SURVEY REPORT

Survey Report: Australia

White Hat, Black Hat and the Emergence of the Gray Hat: The True Costs of Cybercrime

An Osterman Research White Paper

Published August 8, 2018

Sponsored by

Malwarebytes

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

Overview

Malwarebytes engaged Osterman Research to undertake an in-depth survey of security professionals in five countries: The United States, the United Kingdom, Germany, Australia and Singapore. This report focuses on the research that was conducted among organizations in Australia.

The goal of the research was to understand the organizational costs associated with cybercriminal activity, and to understand what motivates some security professionals to join the "dark side" – i.e., to become either "gray hats", who participate in criminal activity while also working as legitimate security professionals; or full-fledged "black hats" who operate solely within the realm of the cybercriminal underworld.

ABOUT THE SURVEY

Osterman Research conducted the survey during May and June 2018 with a total of 175 security professionals in Australia. In order to qualify for the survey, respondents:

- Must be involved in managing or working on cybersecurity-related issues in their organizations.
- Must work for an organization that has between 200 and 10,000 employees

A wide range of industries was surveyed, but the largest industries represented in the Australian survey were manufacturing (13 percent), technology (11 percent), financial services/insurance (nine percent and government (nine percent).

Please note that where dollar values are shown in this report, they are shown in Australian dollars.

Executive Summary

- **The total, direct cost of cybercrime is enormous**
  Organizations of all sizes can expect to spend an enormous amount on cybersecurity-related costs that fall into three basic areas: a) budgeted costs for cybersecurity infrastructure and services, including labor; b) off-budget costs associated with major events like an organization- or function-wide ransomware event; and c) dealing with the costs of insider security breaches. Our research found that an organization of 2,500 employees in Australia can expect to spend nearly A$1.16 million per year for cybersecurity-related costs.

- **The total cost of cybercrime includes the growing allure of cybercrime that motivates security professionals to become "gray hats"**
  A large proportion of security professionals are suspected of being "gray hats" – those who continue as security practitioners while also getting involved in cybercrime. In Australia, one in 29 security professionals are perceived to be gray hats, but this figure is actually higher in some other countries. Globally, mid-sized organizations (500 to 999 employees) are getting squeezed the hardest, and this is where the skills shortage, and the allure of becoming a gray hat, may be the greatest.

- **Most organizations have suffered security breaches**
  Our research found that the vast majority of organizations in Australia have suffered some type of security breach during the 12 months preceding the survey. The most commonly experienced type of attack was from phishing, but other attacks that were experienced included adware/spyware, ransomware and spearphishing. Only 33 percent of organizations reported no attacks of which respondents were aware during the 12 months leading up to the survey.

- **Mid-market companies face the worst of both worlds**
  Globally, mid-market companies – those with 500 to 999 employees – face the most difficult challenges from a security perspective: they encounter a higher rate of attack than smaller companies and similar rates of attack as their larger counterparts, but they have fewer employees over which to distribute the cost of the security infrastructure.

- **"Major" attacks occur with some frequency**
  Our research found that a "major" attack – i.e., one that would cause significant disruption to an organization's operations, such as a major ransomware attack that disrupted normal operations or completely shut down an organization's computing infrastructure for a day more – occur with alarming frequency. In Australia, organizations experienced 0.6 such attacks during 2017.

- **Gray hats are a serious threat**
  In Australia, we found that security professionals believe that 3.4 percent of their fellow security professionals are "gray

hats", or one in every 29 people working in a cybersecurity capacity. Underscoring the depth of the problem is the fact that 11 percent of security professionals admit to considering participation in black hat activity, 21 percent have actually been approached about doing so, and 42 percent either know or have known someone who has participated in this activity.

