SURVEY REPORT

Survey Report: USA

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 the United States.

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 200 security professionals in the United States. 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 US survey were healthcare (13 percent), education (12 percent), financial services/insurance (11 percent) and government (nine percent).

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.

- **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 the United States, one in 20 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 the United States 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, spearphishing and ransomware. Only 24 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 the United States, 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**
  In the United States, we found that security professionals believe that 5.1 percent of their fellow security professionals are "gray hats", or more than one in every 20 people working in a cybersecurity capacity. Underscoring the depth of the problem is the fact that eight percent of security professionals admit to considering participation in black hat activity, 22

percent have actually been approached about doing so, and 51 percent either know or have known someone who has participated in this activity.

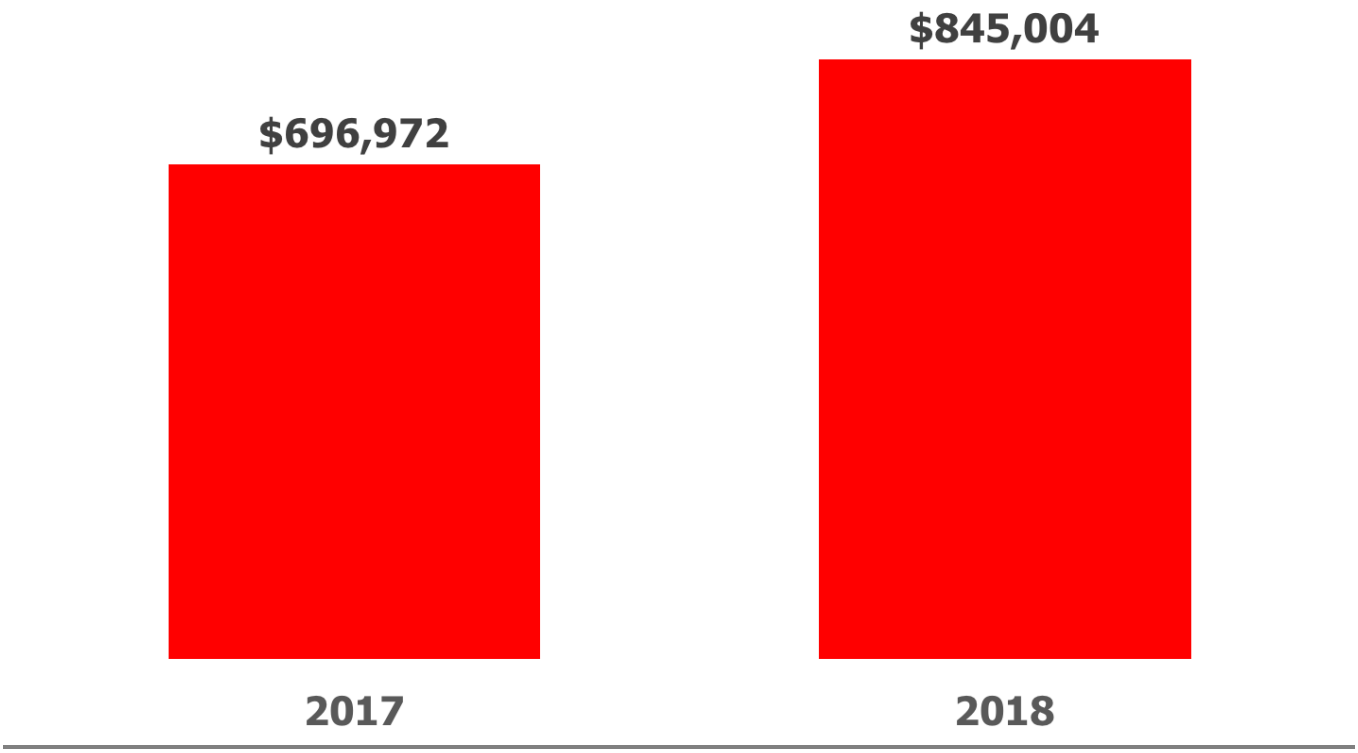
Survey Findings

CYBERSECURITY BUDGETS IN THE UNITED STATES ARE HIGH

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 US organizations of 2,500 employees averaged just under $697,000 in 2017 and will grow to $845,000 in 2018, representing growth of 21.2 percent, the highest among the organizations we surveyed. Security budgets in the US are substantially higher than the global average, but lower than those of organizations in Singapore.

