WEBROOT®
Smarter Cybersecurity™

WEBROOT GLOBAL REPORT:

SMB Cybersecurity Preparedness, 2018

What’s inside

Foreword

Charlie Tomeo
Vice President of Worldwide Business Sales

When it comes to cyber threats, attacks are imminent. That doesn't mean it should stop you from working to secure your organization.

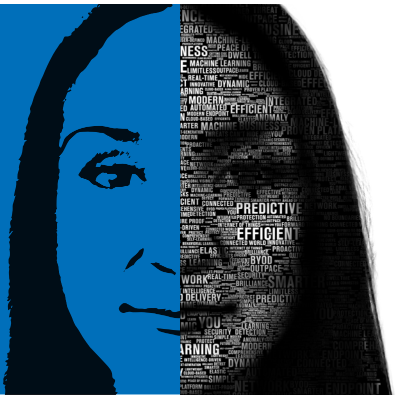
In the span of just five years, our collective memory is stuck on such events as whistleblower Edward Snowden leaking government documents alongside the Target data breach, the first major "wake-up call" around data breaches (2013), worldwide ransomware attacks WannaCry and NotPetya (2017), and Facebook's recent scandals with Cambridge Analytica and private data-sharing agreements with Apple, Samsung, and Huawei (2018). In fact, during the first three months of 2018, there were a total of 686 global data breaches that resulted in the exposure of 1.46 billion records. With so many threats regularly—and more frequently—in the news, it's understandable that confidence levels around security have declined across the globe.

While it's true that all organizations are susceptible to attacks today, almost two-thirds of all cyberattacks are now directed at small- and medium-sized businesses (SMBs), according to the Verizon Data Breach Investigations Report. And with more limited resources, budgets, and staffing than big businesses, many SMBs are significantly more vulnerable to security threats and are struggling to keep pace across this digital divide.

So, what can be done in the era of cyberattacks? IT leaders must become aware of global threat trends. They must implement and adhere to best practices within their organizations. And when there is a gap in in-house IT and security expertise, organizations should consider leaning on an MSP to strengthen security, rather than try to manage the problem single-handedly.

In this report, we hope to shed new light on the evolving security landscape, and provide actionable steps that every organization should consider to protect its data.

Executive Summary



In a recent study of 600 IT decision makers at SMBs across the United States, United Kingdom, and Australia, Webroot found that the cyberattacks organizations believed they would be most susceptible to in 2017 is rapidly shifting in 2018. The Verizon Data Breach Investigations Report found 90 percent of security incidents and breaches in 2018 included phishing, and so it's no surprise that phishing is top of mind for those in the security trenches. Webroot's research uncovered that globally, phishing ranks as the number one concern for SMBs at 48 percent, while DNS attacks followed at 45 percent. Ransomware attacks were closely tethered at 42 percent, likely due to last year's WannaCry crisis.

Interestingly, Webroot also found that the average cost of a data breach has gone down significantly from 2017 in the United Kingdom and Australia, dropping nearly 50 percent. However, the United States only saw a 9 percent drop in expected costs of a data breach. While there are many possible reasons for this shift, it's likely that the EU's new General Data Protection Regulation (GDPR) has played a role in this decline in the U.K. As for Australia, similar legal changes have also gone into effect, including the Notifiable Data Breaches (NDB) scheme. When organizations start focusing on their data, where it is and how secure it is, they begin to recognize everything that a breach can take from them. In addition to these new legal obligations that companies take better care of their customers' data, the regulations have forced businesses to more carefully consider security and auditing, which is bound to bring about some positive changes in their overall protection.

Webroot found that the increase of cyberattacks and data breaches is not new, nor is the concern around cybersecurity. In 2018, 79 percent of respondents globally don't believe their companies are completely prepared to protect against cyber threats.

There may be several reasons for this number, but one could be the level of attention to education that organizations provide. While nearly all organizations provide some level of security training (nearly 100 percent), only 39 percent continuously train employees on best practices for cybersecurity throughout the duration of employment. Further, 36 percent only train employees once, either during onboarding or after a security breach takes place.

SMBs that lack the in-house resources or expertise to educate users and combat the frequency and variety of attacks that are possible should consider outsourcing to a managed service provider. MSPs typically have access to the same level of enterprise-grade security tactics that larger organizations are able to leverage, and can do so without overburdening SMBs' resources.

“

One of the most effective strategies to keep your company safe is with layered cybersecurity that can secure users and their devices at every stage of an attack, across every possible attack vector. And for many businesses, leaning on a managed service provider (MSP) when time and expertise isn’t readily available is a crucial step to strengthen their security efforts.

Charlie Tomeo, Vice President of Worldwide Business Sales, Webroot

”

Key Global Findings: Threats Are Ever-Evolving

Globally, IT decision makers have identified phishing as the most dangerous threat to security in 2018, shifting away from new forms of malware in 2017. In fact, the fear of phishing moved up two spots from the third most concerning threat in 2017, now at 48 percent in 2018.

