2016 Security Pressures Report

BASED ON A SURVEY COMMISSIONED BY TRUSTWAVE

Trustwave®

Table of Contents

Introduction

Welcome to the 2016 Security Pressures Report from Trustwave. When we decided to publish this report for the first time two years ago, we did not know if it would become an annual endeavor. But readers were immediately drawn to the content because it humanizes cybersecurity in a unique way by measuring, quantifying and exposing the varying sources of situational pressure that in-house IT security professionals routinely feel and experience.

From threats to executive demands to post-breach consequences, security practitioners face undeniable anguish and agitation tantamount to other professions that can be greeted at any time with an emergency incident. And the times when something urgent is not happening are not much calmer because security professionals are often overwrought with trying to ensure that every potential threat vector is sealed off – all while working with a diminishing pool of available in-house resources.

Indeed, the job hazards are unmistakable for those whose mission it is to identify, protect, detect and respond to digital harms. Studies have shown that high stress levels at work lead to less productive workers, and security professionals can ill-afford to disengage from their jobs. As always, our hope is that this report will enable organizations to better understand where their security programs are missing the mark, and more specifically where security professionals are being overwhelmed and where their needs are not being met.

Based on a survey of more than 1,400 IT security professionals from around the world, the 2016 Security Pressures Report lends valuable context to the struggles that practitioners face on a regular basis. Every year, the report evolves with the times by including additional options for some questions and even adding in new and timely questions that can help us best assess modern-day security pressures. At its conclusion, the report offers practical recommendations for alleviating the pressure.

For ease of digestion, we have again designed the report into individual sections and have juxtaposed this year's results against last year's, as well as broken out the results by country for the United States, United Kingdom, Canada – and for the first time – Australia and Singapore. Some of that comparison data was particularly interesting.

Happy reading, and we look forward to hearing your feedback!

Key Findings

UNDER PRESSURE: 63% of respondents felt more pressure to secure their organizations in 2015 compared to the prior 12 months, and 65% expect to feel additional pressure this year. Those numbers grew nine and eight percentage points, respectively, versus last year's report.

SKILLS GAP: Shortage of security expertise has climbed from the eighth-biggest operational pressure facing security pros to the third-biggest, behind advanced security threats and adoption of emerging technologies.

BOARD BURDEN: 40% of respondents feel the most pressure in relation to their security program either directly before or after a company board meeting – 1% higher than how they feel after a major data breach hits the headlines.

DETECTION TRUMPS PREVENTION: The largest security responsibilities facing 54% respondents are related to detection of vulnerabilities, malware and compromised systems.

MOVED TO MANAGED: The number of respondents who either already partner or plan to partner with a managed security services provider has climbed from 78% to 86%.

NOT READY FOR PRIMETIME: 77% of respondents are pressured to unveil IT projects that aren't security ready, the same percentage as last year's report.

EMPTY PROMISES: Pressure to select security technologies containing all of the latest features has jumped from 67% to 74% among respondents, but having the proper resources to actually put them to use has fallen from 71% to 69%.

CONNECTIVITY BREEDS CONTEMPT: Internet of Things (IoT) is the emerging technology respondents feel the second-most pressure to adopt/deploy, behind the cloud. Additionally respondents rate it the second riskiest emerging technology, also behind the cloud.

DATA AND DDOS GLOOM: Customer data theft and intellectual property theft remain the top two worrying outcomes following an attack or data breach, but a disabled corporate website – usually inflicted by DDoS attacks – is the biggest riser (from 7% to 13%).

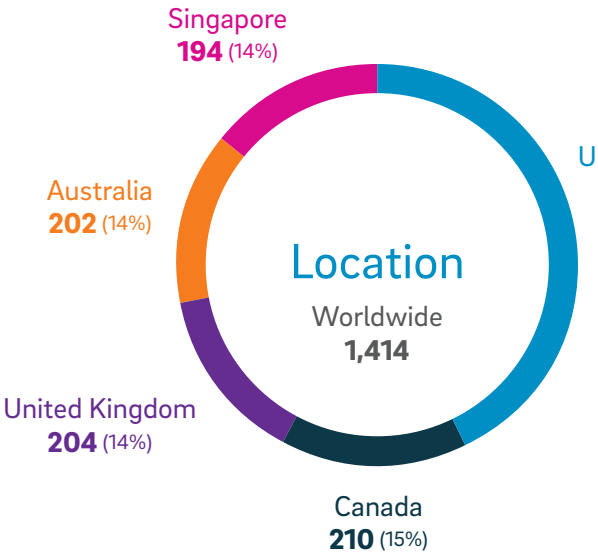
DEMAND OUTPACING SUPPLY: Respondents wishing to quadruple their staff from its current size has risen from 24% to 29%.

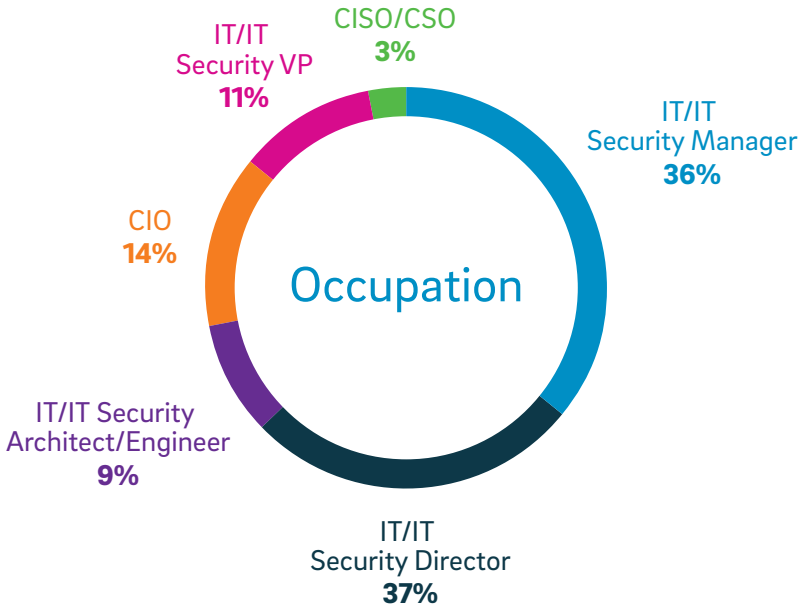
EARLY TERMINATION: Job loss remains as the third-highest post-breach repercussion fear, but has grown from 8% to 11%. It sits behind reputation damage and financial damage to one's company, respectively.