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



Source: Osterman Research, Inc.

THE COSTS OF REMEDIATING MAJOR SECURITY EVENTS

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 US organizations would spend an average of just over $429,000 to remediate a single such event, or most of the total annual security budget. The US figure to address a major security event at $429,133, as shown in Figure 2, is much higher than the global average of $289,624, and the highest in our survey.

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

	USA	GLOBAL AVERAGE
IT and other labor	$70,038	$74,538
Software/hardware solutions	$87,930	$98,211
Direct costs (e.g., paying a ransom)	$41,446	$21,477
Fines	$83,464	$33,024
Legal fees	$83,421	$40,622
Other costs	$62,833	$21,754
TOTAL	**$429,133**	**$289,624**

Source: Osterman Research, Inc.

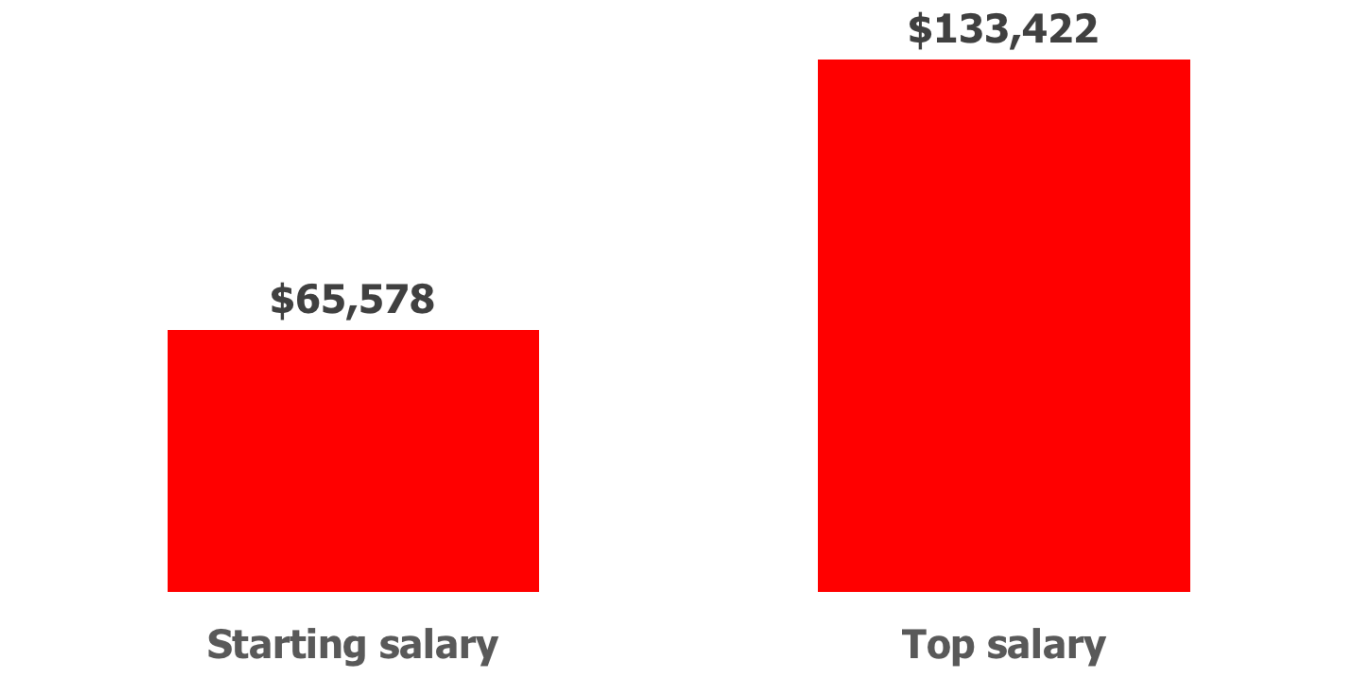
SECURITY EXPENDITURES ADDRESSING ACTIVE COMPROMISES

US organizations spend a significant 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 the United States spent 14.7 percent of their 2017 budget on remediating active compromises, which was higher than the global average of 12.5 percent and the second highest in our survey.

SECURITY STAFF SALARIES ARE SIGNIFICANT

Our survey found that the average starting salary for an entry-level security professional in the United States is $65,578, somewhat higher than the global average of $60,662. As shown in Figure 3, the top annual salary for a US security professional is $133,422, the second highest among the nations in which we conducted the survey. We found that the ratio of the highest salary to the entry level salary was 2.03:1, slightly lower than the global average of 2.15:1.