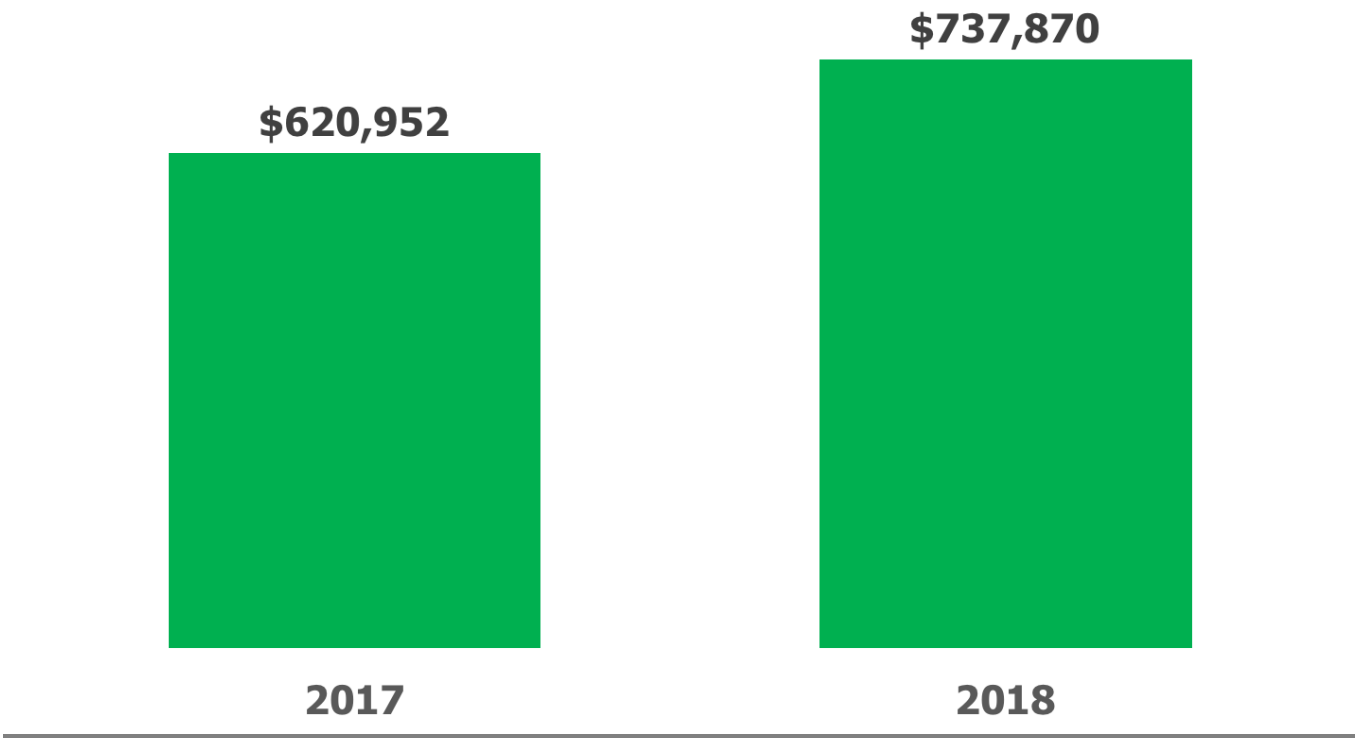
Survey Findings

THE COSTS OF CYBERSECURITY

We queried organizations about the size of their security budgets in 2017 and what they anticipated they would be in 2018. While we tallied these figures, a direct comparison is something of an "apples-to-oranges" comparison, since the organizations we surveyed have somewhat different mean numbers of employees. Instead, we calculated a per-employee figure for security expenditures and then multiplied these figures by 2,500 to show the security budgets evenly across all of the countries that were surveyed.

As shown in Figure 1, security budgets for the average Australian organizations of 2,500 employees was just under A$621,000 in 2017 and will increase to nearly A$738,000 in 2018, an increase of just under 19 percent. These expenditures represent per employee spending of A$248 in 2017 and A$295 in 2018. Our research discovered that security-related spending was the second lowest among the five nations we surveyed.

Figure 1
Security Budgets for a 2,500-Employee Organization
2017 and 2018



Source: Osterman Research, Inc.

REMEDIATING MAJOR SECURITY EVENTS IS LESS EXPENSIVE IN AUSTRALIA

The cost of remediating a major security event – one that would cause significant disruption to an organization's operations, such as a widespread ransomware attack – is not trivial. Our research found that Australian organizations would spend an average of just over A$223,000 to remediate a single such event, as shown in Figure 2. The Australian figure to address a major security event at A$223,180 is substantially lower than the global average of A$389,662, and the lowest in our survey.

Figure 2
Amounts That Would be Spent Remediating a "Major" Security Event

	AUSTRALIA	GLOBAL AVERAGE
IT and other labor	$77,057	$100,283
Software/hardware solutions	$87,717	$132,133
Direct costs (e.g., paying a ransom)	$17,558	$28,895
Fines	$4,362	$44,431
Legal fees	$27,118	$54,653
Other costs	$9,367	$29,267
TOTAL	**$223,180**	**$389,662**

Source: Osterman Research, Inc.

