SURVEY REPORT

Survey Report: Global

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 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 900 security professionals. Two hundred of these individuals were surveyed in the United States and 175 were surveyed in each of the following countries: the United Kingdom, Germany, Australia and Singapore. 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 global survey were financial services/insurance (10 percent), manufacturing (10 percent), retail (nine percent), technology (nine percent) and healthcare (nine percent).

Please note that where dollar values are shown in this report, they were collected in local currencies and converted to US dollars using published exchange rates as of mid-June 2018.

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 the United States can expect to spend nearly $1.9 million per year for cybersecurity-related costs. While the costs are lower in most of the other countries surveyed, the global average exceeds $1.1 million for a 2,500-employee organization.

- **The total cost of cybercrime includes the growing allure of cybercrime that motivates security professionals to become "gray hats"**
  A significant proportion of security professionals are suspected of being "gray hats" – those who continue as security practitioners while also getting involved in cybercrime. Globally, one in 22 security professionals are perceived to be gray hats, but this figure jumps to one in 13 in the UK. 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 greatest.

- **Most organizations have suffered security breaches**
  Our research found that the vast majority of organizations 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, spearphishing, accidental and intentional data breaches, nation-state attacks, and hacktivist attacks. Only 27 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**
  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. Globally, we found that during 2017, 0.8 such attacks occurred to the organizations we surveyed – an average of one attack every 15 months – but US organizations were the hardest hit: an average of 1.8 attacks during 2017, or one every 6.7 months.

- **Gray hats are a serious threat**
  Globally, we found that security professionals believe that 4.6 percent of their fellow security professionals are "gray hats", or more than one in every 22 people working in a cybersecurity capacity. The problem is especially bad in the UK, where 7.9 percent – or one in every 13 security professionals – is suspected of being a gray hat. Underscoring the depth of the problem is the fact that 12 percent of security professionals admit to considering participation in black hat activity, 22 percent have actually been approached about doing so, and 41 percent either know or have known someone who has participated in this activity.

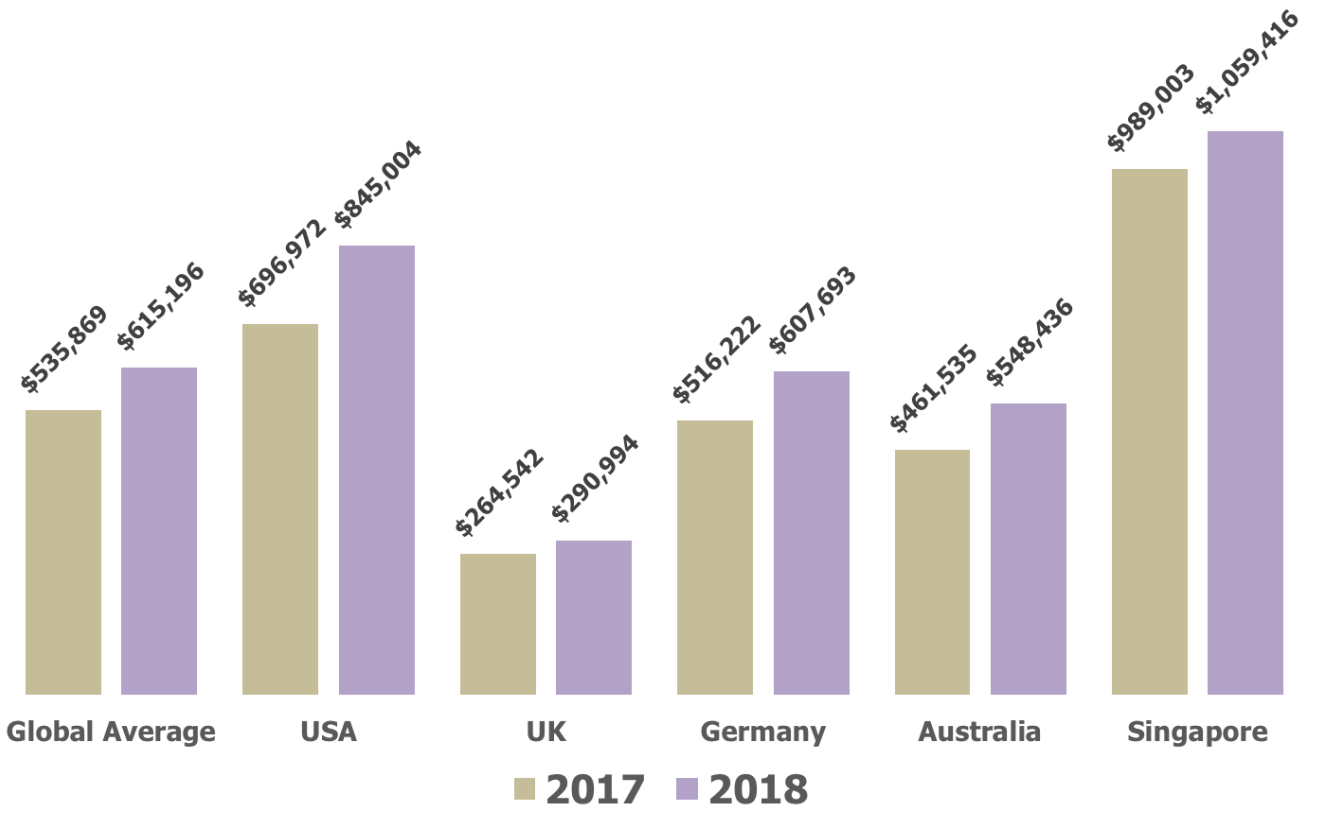
Survey Findings

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, Singaporean organizations had the largest security budgets in 2017 and will continue to have the largest budgets in 2018. By contrast, organizations in the UK and Australia had the lowest budgets in 2017 and also will in 2018. It is worth noting that security budgets in all countries are increasing from 2017 to 2018 – in fact, among the 900 organizations that we surveyed, 66 percent will be increasing security budgets in 2018, 25 percent will maintain the same level of spending, and only nine percent will decrease them.