Figure 3
Entry Level and Maximum Salaries for IT Security Professionals

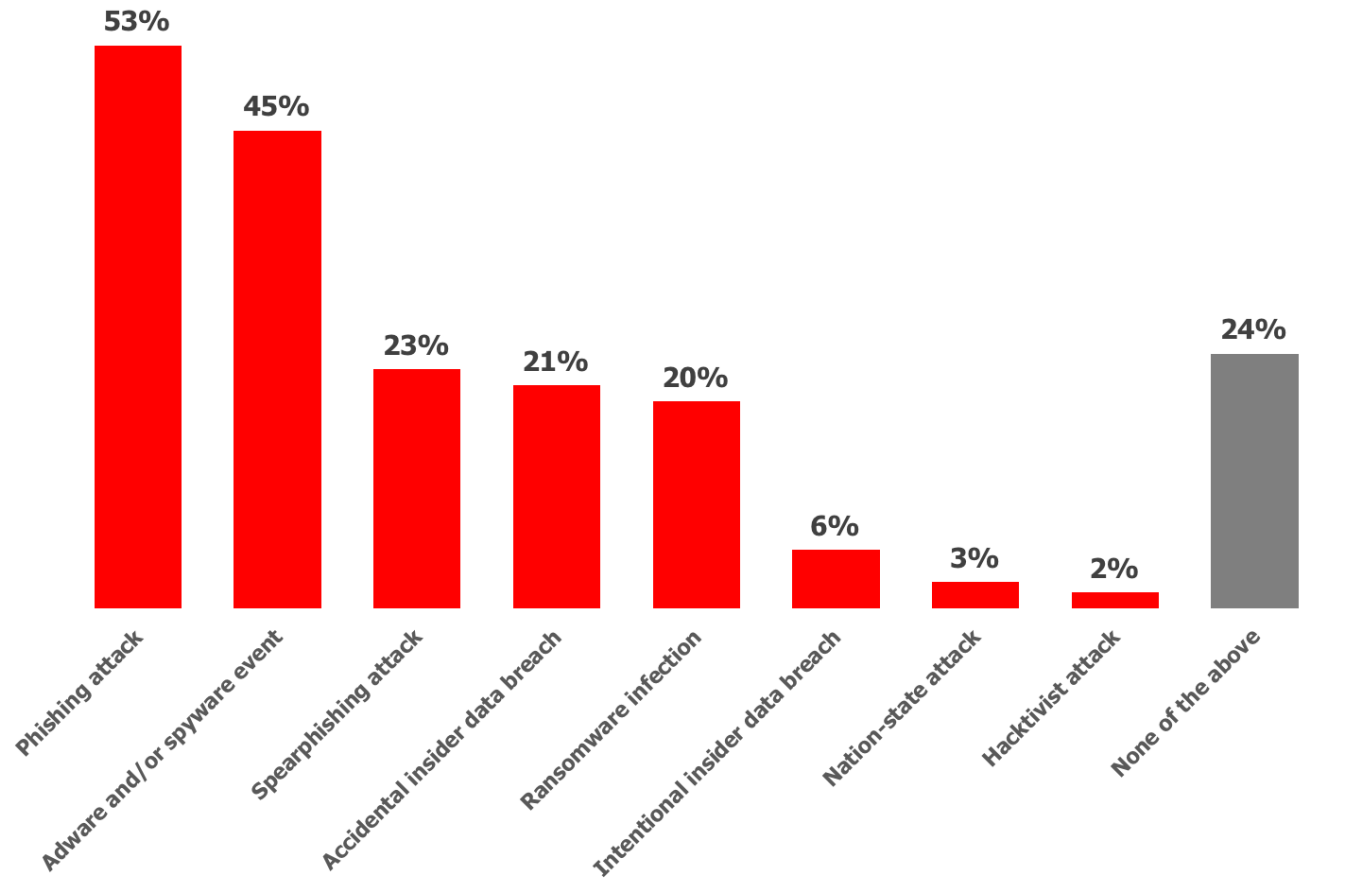


Source: Osterman Research, Inc.

THREATS THAT HAVE IMPACTED ORGANIZATIONS IN THE UNITED STATES

US organizations have experienced a significant level of security attacks direct against them during the past 12 months, most notably around phishing, adware/spyware, spearphishing, accidental data breaches and ransomware, as shown in Figure 4. US organizations experienced the third highest level of infection overall among the five nations surveyed, but the second highest level of phishing following the UK.

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



Source: Osterman Research, Inc.

HOW SERIOUSLY ARE VARIOUS THREATS TAKEN?

