WEBROOT®

2015 SMB Threat Report:

Are organizations completely ready to stop cyberattacks?

A research survey details the security perspective of IT decision makers in the US, UK, and Australia on resourcing, preparedness, and management effort expended on cybersecurity by small and medium sized businesses.

WEBROOT®
Smarter Cybersecurity™

INTRODUCTION & BACKGROUND

The nature of cyber threats has changed dramatically throughout the past five years. From our many discussions and exchanges with organizations, small to medium sized businesses (SMBs) are not fully equipped to manage IT security.

Why? SMBs often believe they are too small for hackers to target, or that they have little of value that cybercriminals would choose to steal. Outside the technology sectors, SMBs often forget that their value to cybercriminals may lie in their potential, as their innovation and IP can lead to growth into tomorrow's large enterprises.

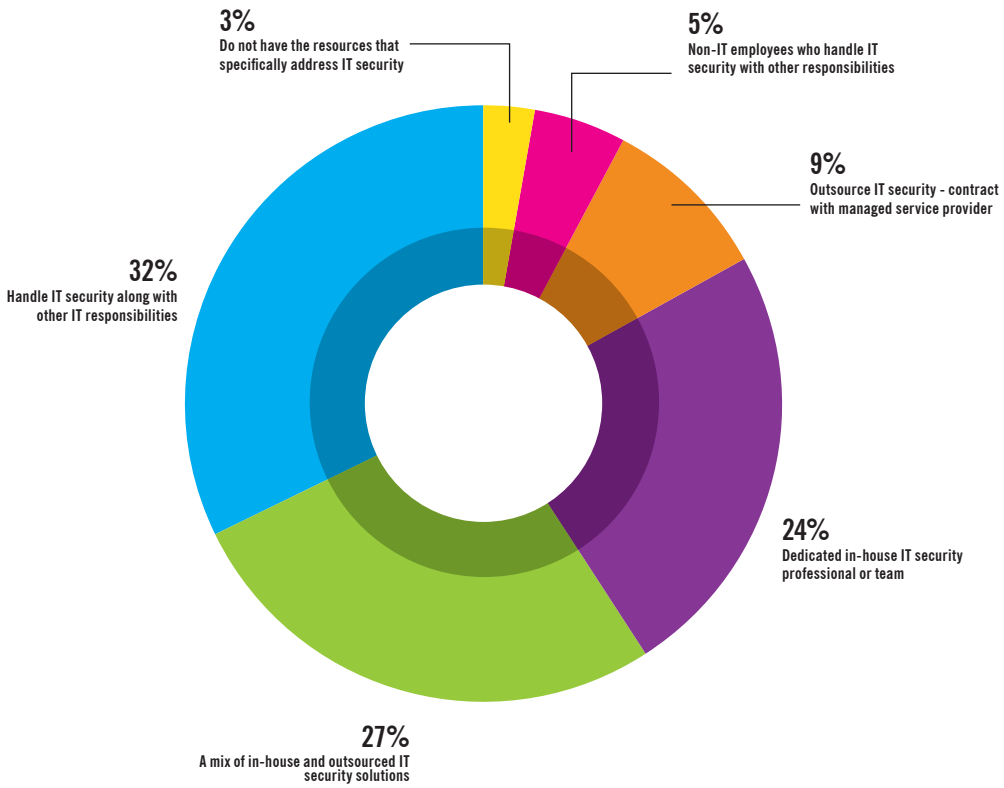
In the past, the 'it won't happen to me' attitude was largely sustainable for many SMBs. However, in today's world, the automation, commoditization, and low upfront costs of becoming a professional cybercriminal are such that it requires minimal skill to set up a cybercrime business and start trawling the internet for victims. Understandably, the under-protected, under-funded small to medium business makes for an attractive target.

Data breaches at massive companies like Target and J.P. Morgan make dramatic headlines, but there are dozens of threats to smaller enterprises each week that don't make the news. In this global study by Wakefield Research, sponsored by Webroot, revealed that many businesses reported not being prepared to protect against cyber threats or address their aftereffects. This report examines the state of IT security in small and medium sized businesses, assesses their readiness in the face of modern threats, and details recommendations for IT decision makers to better secure their businesses in 2016.