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



Source: Osterman Research, Inc.

Not surprisingly, the research discovered that the larger the organization, the less that is spent on cybersecurity per employee because of the economies of scale that benefit larger organizations. For example, small organizations budgeted $850 per employee on cybersecurity in 2017, mid-market organizations spent $515, but for large organizations the budget dropped to just $192 per employee.

THE COSTS OF REMEDIATING MAJOR SECURITY EVENTS

Remediating a major security is expensive: we found that the average global expenditure for remediating just a single event is just under $290,000, although this ranges from a low of $249,562 in the UK to a high of $429,133 in the United States. As shown in Figure 2, the greatest expenditures in remediating a major security event are focused on the various software and hardware solutions that will be brought to bear for recovery, as well as IT and other labor focused on remediation. Together, these account for 60 percent of the costs associated with recovery, although other costs like legal fees, fines and various other costs impose a significant financial penalty on impacted organizations.

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

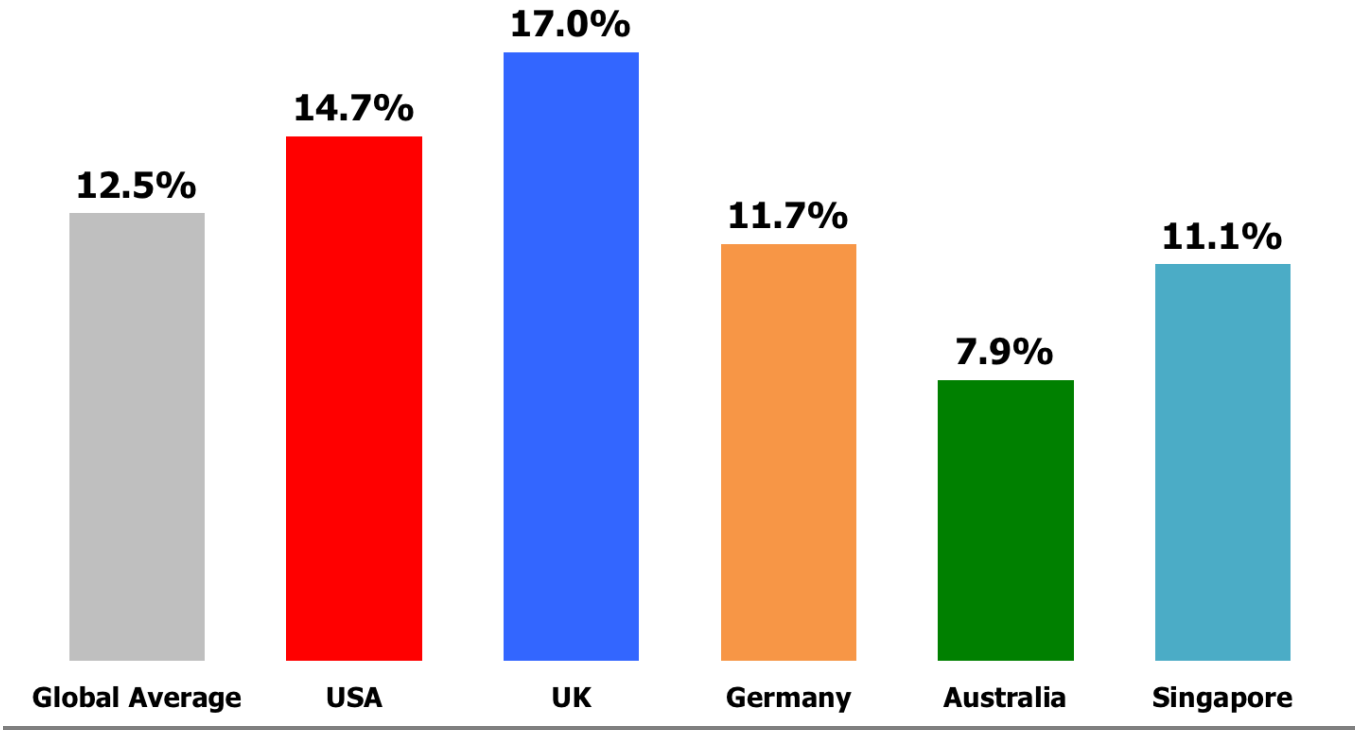
	GLOBAL AVERAGE	USA	UK	Germany	Australia	Singapore
IT and other labor	$74,538	$70,038	$68,322	$123,790	$57,274	$48,377
Software/hardware solutions	$98,211	$87,930	$95,461	$224,918	$65,198	$37,741
Direct costs (e.g., paying a ransom)	$21,477	$41,446	$15,412	$2,635	$13,051	$29,989
Fines	$33,024	$83,464	$11,746	$6,085	$3,242	$46,277
Legal fees	$40,622	$83,421	$39,325	$14,685	$20,156	$27,920
Other costs	$21,754	$62,833	$19,295	$20,219	$6,962	$1,847
TOTAL	**$289,624**	**$429,133**	**$249,562**	**$392,332**	**$165,883**	**$192,150**

Source: Osterman Research, Inc.

SECURITY EXPENDITURES ADDRESSING ACTIVE COMPROMISES

Remediating various types of active compromises consumes a significant proportion of security budgets. As shown in Figure 3, the global average is one in every eight budgeted security dollars, although this ranges from a high of 17 percent in the UK to a low of eight percent in Australia.