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 US organizations take security threats quite seriously: when we averaged the "very serious" responses across all of the various threats for the nations in which we conducted the survey, we found that the average response for US organizations was 34.8 percent, well behind Germany, but significantly ahead of the global average and the other three nations in the survey.

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

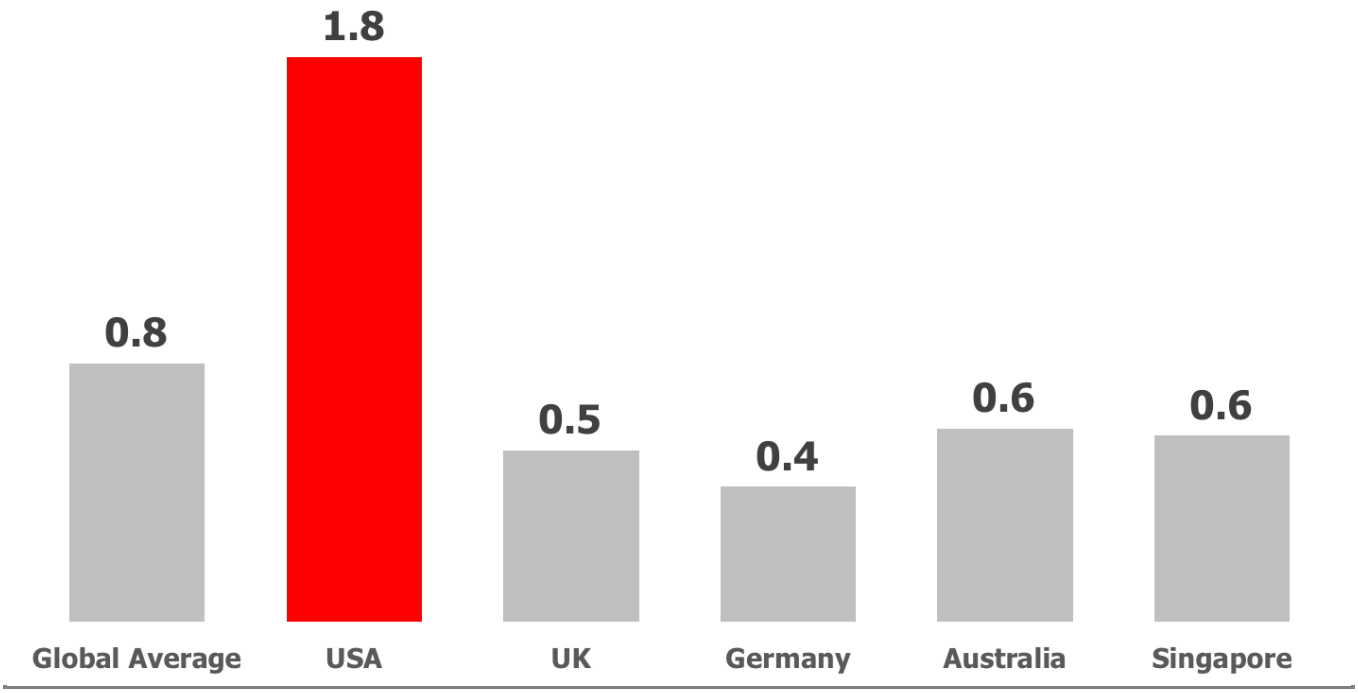
	Very Serious	Serious	Somewhat Serious	Rarely Serious	Never Serious
Ransomware	47.7%	34.2%	14.1%	3.5%	0.5%
Phishing	26.0%	40.0%	21.0%	12.0%	1.0%
Spearphishing	28.1%	41.7%	22.6%	6.5%	1.0%
Intentional insider breaches of data	67.2%	20.7%	8.6%	3.0%	0.5%
Accidental insider breaches of data	41.7%	33.7%	14.1%	10.1%	0.5%
Nation-state attacks/advanced persistent threats	42.7%	28.1%	15.1%	8.5%	5.5%
Hacktivism	19.1%	27.6%	26.1%	21.1%	6.0%
Adware and/or spyware	6.1%	44.4%	36.4%	12.1%	1.0%