Methodology

Trustwave commissioned a third-party research firm to survey 1,414 full-time information technology (IT) professionals who are security decision makers or security influencers within their organizations. The objective of the survey was to measure the variety of pressures they face regarding information security. Respondents consisted mainly of chief information officers (CIOs), chief information security officers (CISOs/CSOs), IT/IT security directors and IT/IT security managers: 1,414 worldwide, which included 604 in the United States, 210 in Canada, 204 in the United Kingdom, 202 in Australia and 194 in Singapore. Respondents work in a variety of sectors, with the most frequent being technology (31%), manufacturing (10%), financial services/banking (9%), and retail and professional services (both 8%). The survey was deployed through emails sent between November and December 2015. Survey results have a margin of error of +/- 3%.

RESPONDENT DEMOGRAPHICS





Overall Security Pressure

First things first: More respondents than ever are feeling their general security pressures growing. Overall pressures for security professionals markedly jumped from 2014 to 2015, and an even larger number of practitioners expect to experience increased pressure in 2016.

Specifically, 63% of respondents experienced more pressure to secure their organizations in 2015 compared to 2014. Compare that number to last year's report, when only 54% of respondents said their overall security pressures had increased year over year (from 2013 to 2014). The spike is most pronounced in the United States, where an eye-popping 70% of security professionals felt the pressures dialed up last year compared to the prior 365 days.

Not surprisingly, just 21% (compared to 34% in last year's report) of respondents felt pressures stay the same in 2015 compared to 2014. On a positive note, 16% of respondents experienced diminishing pressure in 2015, compared to 12% in 2014 who felt their security strains decrease.

Meanwhile, 65% of respondents expect to experience additional pressure to secure their organizations in 2016 – and 72% of U.S. respondents count themselves in that group.

AMOUNT OF PRESSURE FELT IN 2015 (COMPARED TO THE PRIOR YEAR)

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Up	54%	▲	63%	70%	64%	58%	58%	50%
Same	34%	▼	21%	17%	22%	30%	18%	29%
Down	12%	▲	16%	13%	14%	12%	24%	21%

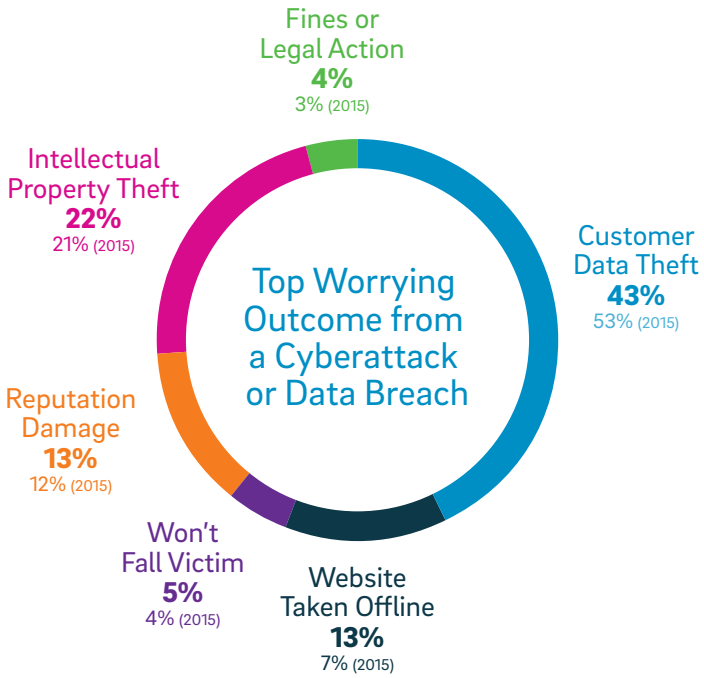
AMOUNT OF PRESSURE EXPECTED TO FEEL IN 2016 (COMPARED TO 2015)

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Up	57%	▲	65%	72%	66%	56%	59%	57%
Same	32%	▼	24%	18%	26%	34%	24%	30%
Down	11%	=	11%	10%	8%	10%	17%	13%

Cyberattack and Data Breach Worries

With the Identity Theft Resource Center placing the number of records exposed from data breaches in 2015 somewhere around 170 million, it's no surprise that theft of information ranks as the top worrying outcome of a breach or cyberattack for nearly two-thirds of respondents. Security professionals rate customer data theft (43%) as their No. 1 worrying result, followed by intellectual property theft (22%). Website disruption made the largest jump year over year, increasing from 7% last year to 13% in this year's report – in Australia, 19% of respondents list their website being taken offline as the top worrying outcome. This change could be related to the fact that the number of distributed denial-of-service incidents reached record highs during 2015, according to Akamai.

