SURVEY: SMALL BUSINESS SECURITY

A look at sentiment and concerns from small business owners around cyber security and how this population is approaching risk mitigation and response.

CSID®

A part of Experian

MAY 2016

SUMMARY

Small Businesses: More at Risk Than They Think

In 2015, CSID, a part of Experian, created Jomoco, a coconut water startup with a fake website, fake email addresses, a prepaid credit card and two fake employees, Rachel and Richard. The idea behind the Jomoco experiment was simple – to see how quickly a small business could be breached and taken down when arming hackers with a single email address and login credential tied to the company. The answer to this question: one hour. In one hour, hackers had accessed personal email addresses for both employees, and in doing so, gained access to Jomoco's web servers, defaced the website, hacked personal social media and email accounts, and used the company credit card.

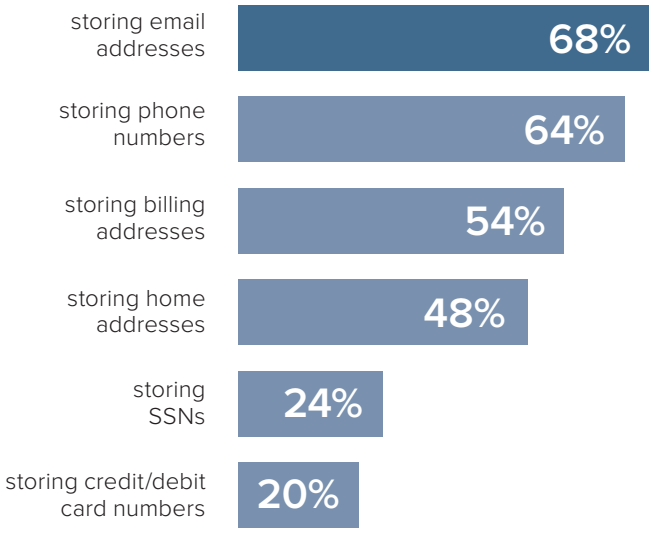
The ease in which Jomoco was taken down by hackers underscores a growing problem in the U.S. and across the globe – cyber criminals increasingly have small businesses in their crosshairs. In fact, Symantec reported over 60% of all attacks in 2014 were directed towards small and midsize companies in its 2015 Internet Security Threat Report.

The reasons behind this trend are simple. Small businesses have more money, accounts, activity and risk than individuals, and they also utilize fewer resources towards defending themselves than large enterprises. But do small businesses understand this threat? Are they taking action?

To better understand how small businesses are approaching the threat of cyber crime, CSID surveyed 150 small business owners (businesses with 1 to 10 employees) across the U.S. on their concerns about cyber security and their approach to risk mitigation and response.

According to CSID's 2016 small business survey, nearly a third (31%) of small business owners are not taking any proactive steps to protect against cyber threats, and half of small business owners (51%) do not allocate any budget for risk mitigation services. The most interesting insight that our survey uncovered, perhaps, is why. While 57% of companies we surveyed said that they are concerned about cyber attacks, the reason 51% of them are not allocating any budget to cyber attack risk mitigation is because they don't believe they are storing data that puts them at risk.

In another question, 52% of companies surveyed said that they don't invest in cyber risk mitigation because they don't store valuable data. Yet according to our survey, small businesses store the following information:



As mentioned above, Jomoco was hacked using just one business email address. This points to a significant educational disconnect for small businesses when it comes to understanding their risk, and the value of personally identifiable information (PII) to cyber criminals. The results from our survey suggest that a majority of small businesses do not understand that PII, even that of employees, can be used to trace an individual's identity and cause harm to the business. This includes information like email address, username, or password credentials.

CSID's 2016 Small Business Security Survey uncovered a number of other interesting trends which are outlined in this whitepaper.