Source: Osterman Research, Inc.

THE FREQUENCY OF MAJOR SECURITY EVENTS IS HIGHEST IN THE UNITED STATES

Major security events – e.g., those that cause significant expenditure of time, finances or other resources – are all-too-common among the US organizations we surveyed, and by a wide margin. As shown in Figure 6, US organizations suffered an average of 1.8 major events during 2017, more than double the global average and three times higher than Australia and Singapore, which came in tied for second place.

Figure 6
Frequency of Major Security Events During 2017



Source: Osterman Research, Inc.

The Growing Threat of Black Hat Activity

BLACK HAT ACTIVITY IS COMMON IN THE UNITED STATES

As shown in Figure 7, a significant proportion of the individuals we surveyed in the United States have either known someone who has participated in black hat activity (at the highest rate among the five nations surveyed), they have been approached about doing so, or they have considered participating in it. US organizations also commonly higher black hat hackers to consult with their organization at the second highest rate of the five nations we surveyed.

Figure 7
Current Practices and Views Related to Black Hat Activity

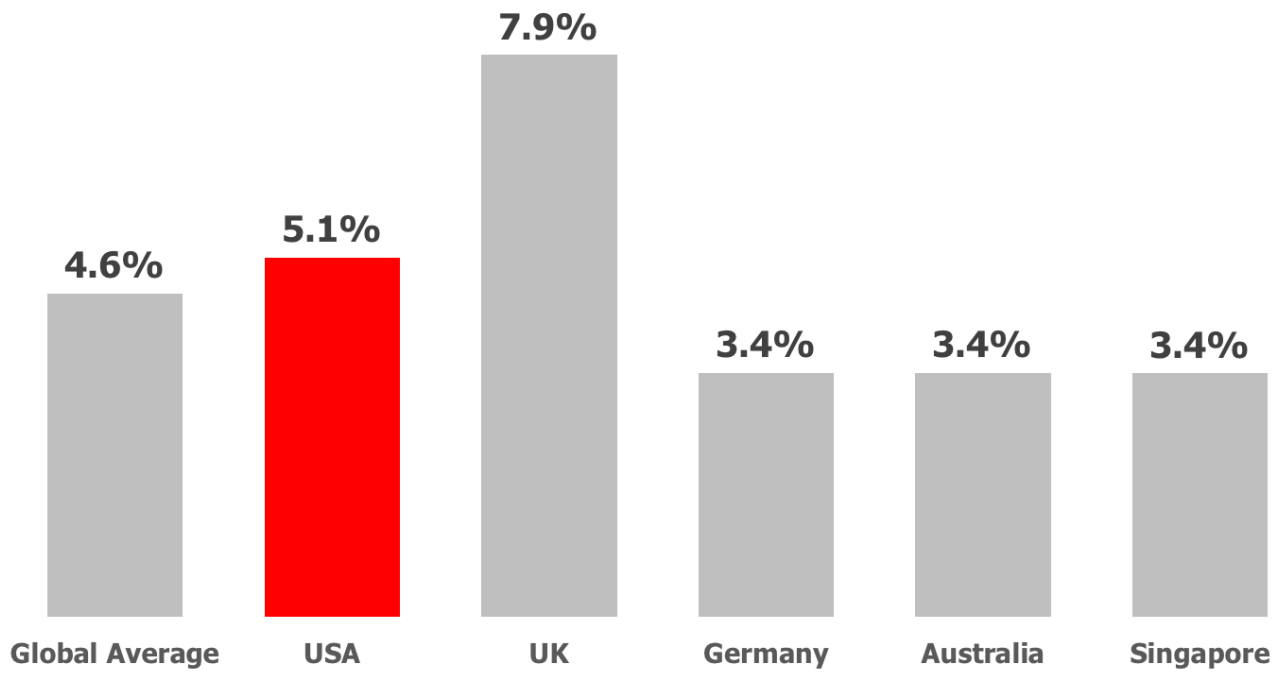
I know/have known someone that has participated in black hat activity	50.5%
We conduct red/blue team activity to test the strength of our cybersecurity defenses	34.0%
I have been approached about participating in black hat activity	22.0%
We have hired a black hat hacker to consult with our organization	11.5%
I have considered participating in black hat activity	8.0%
None of the above	7.0%
We have used a black hat hacker for more than one project	5.5%

Source: Osterman Research, Inc.

THE COSTS OF SECURITY PROFESSIONALS SWITCHING TO CYBERCRIME