Rounding out the list of top worrying outcomes is reputation damage (also 13%) and fines or legal action (4%). 5% of respondents have no outcome worries because they don't believe their business will fall victim. That number ticked up one percentage point from last year. Similarly, the number of respondents who feel safe from security threats rose from 70% to 74%, but the boost was mostly thanks to Australia, where an eye-opening 88% of respondents feel safe from security threats. However, half of Australian respondents admit their organization has experienced a breach. Overall, 46% of respondents report that their organization has sustained a breach, while 48% haven't experienced a breach and 6% aren't sure. 53% of U.S. respondents say their organization has been breached, while only 32% in Singapore say the same.



TOP WORRYING OUTCOME FROM A CYBERATTACK OR DATA BREACH

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Customer Data Theft	53%	▼	43%	43%	47%	53%	34%	37%
Intellectual Property Theft	21%	▲	22%	23%	20%	16%	26%	25%
Website Taken Offline	7%	▲	13%	13%	10%	11%	19%	5%
Reputation Damage	12%	▲	13%	12%	16%	13%	9%	15%
Won't Fall Victim	4%	▲	5%	5%	6%	3%	7%	5%
Fines or Legal Action	3%	▲	4%	4%	1%	4%	5%	3%

RESPONDENTS WHO FEEL SAFE FROM SECURITY THREATS

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Yes	70%	▲	74%	72%	65%	77%	88%	70%
No	30%	▼	26%	28%	35%	23%	12%	30%

NEW FOR 2016

RESPONDENTS WHOSE ORGANIZATION HAS EXPERIENCED A BREACH

	2015 Report Overall	2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
No	N/A	48%	42%	51%	55%	45%	59%
Yes	N/A	46%	53%	45%	40%	50%	32%
Not Sure	N/A	6%	5%	4%	5%	5%	9%

External versus Internal Threats

Which worries security professionals more – external or internal threats? 58% of respondents are more pressured to protect against external threats, while 42% feel the other way, up four percentage points from last year. The split is not surprising, considering attacks orchestrated by participants unknown to the victim typically are the ones that drive the headlines. But insider attacks are more likely to go unreported, yet they can actually have the greater impact because they are being perpetrated – either purposefully or unwittingly – by users who are trusted on the network.

Of the respondents most concerned about internal threats, 24% are bothered by non-malicious individuals who may commit unintended security risks, like emailing a sensitive file to their personal email address or losing a laptop. 18%, meanwhile, are more worried about malicious insiders, a group that may be motivated by greed or frustration to wage harm on the corporate network.

Some notable country-by-country comparisons: Respondents in the U.K. are most pressured by external threats compared to internal ones, by a 64%-36% margin. But last year, just 55% of U.K. security pros deemed external threats the bigger problem. Meanwhile, Australian security pros are evenly split between external and internal threats pressuring them the most. Singapore came in the highest among respondents who consider malicious insiders the most pressure-inducing (25%).

TOP SECURITY THREAT SOURCES

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
External Threats	62%	▼	58%	59%	64%	59%	50%	55%
Non-Malicious Internal Threats	20%	▲	24%	23%	17%	24%	37%	20%
Malicious Internal Threats	18%	=	18%	18%	19%	17%	13%	25%

Riskiest Insider Threats

Considering security pros are more concerned about non-malicious insider threats than they are about the sinister types, it's not surprising the insider threats causing the most pressure are typically inadvertent actions performed by unsuspecting employees, as unauthorized file transfers (31%) and installation of unauthorized software or malware (24%) top the list. Overall, the list did not change much from last year's report, with access and privilege modification/escalation ranking as the third-biggest insider pressure point, followed by weak passwords (which saw a small boost from 9% to 11%), failing to install security updates and patches (9%) and general lack of security training (7%).

Year over year, the number of U.K. respondents who view unauthorized file transfers as their leading insider pressure jumped from 22% to 32%, while access and privilege modification/escalation fell from 26% to 17%. In Canada, 17% of security pros last year considered lack of security training as the third-biggest insider threat they must deal with, while this year that number fell to last, at 4%.

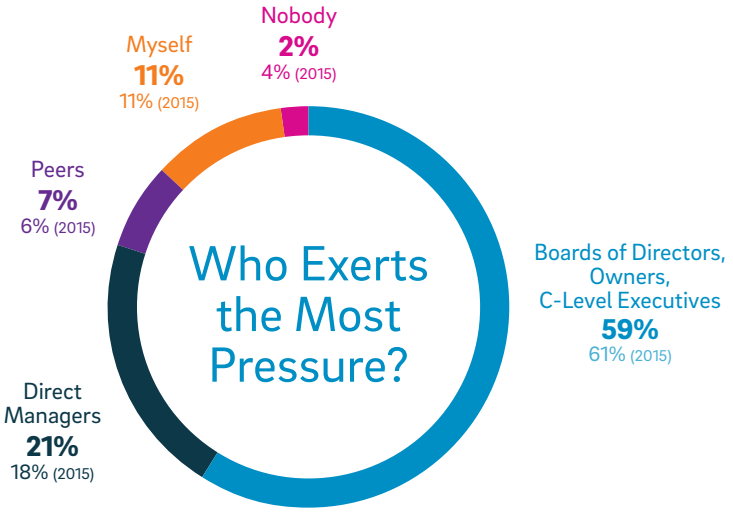
TOP RISKY INSIDER THREATS

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Unauthorized File Transfers, Such as Via Email or the Cloud	28%	▲	31%	27%	32%	32%	33%	38%
Installation of Unauthorized Software or Malware	25%	▼	24%	28%	18%	25%	26%	20%
Access and Privilege Modification/Escalation	18%	=	18%	17%	17%	20%	16%	17%
Weak Passwords	9%	▲	11%	10%	13%	11%	15%	10%
Failing to Install Security Updates and Patches	10%	▼	9%	11%	12%	8%	5%	7%
General Lack of Security Training	10%	▼	7%	7%	8%	4%	5%	8%

Human Pressure Exertion

Cybersecurity is no longer a technology-only issue whose responsibility and accountability is solely placed on the shoulders of the security team. The security field is now being evaluated and prioritized by company leadership who believe cyberattacks can inhibit corporate growth – so it is no surprise that 59% of respondents feel the individuals exerting the most pressure on them are owners, boards of directors and members of the C-suite. They are followed by direct managers (21%), oneself (11%), peers (7%) and nobody (2%).