SURVEY HIGHLIGHTS

31% of small businesses are not taking any proactive measures to mitigate cyber risk

58% of small businesses are worried about cyber attacks

51% are not allocating any budget to risk mitigation

53% of small businesses reported that they do not store valuable data, but 68% store email addresses and 65% store phone numbers

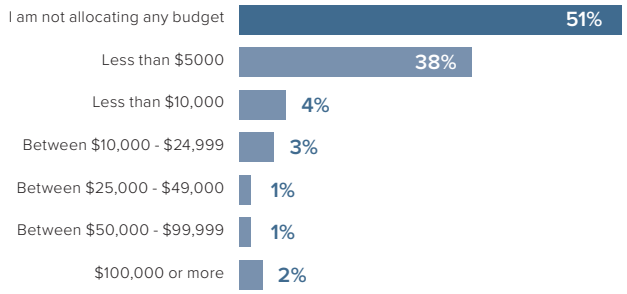
24% of small businesses that are not allocating budget for cyber attacks are not doing so because they already feel well prepared to handle an attack

FINDINGS & CHARTS

MOST SMALL BUSINESSES ARE NOT ALLOCATING ANY BUDGET TOWARD RISK MITIGATION

Most small businesses (51%) do not allocate any budget for risk mitigation, and 38% spend less than $5,000 on services. Small business owners frequently battle tight IT budgets, and cyber security protection does not appear to be a financial priority.

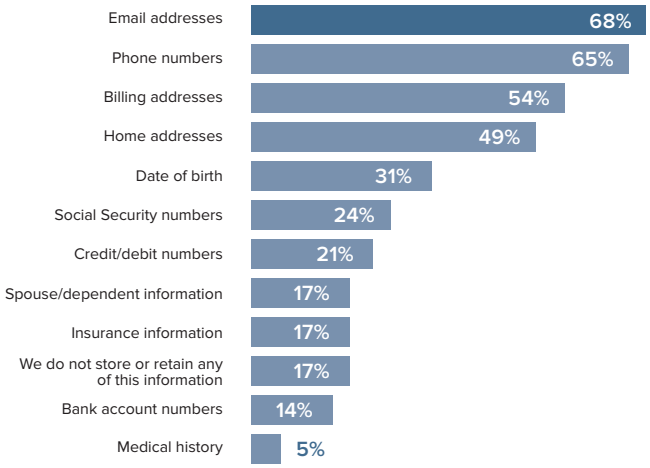
HOW MUCH BUDGET ARE YOU ALLOCATING TO CYBER ATTACK RISK MITIGATION?



SMALL BUSINESSES MAY NOT UNDERSTAND THE VALUE OF THE INFORMATION THEY STORE

More than half (53%) of small businesses reported they do not allocate budget for risk mitigation services because they do not store valuable data, yet the majority of respondents reported they store email addresses (68%) and phone numbers (65%), along with other valuable PII.

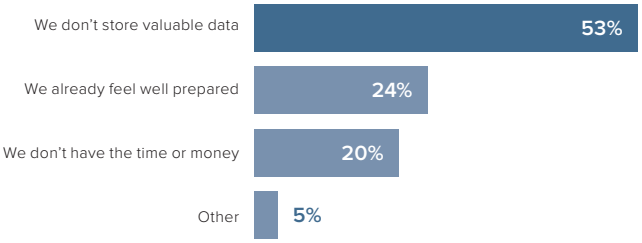
WHICH OF THE FOLLOWING INFORMATION DO YOU STORE OR RETAIN FOR EMPLOYEES, CUSTOMERS, PARTNERS OR ANY OTHER ENTITIES (SELECT ALL THAT APPLY)?



OF THOSE NOT ALLOCATING ANY BUDGET, ONLY A SMALL PORTION FEEL WELL PREPARED TO HANDLE AN ATTACK

Of the 51% of small business owners not spending any budget towards cyber risk mitigation, more than half (53%) reported the reason for this is because they do not feel they store valuable data. Nearly a quarter reported they are not spending any budget towards cyber risk mitigation because they already feel well prepared to handle an attack.

WHY ARE YOU NOT ALLOCATING ANY BUDGET?