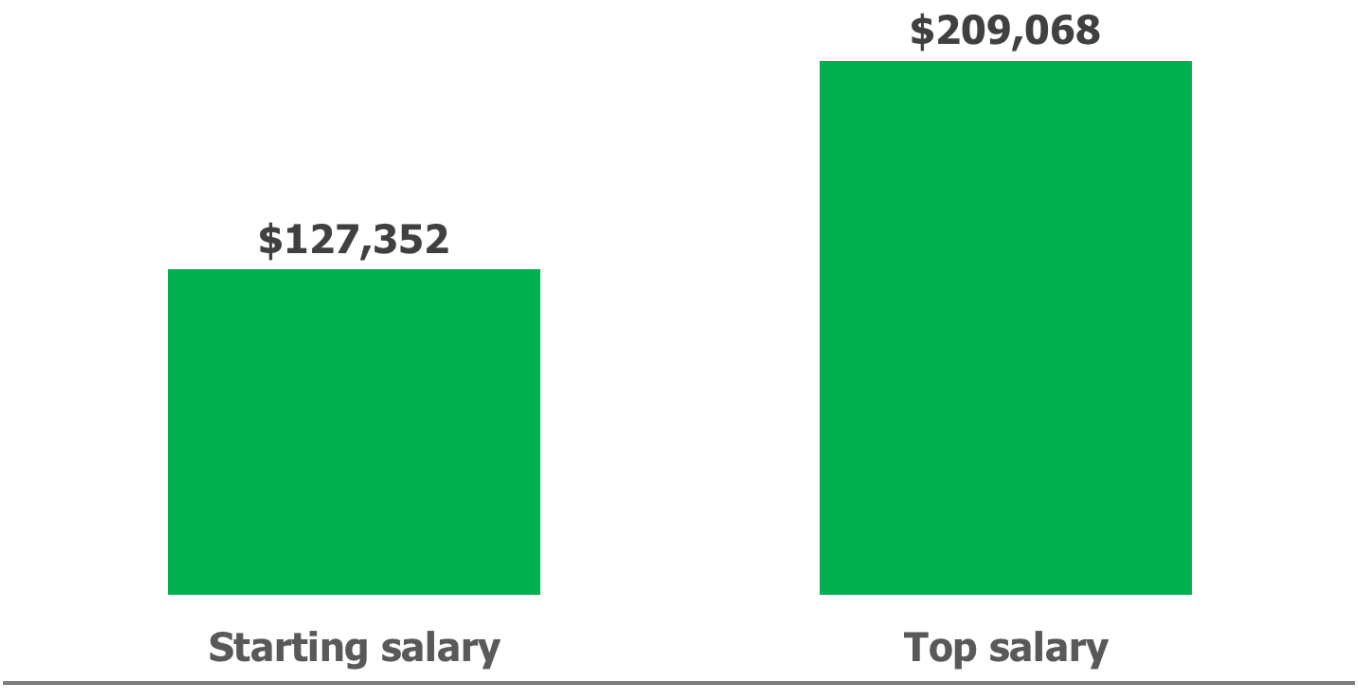
SECURITY EXPENDITURES THAT ADDRESS ACTIVE COMPROMISES

Australian organizations spend a relatively small proportion of their total security budgets remediating active compromises, such as malware intrusions, threat remediation, forensics and other costs associated with major and minor security events. Our research found that organizations in Australia spent just 7.9 percent of their 2017 budget on remediating active compromises. This was much lower than the global average of 12.5 percent and significantly than the other nations in which we surveyed.

SECURITY STAFF SALARIES ARE HIGH IN AUSTRALIA

Our survey found that the average starting salary for an entry-level security professional in Australia is just over A$127,000, by far the highest among the organizations we surveyed. As shown in Figure 3, the top annual salary for an Australian security professional is more than A$209,000, the highest among the nations in which we conducted the survey. Interestingly, we found that the ratio of the highest salary to the entry level salary was only 1.64:1, the lowest among the nations surveyed.