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 the United States believe that 5.1 percent of their security colleagues are gray hats, slightly higher than the global average, but well below the UK, where 7.9 percent of security professionals are considered by their peers to be gray hats.

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



Source: Osterman Research, Inc.

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

There is a perception that it's quite easy to become involved in gray hat activity without being discovered, although a plurality do not agree that becoming a cybercriminal is more lucrative than fighting cybercrime. For example, as shown in Figure 9, nearly one-half of those we surveyed in the United States either agree or strongly agree that "it's easy to get into cybercrime without getting caught". Nearly the same proportion 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	11.6%
Agree	35.9%
Neutral	21.7%
Disagree	23.2%
Strongly Disagree	7.6%

There is more money to be made in fighting cybercrime than being a cybercriminal	
Strongly Agree	15.7%
Agree	30.3%
Neutral	26.8%
Disagree	23.7%
Strongly Disagree	3.5%

Source: Osterman Research, Inc.

MANY BELIEVE BLACK HATS EARN MORE MONEY

The reasons for becoming a cybercriminal vary, as shown in Figure 10. Nearly three in five of those surveyed in the United States believe that people become black hats because it offers greater financial rewards than they can realize as a security professional, more than one-half believe the motivation is to retaliate against an employer, and one-half believe that some sort of cause of philosophical reason is the drive factor in becoming a black hat. Interestingly, those surveyed in the United States are the most likely to believe that the motivation for becoming a black hat is driven by a desire to retaliate against an employer – 53.3 percent of those surveyed in the United States believe this compared to the global average of 39.7 percent.