Figure 3
Percentage of Total Security Expenditures in 2017 Spent on Remediating All Active Compromises

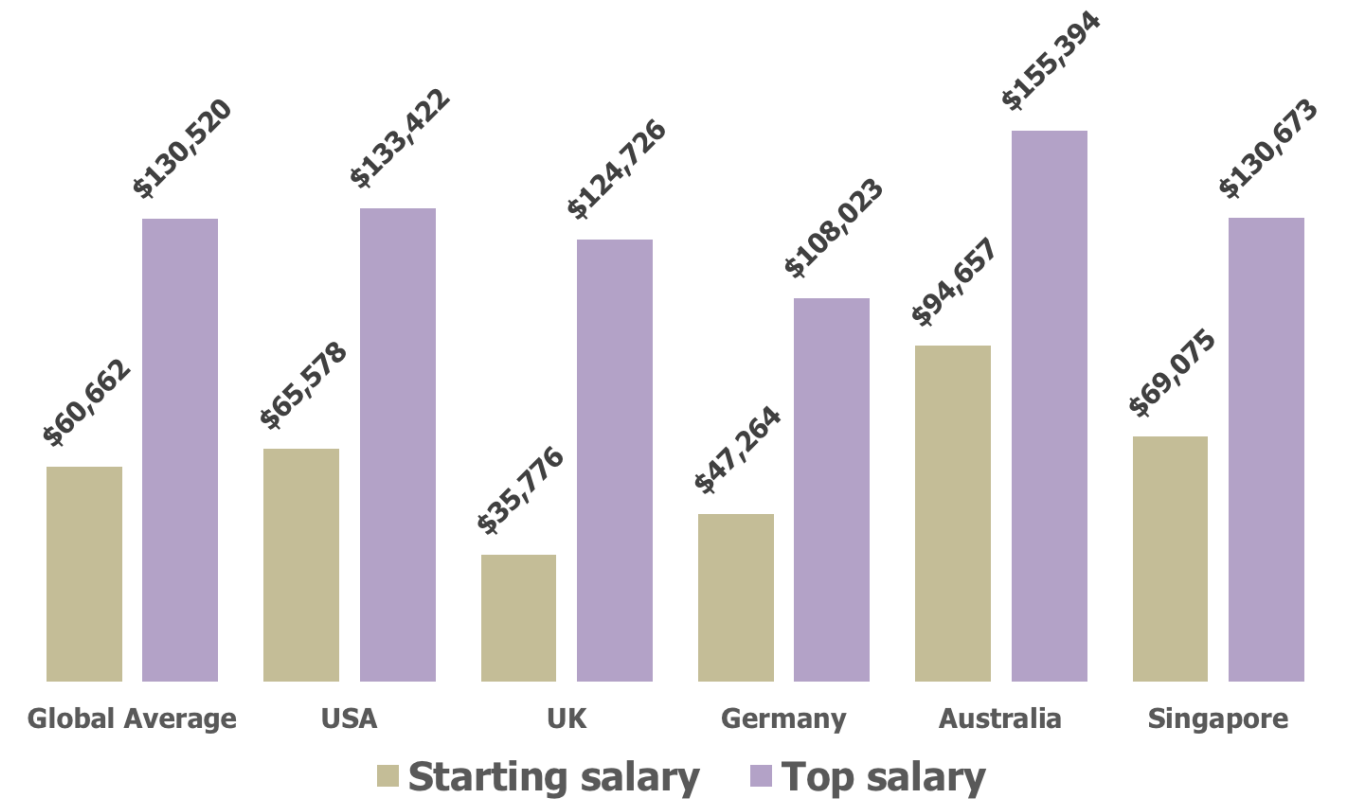


Source: Osterman Research, Inc.

SECURITY STAFF COSTS

The salaries for entry level and senior IT security staff covers a wide range depending on the country in question, as shown in Figure 4. For example, the highest starting salary for an entry-level IT staffer in Australia came in the highest at nearly $95,000 per year, while the lowest salaries were in the UK and Germany. Not surprisingly, the highest salaries for senior IT security staff members are in Australia, but we found the smallest difference between entry-level and highest salaries in Australia, as well. For example, as shown in Figure 4, the ratio of highest-to-entry-level security staff salaries in Australia was only 1.64, while the UK had the highest upside potential with a ratio of 3.49.