Figure 3
Entry Level and Maximum Salaries for IT Security Professionals

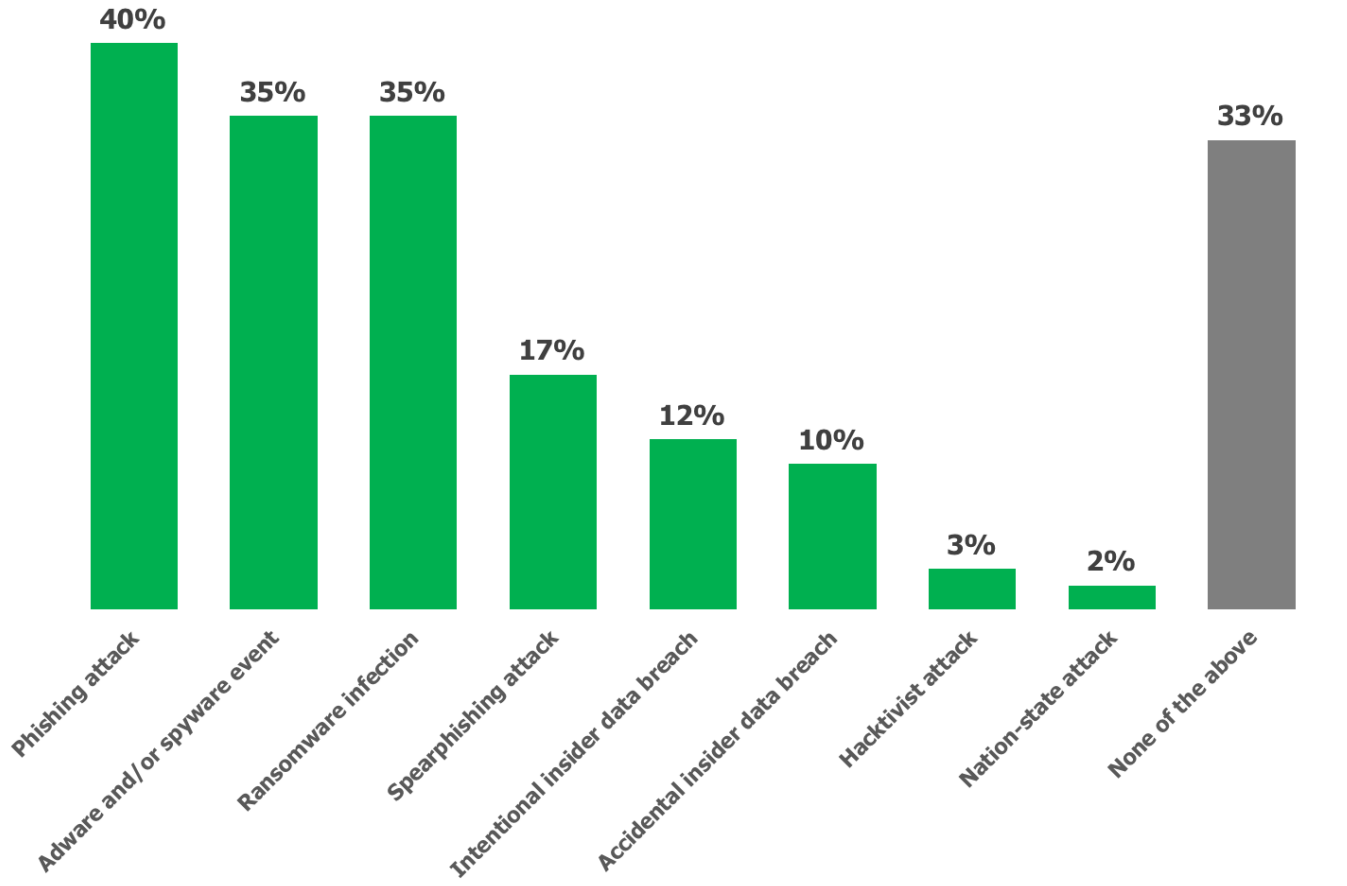


Source: Osterman Research, Inc.

TWO-THIRDS OF ORGANIZATIONS HAVE BEEN IMPACTED IN THE LAST YEAR

Australian organizations had a significant rate of infection during the last 12 months: 67 percent of Australian organizations were impacted by some sort of threat during the previous year, as shown in Figure 4, although this actually represented the second lowest rate of infection behind Germany. The most common attacks in Australia were focused on phishing, adware/spyware and ransomware, although several other types of attacks successfully infiltrated Australian organizations.

Figure 4
Security Events That Have Occurred During the Past 12 Months



Source: Osterman Research, Inc.

JUST HOW SERIOUS ARE VARIOUS THREATS?

Obviously, all security threats are serious to varying degrees, but we wanted to determine just how serious various threats actually are to security-focused decision makers in various countries. Toward that end, we asked decision makers to rate the following threats on a scale that ranged from "never serious" to "very serious":

- Ransomware
- Phishing
- Spearphishing
- Intentional insider breaches or losses
- Accidental insider breaches or losses
- Nation-state attacks/advanced persistent threats (APTs)
- Hacktivism
- Adware and/or spyware

Our research showed that Australian organizations take security threats very seriously: 62 percent of Australian organizations consider intentional insider breaches of data to be "very serious", and 41 percent take ransomware this seriously. When

averaging the "very serious" responses for Australian organizations, the average is 29 percent, the second lowest of the nations we surveyed.