- 2018 -

#1 Phishing attacks (48 percent)

#2 DNS attacks (45 percent)

#3 Ransomware attacks (42 percent)

- 2017 -

#1 New forms of malware infections (56 percent)

#2 Mobile attacks (48 percent)

#3 Phishing attacks (47 percent)

After phishing attacks, 45 percent of those surveyed in 2018 are concerned with DNS attacks, and 42 percent are worried about ransomware attacks. Compared to the study in 2017, new forms of malware were top of mind, coming in at 56 percent, with mobile attacks (48 percent) and phishing attacks (47 percent) close behind.

Following WannaCry in May of 2017, ransomware rose from the fifth most worrisome attack to the third globally, and topped the charts as the number one threat in the United Kingdom.

Now five years removed from Edward Snowden's whistleblowing incident, only 25 percent of businesses reported being susceptible to insider threats in 2018 globally.

Checking the Box with Training Is No Longer Enough

Almost all businesses (nearly 100 percent) educate their employees in some capacity on cybersecurity best practices, with the U.S. taking the lead on implementing continuous training. Businesses in the U.S. are more likely to offer continuous training to employees (54 percent) compared to those in the U.K. (31 percent) and Australia (32 percent).

In the U.K., businesses are more likely than other regions surveyed to conduct security training only after a data breach has occurred.

Despite the training, 79 percent of those surveyed are unable to say they're "completely ready to manage IT security and protect against threats." This may be due in part to the type of security education businesses are conducting. For example, if we look at the U.K. and Australia, only one-third of businesses conduct continuous training, which leaves two-thirds who have not yet implemented continuous training. This is both surprising and disheartening, given that the U.K. experiences the most ransomware attacks and Australia the most phishing attacks. Simply conducting security awareness training annually, during initial onboarding, or after a security breach is ineffective and overall inefficient.

Security awareness training will only work on a continuous basis; as such, it's encouraging to see over half of U.S. respondents conducting ongoing training. Testing users via phishing simulations and other simulated attacks, in addition to continuous and relevant education on IT security and regulatory compliance is what changes user behavior—the ultimate goal of awareness training. And, with the right awareness and understanding, users can become resilient to attack techniques such as social engineering and scamming.

The Cost of Breaches Drops

While breaches are occurring more frequently in 2018, the estimated cost of a breach is declining. The survey found that what IT decision makers estimate a cyberattack involving customer records or critical business data would cost varied by region. While the cost of a breach in 2018 in the U.S. is, on average, more than half a million dollars, it has decreased nine percent from 2017. However, in the U.K. and Australia, the cost decreased significantly, at 59 percent and 48 percent, respectively (£305,357 and AU$994,025).

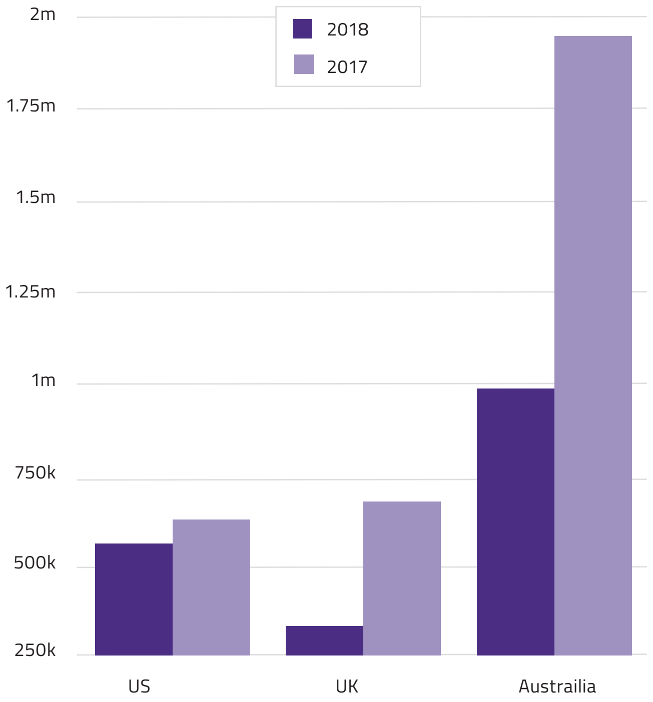


Figure 1: The Cost of Security Breaches for SMBs

Passing the IT Security Exams

When asked to grade themselves, most businesses (59 percent globally) gave themselves a 'B' for their ability to manage IT security, with just four percent of respondents self-ranking as a 'D' or 'F,' i.e. unable to protect themselves against threats. However, with over 2.6 billion records reportedly stolen or compromised in 2017 alone, businesses may simply be unwilling to admit a kind of defeat.

U.S. Spotlight

More than half (56 percent) of U.S. IT decision makers believe phishing attacks will be the biggest external security threats they will face this year, compared to two-in-five IT decision makers in Australia (46 percent) and in the U.K. (42 percent). Following closely behind, Americans are concerned about DNS attacks (54 percent) and DDoS attacks (52 percent).

Fueling concern about the broader country's ability to protect data is IT decision makers' belief that their companies aren't up to the task. In fact, nearly three-fourths (72 percent) of U.S. IT decision makers don't believe their business is completely ready to manage IT security and protect against threats, compared to 80 percent in 2017.