The United States leads the pack with 64% of security professionals ranking corporate executives as the largest source of human pressure. On the other hand, Australian businesses have been somewhat slower to this trend, with respondents there feeling comparatively less pressure from boards, owners and executives (47%), but more from direct managers (28%).



WHO EXERTS THE MOST PRESSURE?

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Boards of Directors, Owners, C-Level Executives	61%	▼	59%	64%	57%	56%	47%	61%
Direct Managers	18%	▲	21%	20%	22%	18%	28%	20%
Myself	11%	=	11%	11%	11%	13%	11%	11%
Peers	6%	▲	7%	4%	7%	9%	10%	6%
Nobody	4%	▼	2%	1%	3%	4%	4%	2%

Speed versus Security

Two years ago, in the inaugural edition of this report, one of the most quoted statistics was the finding that nearly four out of five respondents were pressured to unveil IT projects before they were security ready. Since then, that number hasn't worsened, but it hasn't gotten much better either, with this year's report showing that 77% of security professionals are feeling the squeeze to greenlight IT projects that aren't ready for primetime – the same percentage as last year.

Why have few companies learned their lesson? It may be a question of math. Companies are likelier deploying exponentially greater numbers of IT projects, such as new applications, including mobile, this year compared to just two years ago. So, any new efforts to factor in security amid the rush to release hasn't made much of a dent because of the sheer numbers of new projects going out the door. According to the 2015 Trustwave Global Security Report, 98% of applications tested by our researchers contained at least one vulnerability, with the median number per application an eye-opening 20. Flaws in applications can lead to malware infiltration and data leakage.

The United States houses the most egregious offenders, where 83% of security pros feel pressure to roll out IT projects too early. The United Kingdom, where 70% are pressured to release early, made the biggest improvement from last year, when 78% said they were pinched to prematurely roll out new tech.

PRESSURE TO ROLL OUT IT PROJECTS NOT SECURITY READY

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Yes, Once or Twice	61%	▼	60%	65%	50%	56%	62%	57%
Yes, Frequently	16%	▲	17%	18%	20%	15%	13%	20%
No	23%	=	23%	17%	30%	29%	25%	23%

Top Operational Pressures

For the third consecutive year, respondents rank advanced security threats (26%) and adoption of emerging technologies (22%) as the top two operational pressures they face in relation to their information security programs. Security practitioners have become inured to both of those pressures as threats become more predatory and professionalized, and technologies like cloud, mobile and IoT give rise to wider attack surfaces. But what did enter the spotlight for the first time in this year's report is shortage of expertise (14%), which rose from the eighth-biggest operational pressure in last year's report to the third-biggest this year. Organizations are apparently finding it harder than ever to find skilled security staff, and this gap in talent has been supported by numerous studies. Singaporean respondents actually rank shortage of expertise as their second-biggest operational pressure, and adoption of emerging technologies third.

Overall, the pressure caused by a dearth of expertise surpassed lack of budget (12%), lack of time (9%), security technology/product complexity (9%), lack of personnel (4%), ensuring third-party contractor security (3%) and requests from business-line managers, which fell from 6% to only 1% this year.

Canadian security pros agree with the consensus that advanced security threats (20%) and adoption of emerging technologies (21%) present the two greatest operational pressures, but they rate lack of budget nearly as close, with 19% of respondents most concerned about a lack of funds to devote to security.

TOP OPERATIONAL PRESSURES FACING SECURITY PROS

1. **ADVANCED SECURITY THREATS**
2. **ADOPTION OF EMERGING TECHNOLOGIES**
3. **SHORTAGE OF EXPERTISE**

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Advanced Security Threats	24%	▲	26%	28%	27%	20%	19%	31%
Adoption of Emerging Technologies	25%	▼	22%	24%	24%	21%	21%	15%
Shortage of Expertise	5%	▲	14%	12%	14%	14%	14%	19%
Lack of Budget	12%	=	12%	9%	11%	19%	14%	13%
Lack of Time	6%	▲	9%	7%	9%	12%	17%	3%
Security Technology/Product Complexity	11%	▼	9%	11%	6%	5%	7%	10%
Lack of Personnel	5%	▼	4%	5%	3%	4%	4%	4%
Ensuring Third-Party Contractor Security	6%	▼	3%	3%	3%	4%	2%	4%
Requests from Business-Line Managers	6%	▼	1%	1%	3%	1%	2%	1%

Emerging Technologies

As the previous section referenced, the adoption of emerging technologies is the second-most pressure-filled operational activity that security pros undertake. Drilling deeper into the data, the cloud (44%) overwhelmingly presents the emerging technology that security professionals are under the most pressure to adopt and deploy. Next on the list are Internet of Things (IoT) technologies (17%), which was not an option for respondents last year. But the trend is exploding: Research studies predict that tens of billions of connected devices will be on the scene by 2020, many of which will invade the enterprise and inevitably contain security vulnerabilities.