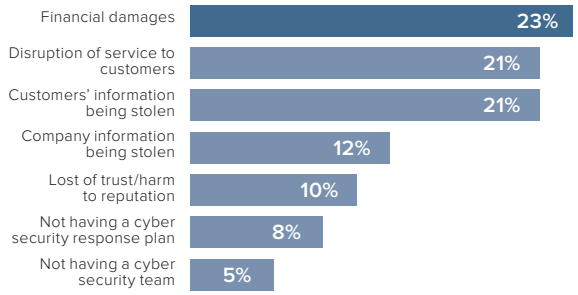


FIFTY-EIGHT PERCENT OF RESPONDING BUSINESSES ARE CONCERNED ABOUT CYBER ATTACKS

OF THOSE SMALL BUSINESSES THAT ARE CONCERNED ABOUT CYBER ATTACKS, MOST ARE WORRIED ABOUT FINANCIAL DAMAGES TO THE BUSINESS AND DISRUPTION OF SERVICE TO CUSTOMERS

While 23% of small businesses are concerned about financial damages and 21% are concerned about the disruption of service to customers, only 8% are concerned about not having a cyber security response plan, and 5% are concerned about not having a cyber security team. Small business owners may not understand the value of internal support and a response plan in the face of a data breach or don't have the resources to obtain either.

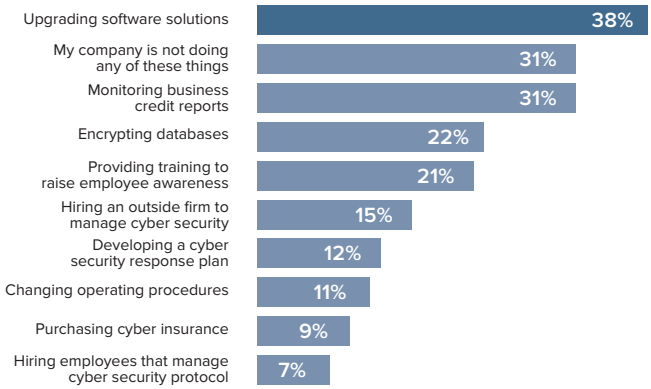
WHAT ARE YOU MOST CONCERNED ABOUT?



ALMOST A THIRD OF SMALL BUSINESSES ARE NOT TAKING ANY PROACTIVE MEASURES TO PREPARE FOR CYBER ATTACKS

Only 38% of small businesses upgrade software solutions, 31% monitor business credit reports, and nearly a third (31%) reported they do not take any sort of proactive measure to prepare for a cyber attack.

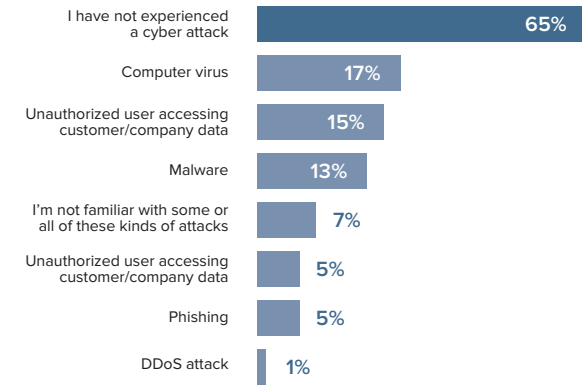
WHICH OF THESE ARE YOU CURRENTLY DOING TO PREPARE FOR POTENTIAL CYBER ATTACKS (SELECT ALL THAT APPLY)?



SMALL BUSINESSES SUFFER COMPUTER VIRUSES, PHISHING ATTACKS, AND MALWARE

Roughly two-thirds (65%) of small businesses reported they have not experienced a cyber attack in the last six months. Of those that did, malware, computer viruses and phishing attacks were the main types of attacks.

HAS YOUR BUSINESS EXPERIENCED ANY OF THE FOLLOWING CYBER ATTACKS IN THE PAST SIX MONTHS (SELECT ALL THAT APPLY)?



TAKEAWAYS

CSID's small business survey indicates that while the majority of small businesses are concerned about cyber threats, they are largely not taking proactive measures to combat these threats, nor are they allocating budget for risk mitigation and response services.

EDUCATION: UNDERSTANDING WHAT ACTIVITIES PUT A BUSINESS AT RISK AND HOW COMPROMISE OCCURS

The main take away from the 2016 CSID survey is that many small businesses don't understand the value of certain types of data and how this data puts them at risk. According to Symantec's 2015 Internet Threat Security Report, attacks on small businesses comprised 43% of all spear phishing incidents in 2014. Cyber criminals know that this is an easy way to penetrate a small business' network as all it takes is one employee to click on a link in a malicious email. Once information has been compromised, it may take small business owners months to realize that they have been the victim of an attack.