Figure 4
Entry Level and Maximum Salaries for IT Security Professionals

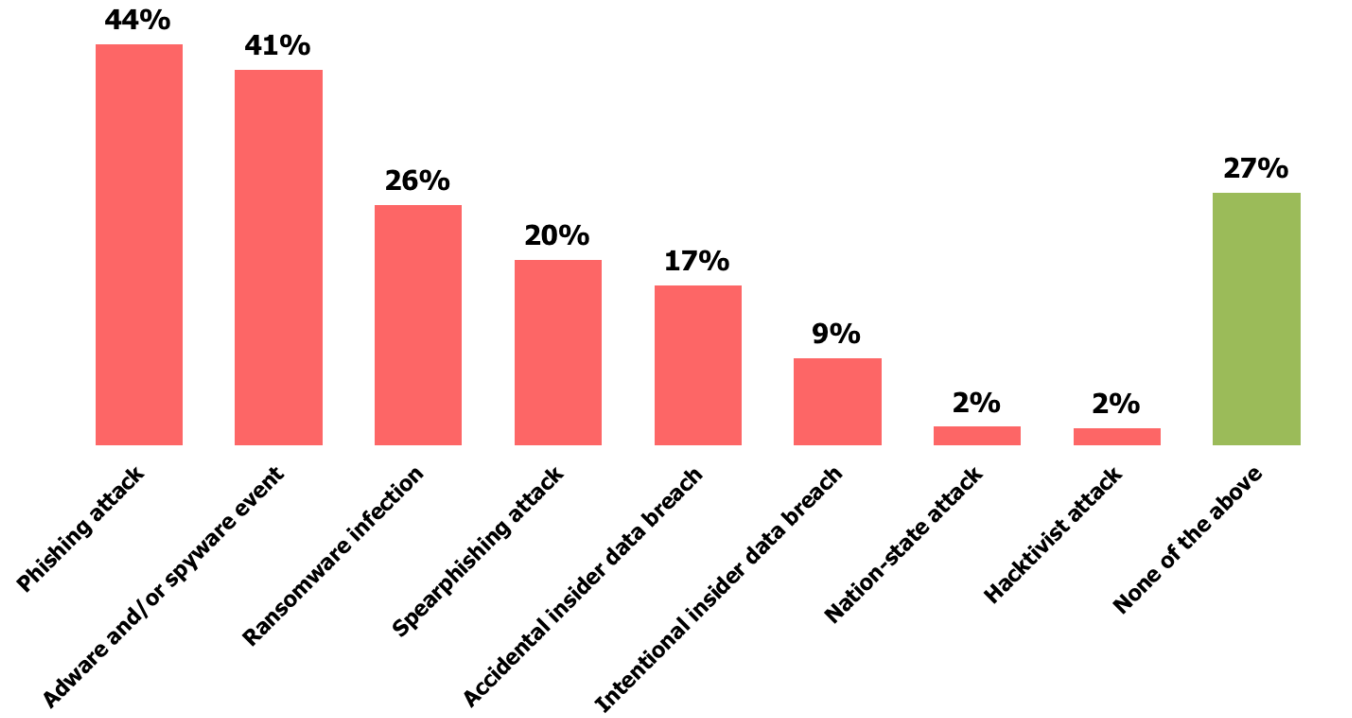


Source: Osterman Research, Inc.

THREATS THAT HAVE IMPACTED ORGANIZATIONS

Our research found, during the past 12 months, that the vast majority of organizations have been impacted by some type of security "event", as shown in Figure 5. While the most common type of attack was focused on phishing, which represented 44 percent of attacks (and the vast majority of that through email), adware or spyware (41 percent), ransomware (26 percent), spearphishing (20 percent), accidental data breaches (17 percent), intentional data breaches (nine percent), and nation-state and hacktivist attacks (each at two percent). In fact, on a global level 73 percent of organizations were impacted by a threat of some kind during the past 12 months.

Figure 5
Security Events That Have Occurred During the Past 12 Months



Source: Osterman Research, Inc.

It is important to note three things about the survey data in the figure above:

1. There are significant differences between the results for the individual countries in which surveys were conducted. For example, while phishing was quite common in the UK and United States, the incidence of phishing in Germany was substantially lower.

2. Mid-market organizations (those with 500 to 999 employees) actually received slightly more phishing attacks than their larger counterparts and significantly more than their smaller ones. It is noteworthy that as the size of the organization increases, so does the likelihood of becoming a victim of cybercrime.

HOW SERIOUS ARE VARIOUS THREATS?

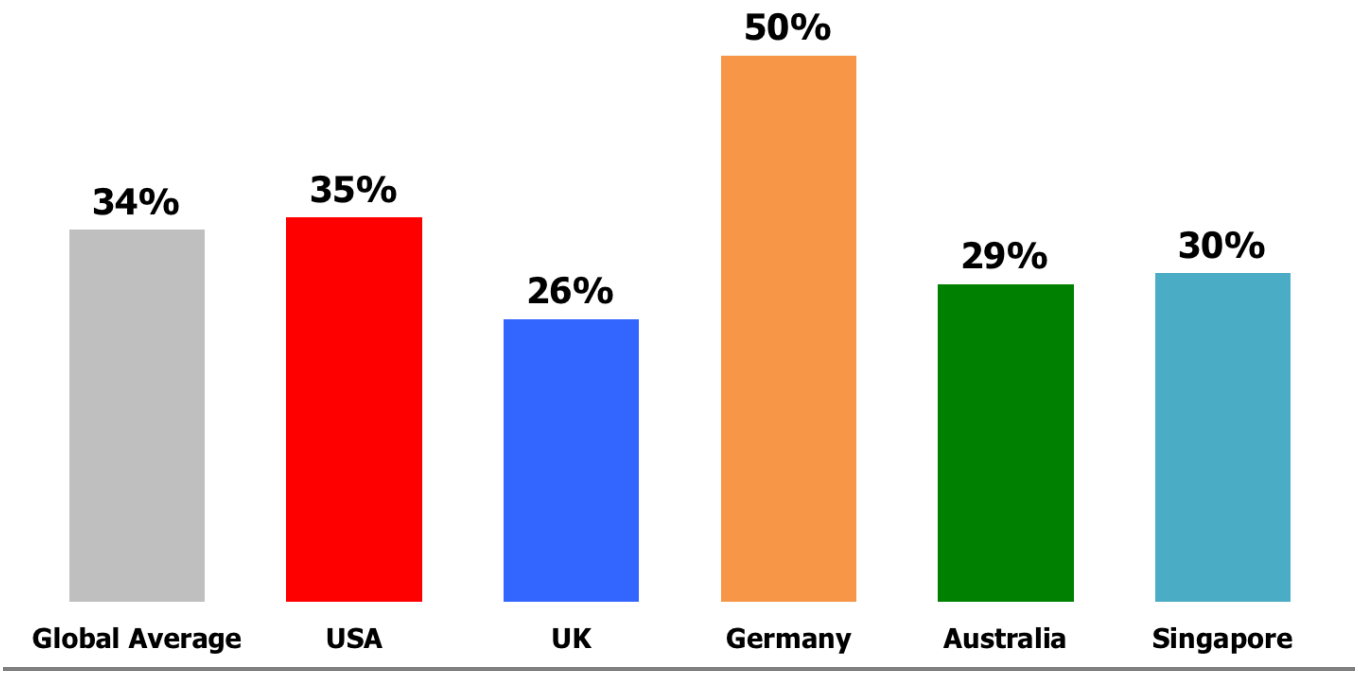
Obviously, all security threats are serious to varying degrees, but we wanted to determine just how serious various threats actually are to security-focused decision makers in various countries. Toward that end, we asked decision makers to rate the following threats on a scale that ranged from "never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

The research found significant disparity among the individual countries and threats. For example, 63 percent of German organizations consider ransomware to be a "very serious" threat compared to only 30 percent of UK-based organizations. By contrast, while 43 percent of US-based organizations consider nation-state attacks/APTs to be "very serious", only 14 percent of Australian organizations consider them to be this serious.