Next on the list is BYOD (16%), which continues its steamroll as more businesses rely exclusively on employee-owned smartphones, tablets and other devices. Rounding out the pack are social media (10%), mobile applications (7%) and Big Data (6%).

While the cloud continues to lead in terms of pressure to adopt and deploy, the risk posed by the technology is dropping. The fall is likely attributable to comfort levels over cloud security capabilities increasing, as well as the inclusion of IoT as a polling option in this year's report. The number of respondents who viewed the cloud as the emerging technology posing the greatest risk fell from 40% last year to 32% in this year's report. The pack tightens after that: IoT (19%), BYOD (19%), social media (15%), mobile applications (10%) and Big Data (5%).

EMERGING TECHNOLOGY: MOST PRESSURED TO ADOPT/DEPLOY

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Cloud	47%	▼	44%	44%	49%	46%	37%	42%
Internet of Things (IoT)	N/A		17%	17%	17%	16%	16%	20%
BYOD	22%	▼	16%	17%	15%	15%	18%	13%
Social Media	9%	▲	10%	9%	8%	8%	19%	11%
Mobile Applications	15%	▼	7%	9%	7%	6%	6%	5%
Big Data	7%	▼	6%	4%	4%	9%	4%	9%

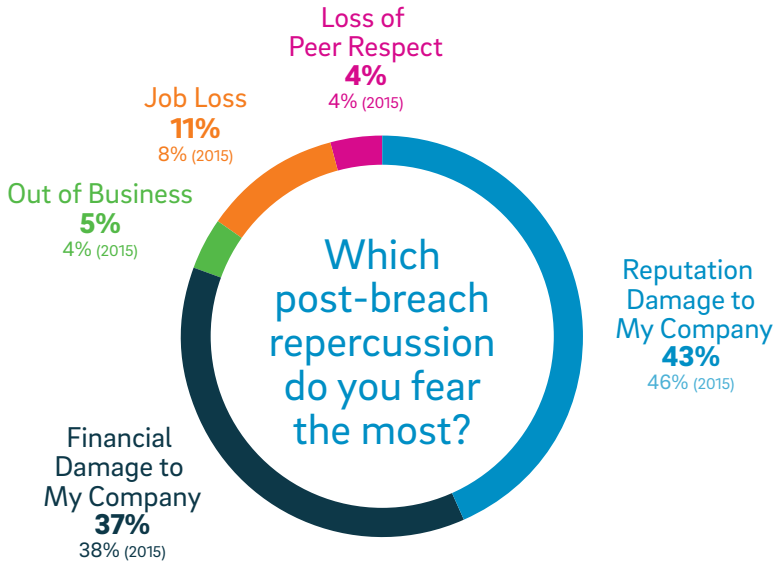
EMERGING TECHNOLOGY: POSES THE GREATEST RISK

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Cloud	40%	▼	32%	33%	31%	32%	29%	35%
Internet of Things (IoT)	N/A		19%	18%	16%	17%	27%	19%
BYOD	27%	▼	19%	19%	25%	20%	16%	15%
Social Media	13%	▲	15%	14%	12%	14%	22%	17%
Mobile Applications	14%	▼	10%	11%	9%	10%	4%	8%
Big Data	6%	▼	5%	5%	7%	7%	2%	6%

Breach Repercussions

This report already has stated that more than half of respondents have experienced a breach or aren't sure if they have. Other studies completed over the past few years have put that number even higher. As a result, one would be hard-pressed to find a security professional who hasn't considered the consequences of a major data-loss incident.

Across the board, respondents rank damage as the highest post-breach repercussion, with reputation damage being the top fallout (43%) and financial damage (37%) placing second. One interesting note is that the potential for job loss rose from 8% last year to 11% this year, evidence that more security professionals fear termination if a major incident occurs under their watch. Rounding out the list is going out of business (4%) – which has happened to a few, but not many, breached organizations – and loss of peer respect (4%).



WHICH POST-BREACH REPERCUSSION DO YOU FEAR THE MOST?

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Reputation Damage to My Company	46%	▼	43%	46%	42%	42%	39%	41%
Financial Damage to My Company	38%	▼	37%	35%	37%	40%	41%	36%
Job Loss	8%	▲	11%	11%	13%	10%	12%	12%
Out of Business	4%	▲	5%	5%	5%	2%	5%	7%
Loss of Peer Respect	4%	=	4%	3%	3%	6%	3%	4%

Features versus Resources

Are security professionals getting the most out of their technology investments? That answer appears to be "no," considering 74% of respondents (seven percentage points more than last year) face pressure to purchase security technologies containing all of the latest features, while nearly three out of ten lack the adequate resources to properly adopt, deploy and use them.

Why is this happening? Companies understandably are drawn to the allure of shiny new boxes. But once these technologies arrive, in-house IT teams often lack the time and/or manpower to ensure the solutions are installed and working properly. Security technologies also are complex. They require a specific set of skills to understand how to use them to their fullest. Due to these challenges, security products can end up as 'shelfware,' sitting unused somewhere and collecting dust.

Pressure to Select the Latest Security Technologies

Lack the Proper Resources to Use the Latest Security Technologies

FACE PRESSURE TO SELECT THE LATEST SECURITY TECHNOLOGIES

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Yes	67%	▲	74%	77%	71%	72%	71%	73%
No	33%	▼	26%	23%	29%	28%	29%	27%

HAVE THE PROPER RESOURCES TO USE THESE TECHNOLOGIES

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Yes	71%	▼	69%	72%	60%	73%	72%	65%
No	29%	▲	31%	28%	40%	27%	28%	35%

NEW FOR 2016

Security Threats

The responsibilities facing today's security professional are enough to overwhelm even the most competent and seasoned practitioner. But as hard as it may be to believe, there was a time when life was easier, when following prevention best practices was enough to block attacks at their source.