How SMBs are Coping with IT Security Today

At Webroot, we are constantly monitoring the state of IT security within small and medium businesses. To complement our Smarter Cybersecurity™ solutions and collective threat intelligence services, we commissioned new research on how small and medium businesses are preparing to stop cyberattacks and if outsourcing IT security would increase their cybersecurity. The results that follow cover three countries: US, UK, and Australia. In total, 700 IT decision-makers were surveyed across organizations with 1,000 employees or fewer.

How is your IT security managed?



Lack of resources and skills are a major issue within small to medium sized organizations. On average, less than a quarter of the organizations surveyed (24%) had a dedicated in-house cybersecurity team or individual. The majority surveyed (32%) had employees who handled cybersecurity along with other general IT responsibilities, followed by (27%) who had a mix of in-house and outsourced cybersecurity resources. However, only 14% of organizations relied solely on non-IT staff or outsourced resources.

How do you rate your IT security preparedness?

There is a direct correlation between the 24% of organizations with dedicated cybersecurity resources and the 24% who were far from, or only somewhat ready to handle online threats. In fact, only 37% of those surveyed reported they were completely ready to protect against and remediate threats, while 39% reported being "almost ready." Thus, 63% of all surveyed were not completely confident in their readiness to counter attacks and protect themselves.

0% Never be ready to manage and protect against threats

3% Far from ready to manage and protect against threats

21% Somewhat ready to manage and protect against threats

37% Completely ready to manage and protect against threats

39% Almost ready to manage and protect against threats

What IT security threats are you completely prepared for?

The study focused on four different security threat areas, including web, endpoint, network, and the insider threat. What emerged was a revealing insight into what respondents considered 'completely ready to manage and protect against threats'. Insider threats constituted the lowest percentage, with only 52% of organizations labelling themselves as completely ready to deal with these. Unsecured endpoints continue to cause major issues, as only 60% of respondents were confident they could respond to malware infecting a computer or mobile device.

From these results, we can see that the majority of SMBs are not completely prepared to handle cybersecurity incidents within their organizations, even in key security areas.

8% None of these

52% Insider threats, such as employees

55% Unsecured internal and external networks (public Wi-Fi)

60% Unsecured endpoints including PCs and smart devices

64% Unsecure websites and phishing attempts

Fewer Resources than Enterprise IT

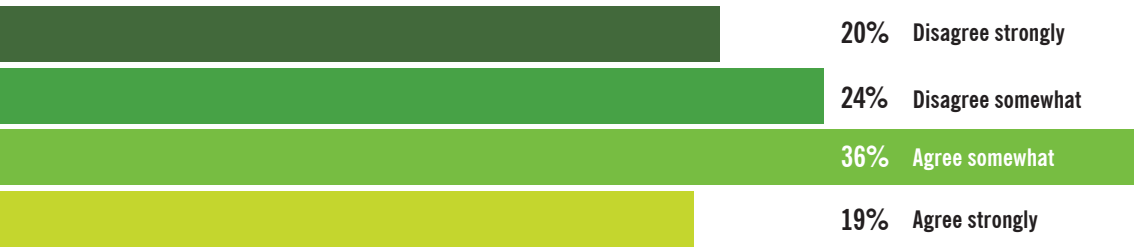
Is your business prone to cybersecurity attacks because you don't have the same resources as larger enterprises?

Skilled cybersecurity resources are in short supply in all sectors, so it's unsurprising that 59% of SMBs perceive themselves at a disadvantage to better funded enterprise organizations with more resources. The issue lies in acquiring or reallocating resources to address the lack without damaging the business' bottom line.

Not Enough Time to Keep Up on Cybersecurity

Do you have enough time to stay up-to-date on cybersecurity threats?

Keeping up with cybersecurity updates and the latest vulnerability patches is a crucial part of defending an organization. This graph and the next look at the time SMBs are able to dedicate to IT security matters. First we asked if respondents believed they had enough time to stay up-to-date on cybersecurity threats. More than half of respondents (55%) at least somewhat agreed that they do have enough time.