Figure 5
Percent of Key Security Threats Considered to be Very Serious

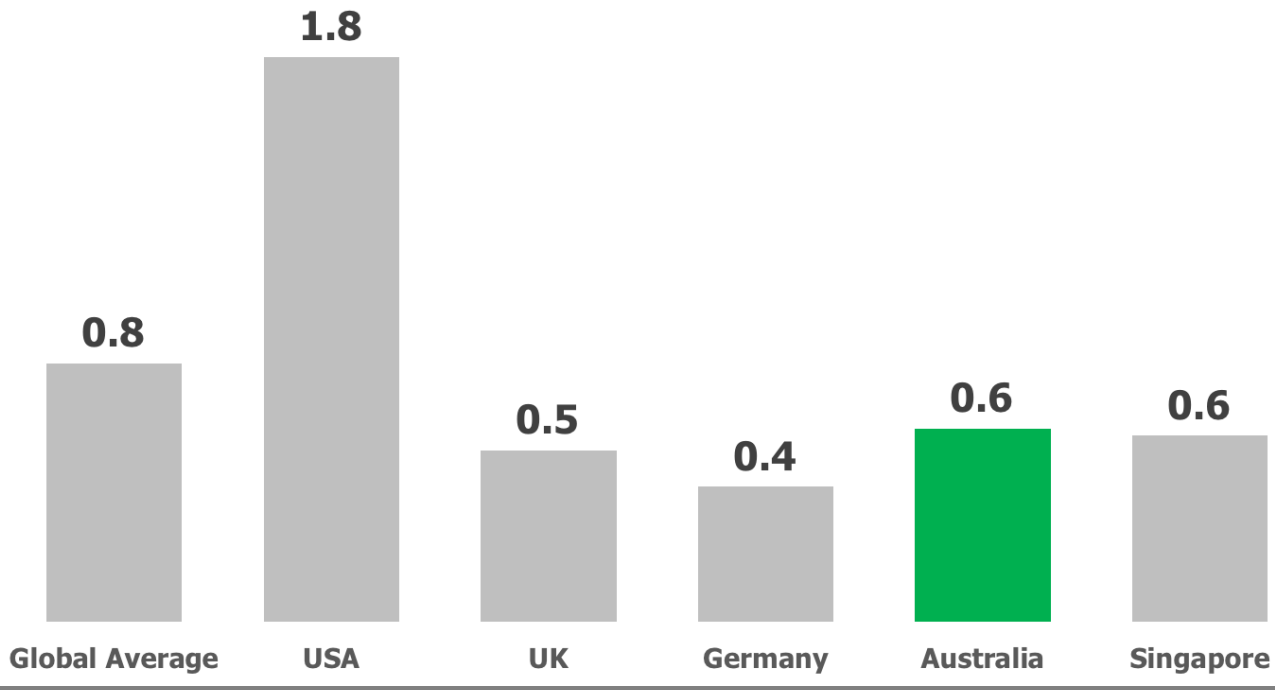
	Very Serious	Serious	Somewhat Serious	Rarely Serious	Never Serious
Ransomware	41.1%	20.6%	25.7%	12.6%	0.0%
Phishing	21.1%	32.6%	29.1%	17.1%	0.0%
Spearphishing	37.1%	49.1%	12.0%	1.7%	0.0%
Intentional insider breaches of data	62.3%	26.3%	9.7%	1.7%	0.0%
Accidental insider breaches of data	26.9%	39.4%	28.0%	5.7%	0.0%
Nation-state attacks/advanced persistent threats	14.3%	16.0%	33.7%	31.4%	4.6%
Hacktivism	8.6%	18.3%	51.4%	17.1%	4.6%
Adware and/or spyware	18.9%	29.1%	33.7%	18.3%	0.0%

Source: Osterman Research, Inc.

MAJOR SECURITY EVENTS ARE NOT COMMON IN AUSTRALIA

Major security events – e.g., those that cause significant expenditure of time, finances or other resources – are not common among the Australian organizations we surveyed, as shown in Figure 6. We found that during 2017, an average of only 0.6 such events occurred, tied for second lowest. This compares quite favorably with the global average of 0.8, and the 1.8 such events that occurred among organizations based in the United States.

Figure 6
Frequency of Major Security Events During 2017



Source: Osterman Research, Inc.

The Growing Threat of Black Hat Activity

BLACK HAT ACTIVITY IS A PROBLEM IN AUSTRALIA

As shown in Figure 7, a significant proportion of the individuals we surveyed in Australia have either considered participating in black hat activity, they have known someone who did so, or they have been approached about doing so. Even so, the Australian individuals we surveyed are among the lowest to have participated in black hat activity or to consider doing so. For example, when averaging the various practices and views shown in the table below, the average for Australian organizations was the second lowest among the nations surveyed.

Figure 7
Current Practices and Views Related to Black Hat Activity

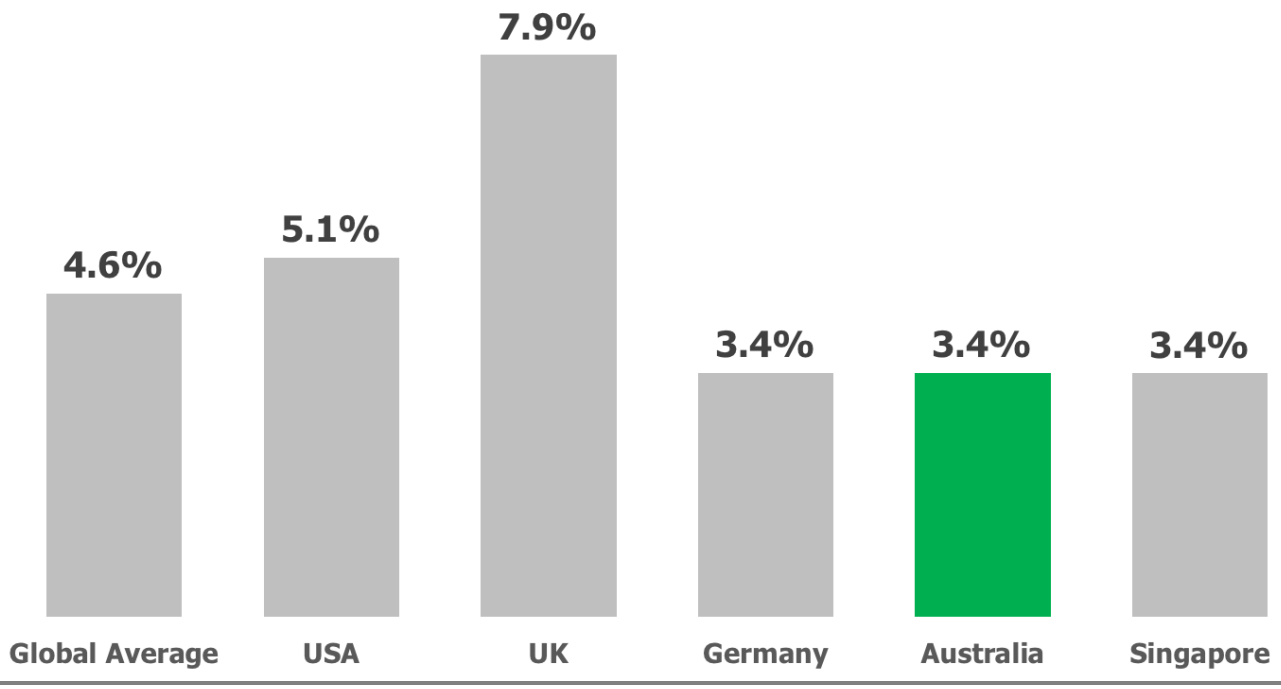
I know/have known someone that has participated in black hat activity	42.3%
I have been approached about participating in black hat activity	20.6%
We have hired a black hat hacker to consult with our organization	11.4%
I have considered participating in black hat activity	10.9%
We have used a black hat hacker for more than one project	8.0%
We conduct red/blue team activity to test the strength of our cybersecurity defenses	4.6%
None of the above	0.0%