But as companies improved their ability to deter the so-called low-hanging fruit, hackers shifted their focus to plotting more sophisticated, custom and targeted attacks that can only be averted by monitoring and detecting them first. That is because in many cases, attackers have already stolen legitimate credentials, through password cracking, spear phishing or otherwise, and now these adversaries simply appear like trusted users. Unfortunately, Trustwave SpiderLabs researchers have shown it takes a median of nearly three months for companies to flag an intrusion like this, more than enough time for foes to expand their foothold and ransack sensitive data.

Not surprisingly, a majority of respondents (54%) list detection of vulnerabilities, malware, malicious activity or compromises as their most pressure-inducing security responsibility. Finding the holes that criminals can use to penetrate a victim organization and advance once inside – or identifying an incident before chaos can ensue – is far less costly than dealing with the ramifications of a breach. Yet many lack the expertise and in-house resources to do this effectively.

Somewhat surprisingly, containing/responding to incidents brought up the rear (4%). Incident response is a traditionally overlooked area in terms of security investment, but last place is still somewhat surprising considering the sheer number of data breaches that have occurred over the last several years.

WHICH SECURITY RESPONSIBILITIES ARE YOU FACING THE MOST PRESSURE TO ADDRESS?

	2015 Report Overall	2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Detecting Vulnerabilities	N/A	21%	20%	17%	29%	21%	22%
Detecting Malicious Activity/ Compromises	N/A	19%	21%	18%	15%	13%	20%
Detecting/Preventing Malware	N/A	14%	12%	12%	20%	17%	15%
Preventing Social Engineering/Phishing Attacks	N/A	12%	12%	13%	11%	9%	15%
Strengthening Passwords and Remote Access	N/A	12%	12%	13%	6%	15%	11%
Managing Network-Connected Devices and Remote Users	N/A	10%	11%	12%	8%	11%	6%
Patching Vulnerabilities	N/A	8%	8%	10%	8%	11%	6%
Containing/Responding to Incidents	N/A	4%	4%	5%	3%	3%	5%

NEW FOR 2016

Career Pressure

The security skills shortage is well documented and is a leading source of grief for professionals who rely on headcount and acumen to help ensure their security program is getting the most in return for its investments. But do established professionals feel strained by this dearth of available and adequate talent – or actually feel a sense of relief knowing their jobs are safe?

Indeed, 76% of respondents feel more pressure because the demand for professionals means there is more for them to do, versus 24% who feel less pressure because they have a sense of job security. The answer may surprise you, until you remember that humans tend to be more affected by what they are actually feeling on a regular basis versus some hypothetical situation, such as – in this case – being fired.

DOES THE HIGH DEMAND FOR PROFESSIONALS IN THE SECURITY INDUSTRY MAKE YOU FEEL MORE OR LESS PRESSURE TO EXCEL IN YOUR CAREER?

	2015 Report Overall	2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
More pressure: This means there is more for me to do	N/A	76%	78%	74%	74%	75%	76%
Less pressure: I feel a sense of job security knowing there is a shortage of professionals in my industry	N/A	24%	22%	26%	26%	25%	24%

NEW FOR 2016

Personal Pressure

Cybersecurity has become a top priority in the boardroom amid a never-ending rash of highly publicized data breaches and other security incidents. In fact, some businesses are treating cyber risk as an executive-level responsibility. Because of that, security professionals are finding themselves being more pressured by what happens in the boardroom than in the server room. Just how important – and anxiety-riddling – are those meetings and the consequences that result from them?

The numbers tell the story. 40% of respondents feel the most pressure related to their security program either directly before or directly after their company's board meeting. Specifically, 17% feel the pressure before the meeting, and 23% after. Combined, that's a percentage point higher than the number of respondents (39%) who feel the most pressure directly following a major security breach in the headlines. Another 11% take on the most pressure at the end of each quarter, while 5% each say the end of the fiscal year and during the holidays are the most pressure-packed times of the year.

Interesting country-by-country data: Just 29% of Australian respondents feel the most pressure in relation to their security program following a well-publicized breach, compared to a whopping 50% either before or after a board meeting. On the other hand, U.K. security pros absorb the most pressure (44%) directly after a big breach happens, compared to 37% either before or after a board meeting.

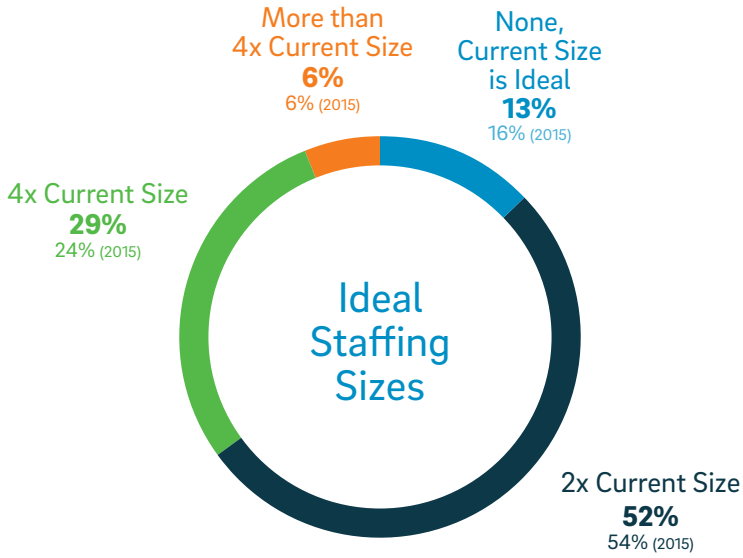
WHEN DO YOU FEEL THE MOST PRESSURE IN RELATION TO YOUR SECURITY PROGRAM?