Figure 6 shows the average percentage of the eight security threats shown above that are considered to be "very serious". The data clearly reveal that German organizations take a much higher view of the seriousness of various types of security threats, while UK-based organizations are, on balance, less concerned.

Figure 6
Percent of Key Security Threats Considered to be Very Serious

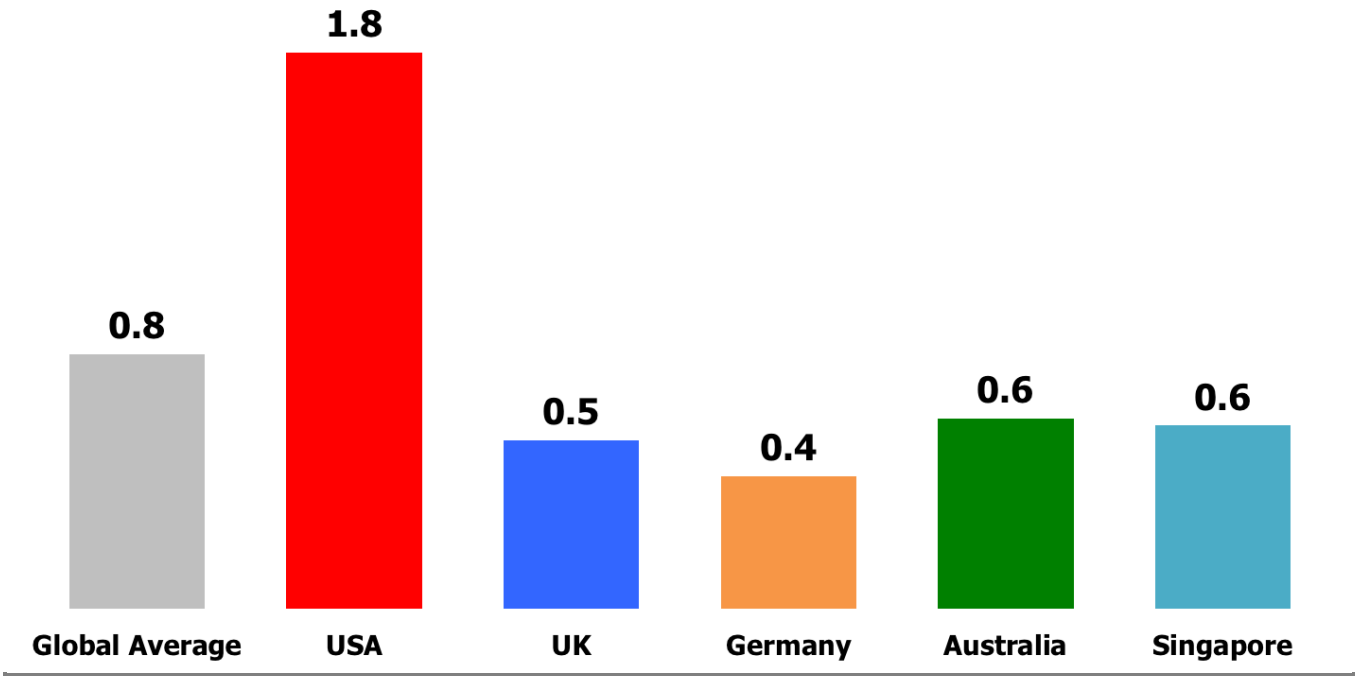


Source: Osterman Research, Inc.

FREQUENCY OF MAJOR SECURITY EVENTS

Our research also focused on the frequency of "major" security events. By a "major" event, we meant 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. We found that US-based organizations experienced a much higher number of these types of very serious events – an average of 1.8 of them in 2017 – compared to the organizations in the other countries we surveyed, as shown in Figure 7.

Figure 7
Frequency of Major Security Events During 2017



Source: Osterman Research, Inc.

When the data on major events was broken out by size of organization, we discovered, that mid-market and large organizations had roughly the same level of such events during 2017: 0.9 and 1.0, respectively. We also discovered that the larger the organization, the more it spends on remediating all active compromises. For example, smaller organizations spent 9.9 percent of their 2017 budget on remediating these compromises, whereas mid-market organizations spent 12.2 percent of their budget and large organizations spent 14.1 percent.

The Growing Threat of Black Hat Activity

BLACK HAT ACTIVITY IS COMMON

Our research discovered a number of interesting findings about the commonality of black hat activity, as shown in Figure 8:

- Globally, 41 percent of survey respondents admitted that they either know or have known someone who has participated in black hat activity. Survey respondents in the United States were most likely to make this admission (51 percent) and least likely in Germany (26 percent). In fact, globally 12 percent of survey respondents themselves have actually considered participating in black hat activity, with the most common prevalence of this in the UK (21 percent) and the lowest likelihood in the United States (eight percent).

- Twenty-two percent of survey respondents have been approached about participating in black hat activity. This was most common in the UK (32 percent) and least common in Germany (14 percent).

- Eleven percent of respondent organizations have hired a black hat hacker to consult with them about security issues. This was most common in Singapore (19 percent) and least common in Germany (six percent).

- Globally, 17 percent of organizations conduct red/blue team activity to test the strength of their cybersecurity defenses. However, US organizations are twice as likely to do so (34 percent) and Australian organizations the least likely (five percent).

Figure 8
Current Practices and Views Related to Black Hat Activity

	GLOBAL AVERAGE	USA	UK	GERMANY	AUSTRALIA	SINGAPORE
We have hired a black hat hacker to consult with our organization	**11.3%**	11.5%	8.6%	6.3%	11.4%	18.9%
We have used a black hat hacker for more than one project	**8.4%**	5.5%	9.7%	2.9%	8.0%	16.6%
I know/have known someone that has participated in black hat activity	**41.4%**	50.5%	40.0%	26.3%	42.3%	46.9%
I have considered participating in black hat activity	**12.2%**	8.0%	20.6%	8.6%	10.9%	13.7%
I have been approached about participating in black hat activity	**21.7%**	22.0%	32.0%	14.3%	20.6%	19.4%
We conduct red/blue team activity to test the strength of our cybersecurity defenses	**17.3%**	34.0%	10.3%	15.4%	4.6%	20.0%
None of the above	**1.6%**	7.0%	0.0%	0.0%	0.0%	0.0%

Source: Osterman Research, Inc.