Figure 10
Perceived Reasons for Becoming a "Black Hat"

Earn more money than as a security professional	58.8%
Retaliation against an employer	53.3%
Philosophical reasons or some sort of cause	49.7%
The challenge that it offers	47.7%
It is not perceived as wrong	22.1%

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 $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:

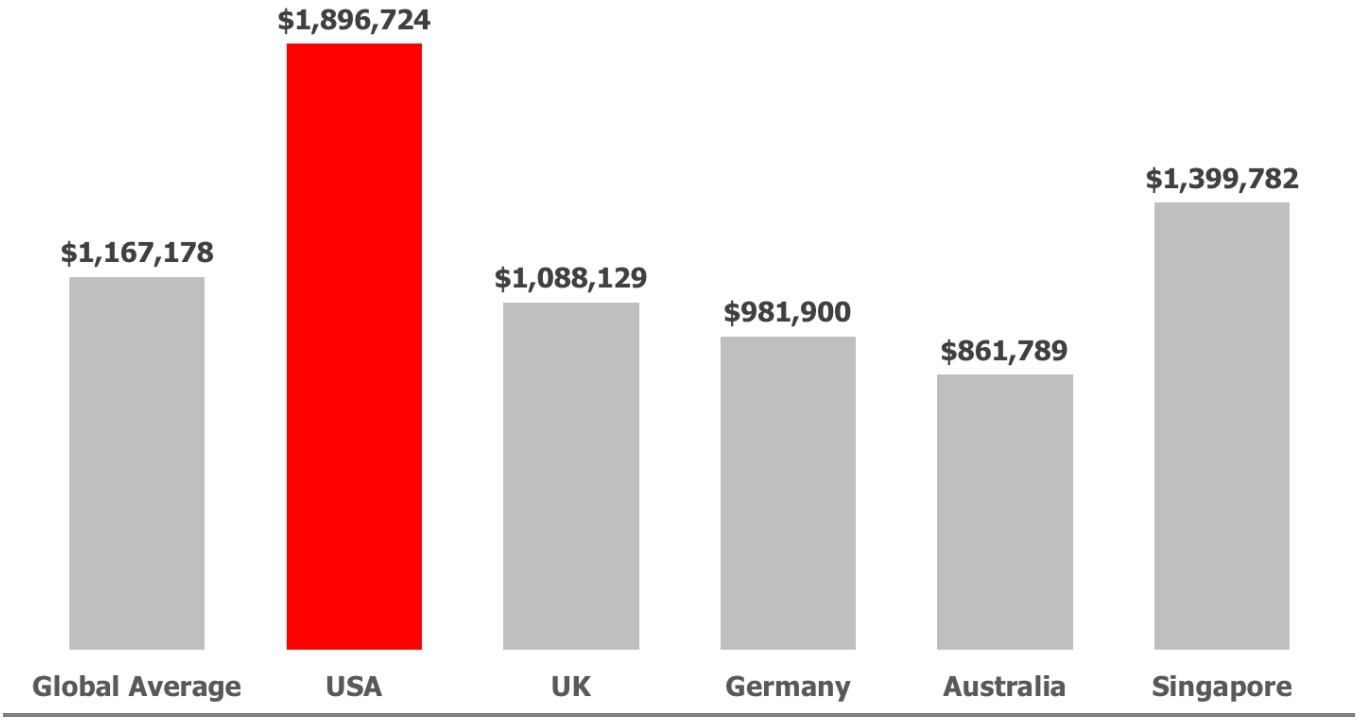
- The normal, budgeted costs of deploying and managing a security infrastructure.
- The off-budget costs associated with major events that require additional staff time, consultants, hardware, software, etc., and that can result in fines, legal costs and other expenses.
- The costs of insider threats – 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 11 shows that the average annual security costs for a 2,500-employee US organization is $1.90 million. Across the regions we surveyed, this was by far the highest figure among the five nations we surveyed.