	2015 Report Overall	2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Directly following a major security breach in the industry	N/A	39%	41%	44%	37%	29%	37%
Directly following my company's board meeting	N/A	23%	22%	23%	23%	29%	23%
Directly before my company's board meeting	N/A	17%	18%	14%	16%	21%	15%
At the end of each quarter	N/A	11%	11%	12%	13%	12%	12%
At the end of fiscal year	N/A	5%	4%	2%	7%	5%	6%
During the holidays	N/A	5%	4%	5%	4%	4%	7%

Staffing Levels

A notable security skills shortage is causing an estimated one million cybersecurity jobs to go unfilled around the world, according to labor statistics. Because the demand for adept security practitioners is so intense, companies also must grapple with excessive turnover. In many cases, the problem isn't finding the budget dollars to fill open headcounts – it is discovering and acquiring the right people for the job (and who want to stay). As a result, many organizations are looking to security service providers to help them fill the void.

And a void there is: 87% of respondents want additional security staff, up three percentage points from last year. Specifically, 52% want the size of their team doubled and 29% (five percentage points more than last year) want the size quadrupled. Another 6% are seeking a team more than four times its current size.



IDEAL STAFFING SIZES

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
None – Current Size is Ideal	16%	▼	13%	12%	16%	13%	14%	13%
2x Current Size	54%	▼	52%	49%	49%	57%	53%	58%
4x Current Size	24%	▲	29%	31%	32%	25%	25%	23%
More than 4x Current Size	6%	=	6%	8%	3%	5%	8%	6%

In-House versus Managed Services

The previous section alluded to the fact that more and more organizations are partnering with managed security services providers (MSSPs) to help them compensate for – and amplify – their in-house resource constraints.

As last year's report explained, organizations can turn to an MSSP for many different reasons. For example, smaller businesses may seek to delegate their entire security workload to a partner that can handle their data protection soup to nuts. Larger businesses, meanwhile, often opt for an MSSP to help them augment their security coverage around more specialized tasks, like security testing, anti-malware and threat management. These are functions where meaningful results depend more on deep understanding of a powerful security solution than intimate knowledge of an enterprise's inner workings.

While most organizations initially assume the primary benefit of an MSSP is improving security outcomes, the accelerated pace at which the MSSPs allow security to be deployed and maintained can actually expedite IT projects that affect the top line of the business. And while this may sound counterintuitive, MSSPs can also lend job security to existing in-house IT staff because they lend broader coverage – therefore making data breaches (and the resulting fallout, such as firings) potentially less likely to happen.

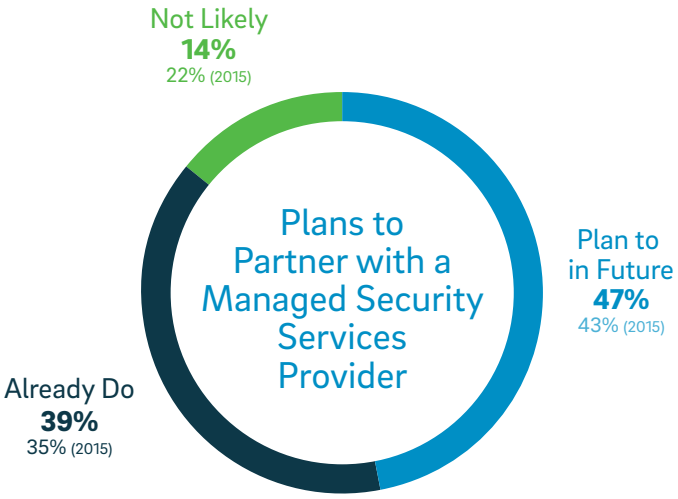
For many, the case for an MSSP really has gone from being a convenience to the only viable way to effectively expand the breadth and depth of an organization's security coverage to acceptable levels.

Respondents who solely rely on their in-house staff to install and maintain security has fallen from 76% last year to 69% in this year's report, and the percentage of respondents who now use a partnership between in-house staff and an MSSP has risen from 20% to 26%.

Reflective of that trend, 86% of respondents either already partner with an MSSP or plan to in the future, up from 78% last year. The percentage of security professionals who do not consider a managed security partnership a likely prospect for their company has dropped from 22% to 14% year over year.

WHO IS CURRENTLY RESPONSIBLE FOR INSTALLING AND MAINTAINING YOUR SECURITY SOLUTIONS?

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Our In-House IT Staff/Security Team	76%	▼	69%	72%	75%	68%	59%	65%
Third-Party MSSP and Our In-House IT Staff/Security Team	20%	▲	26%	24%	22%	27%	34%	29%
Third-Party MSSP Manages All of Our Security	3%	▲	4%	3%	2%	5%	5%	4%
Other	1%	=	1%	1%	1%	0%	2%	2%



PLANS TO PARTNER WITH A MANAGED SECURITY SERVICES PROVIDER

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Plan to in Future	43%	▲	47%	48%	49%	45%	40%	51%
Already Do	35%	▲	39%	39%	31%	40%	47%	39%
Not Likely	22%	▼	14%	13%	20%	15%	13%	10%

2016 Wish List

This report has comprehensively documented the pressures facing today's security professionals. The only question left to ask is: What would their security wishes be if they had a genie in the bottle?

First and foremost, respondents want to be shown the money, as additional budget tops their 2016 wish list (33%), with security expertise (20%) and fewer complex technologies (15%) coming in second and third, respectively. Respondents next most commonly yearned for more time to focus on security (14%), service providers to help them manage their security (8%), fewer requests from business-line managers (7%) and, finally, more staff (3%).

Last year, fewer complex technologies sat fifth on the list at 7%, but rose eight percentage points this year – a move in line with the "Features Versus Resources" question posed earlier in the report. It is somewhat surprising seeing additional personnel at the bottom of the wish list once again, but it appears security professionals seek quality over quantity given that their longing for more security expertise comes in as their second most-common wish list item. Meanwhile, a desire for more time fell from third spot last year to fourth this year (21% to 14%), but it appears that is due to respondents from Australia and Singapore not ranking it as too high of a need.

Responses to this question varied across geographies more than any other from the report. Some interesting country-by-country revelations:

- U.S. respondents (12%) yearn for a managed security service provider more than anyone else, outpacing the others by about three times as much.
- Canadian (42%) and U.K. (41%) respondents crave budget the most of any other country.
- Singaporean (29%) respondents desire security expertise more than any other country.
- Australian (21%) respondents want fewer complex technologies/products compared to anyone else. Meanwhile, 17% want fewer requests from business-line managers, nearly three-times more than the next-closest country.

SECURITY PROFESSIONAL'S WISH LIST FOR 2016

33% MORE BUDGET

20% MORE SECURITY EXPERTISE

15% FEWER COMPLEX TECHNOLOGIES/PRODUCTS

SECURITY PROFESSIONAL'S WISH LIST FOR 2016

	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
More Budget	29%	▲	33%	25%	41%	42%	33%	36%
More Security Expertise	24%	▼	20%	22%	20%	16%	14%	29%
Fewer Complex Technologies/Products	7%	▲	15%	17%	14%	10%	21%	15%
More Time	21%	▼	14%	16%	14%	17%	9%	7%
Service Provider to Help Manage Security	11%	▼	8%	12%	5%	5%	4%	4%
Fewer Requests Business-Line Managers	4%	▲	7%	5%	3%	9%	17%	6%
Staff Augmentation	4%	▼	3%	3%	3%	1%	2%	3%

Conclusion and Recommendations

Despite what your security maturity level looks like, whether you are laggard or leader – or, more likely, somewhere in between – you have security pressures you would like to alleviate. We know that old habits die hard. And this expression carries particular weight in the world of security, where the old way of doing things often maintains surprising relevancy and persistence despite breach after breach, headline after headline, apology tour after apology tour.

But the status quo isn't working anymore. Security pressures are a lot like risk. They can never been fully expunged, but they can be mitigated and brought down to acceptable levels. The recommendations we present to you here are not particularly groundbreaking, but they can serve as a reliable compass of where your security efforts need to be in 2016. Use these suggestions to not only help placate the pressure, but to help make your organization more secure.

Understand and Prioritize Your Data and Systems: Security isn't only about safeguarding the sensitive data under your control. Assessing, inventorying and classifying that critical information – including where it lives and how it moves – will help you understand your risk exposure and allow you to more methodically protect the data. Similarly, you should focus on key systems, evaluating their criticality and verifying their patch status. Remember to also account for data and IT shared with third-party business partners, which are just as susceptible to attacks as you are and which can serve as a launching pad into your environment.

Recognize the Enormity of the Attack Surface: If you think you have your points of exposure under control and locked down, think again. It's likely you are sorely mistaken. Your attack surface – defined as the cumulative vulnerabilities across your network, applications, databases and user population – is brimming with exploitability. From SQL vulnerabilities to weak admin passwords to crafty phishing messages, vulnerabilities underpin every single successful breach. To counter these deficiencies and limit risk, you must architect your environment with security in mind. Accomplish this through risk assessments, threat modeling, security testing and security awareness education and training.

Increase Emphasis on Detection and Response: There is an old adage that for a breach to occur, an attacker needs to be right only once, but to protect against a breach, a defender must be right every time. That's true – sort of. Organizations that have implemented advanced threat detection, monitoring and management capabilities through technologies like intrusion detection, log management and SIEM may not close off every entryway, but they can sniff out indicators of compromise and shut down a live attack before intruders can access the most sensitive areas of your environment. And if an incident is detected, a quick and efficient response to an attack on your network can save an untold amount of time, money and staff hours. Incident response is a traditionally underfunded component of the security puzzle, but it shouldn't be. Not only do you need an IR plan, but you must regularly test it and run attack simulations.

Instill Security as a Culture: Every single user on your network has a role to play in keeping the company secure. After all, human error, in some capacity, is responsible for nearly all security incidents. But for this reality to resonate, you must create a culture of cross-departmental security. C-level executives can lead the charge from the top down, but ultimately the culture must be established as a collective effort among everyone.

Be Open to Sharing the Burden: The human problem isn't only reserved for employees who may click on an email they shouldn't or log into unsecure Wi-Fi from their local coffee shop – it also extends to the IT department. Companies should consider working with a partner more likely to follow sound security practices without taking any shortcuts. Compared to in-house efforts, managed security services providers (MSSPs) can help cover more threat vectors, keep systems more up to date, reduce unused technologies, spot emerging threats and implement leading-edge security practices. And if necessary, they can redouble their security arsenal by boosting their tools, capacity and skills at a faster rate than the average in-house IT team can. As we've said in the past, there is no shame in admitting you can't do it all – or any of it – on your own. An MSSP can help you divide and conquer.

IS YOUR PRESSURE RUNNING HIGH?

VISIT WWW.TRUSTWAVE.COM TO CONTACT AN ADVISOR TODAY.