Other research underscores just how serious the black hat phenomenon has become: a 2017 study[i] by the UK's National Crime Agency discovered that 61 percent of hackers, many of whom began by trying to cheat in video games, started their criminal activity before the age of 16, while the average age of those arrested for hacking activity is 17 years of age. The report concluded that there are a number of motivating factors for young people to get into hacking:

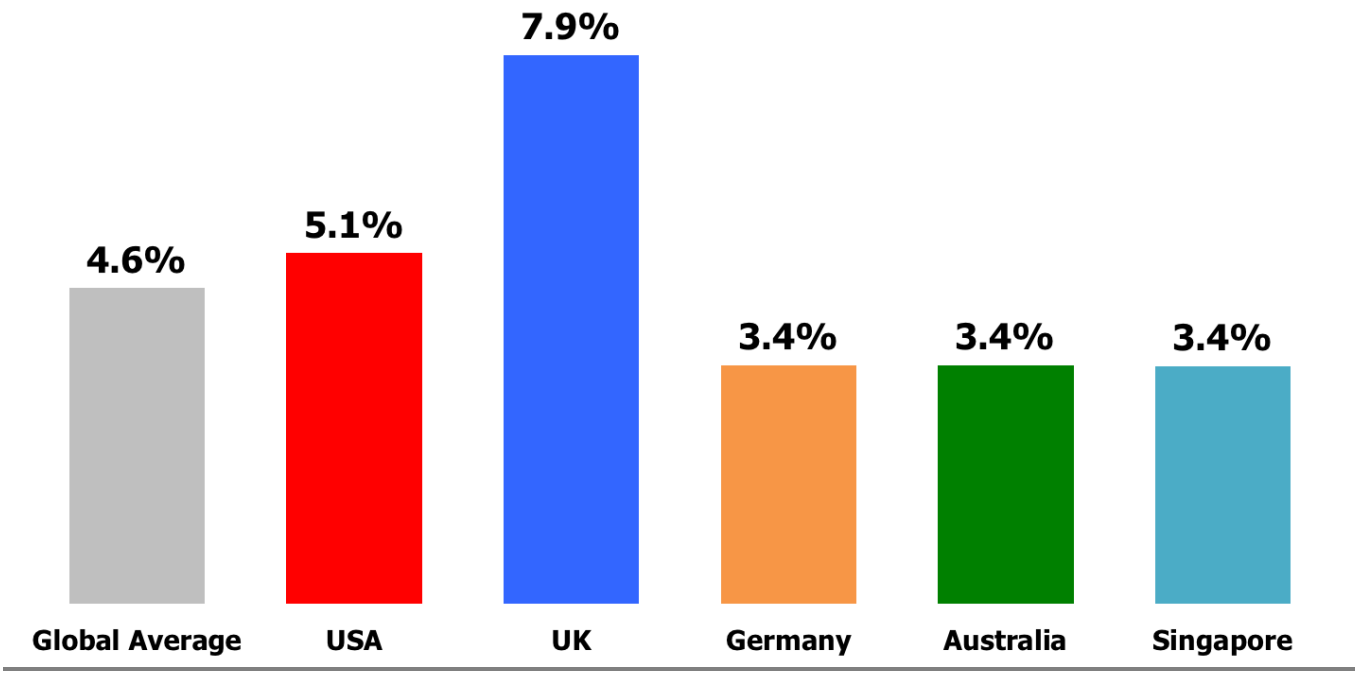
- Their access to technology
- The perception that hacking is a "victimless" crime
- Simple curiosity
- A desire to increase personal skills
- The perception that hacking can make its perpetrators popular
- The ability to enhance reputation among their peers.

While the stereotype of the lone hacker is a common one, the study found that online social relationships are a key component in motivating young people to become black hats and to continue in the activity. More ominously, the study found that young black hats are unlikely to be involved in traditional forms of crime.

THE COSTS OF SECURITY PROFESSIONALS SWITCHING TO THE "DARK SIDE"

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 9, respondents globally believe that 4.6 percent of their security colleagues are gray hats, although the highest prevalence is in the UK, where 7.9 percent of respondents told us that they believe their security colleagues are gray hats.

Figure 9
Percentage of Employees Perceived to be "Gray Hats"



Source: Osterman Research, Inc.

Our research discovered that the proportion of gray hats increases with the size of the organization. For example, while gray hats represent 2.8 percent of IT security professionals in small organizations, this figure increases to 4.2 percent for mid-market organizations and 5.7 percent for large ones.

MANY AGREE THAT BLACK HAT ACTIVITY IS EASY TO ENTER AND LUCRATIVE

Is it easy to get involved in cybercrime without getting caught? Forty-six percent of those we surveyed globally believe that's the case, as shown in Figure 10. We found quite a bit of difference in the survey results for this question, from a low of only seven percent in the UK who "strongly agree" that it's easy to get into cybercrime without getting caught to a high of 25 percent in Australia. We also found that security professionals in mid-market organizations are the most likely to "strongly agree" that it's easy to get into cybercrime without being caught.

Conversely, most agree that there is more money to be made in fighting cybercrime than in being a cybercriminal, as shown in Figure 10. We did not encounter significantly variability for this question.

