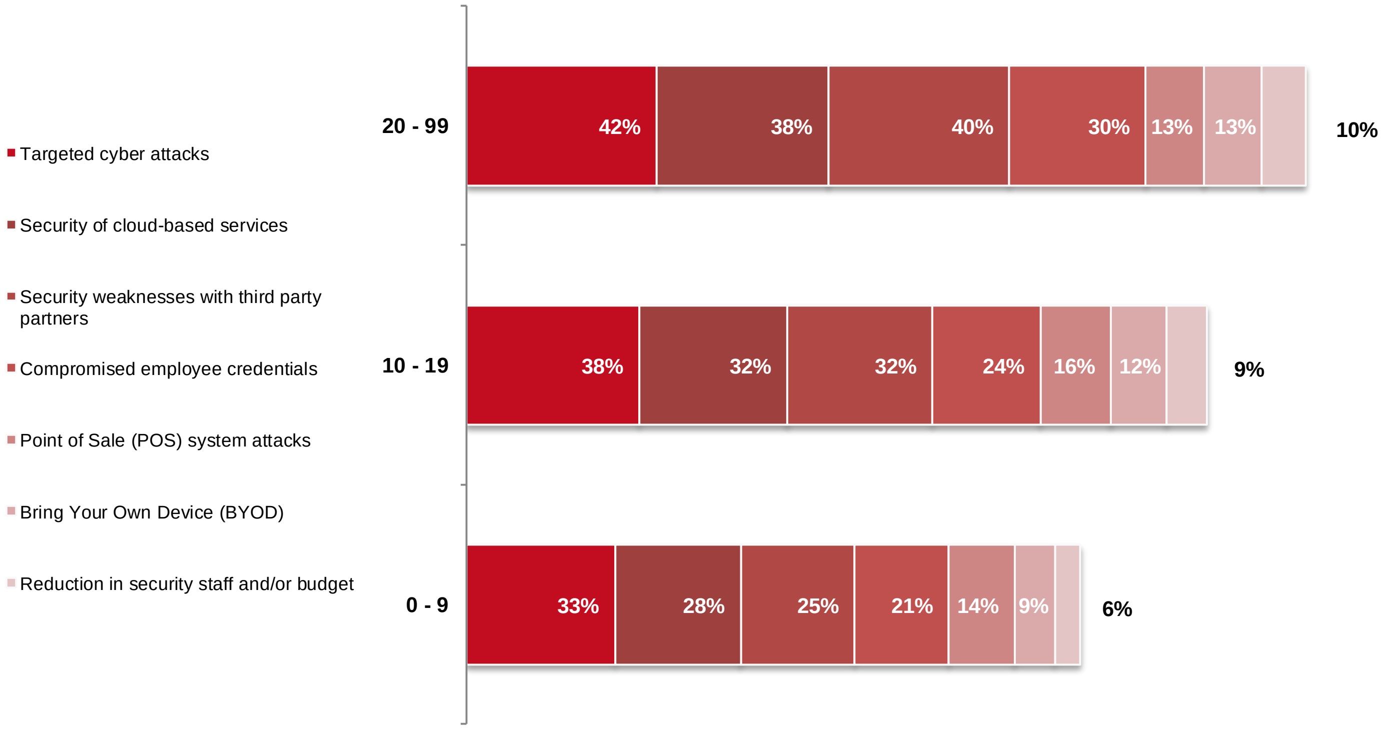
ACTIONS THAT SMBS ARE TAKING TO PROTECT AGAINST SECURITY RISKS VS. SIZE OF SMB (NUMBER OF EMPLOYEES)



LARGER SMALL BUSINESSES TEND TO BE MORE CONCERNED WITH SECURITY RISKS THAN THEIR SMALLER-SIZED COUNTERPARTS.

Small businesses with 20 – 99 employees are more concerned about risks like targeted cyber attacks, security of cloud-based services, security weaknesses with third party partners and compromised employee credentials when compared to their smaller-sized counterparts with 0 – 19 employees.

TOP SECURITY CONCERNS OF SMBS VS. SIZE OF SMB (NUMBER OF EMPLOYEES)



TAKEAWAYS

This survey reveals that small businesses need to better understand the varying security risks during each stage of business growth and how to combat these risks. Results also showed that as small businesses become aware of these risks, there is still a gap that needs to be bridged between understanding threats and take action against them.

Business credit plays a huge role in the business' viability at inception, and actively monitoring a business credit report can identify if the business' credit is being misused. The majority of small business decision makers (73%) are aware that their small business has a credit report and 43 percent understand that their business credit score is important to their business. Despite this, only about one out of every four (26%) small business owners know their credit score and 44 percent of owners never check their small business credit report. There is a disconnect between awareness of importance and action when it comes to monitoring credit reports.