Common attacks targeted at small businesses through phishing and other tactics include Denial of Service (DoS) Attacks, where criminals are able to render a machine or network unavailable to its intended users, malware - malicious software which includes viruses and spyware, and zero-day attacks - where hackers exploit holes in software. These attacks are becoming increasingly more sophisticated and difficult for the average business owner to identify without the support of a third-party monitoring service.

This year's survey also revealed that while most small businesses reported that they had not experienced an attack in the past six months, a considerable portion of them suffered from computer viruses (17%), phishing attacks (15%), and malware (13%). Another 7% were unfamiliar with these types of attacks, indicating that some small businesses have not received the education to adequately identify these attacks when they occur. For example, the discrepancy between the small businesses reporting phishing attacks (15%) and those in Symantec's report (43%) may suggest that a large number of attacks are going unnoticed by small business owners.

CONCERNED, BUT NOT TAKING ACTION

Small businesses know that cyber crime is a threat, but this knowledge is not translating into action. A majority (58%) of small businesses are concerned about cyber attacks, especially in the context of financial damages, disruption of service to customers and stolen customer information. Yet, the survey indicates that small businesses are doing little to proactively prepare for such attacks. Upgrading software solutions is a critical way for businesses and individuals to stay secure, but only 38% reported doing this. Additionally, only 31% monitor business credit reports, and 22% encrypt databases.

While concerned about cyber attacks, only 8% of small businesses are concerned about not having a cyber security response plan, and a meager 5% are concerned about not having a cyber security team. This suggests that small businesses may not understand the value of internal support and a plan for response preparedness in the face of a data breach.

Overall, a considerable percentage of small businesses, while concerned about cyber risk, are not taking any proactive measures or allocating any budget to mitigation and response. This disconnect between fear and action seems to stem primarily from a lack of awareness from this group around the value of the data they have in their possession.

RECOMMENDATIONS

What proactive measures can small businesses take to avoid combat cyber risk?

AWARENESS

It will take a collaborative effort on the part of the security industry and the public and private sectors to spread awareness around this issue and prompt small business owners to protect themselves in the face of cyber crime. It's imperative that security practices go from being put on the back burner to becoming top-of-mind, especially through educating small businesses on the value of the PII they store. The National Cyber Security Alliance (NCSA) and the Federal Communications Commission (FCC) have a number of free, easily accessible resources for businesses looking to improve their cyber security.

EDUCATION

Small business owners must begin baking-in cyber security best practices into their business plan and corporate cultures. Understanding and staying aware about the different types of attacks, and knowing what to do in the event of one, is critical in staying ahead of cyber threats and minimizing damage. Educating employees and enforcing policies around passwords, bring your own device (BYOD) and social media from day one will be essential in staying one step ahead of cyber crime. Employees are often the weakest link when it comes to business security, but by arming them with the tools and knowledge they need from day one, the entire business will have a stronger change at staying secure.

MONITORING

Small businesses should enlist a third-party monitoring service to watch for fraudulent activity related to employee and business information. This can help business owners stay ahead of cyber threats. They should also take advantage of the number of software solutions – like anti-virus protection and VPNs – available to help businesses stay secure.

RESPONSE

Although CSID's survey indicated only 12% of small businesses have a breach preparedness plan in place, a plan is essential in minimizing the damage brought on by cyber attack. By having a damage control plan, small businesses can help maintain trust with their customers, bounce back from an attack more quickly, and get back to what's most important: running their business.

ABOUT CSID

CSID

CSID, a part of Experian, is a leading provider of global identity protection and fraud detection technologies for businesses, their employees, and consumers. With CSID's enterprise-level solutions, businesses can take a proactive approach to protecting the identities of their consumers all around the world. CSID's comprehensive identity protection services extend beyond credit monitoring to include a full suite of identity monitoring and fraud detection services; identity theft insurance provided under policies issued to CSID; full-service restoration services; and proactive data breach services.

Methodology

CSID and digital data collection firm Research Now teamed up to survey a demographically representative sample of 150 owners of small businesses in the U.S. with 1-10 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.

Contact Us

Join CSID on Facebook at facebook.com/CSID and on Twitter at @CSIdentity.

For more information, please contact Director of Marketing, Cody Gredler at cgredler@csid.com.

LEARN MORE AT

CSID.COM