Figure 10
Views on Key Issues Related to Cybercrime

It's easy to get into cybercrime without getting caught	GLOBAL AVERAGE	USA	UK	GERMANY	AUSTRALIA	SINGAPORE
Strongly Agree	**14.1%**	11.6%	7.4%	19.4%	24.6%	8.0%
Agree	**32.4%**	35.9%	38.9%	32.0%	27.4%	27.4%
Neutral	**21.6%**	21.7%	20.6%	21.1%	21.1%	23.4%
Disagree	**26.9%**	23.2%	30.3%	20.6%	26.3%	34.9%
Strongly Disagree	**4.9%**	7.6%	2.9%	6.9%	0.6%	6.3%

There is more money to be made in fighting cybercrime than being a cybercriminal	GLOBAL AVERAGE	USA	UK	GERMANY	AUSTRALIA	SINGAPORE
Strongly Agree	**16.4%**	15.7%	11.4%	16.6%	24.6%	13.7%
Agree	**36.7%**	30.3%	38.9%	39.4%	39.4%	36.6%
Neutral	**21.2%**	26.8%	17.1%	20.0%	20.6%	20.6%
Disagree	**21.7%**	23.7%	30.9%	17.1%	14.3%	22.3%
Strongly Disagree	**4.0%**	3.5%	1.7%	6.9%	1.1%	6.9%

Source: Osterman Research, Inc.

While financial gain is clearly a motivator for many to become involved in black hat activity, this is not as important a driver as one might think. For example, one study[ii] found that 86 percent of hackers enjoyed the challenge of the activity and were motivated by curiosity and wanting to learn more about hacking and related activities. The same study found that 35 percent enjoy the entertainment of hacking, 21 percent of hackers were motivated by financial gain, while six percent are motivated by political or social reasons.

MANY BELIEVE BLACK HATS EARN MORE MONEY

There are a number of reasons that security professionals see as reasons for becoming a black hat, but the most common reason cited in our research is the ability to earn more money than by working as a security professional, as shown in Figure 11. This view is most widely held in Singapore, and least widely held in the UK and Germany. A number of other reasons were cited by survey respondents as reasons for becoming a black hat, including the challenge that it offers, some sort of retaliation against an employer, and philosophical reasons.

Figure 11
Perceived Reasons for Becoming a "Black Hat"

	GLOBAL AVERAGE	USA	UK	GERMANY	AUSTRALIA	SINGAPORE
Earn more money than as a security professional	**62.5%**	58.8%	53.7%	55.4%	66.3%	78.9%
The challenge that it offers	**50.4%**	47.7%	53.1%	61.1%	47.4%	42.9%
Retaliation against an employer	**39.7%**	53.3%	38.3%	50.3%	16.0%	38.9%
It is not perceived as wrong	**33.7%**	22.1%	29.7%	40.0%	29.1%	49.1%
Philosophical reasons or some sort of cause	**38.8%**	49.7%	31.4%	53.7%	21.7%	36.0%

Source: Osterman Research, Inc.

As noted in Figure 11, the majority of those surveyed by Osterman Research believe that a key reason for becoming a black hat is that participants can earn more than they can as a security professional. Corroborating this finding is a study[iii] that showed the most lucrative cybercriminals can earn in excess of $166,000 per month, mid-range earners can make $75,000 per month, and that even at the low end of the earnings scale, cybercriminals can earn more than $3,500 per month – more than some entry-level security professionals make. Moreover, cybercriminals can earn 10 percent to 15 percent more than traditional criminals. A PayScale analysis[iv] finds that ethical hackers can earn approximately $72,000 per year – about the mid-range of what the typical hacker earns – and that ethical hacking consultants can earn anywhere from $15,000 to $45,000 per assignment.

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[v]. However, ransomware compromises in retail operations, legal firms and manufacturing operations[vi] have also shown these industries vulnerable.

- For APT attacks, government agencies were the leading target[vii].

- For Distributed Denial of Service (DDoS) and Trojan attacks, financial services firms are the primary target[viii].

From a cross-industry perspective, a 2017 Black Hat survey[ix] 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[x] estimated the total impact of cybercrime at around $1.5 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:

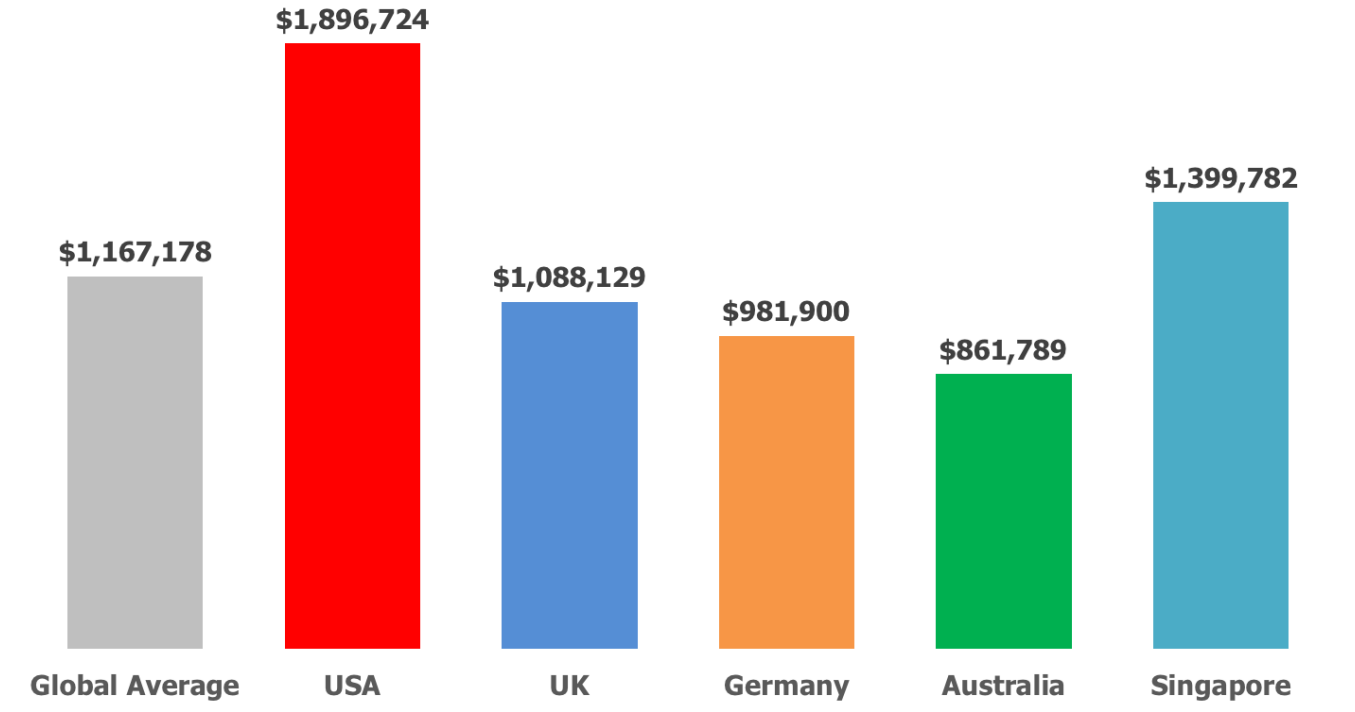
- We used the security budget data collected in the survey, calculated the per-employee budget, and multiplied by 2,500 to simulate the costs for a 2,500-employee organization.