Source: Osterman Research, Inc.

GRAY HATS ARE NOT A COMMON PROBLEM IN AUSTRALIA

We asked survey respondents about their co-workers in the context of cybersecurity and their willingness to become "gray hats" – i.e., staying in their job as a security professional while becoming a black hat hacker on the side. As shown in Figure 8, respondents in Australia believe that *only* 3.4 percent of their security colleagues are gray hats, tied for the lowest among the five nations we surveyed. This is in contrast to the UK, where 7.9 percent of security professionals are perceived to be gray hats.

Figure 8
Percentage of Employees Perceived to be "Gray Hats"



Source: Osterman Research, Inc.

BLACK HAT ACTIVITY IS EASY TO ENTER, BUT LEGAL ACTIVITY IS MORE LUCRATIVE

There is a perception among Australian security professionals that it's relatively easy to become involved in gray hat activity without being discovered, although most do not agree that becoming a cybercriminal is more lucrative than fighting cybercrime. For example, as shown in Figure 9, more than one-half of those we surveyed in Australia either agree or strongly agree that "it's easy to get into cybercrime without getting caught". However, nearly two-thirds of those surveyed agree or strongly agree that a career focused on fighting cybercrime will be more lucrative than actually becoming a cybercriminal.

Figure 9
Views on Key Issues Related to Cybercrime

It's easy to get into cybercrime without getting caught	
Strongly Agree	24.6%
Agree	27.4%
Neutral	21.1%
Disagree	26.3%
Strongly Disagree	0.6%

There is more money to be made in fighting cybercrime than being a cybercriminal	
Strongly Agree	24.6%
Agree	39.4%
Neutral	20.6%
Disagree	14.3%
Strongly Disagree	1.1%

Source: Osterman Research, Inc.

MANY BELIEVE BLACK HATS JUMP TO THE "DARK SIDE" FOR MONEY, CHALLENGE

The reasons for becoming a cybercriminal vary, as shown in Figure 10. Sixty-six percent of those surveyed in Australia believe that people become black hats because there is a perception that black hats earn more money than security professionals, 47 percent believe it offers interesting challenges, and 29 percent believe it's not wrong.

Figure 10
Perceived Reasons for Becoming a "Black Hat"

Earn more money than as a security professional	66.3%
The challenge that it offers	47.4%
It is not perceived as wrong	29.1%
Philosophical reasons or some sort of cause	21.7%
Retaliation against an employer	16.0%

Source: Osterman Research, Inc.

WHAT ARE THE MOST VULNERABLE INDUSTRIES?

The degree to which various industries are vulnerable to different types of threats varies. For example:

- Malwarebytes researchers have identified that healthcare is an industry exceptionally vulnerable to the threat posed by ransomware[i]. However, ransomware compromises in retail operations, legal firms and manufacturing operations[ii] have also shown these industries vulnerable.
- For APT attacks, government agencies were the leading target[iii].
- For Distributed Denial of Service (DDoS) and Trojan attacks, financial services firms are the primary target[iv].

From a cross-industry perspective, a 2017 Black Hat survey[v] found that 32 percent of respondents reported accessing privileged accounts was the leading option for easy and fast access to sensitive data, while accessing users' email was also a good option for accessing this data.

The Total Cost Impacts of Cybercrime

Cybercrime is a lucrative industry: while estimates of the impact of cybercrime vary, a recent analysis[vi] estimated the total impact of cybercrime at around A$2.0 trillion annually. The same analysis found that the five most lucrative forms of cybercrime – in terms of the annual revenue they generate – are crimeware/cybercrime-as-a-service; ransomware; illicit, illegal online markets; trade secret and IP theft; and data trading.