Inadequate preparation leads to an inability to quickly and effectively address threats and has a direct impact on the cost of an attack. On average, U.S. IT decision makers estimate it would cost their mid-sized companies more than half a million dollars ($527,256) if customer records or critical business data were lost as a result of a cyberattack this year alone. This represents only a 9 percent decrease from the estimated cost in 2017 ($579,099).

> *"It's encouraging to see that SMBs in the U.S. are taking note of the danger posed by DNS attacks. The DNS connection is involved in every aspect of internet usage, but it's becoming increasingly vulnerable to attacks. Cybercriminals are launching dynamic, stealth attacks that are designed to infiltrate defenses through multiple network points of entry. Once compromised, criminals may be able to view browser history, gain access to login information, redirect searches to malicious pages, and much more."*
>
> *Charlie Tomeo*
> *Vice President of*
> *Worldwide Business Sales*

Australia Spotlight

Eighty-eight percent of Australian IT decision makers do not believe their companies are completely prepared to protect against cyber threats. This figure is significantly higher than in the U.K. (78 percent) and the U.S. (72 percent), indicating that Australian SMBs feel significantly less prepared to address attacks in 2018 than they did in 2017 (60 percent). Only a third (32 percent) of Australian organizations continuously train employees on best practices for cybersecurity throughout the duration of employment. Almost half (51 percent) only train employees once: either during onboarding or annually. 19 percent provide training only after a security breach has taken place.

In Australia, the leading concern for SMBs is DNS attacks (52 percent). Interestingly, when it comes to insider threats, Australian businesses show more of a concern than the rest of the world, with almost one third (32 percent) listing it as a threat, as opposed to just 25 percent globally.

Following global trends, the cost of a threat was estimated to be on average AU$1,893,363 last year. In 2018, the estimated average loss is $994,025, which is almost half of the previous year's estimate.

Only a third of Australian organizations continuously train employees on best practices for cybersecurity throughout the duration of employment.

U.K. Spotlight

Mimicking global trends, the cost of a data breach fell from an average of £737,677 in 2017 to £305,357 in 2018. This drop of 59 percent from 2017 represents the most significant year-over-year decrease in the study.

In terms of threats, the U.K. is most concerned with ransomware attacks (44 percent). SMBs in the U.K. are significantly less concerned about DDoS attacks (17 percent) than the U.S. (52 percent) and Australia (49 percent). Ransomware fell from 50 percent in 2017 to 44 percent in 2018, with phishing and mobile attacks both trailing behind at 42 percent each this year.

In terms of their ability to manage IT security and protect against threats today, SMBs in the U.K. feel more prepared when comparing 2018 to 2017. Those who reported feeing "almost ready" skyrocketed from 39 percent in 2017 to 69 percent in 2018. When it came to feeling "completely ready," the numbers fell slightly from 28 percent in 2017 to 22 percent in 2018.

SMBs in the U.K. are significantly less concerned about DDoS attacks than the U.S. and Australia.

Takeaways: Cybersecurity Guidelines for SMBs

Implement a Continuous Education Program

As threats continue to evolve, employee cybersecurity training must follow suit. Training during onboarding isn't enough. Employees need continuous training to address the latest and most dangerous attacks. We highly recommend implementing a trust and security culture program within your organization.

Develop a Holistic Security Plan That Includes Mobile

Cyberattacks don't stop at laptops, and neither should your cybersecurity software. Mobile devices run through the cloud and are always-on, making them easy targets for attackers. Think about your security plan from a holistic perspective, and implement reliable mobile security as well to protect mobile network assets from malicious apps and other mobile threats.

Combine Security Technology and Employee Awareness to Combat Phishing

Cybercriminals are more sophisticated than ever, and phishing is at the top of their list of attack vectors. To combat this phenomenon, neither security technology nor awareness alone is enough. A key formula for success includes combining employee education to garner awareness of what the warning signs of a phishing attack look like alongside machine learning-based cybersecurity solutions that block malicious sites and URLs before users can click or download.

Evaluate Your Risk Profile and Outsource Help When Necessary

Every business has vulnerabilities and risk factors. If your organization lacks the in-house expertise to self-evaluate, a managed service provider (MSP) can assess your security posture and work with you to develop a plan for ongoing risk mitigation.

Develop a Data Breach Response Plan

When it comes to an attack, it's no longer a question of "if," but "when." Organizations that tend toward proactivity, rather than reactivity, will benefit in the security space. Develop a comprehensive data breach response structure that includes a communications plan to notify customers, staff, and the public. Provide counsel from security experts, and ensure they are available by phone for affected customers. Install remote computer backups to avoid data loss and downtime in the event of an attack. Those who are prepared will be able to act quickly and efficiently.

About Webroot

Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

385 Interlocken Crescent   Suite 800   Broomfield, Colorado   800.870.8102   webroot.com

© 2018 Webroot Inc. All rights reserved. Webroot, BrightCloud, SecureAnywhere, FlowScape, and Smarter Cybersecurity are trademarks or registered trademarks of Webroot Inc. in the United States and/or other countries. All other trademarks are the properties of their respective owners. Webroot Global Report _ 062518 _ US