- 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 $8.7 million by the percentage of security professionals who are perceived to be gray hats.

Based on this data and these assumptions, Figure 12 shows that the average annual security costs for a 2,500-employee organization worldwide is $1.17 million. Across the regions we surveyed, these figures differ widely, from a low of just under $862,000 in Australia to a high of $1.90 million in the United States.

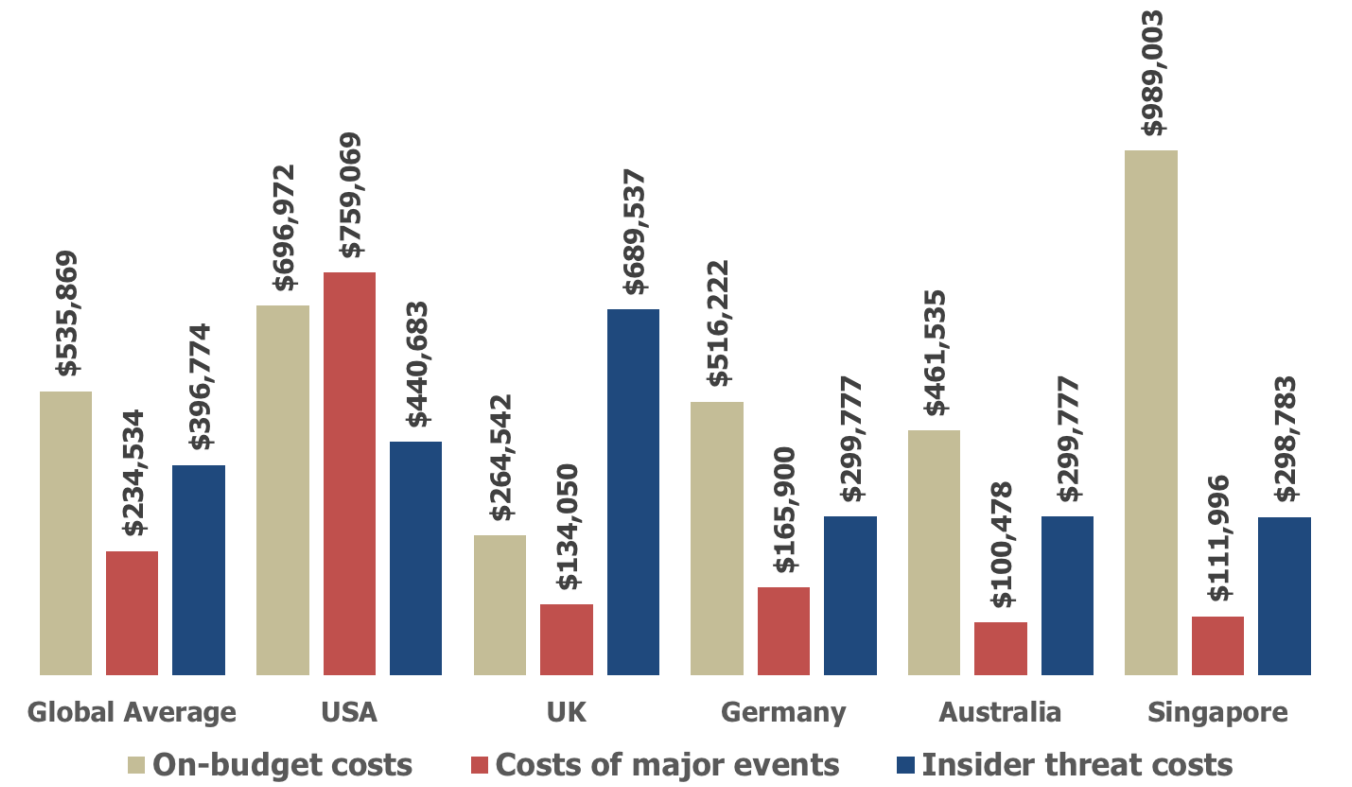
Figure 12
Total Annual Security Costs for a 2,500-Employee Organization



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 global costs are composed primarily of budget expenditures at 46 percent of the total, followed by insider threat costs at 34 percent and the cost of major events at 20 percent. However, the breakdown of security costs in the UK is dominated by the costs of insider threats at 63 percent of the total, whereas in Singapore the primary cost is the security budget itself at 71 percent. The breakdown of security costs globally and by country is shown in Figure 13.

Figure 13
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] http://www.nationalcrimeagency.gov.uk/publications/791-pathways-into-cyber-crime/file

[ii] https://www.nuix.com/sites/default/files/report_nuix_black_report_2018_web_us.pdf

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

[iv] https://www.payscale.com/research/US/Job=Certified_Ethical_Hacker_(CEH)/Salary

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

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

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

[viii] 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

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

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