Ability to Handle a Cyberattack

How confident are you that someone on your staff could thoroughly address a cyberattack?

When asked how confident IT decision makers would be that someone on their staff could deal with a cyberattack, a surprising 84% responded confidently. Given the other responses to this survey, this was unexpected, and indicates a discrepancy and possible misperception of IT resources, knowledge, and capability to thoroughly address a cyberattack. The response is particularly optimistic when considered alongside the data in the next graph.

Time Spent on Cybersecurity

How much time did you spend on cybersecurity in the past 6 months?

We asked IT decision makers how much time was spent actually working on cybersecurity issues over the past 6 months. An unexpected 56% reported having spent less than 17 hours (2 business days) in the past six months on cybersecurity. This is likely due to a lack of adequate IT support and resources dedicated to security education and prevention.

Outsourcing IT Solutions: Help or Hindrance

Would outsourcing increase your bandwidth to address other areas?

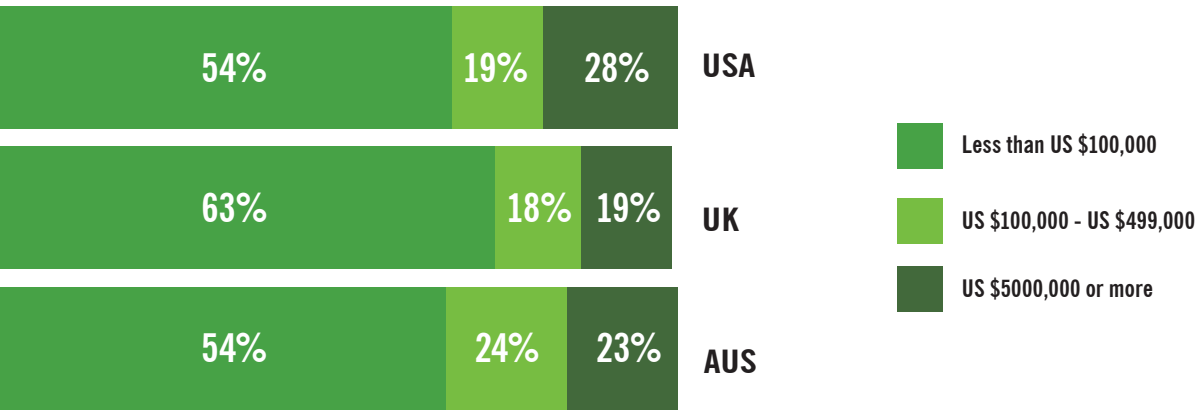
Many SMBs are outsourcing cybersecurity to managed services providers (MSPs) to make up for the lack of time and in-house expertise. 81% of respondents agreed such outsourcing would improve their bandwidth for addressing other tasks, while 53% agreed somewhat.

By what percentage do you expect to increase your Annual IT Security Budget for 2016?

Given the daily news about breaches at major retailers and other organizations, the majority of SMBs plan to increase their cybersecurity budget in 2016. This chart shows 81% increasing their budget by an average of 22%. This should help SMBs considerably improve their security postures, as they acquire or improve on cybersecurity resources and practices.

How much do you estimate the total cost of a cyberattack on your business would be in 2016?