The primary goal of the survey discussed in this report was to gain a deep understanding of the total direct costs of cybercrime. While other studies have focused on the total economic impact of cybercrime, our goal was to answer this question: what does it cost an organization *directly* to deal with cybercrime.

Our research focused on three primary cost components:

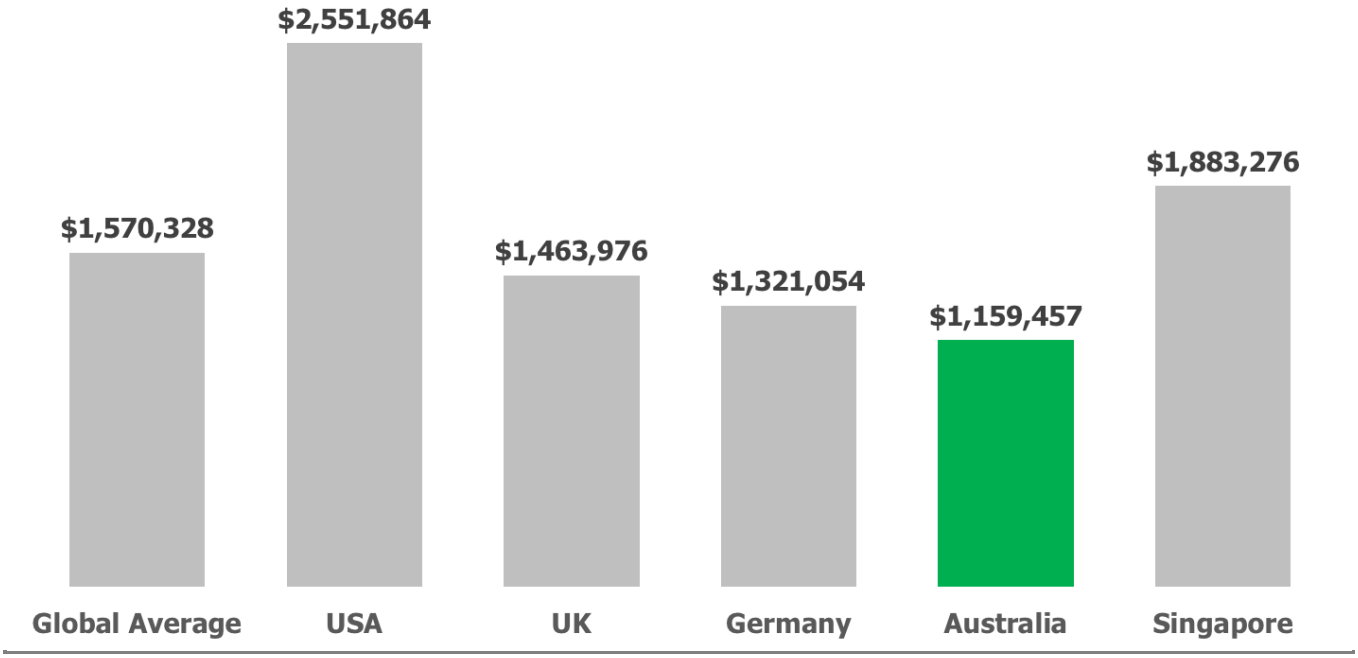
- The normal, budgeted costs of deploying and managing a security infrastructure.
- The off-budget costs associated with major events that require additional staff time, consultants, hardware, software, etc., and that can result in fines, legal costs and other expenses.
- The costs of insider threats – namely, breaches associated with gray hat activity.

We made the following assumptions in developing the calculations below:

- We used the security budget data collected in the survey, calculated the per-employee budget, and multiplied by 2,500 to simulate the costs for a 2,500-employee organization.
- We calculated the costs per employee for "major" events, multiplied these figures by the annual frequency of these types of events.
- We then used the Ponemon Institute's data on the average cost of a cybersecurity breach perpetrated by insiders. We assumed one such major breach per year and multiplied the figure of A$11.7 million by the percentage of security professionals who are perceived to be gray hats.

Based on this data and these assumptions, Figure 11 shows that the average annual security costs for a 2,500-employee Australian organization is A$1.16 million, the lowest among the nations we surveyed.