This disconnect is reflected throughout the survey findings. Sixty-three percent of SMBs reported that they are worried about undetected malware, 38 percent are worried about phishing attacks and 41 percent are concerned about breaches caused by human error. Yet a third of small businesses (31%) reported that they are not doing anything to protect against these threats.

While some small businesses are not focusing efforts on security, many more are. Twenty-two percent of businesses surveyed this year plan on increasing their budget for security-related measures. This is compared to only 15 percent of businesses in CSID's 2013 survey. Similarly, 17 percent of businesses surveyed have a breach preparedness plan, compared to 11 percent in 2013.

This year's survey also found that as a small business grows, so too does the business' attention to security measures. Small businesses with fewer than 10 employees are less likely to take measures to protect against security threats. Forty-two percent of businesses with one to nine employees reported they are not taking any measures, compared to 28 percent of businesses with 10 to 19 employees and 23 percent of businesses with 20 to 99 employees. Similarly, 29 percent of small businesses with one to nine employees are working with a third party vendor to help with security, compared with 45 percent of businesses with 10 to 19 and 20 to 99 employees.

Business credit plays a huge role in the business' viability when first starting out and actively monitoring a business credit report can identify if this credit is being misused.

These numbers make sense. As a business grows and has more sensitive data to store and potential entry points into the business, security becomes a higher priority. This year's survey found that larger SMBs (20 to 99 employees) are more concerned about targeted cyber attacks, security of cloud-based services, security weaknesses with third party partners and compromised employee credentials, compared to their smaller-sized counterparts (see chart on page 7).

Security weaknesses caused by employee's online activities were a focus of this year's SMB survey. About a third of small businesses (32%) consider employees' social media use to be a security risk for their business and take active measures to mitigate that risk, including establishing social media policies (39%) and considering potential employees' social media habits as a part of the hiring process (29%). CSID found that as a small business grows, employee social media use becomes more of a concern and risk to the business' security and reputation. Nineteen percent of small businesses with 20 to 99 employees have had an employee post something inappropriate, compared to nine percent of businesses with fewer than 10 employees.

Overall, the survey demonstrates that small businesses are becoming more aware that they are targets for hackers. The larger the small business, the more likely they are to adopt measures to protect against these threats. However, there is still a gap between business awareness about security threats and business action against security threats that needs to be bridged. To provide solutions and resources to small businesses, CSID hosted a webinar as a part of their cyberSAFE webinar series titled "Small Business Security for Every Phase of Growth." To view a recording of the webinar, visit http://www.csid.com/secureSMB2014.

RECOMMENDATIONS

What exactly can SMBs do to avoid risks? It boils down to awareness, education, monitoring and damage control.

AWARENESS

First and foremost, individuals who are interested in starting a business must be aware of security implications and costs when building a business plan. Security is typically not top of mind when an entrepreneur is ready to start a business. The security industry, government and entrepreneur startup communities must work together to build awareness around new business security.

EDUCATION

As a business begins to expand, it is vital to educate employees on the importance of workplace security and choose vendors with superior security reputations. Businesses should build and enforce password, BYOD and social media policies from day one. The more well-educated the workforce is on the importance of security, the more likely they will be to employ better online habits at work as well as in their personal lives.

MONITORING

Take advantage of software solutions that can help monitor the security of your business. Anti-virus solutions can help protect against malicious malware and VPNs can help protect business data when conducting business outside of the company network. Businesses should also consider a monitoring service to keep track of your SMB's overall health and mitigate the risk of breach. An SMB should monitor employee and customer credentials, its credit score and credit report to detect fraudulent activity.

DAMAGE CONTROL

Be sure to have a breach preparedness plan. More than half of U.S. SMBs experienced a data breach in 2012, but only 12 percent had a breach preparedness plan in place. While a damage control plan may not reduce the cost of repairing the data breach, it certainly helps keep your customer relationships intact and reduces business reputation damage.

METHODOLOGY

CSID and digital data collection firm Research Now teamed up to survey a demographically representative sample of 505 owners of small businesses in the U.S. with 1 – 99 employees from the Research Now Small Business Owners Panel. The sample framework is balanced based on industry vertical, number of employees, annual revenue, years in business, legal entity type and personal service business types

ABOUT CSID

CSID is the leading provider of global identity protection and fraud detection technologies and solutions for businesses, their employees, and consumers. With CSID's advanced solutions, businesses can take a proactive approach to protecting the identities of their consumers all around the world. CSID's comprehensive identity protection products advance from credit monitoring to include a full suite of identity monitoring services; insurance and full-service restoration; identity authentication and voice biometrics; and proactive breach mitigation and resolution.

www.csid.com

ABOUT RESEARCH NOW

Research Now, the leading digital data collection provider, powers market research insights. They enable companies to listen to and interact with the world's consumers and business professionals through online panels, as well as mobile, digital and social media technologies. Their team operates in 24 offices globally and is recognized as the market research industry's leader in client satisfaction. They foster a socially responsible culture by empowering our employees to give back.

www.researchnow.com