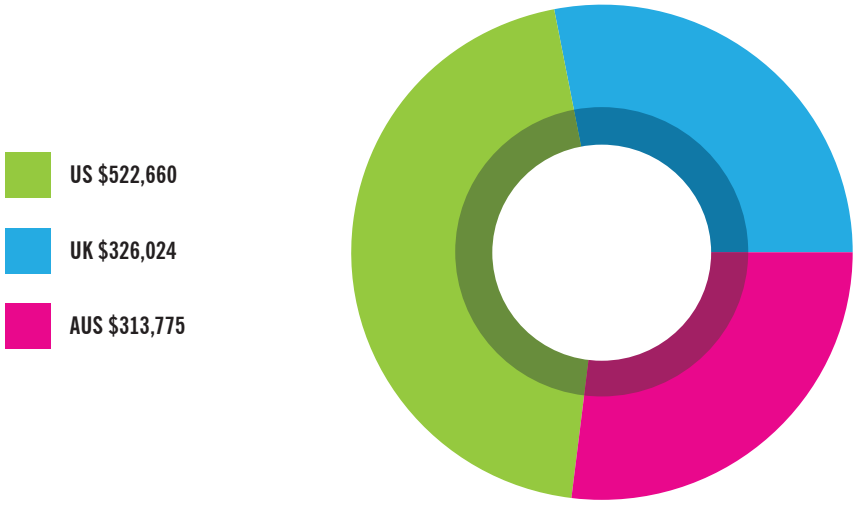
These figures from the survey illustrate why so many SMBs are planning to spend more on IT security in 2016. The impact of a cyberattack on lost customer records or other critical business data is severe. It's important to note there are some regional differences in the cost impact. The survey sample size for the US and Australia was very similar, while the UK had a 33% larger respondent group. This may explain the seemingly large differences in the graph. On average, however, between 37% and 47% of losses across all regions to a cyberattack would total at least a $100,000.



Financial Loss from Cyberattack by Region

Cyberattack Loss by Survey Region

When looking at the average losses measured in US dollars, we saw that losses in the US were considerably higher than in the UK or Australia. These estimates were based upon losses due to a potential cyberattack in 2016 that compromised customer or critical business records.



Regional Findings

Of particular note in the findings is the similarity between the US, UK and Australia. On nearly every measure, the responses were very close in percentile terms. Universally, SMBs across these regions are in a very similar situation with regard to these measures and pain points.

Notable disparities include: 50% of US respondents feel they don't have time to stay up-to-date latest cybersecurity threats, compared to 61% in Australia. Respondents in the US and UK also expressed more confidence in their endpoint protection capabilities (63%) than Australian respondents (55%).

Conclusions and Recommendations

Although SMBs appear more aware of cybersecurity-related risks to their organizations, many are still unsure or under-informed about their own readiness to handle such risks.

SMBs would benefit from researching newer technologies and cybersecurity practices, such as next-generation endpoint protection and threat intelligence. Endpoint security should not only stop infections effectively, but should also automate security management. By reducing or eliminating time-consuming operational burdens, such as ensuring all devices have the latest software updates, maintaining on-premise management and update servers, remediating infections or reimaging machines manually, etc., SMBs can free up their IT resources for other tasks.

The survey shows that respondents are open to strategies for improvement, with over 81% agreeing that outsourcing cybersecurity would improve their security posture and give them the bandwidth to address other critical areas of their business. With better targeting and funding, the goal of achieving that security posture is becoming increasingly attainable. For example, managed service providers can now deliver solutions that leverage new cloud-based cybersecurity architectures and allow organizations of all sizes to implement cost-effective protection that doesn't require high management costs or investing in new infrastructure.

SMBs no longer need to go it alone. Through a carefully considered mix of stronger cybersecurity approaches, increased spending, and management outsourcing, they can deploy and maintain the same business security as larger enterprises, for a fraction of the cost.

Survey Methodology

The Webroot SMB Cybersecurity Survey was conducted by Wakefield Research among 300 IT decision-makers in the UK, 200 IT decision-makers in the US, and 200 IT decision-makers in Australia from SMBs between October 28th and November 12th, 2015, using an email invitation and an online survey.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 3.7 percentage points for the overall sample and by more than 5.7 percentage points for the UK audience and 6.9 percentage points for the US and Australia audiences from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

About Webroot

Webroot provides Smarter Cybersecurity™ solutions. We provide intelligent endpoint protection and threat intelligence services to secure the Internet of Everything. By leveraging our cloud-based collective threat intelligence platform, computers, tablets, smartphones, and more are protected from malware and other cyberattacks. Our award-winning SecureAnywhere™ intelligent endpoint protection and BrightCloud® threat intelligence services protect tens of millions of consumer, business, and enterprise devices. Webroot technology is trusted and integrated into market-leading companies including Cisco, F5 Networks, HP, Microsoft, Palo Alto Networks, RSA, Aruba and many more. Webroot is headquartered in Colorado and operates globally across North America, Europe, and the Asia Pacific region. Discover Smarter Cybersecurity solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900