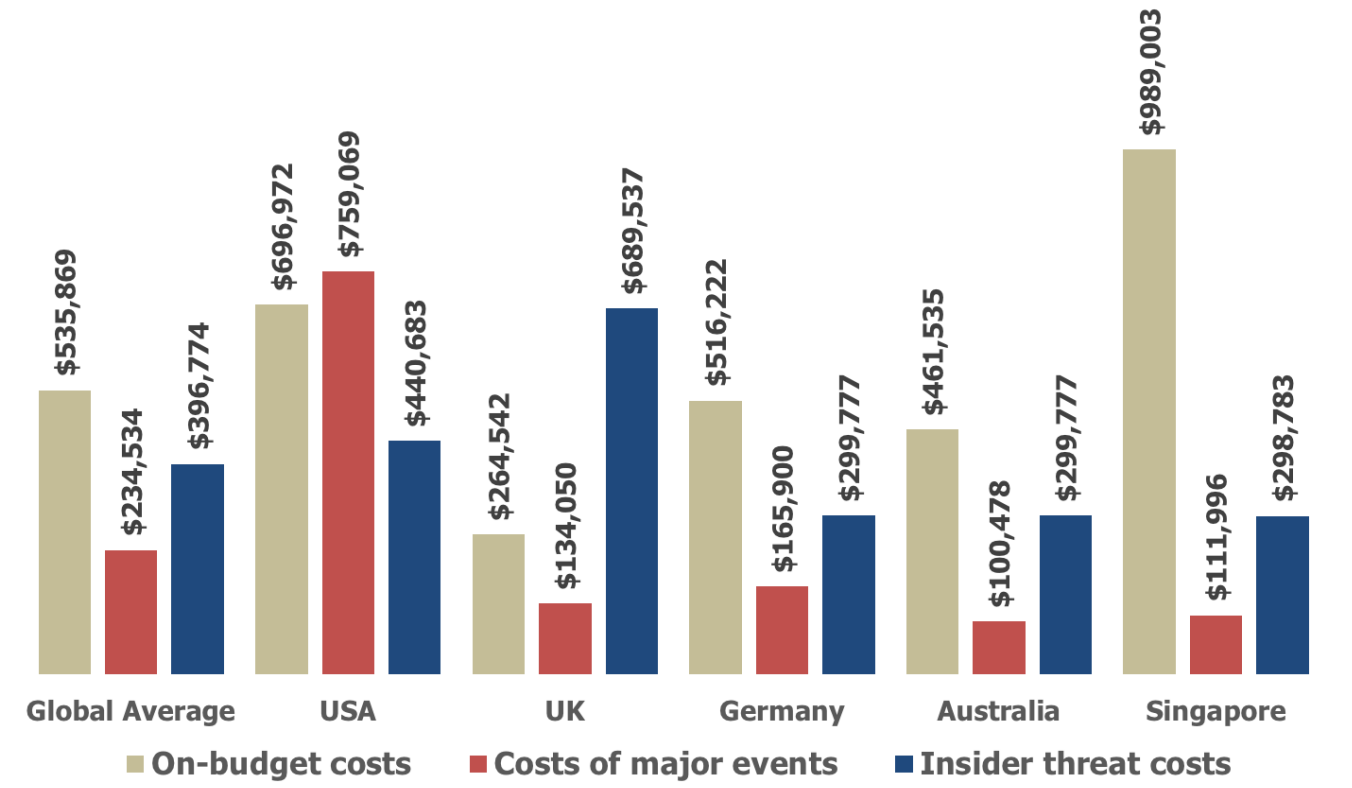
Figure 12/Q24b
Total Annual Security Costs for a 2,500-Employee Organization



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 for US organizations are composed primarily of the costs associated with dealing with major events (40 percent of total costs), security budgets themselves (37 percent) and insider threat costs (23 percent). The breakdown of security costs in the United States 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.scribd.com/document/377159562/Into-the-Web-of-Profit-Bromium-Final-Report