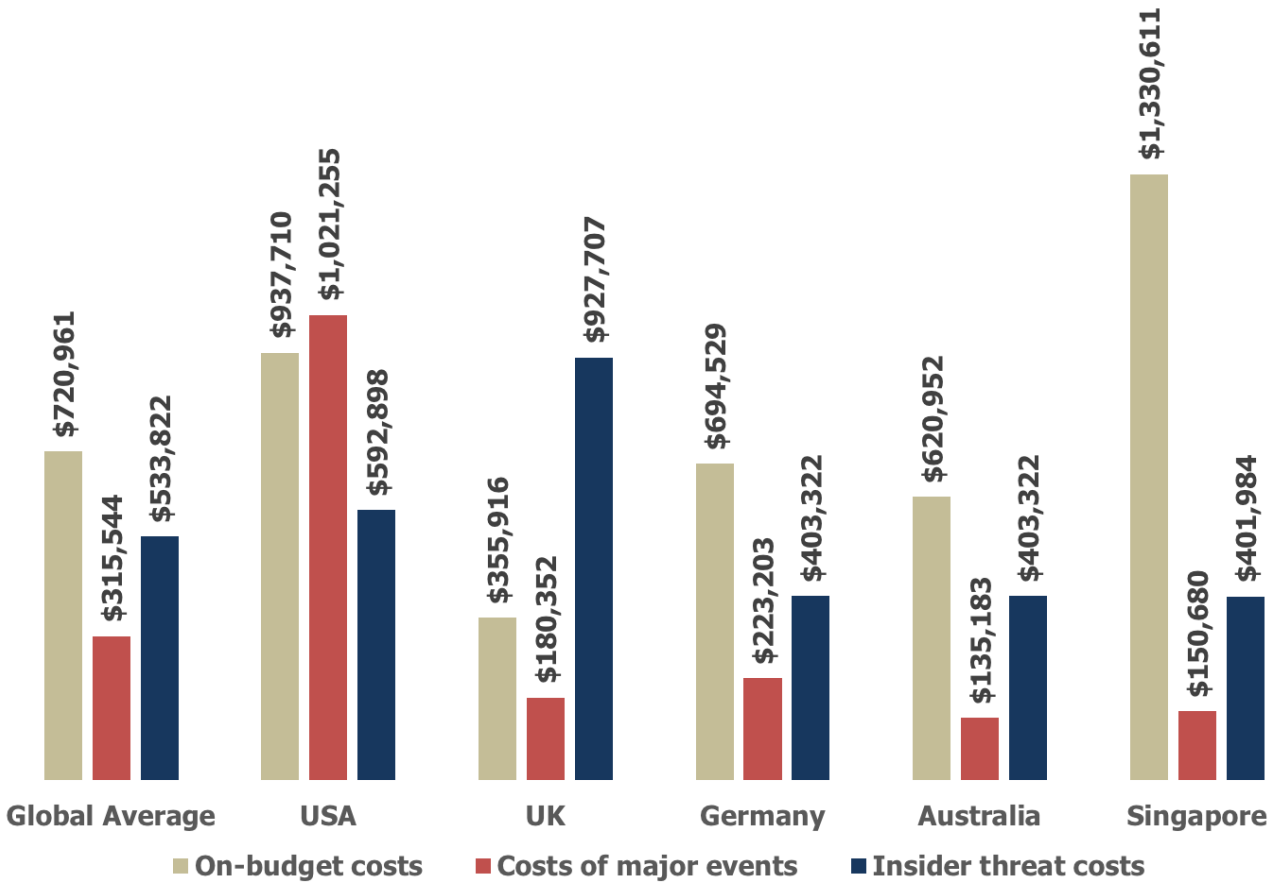
Figure 11
Total Annual Security Costs for a 2,500-Employee Organization



Source: Osterman Research, Inc.

The individual costs that make up total security costs vary widely across the three cost components noted above. For example, the costs in Australia are composed primarily of budget expenditures at 54 percent of the total, followed by insider threat costs at 35 percent and the cost of major events at only 12 percent. The breakdown of security costs in Australia and across the other countries in which the survey was conducted is shown in Figure 12.

Figure 12
Breakout of Total Annual Security Costs for a 2,500-Employee Organization



Source: Osterman Research, Inc.

About Malwarebytes

Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware and exploits that escape detection by traditional antivirus solutions. Malwarebytes completely replaces antivirus with artificial intelligence-powered technology that stops cyberattacks before they can compromise home computers and business endpoints. More than 60,000 businesses and millions of people worldwide trust and recommend Malwarebytes solutions. Our team of threat researchers and security experts process emerging and established threats every day, from all over the globe. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia. For more information, please visit us at http://www.malwarebytes.com/.

Malwarebytes founder and CEO Marcin Kleczynski started the company to create the best disinfection and protection solutions to combat the world's most harmful Internet threats. The market continues to recognize Marcin's advancements in cybersecurity with the recent recognition as "CEO of the Year" in the Global Excellence awards. He has also been named to the Forbes 30 Under 30 Rising Stars of Enterprise Technology list and received both the Silicon Valley Business Journal's 40 Under 40 and Ernst & Young Entrepreneur of the Year awards.

REFERENCES

[i] https://blog.malwarebytes.com/security-world/2016/03/canadian-hospital-serves-ransomware-via-hacked-website/

[ii] https://blog.malwarebytes.com/cybercrime/2017/07/real-problem-ransomware/

[iii] https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/rpt-government-atr-backgrounder.pdf

[iv] https://www.ibm.com/security/data-breach/threat-intelligence?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US&cm_mc_uid=26049271556314924539145&cm_mc_sid_50200000=75013371528812511957&cm_mc_sid_52640000=49751971528812511989

[v] https://www.blackhat.com/docs/us-17/2017-Black-Hat-Attendee-Survey.pdf

[vi] https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf