Trustwave® | Singtel

REPORT

2018 Security Pressures

BASED ON A SURVEY COMMISSIONED BY TRUSTWAVE

CONTENT

Five years ago, we published the inaugural Security Pressures Report from Trustwave because we wanted to better understand which triggers generated torment for security professionals. We had a pretty good idea that you were growing increasingly squeezed due to a variety of causes, from advanced threats and breaches to skills and budget shortages, and your hardship only seemed to be accelerating. But we hoped to quantify this new reality in a more personal way – by examining it through the lens of "pressures" affecting real people.

At the time, the role of infosec leader was continuing its ascent toward prominence within the wider organizational structure, and it became apparent to us that the individual – not the climate in general – needed to be studied more intimately. Because across many companies, cybersecurity was becoming just as much about the men and women behind it as it was about the mission they sought to achieve.

Since 2014, this annual report has served to remind readers of the many diverse drivers that shape the daily workload and overall psyche of a security decision-maker, and the toll these instigators might be taking. In fact, not long before this report was published, Jon Oltsik, senior principal analyst at Enterprise Strategy Group, penned a column for *CSO Online* suggesting that due to the high-stress nature of their jobs, a mental health crisis is brewing that is leading to, at best, career frustrations and, at worst, complete burnout.

Our report feels as relevant and vital as ever, if for no reason than to help project much-needed awareness on what you are up against. We are back with the fifth-annual edition this year, and to commemorate the anniversary, we asked respondents to harken back to a half-decade ago and assess how their sanguinity has shifted.

Otherwise, the report delivers the same reliable statistics and insight concerning all that goes into your grind as a security decision-maker and influencer. The report is once again conveniently distilled into individual sections of "pressures," with the data findings juxtaposed against last year's numbers for easy comparison. And as a special addition this year, we call out any interesting trends that have emerged since the first time we surveyed our respondent pool five years ago.

We hope this report finds you well, draws a clearer picture of where your peers are making strides or experiencing setbacks, and, most importantly of all, empowers pressure reduction in the year ahead. Please enjoy the read.

OK, let's go.

KEY FINDINGS

PRESSURES REMAIN HIGH

54% of respondents experienced more security pressures in 2017, compared to 2016, to secure their organization. n addition, 55% of respondents expect 2018 to bring more pressure than 2017 did.

GEARING UP FOR GDPR

Although it has yet to take effect, the EU Global Data Protection Regulation is the compliance mandate exerting the most pressure on 26% of respondents, just one percentage point less than the Payment Card Industry Data Security Standard.

FALLING FOR THE BAIT

Preventing phishing attacks was the biggest responsibility threat and responsibility for 13% of respondents (increasing from 8% in last year's report), as criminals turn to more malware-free attacks, including business email compromise.

MONEY STILL TALKS

Lack of budget is the second-biggest pressure respondents face in regard to operating their security program, and accruing additional budget dollars tops their 2018 wish list.

TURNING OFF THE BELLS AND WHISTLES

Only 56% of respondents (down eight percentage points from last year's report and a whopping 18 percentage points from two years ago) reported feeling pressure to select and purchase security technologies containing all the latest features.

TWO IS BETTER THAN ONE

The number of organizations that exclusively install and maintain security solutions themselves dipped five percentage points in this year's report to 62%, with most of the remainder of businesses shifting to a hybrid in-house/managed security services model.

BEYOND COMPLIANCE

More than one out of five organizations (22%) are not feeling any compliance pressures at all.

ANOTHER YEAR OF MALWARE MISERY

Advanced security threats apply the most pressure on the operation of respondents' security programs; not surprisingly, preventing malware is the largest security responsibility for respondents.

STRAPPED FOR SKILLS

The much-lamented security talent deficit is the third-largest security program pressure pusher for respondents, and growing security skills ranks as their second-biggest wish for 2018.

TAKING THE PEDAL OFF THE METAL

A majority of organizations still emphasize speed over security (58%) with IT projects, but the divide continues to shrink, down 20 percentage points over five years, a likely sign that more organizations are embracing secure code development and security testing.

METHODOLOGY

Trustwave commissioned a third-party research firm to survey 1,600 full-time IT professionals who are security decision-makers or security influencers within their organization. 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), IT/IT security directors and IT/IT security managers and comprised 600 in the United States and 200 each in Canada, the United Kingdom, Australia, Singapore and Japan. Respondents work in a variety of sectors, with the most frequent being technology, manufacturing, professional services, health care, retail and finance. Respondents work at organizations that employ a mean of 4,390 people. The survey was deployed through emails sent in January 2018. Survey results have a margin of error of +/- 5%.

	2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
CIO	18%	18%	26%	17%	27%	9%	15%
CSO/CISO	6%	6%	4%	5%	8%	6%	7%
IT or IT Security VP	13%	16%	11%	14%	10%	12%	9%
IT or IT Security Director	18%	17%	22%	16%	10%	16%	26%
IT or IT Security Manager	35%	33%	29%	40%	40%	42%	29%
IT or IT Security Architect	10%	10%	7%	7%	5%	13%	13%

JOB ROLES (BY COUNTRY)

Note: Not all percentages throughout the report will add to 100 due to rounding.

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Up	53%	↑	54%	61%	46%	51%	45%	54%	55%
Same	30%	↑	33%	25%	42%	33%	42%	28%	39%
Down	17%	↓	13%	13%	12%	15%	12%	18%	6%

AMOUNT OF PRESSURE FELT IN 2017 (COMPARED TO THE PRIOR YEAR)

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Up	58%	↓	55%	59%	48%	53%	46%	57%	59%
Same	31%	↑	35%	29%	43%	34%	48%	30%	37%
Down	12%	↓	10%	12%	8%	12%	6%	12%	3%

AMOUNT OF PRESSURE EXPECTED TO FEEL IN 2018 (COMPARED TO 2017)

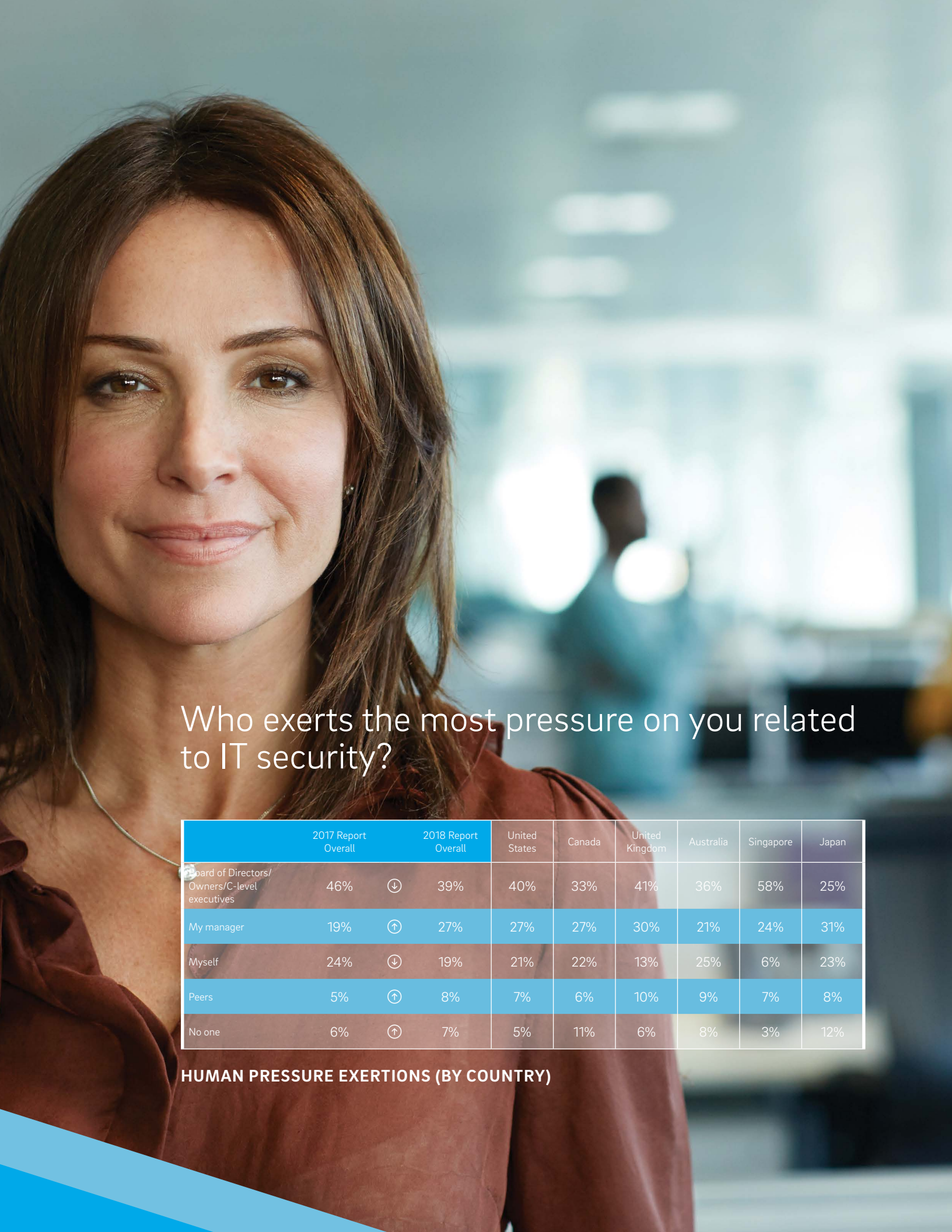
OVERALL SECURITY PRESSURES

The heat is on once again. More than half of respondents (54%) encountered increasing pressures to secure their organizations in 2017, compared to 2016. This is the fifth-consecutive Security Pressures Report from Trustwave in which a majority of respondents reported rising security pressures when contrasted with the previous 12 months. And once again, the United States is the country with the most respondents citing advancing pressures (61%).

Considering the continuously flush cybercrime news cycle, it would stand to reason that security professionals will be forecasting year-over-year pressure expansions for, well, years to come. Indeed, 55% of respondents expect 2018 to bring greater pressures than 2017 – but this is actually an improvement compared to last year's report, when 58% of respondents anticipated greater pressures incoming and in the 2016 report, when 62% of respondents expected pressures to intensify.

The question then is, do these numbers signal a positive trend steeped in reality – or are respondents just growing more optimistic? There is no way to know for sure, but as this report will later show, security practitioners are finding better ways to relieve some of their security pressures.

55% of respondents expect 2018 to bring greater pressures than 2017 – but this is actually an improvement compared to last year's report.



Who exerts the most pressure on you related to IT security?

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Board of Directors/ Owners/C-level executives	46%	↓	39%	40%	33%	41%	36%	58%	25%
My manager	19%	↑	27%	27%	27%	30%	21%	24%	31%
Myself	24%	↓	19%	21%	22%	13%	25%	6%	23%
Peers	5%	↑	8%	7%	6%	10%	9%	7%	8%
No one	6%	↑	7%	5%	11%	6%	8%	3%	12%

HUMAN PRESSURE EXERTIONS (BY COUNTRY)

HUMAN PRESSURE EXERTIONS

Before we delve into the intangibles that ratchet up pressures for security professionals, let us focus for a few moments on the living, breathing catalysts holding one's feet to the fire.

Just under half (46%) of respondents pointed the finger at themselves or their direct manager as the largest sources of pressures. Thirty-nine percent of respondents, meanwhile, indicated pressures originate higher up the food chain: at the boardroom and C-suite level. But the 39% figure continues an impressive retreat, down seven percentage points from last year's report and 20 percentage points from two years ago. Singapore, where 58% of respondents are most pressured by their company's head honchos, is a notable holdout from this decline.

While senior management and board interest in security is more prevalent than ever, the statistics continue to convey that executive pressures do not translate into performance, especially in an industry with as much stress, worry and employee demand as this one. Instead, it appears those who are most deeply and personally connected to the security outcomes at a given organization – the very respondents to this report – are the ones exerting the highest degree pressure, which is a far healthier solution.

COMPLIANCE PRESSURES

Compliance is always lurking in the background of every organization's security program, some more conspicuously than others. After all, rules and regulations help drive security spending, instill a proven risk management model and stimulate boardroom interest in protecting sensitive assets.

Security compliance mandates have become more prescriptive and rigorous over time, even as they typically set forth only baseline protections. As a result, they necessitate plentiful skills and resources, of which many organizations are in short supply.

That will be important to remember now that compliance is again making headlines, with the forthcoming General Data Protection Regulation (GDPR) evoking the most compliance pressures for 26% of respondents. Not surprisingly, the largest share of respondents feeling pressure from the European Union-based regulation reside in the U.K. (41% compared to, for example, 27% in the United States).

The GDPR, which becomes enforceable May 25, 2018, only slightly trailed the Payment Card Industry Data Security Standard (PCI DSS) (27%), which was first released in 2004 but receives continual modifications to address new threats, for placing the most pressure on respondents.

Stiff fines await organizations that fail to comply with the GDPR, PCI DSS and a host of other mandates that currently exist. But even bigger consequences could await those stubborn companies that treat security as merely a necessarily evil and compliance as their ceiling. Conversely, those organizations that regard compliance as table stakes on their way to ingraining security into their overall culture will be the biggest benefactors of all.

The best news of all may be that nearly a quarter of respondents are not feeling any compliance pressures at all – an indication that they have significantly grown the maturity of their security program, in which case compliance challenges are less frequent. Other options include respondents are not greatly affected by compliance requirements or that they are disregarding their obligations at their own risk.

Name the cybersecurity regulation or mandate currently placing the most pressure on your organization.*

	2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
The Payment Card Industry Data Security Standard (PCI DSS)	27%	30%	24%	29%	20%	29%	28%
The General Data Protection Regulation (GDPR)	26%	27%	21%	41%	23%	32%	11%
Some other national, regional or local law	14%	13%	11%	8%	19%	14%	19%
Some other industry-specific requirement or security framework	11%	11%	8%	7%	7%	13%	16
Not feeling any compliance pressure	22%	20%	35%	15%	30%	10%	25%

COMPLIANCE PRESSURES (BY COUNTRY)

** New question for 2018*

OPERATIONAL PRESSURES

2018 SECURITY
PRESSURES REPORT

Comparing the results of this section with data from the first time we asked this question five years ago paints arguably the most realistic view of the current state of cybersecurity.

For one, advanced security threats still present the most extreme operational pressures (26%), which is telling of how complex and evasive attacks continue to be. What was considered advanced a half-decade ago may not meet that definition today, but adversaries are always creating the latest and greatest threat designed to subvert security efforts and inflict maximum harm on a company's network. Advancements in methodology and malware design allow professional cybercriminals to continue slaying targets in long-duration compromises, and traditional defensive approaches are failing to match wits with these knowledgeable adversaries.

Second, worries over emerging technology adoption have waned. Organizations have become much more comfortable investing in and deploying technologies such as the cloud, mobile and social networking. Five years ago, 18% of respondents ranked the adoption of emerging technologies as their top operational pressure, but that number has dipped to 12% of respondents. Trust issues seemed to have faded, but waiting in the wings – if not already here – is the Internet of Things (IoT) revolution. IoT seems to be inciting only a casual concern among security professionals, but as more and more devices with business use cases come online[1], and more high-profile attacks are related to IoT, we expect to see this number tick back upward in the coming years.

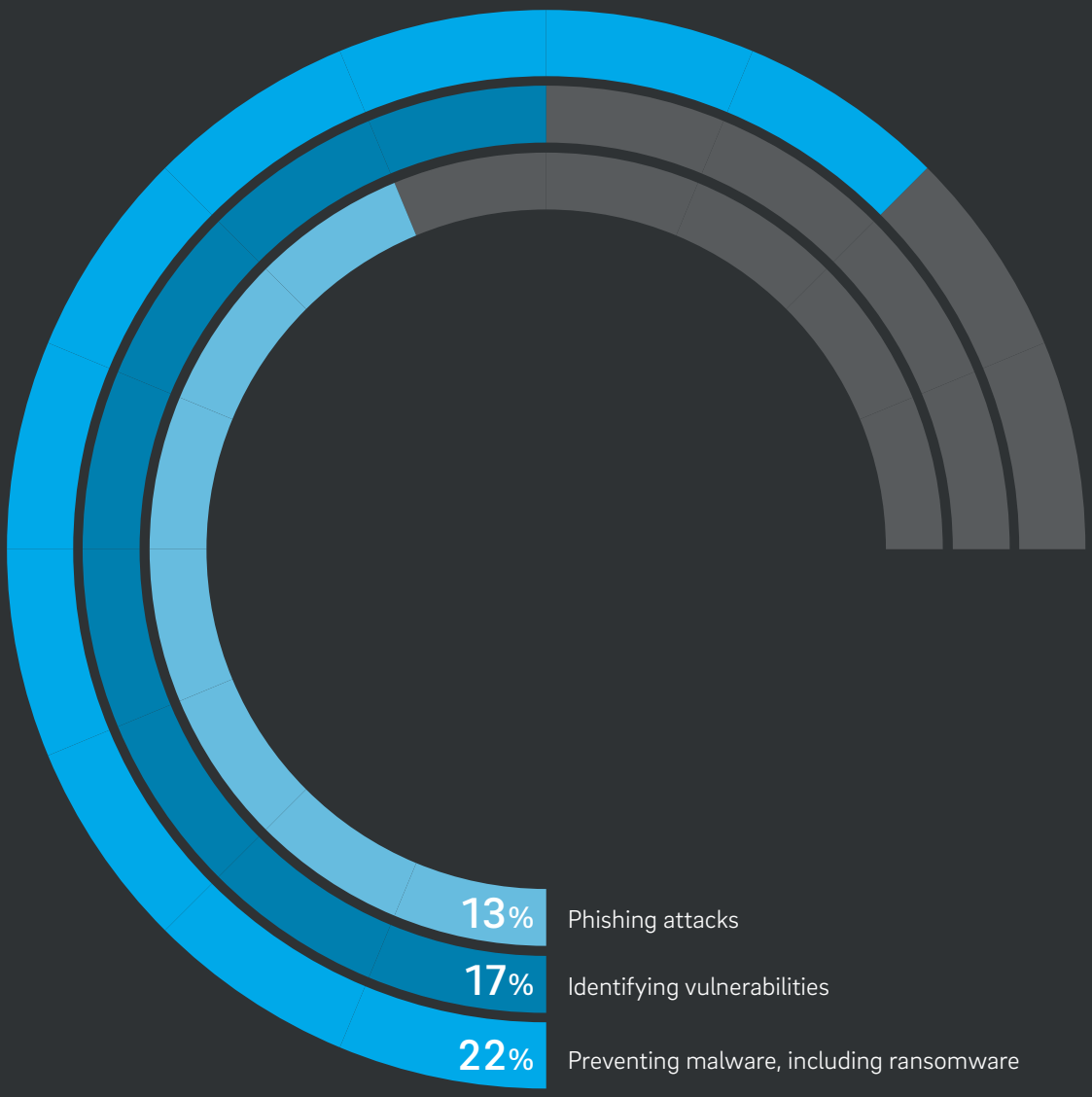
And third is the operational pressure that needs no introduction: shortage of skills and expertise. Industry observers have long lamented the talent deficit facing internal security teams and how this shortcoming has delivered a swarm of bad outcomes for organizations, including increasing workloads, staff burnout, junior employees being prematurely promoted, employee churn and a disproportionate focus on putting out fires instead of spending time building a mature security program from the ground up. No surprise, then, that 16% of respondents cited this operational pressure as their largest, rising from just 7% five years ago.

[1] https://www.forbes.com/sites/forbespr/2018/01/16/business-is-embracing-internet-of-things-as-most-important-technology-says-new-study/

Name the top pressure you currently face in regard to your information security program.

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Advanced security threats	29%	↓	26%	23%	25%	25%	21%	28%	38%
Lack of budget	14%	↑	17%	15%	21%	21%	19%	19%	12%
Lack of security skills/ expertise	15%	↑	16%	16%	10%	9%	18%	17%	27%
Pressures to adopt emerging technologies	13%	↓	12%	13%	10%	19%	11%	13%	6%
Lack of time	9%	↓	7%	8%	9%	8%	7%	5%	2%
Lack of staff members	5%	↑	7%	7%	5%	6%	7%	5%	8%
Security technology and product complexity	9%	↓	7%	10%	7%	5%	5%	7%	3%
Ensuring third-party providers or contractors follow best security practices	5%	↑	6%	6%	8%	5%	10%	4%	1%
Requests from business-line managers	2%	⊘	2%	2%	2%	2%	0%	0%	1%

OPERATIONAL PRESSURES (BY COUNTRY)



Which security threats and responsibilities are you facing the most pressure to address?

SECURITY THREATS AND RESPONSIBILITIES

Whether it is mining for cryptocurrency, emptying cash from ATMs, filching credit card numbers off a point-of-sale device, corrupting a mobile app, keylogging bank account information, exploiting a high-profile vulnerability, or performing any number of other malicious activities, malware is everywhere. And it remains the primary weapon of the duplicitous and marauding operating online.

For the largest number of respondents (22%), preventing malware, including ransomware, is their largest security threat and responsibility. It assumes the top spot from "identifying vulnerabilities," which fell from 22% to 17%. This appears to be positive news that vendors and users are doing a more formidable job of recognizing software and hardware flaws before attackers can pounce on the weaknesses, even as the number of reported vulnerabilities reached record-breaking levels in 2017 (14,712 compared to 6,447 in 2016).[2]

And what is responsible for the majority of malware? Phishing attacks – which were the biggest threat and responsibility riser, increasing from 8% to 13% of respondents. Cybercriminals relish duping unsuspecting users into enabling their sinister handiwork. Phishing appears as timeless as ever, as new iterations of the age-old fraudulent practice continue to emerge, including business email compromises (in which senders impersonate a company's CEO or some other company leader), which reportedly will cost organizations billions again in 2018.

Surprisingly low on the list for another year in a row is the detection of malicious activity and compromises, after peaking at 19% in the 2016 version of this report. While anecdotally more businesses are embracing the shift away from a prevention-focused strategy as data breaches and other successful attacks continue virtually unabated, it appears these companies have a long way to go. The lower-than-expected number here may be related to the possibility that organizations simply lack the internal resources to address threat detection at a level that would invite pressure.

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Preventing malware, including ransomware	20%	↑	22%	21%	23%	21%	22%	24%	20%
Identifying vulnerabilities	22%	↓	17%	20%	24%	15%	15%	14%	9%
Preventing social engineering and phishing attacks	8%	↑	13%	14%	10%	12%	13%	13%	11%
Patching vulnerabilities	12%	⊘	12%	10%	12%	14%	10%	9%	21%
Strengthening passwords and remote access	13%	↓	11%	11%	8%	15%	12%	10%	12%
Detecting malicious activity and compromises	12%	↓	11%	10%	10%	9%	12%	11%	12%
Managing network-connected devices (including IoT and mobile) and remote users	9%	↑	10%	10%	9%	5%	10%	11%	12%
Containing and responding to incidents and breaches	4%	⊘	4%	4%	3%	7%	4%	5%	2%

SECURITY THREATS AND RESPONSIBILITIES (BY COUNTRY)

[2] https://www.cvedetails.com/browse-by-date.php

Arguably the most memorable of his quirky quotes, baseball great Yogi Berra liked to say: "It's déjà vu all over again." It was in this very space last year that we mentioned that the previous 12 months had broken a record for most data reported data breaches ever in the United States, according to the Identity Theft Resource Center. And wouldn't you know it? Here we are back again – and the news is the same. 2017 smashed the old mark, with 1,579 "data breach incidents" tracked by the nonprofit organization.[3]

For many security professionals, data breaches – at least the prospect of them – are the new normal. Still, just because one has come to expect the possibility does not make it any less disquieting when one arrives.

But the worrying outcomes associated with cyberattacks and breaches are not new either. For respondents, 2017 was déjà vu all over again. The largest number of respondents, for a fifth consecutive year, graded customer data theft (34%) as the most vexing post-breach consequence, up four percentage points from the previous year's report.

Also rising was "data or system access restricted due to ransomware" at 22%, a jump of four percentage points from last year. Ransomware incidents reached a fever pitch in 2017, with several external studies suggesting ransomware infections were responsible for the historic surge in security incidents. Concerns over losing system and data access in Singapore was most notable, with significantly more respondents touting it as their largest worrying outcome compared to last year's report (18% to 26%).

Looking ahead to next year's report, we would expect ransomware to continue its rampage, with more advancements being made and new targets experiencing infections, including cloud services and IoT devices. However, if early reports are any indication, ransomware will likely share the landscape with other threats, especially crypto-mining software, rogue code that harnesses the computing power of victim's machines and devices to mine increasingly popular cryptocurrencies.

34% of respondents graded customer data theft as the most worrying post-breach consequence

[3] https://www.idtheftcenter.org/2017-data-breaches

What outcome worries you the most about cyberattacks and data breaches?

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Customer data theft	30%	↑	34%	37%	31%	36%	34%	25%	34%
Data or system access restricted due to ransomware	18%	↑	22%	22%	24%	18%	19%	26%	23%
Intellectual property theft	16%	⊘	16%	14%	20%	14%	21%	14%	17%
DDoS attack/website taken offline	14%	↓	10%	10%	6%	8%	6%	19%	12%
Reputation damage	12%	↓	9%	8%	6%	12%	8%	8%	11%
I do not think my organization will fall victim to a cyberattack or breach	7%	⊘	7%	5%	11%	9%	10%	3%	1%
Fines or legal action	3%	⊘	3%	4%	0%	2%	1%	3%	0%

CYBERATTACK AND DATA BREACH WORRYING OUTCOMES (BY COUNTRY)

CYBERATTACK AND DATA BREACH REPERCUSSIONS

What if you do lose customer data or are unable to access critical systems or data due to a security incident? What does the fallout look like for a security professional?

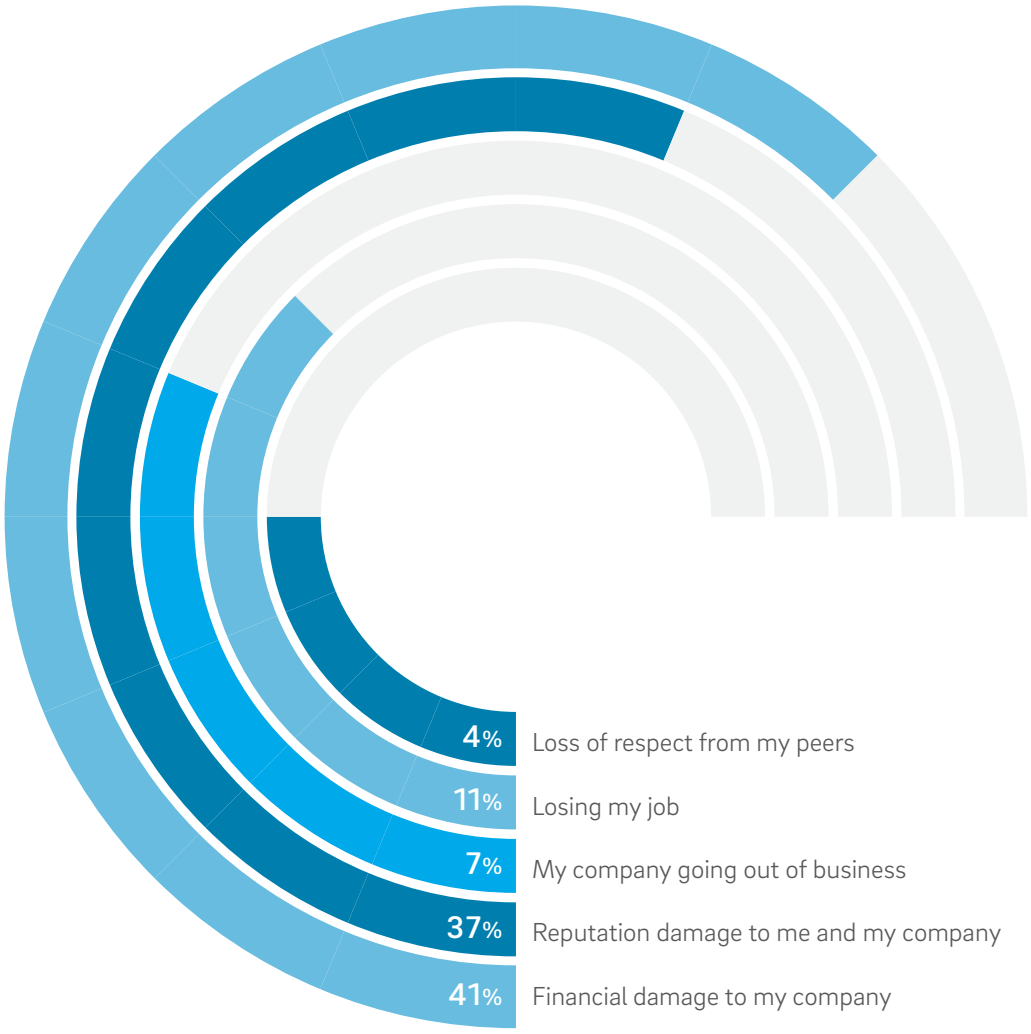
We were especially interested in asking this question as it can speak to the emotional element of an attack or breach, as well as the enduring ramifications that a business experiences in the days, weeks and months after news of the event is first reported by the media and to affected individuals.

The results of this question – "Which repercussion do you fear the most if your organization is breached?" – have remained relatively consistent since we first asked it in the *2016 Security Pressures Report*.[4] Reputation damage and financial damage considerably outdistance the others, with the latter (41%) flip-flopping with the former (37%) in this year's report.

In many ways, the two are intertwined. Indeed, the fiscal consequences related to a major security incident, from lost customers to recovery costs to litigation fees, do take their toll, as does a company's name being dragged through the mud, which leads to customer churn and legal actions.

For the third consecutive year, the fear of being fired came in as the most-feared post-breach repercussion among 11% of respondents, with the rarer prospect of a company going out of business at 7%. Surprisingly "the loss of respect from my peers" trailed (at 4%), but considering how common breaches are and how difficult it is to safeguard an organization these days, perhaps security professionals give their industry counterparts the benefit of the doubt if they succumb to an incident.

[4] https://www2.trustwave.com/security-pressures-report-2016.html



Which repercussion do you fear the most if your organization is attacked or breached?

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Financial damage to my company	38%	↑	41%	40%	51%	36%	47%	40%	33%
Reputation damage to my company	42%	↓	37%	33%	37%	40%	31%	37%	54%
Losing my job	11%	⊘	11%	14%	5%	10%	12%	15%	2%
My company going out of business	6%	↑	7%	9%	4%	9%	6%	7%	6%
Loss of respect from my peers	4%	⊘	4%	5%	2%	4%	4%	1%	3%

CYBERATTACK AND DATA BREACH REPERCUSSIONS (BY COUNTRY)


43%
INTERNAL VS
EXTERNAL THREATS
57%

20% answered accidental internal threats and 23% answered malicious internal threats.

In the context of words, the subtle way in which a question is phrased makes all the difference. For example, if you were to query security professionals on who poses the greatest risk to their organization – insiders or outsiders – most respondents will likely answer the former, as they are aware of the access that internal employees have to sensitive information and devices, as well as the complacency and negligence by which some operate.

However, if the wording were changed to which threat – internal or external – poses the greatest pressure on security professionals, as we do each year for the purposes of this report, the responses tend to dramatically swing in the other direction. Why? Because respondents know just how adept the enemy is at abusing their business. Put simply, it is difficult to defend against external threats, which is why many organizations are slowly but surely shifting their concentration toward detection and response.

Back to the survey question, 57% of respondents answered external threats (up six percentage points from last year's report), 20% answered accidental internal threats (interestingly down to a five-year low) and 23% answered malicious internal threats (up one percentage point from last year's report). Respondents from Canada and Australia reported being especially tormented by external threats.

It is worth keeping an eye on the findings related to accidental and malicious insider threats, as typically the former exerts the most pressure due snafus committed by the well-intentioned, if unwitting, like clicking on phishing links and introducing malware, or surfing the web on an unsecured connection. Perhaps the fluctuation is just a blip, or perhaps security awareness education and training programs are making a discernible dent.

Additionally worth noting is that there is no clear definition for internal versus external threats. Some companies, for example, may define most threats as insider threats, considering the goal of intruder is to acquire insider privileges and access.

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
External threats (malicious hackers, data-stealing malware, etc.)	51%	↑	57%	55%	65%	54%	63%	56%	53%
Internal threats (employee malfeasance, deliberate leakage of data, etc.)	22%	↑	23%	22%	19%	25%	21%	28%	26%
Internal threats (employee accidents, non-malicious mishaps, etc.)	27%	↓	20%	23%	15%	21%	16%	16%	21%

WHICH TYPE OF THREAT PRESSURES YOU THE MOST (BY COUNTRY)?

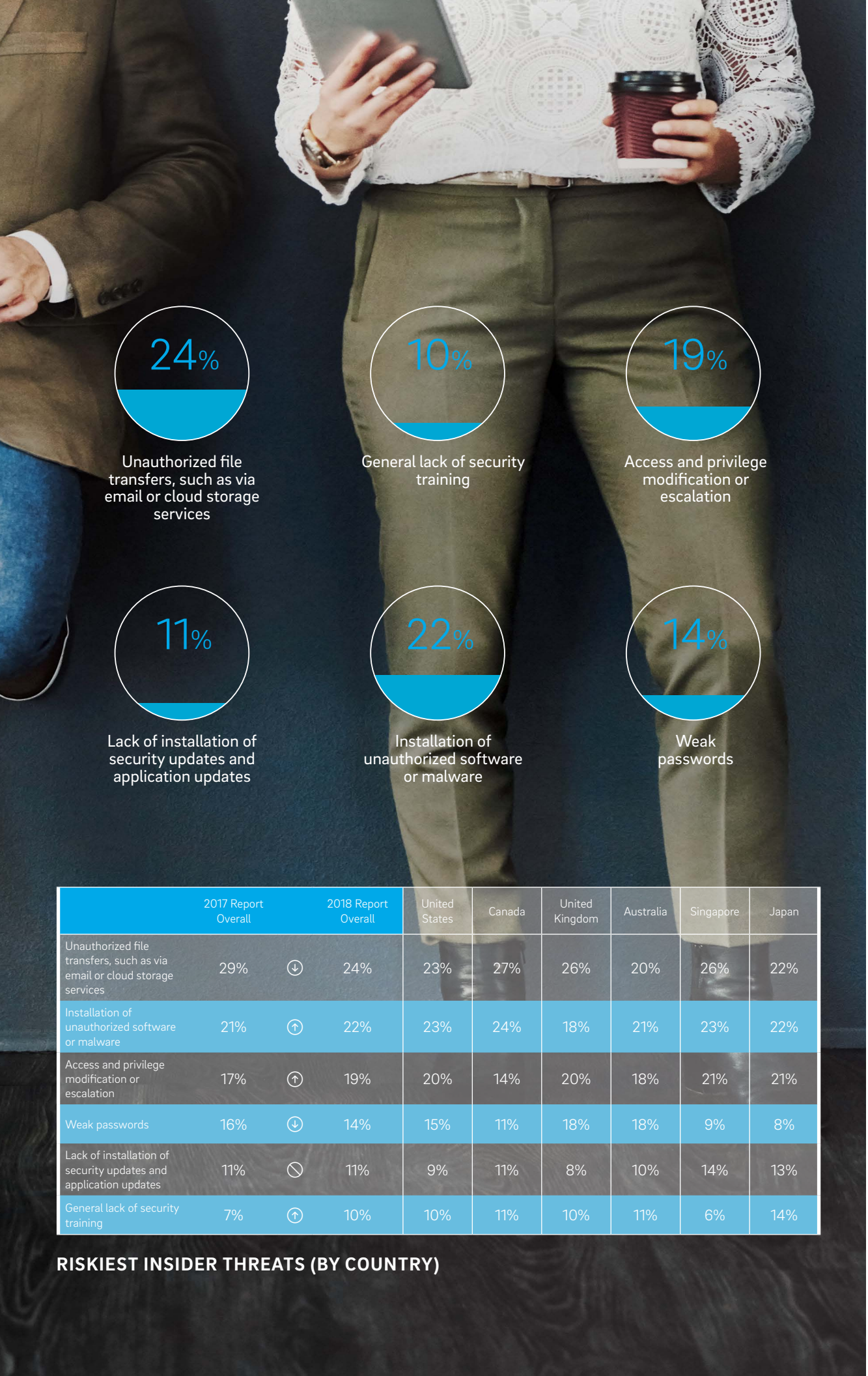
RISKIEST INSIDER THREATS

Fortunately, we have data that can help define exactly which risky insider activities are provoking the most pressures for security professionals. The more difficult part is classifying whether the activity took place deliberately or unintentionally.

For another consecutive year, respondents ranked unauthorized file transfers (24%) as the riskiest insider threat. The motivation for this risky insider activity is less clear. For example, such a scenario could involve a vengeful employee sending a list of sales contacts to her personal email before she joins a competitor – or a well-meaning employee sending himself an email containing sensitive information so he can work from home.

Ranking second was installation of unauthorized software or malware (22%). Again, this is another example where a scenario in which malware is implanted on the network could be inadvertent or premeditative. Access and privilege modification or escalation, which is usually the sign of malicious intent, earned the top insider threat pressure for 19% of respondents.

Weak passwords (14%), lack of proper patching (11%) and lack of security training (10%) rounded out the list.



24%

Unauthorized file transfers, such as via email or cloud storage services

10%

General lack of security training

19%

Access and privilege modification or escalation

11%

Lack of installation of security updates and application updates

22%

Installation of unauthorized software or malware

14%

Weak passwords

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Unauthorized file transfers, such as via email or cloud storage services	29%	↓	24%	23%	27%	26%	20%	26%	22%
Installation of unauthorized software or malware	21%	↑	22%	23%	24%	18%	21%	23%	22%
Access and privilege modification or escalation	17%	↑	19%	20%	14%	20%	18%	21%	21%
Weak passwords	16%	↓	14%	15%	11%	18%	18%	9%	8%
Lack of installation of security updates and application updates	11%	⊘	11%	9%	11%	8%	10%	14%	13%
General lack of security training	7%	↑	10%	10%	11%	10%	11%	6%	14%

RISKIEST INSIDER THREATS (BY COUNTRY)

SPEED VS SECURITY

Patience may be a virtue, but in the past a large majority of organizations failed to heed this proverb, as they notoriously rushed IT projects to completion before fully considering and baking in security. However, the tide is unquestionably turning because for a second year in a row, respondents reported marked improvements around the pressure they feel to roll out IT projects before they are security ready.

The bulk of organizations still emphasize speed over security (58%), more than security over speed (42%), but the divide continues to shrink.

When we first published this report, 79% of respondents reported feeling pressures to roll out IT projects – such as applications and other software – despite security issues, usually due to drivers such as time-to-market and a desire to place features over resiliency.

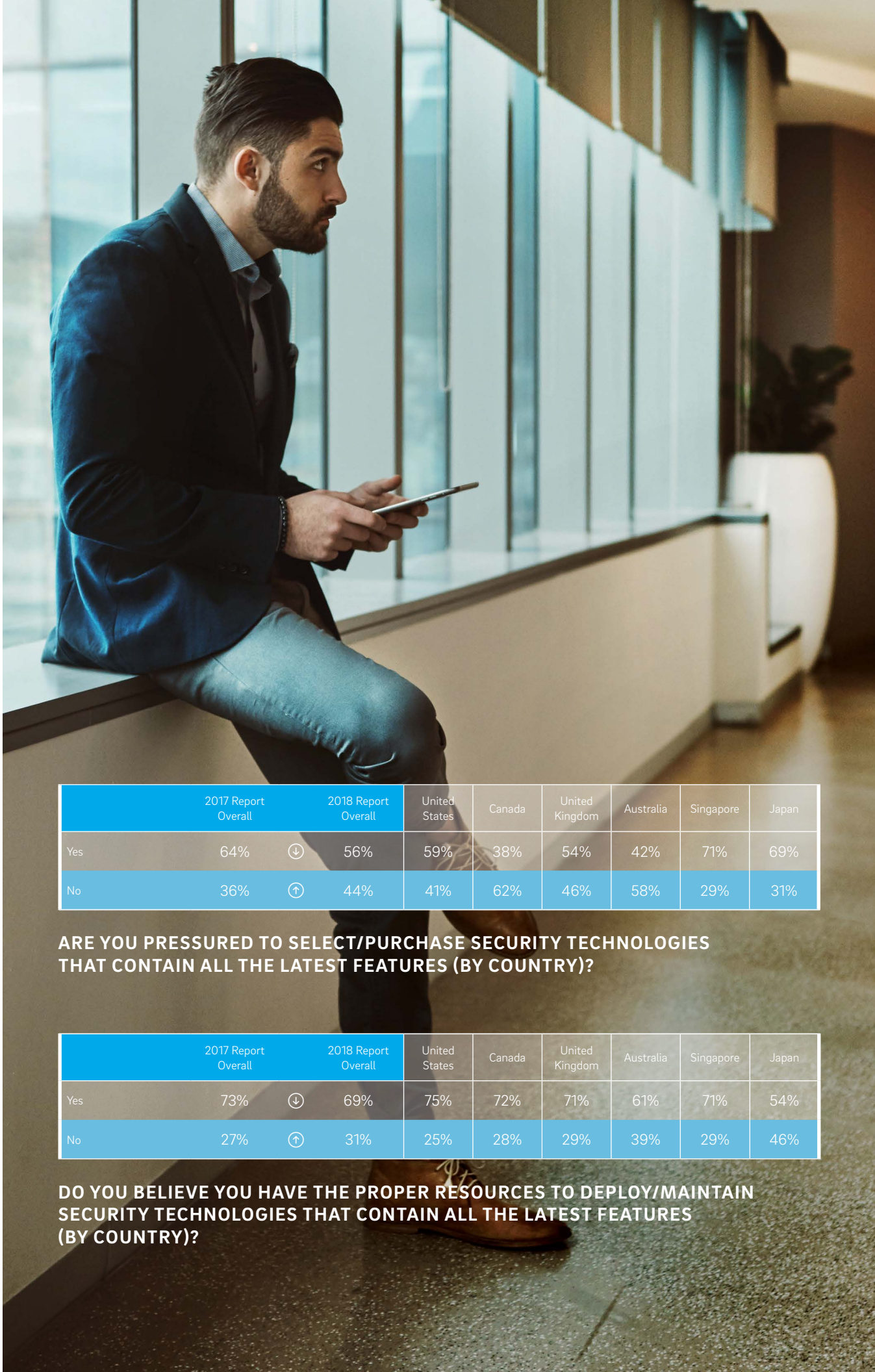
That number, however, has plummeted 20 percentage points in five years, a clear sign that the necessary checks and repairs, which can be completed through security testing and stronger code development, are becoming more the norm than the exception. This apparent reduction in shortcuts and incurrence of so-called technical debt during the software development lifecycle can help mitigate the costly consequences that result from an attack or breach. Still, there is a long way to go, as 2017 brought a record year of reported vulnerabilities.

Among countries, respondents in Canada, Australia and the United States experienced the largest amount of pressure relief in this category.

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Yes - once or twice	50%	↓	42%	48%	29%	41%	30%	52%	45%
Yes - frequently	15%	↑	16%	13%	11%	17%	17%	24%	18%
No	35%	↑	42%	39%	59%	42%	53%	24%	36%

WERE YOU PRESSURED TO ROLL OUT IT PROJECTS DESPITE YOUR CONCERNS THEY WERE NOT SECURITY READY (BY COUNTTRY)?


58%
Speed over Security
42%
Security over Speed



	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Yes	64%	↓	56%	59%	38%	54%	42%	71%	69%
No	36%	↑	44%	41%	62%	46%	58%	29%	31%

ARE YOU PRESSURED TO SELECT/PURCHASE SECURITY TECHNOLOGIES THAT CONTAIN ALL THE LATEST FEATURES (BY COUNTRY)?

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Yes	73%	↓	69%	75%	72%	71%	61%	71%	54%
No	27%	↑	31%	25%	28%	29%	39%	29%	46%

DO YOU BELIEVE YOU HAVE THE PROPER RESOURCES TO DEPLOY/MAINTAIN SECURITY TECHNOLOGIES THAT CONTAIN ALL THE LATEST FEATURES (BY COUNTRY)?

FEATURES VS RESOURCES

While features help enhance the appeal of a product for potential buyers, the downside is that these enticing components may be distracting, overvalued or, at worst, useless. Fancy new tools can be overkill for organizations that still fail to have a basic understanding of how their security systems function, a significant cost burden for organizations constrained by budget, and, most extreme of all, fruitless for organizations lacking the technical proficiency to implement them properly and extract expected value.

But like the previous section of this report, security teams appear to be pushing back against another pressures instigator. Only 56% of respondents (down eight percentage points from last year's report and a whopping 18 percentage points from two years ago) reported feeling pressure to select and purchase security technologies containing all the latest features.

However, for those 56% of respondents still feeling coercion to adopt and deploy the security technology de rigueur, 31% do not believe they have the adequate resources to get them up and running – a number relatively equal to last year's report and yet another symptom of the ongoing enterprise security skills shortage facing internal teams.

56% feel pressured to select and purchase security technologies containing all the latest features

STAFFING LEVELS

2018 SECURITY
PRESSURES REPORT

Cybersecurity is an explosive industry with a shrinking talent pool. This dichotomy means security leaders are desperately seeking employees, but finding extreme difficulties recruiting suitably qualified workers. Not only is competition fierce to attract candidates, maintaining them is another key challenge. This demand is not expected to wane anytime soon, with millions of unfilled jobs expected to persist into at least the next decade.[5]

And for another year, it appears a majority of organizations are failing to infuse the right amount of talent within their ranks. Sixty-nine percent of respondents either want to double or quadruple the size of their security team, while 5% want to more than quadruple its size. Just 26% (a rise of two percentage points from last year's report) believe their team is appropriately sized – although that figure is significantly improved from five years ago, when a mere 11% said their team consisted of the right size. This points to a possibility that organizations are at least trying to throw bodies at the needs created by cybersecurity (although many likely lack the preferred qualifications) – or, more likely, that they've developed beneficial relationships with managed security services providers, arrangements that are essentially eliminating the need for additional internal security staff growth.

Skills shortages appear to be the main driver of the labor crunch, but limited budgets are probably not helping either. Because demand is so high, the most competent and capable talent will cost a pretty penny to be lured away from their current employer and kept satisfied in their new role, with the cost including not just salary but also career development.

The paucity of insufficient staff and skills leads to potentially dire consequences for businesses, including increased workload on existing employees and a disproportionate focus on security functions that are either basic in nature (because that it is all the team is trained to handle) or emergencies (because there has been little concentration on more proactive work, such as vulnerability identification, threat detection and incident readiness, which in turn leads to more security fires to extinguish).

[5] https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Double (2 times the current size)	44%	↑	45%	46%	42%	41%	41%	54%	45%
Quadruple (4 times the current size)	26%	↓	24%	26%	18%	25%	18%	27%	24%
More than quadruple the current size	6%	↓	5%	5%	3%	3%	4%	5%	7%
None - current size is ideal	24%	↑	26%	23%	37%	31%	37%	13%	24%

PREFERRED SECURITY TEAM STAFFING LEVEL (BY COUNTRY)

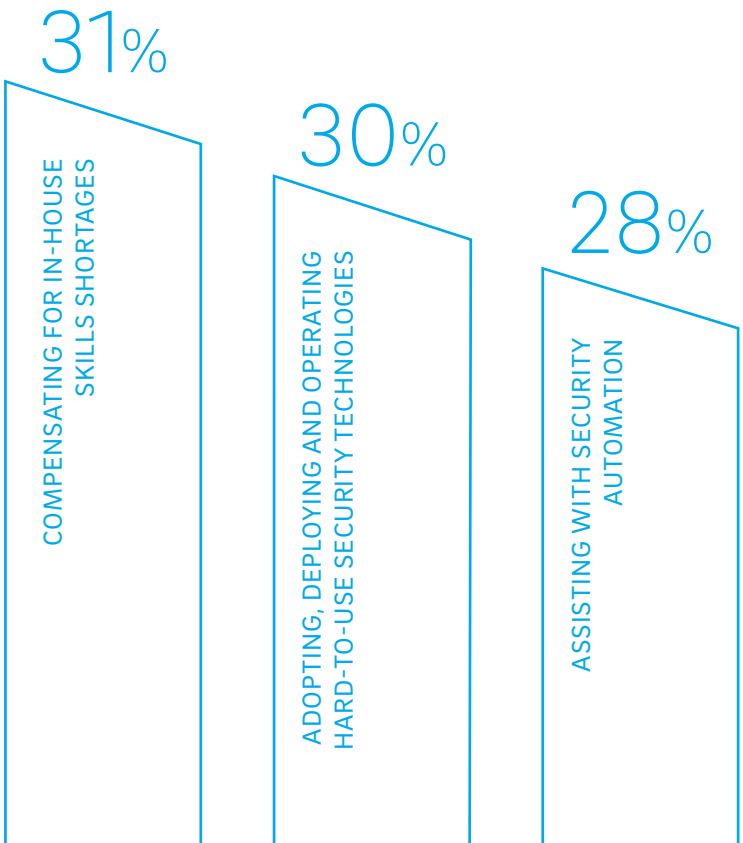
We have reached the point of this report where the dramatic and untenable pressures facing security professionals have been laid bare, and you are likely ready for some answers.

Among the most rapidly growing – and recommended – responses for overcoming the anguish that has become routine for so many in the industry is managed security services providers. MSSPs are attractive because of the breadth and depth of their portfolios, often enabled by round-the-clock security operations centers that offer expertise and intelligence that most organizations lack internally. Managed security services can range from unified threat management, secure web gateways and SIEMs to vulnerability testing, endpoint detection and response and IR.

Respondents were asked, for a second year in a row, what is influencing or would influence their decision to partner with an MSSP. Due to the diverse reasons why organizations might seek to offload their security tasks to an external provider, this is the only question of the survey in which respondents were able to choose multiple options.

Of the top three, the largest number of respondents (31%) pointed toward MSSPs' ability to compensate for in-house skills shortages, followed by 30% who cited an MSSP being able to help with adopting, deploying and operating hard-to-use security technologies. Another 28% said they are drawn to MSSPs for security automation.

Security automation was not an option last year, but we decided to add it as a possible selection in this year's report because many organizations are so clearly struggling with rapidly making decisions and taking actions around the bombardment of security alerts they face. Automation can serve as a force-multiplier that can efficiently identify, contain and eradicate real-time threats before they impart serious harm.



Why do you or why would you partner with a managed security services provider?

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
To compensate for in-house skills shortages	31%	⊘	31%	27%	25%	31%	31%	41%	41%
To adopt, deploy and operate hard-to-use security technologies	33%	↓	30%	29%	24%	26%	31%	39%	34%
To help with security automation	--	--	28%	27%	25%	32%	35%	39%	15%
To provide intelligence and extend security coverage against sophisticated threats	34%	↓	27%	28%	32%	28%	27%	29%	17%
To address complex security tasks, like vulnerability testing and incident response	26%	↓	25%	24%	22%	24%	27%	35%	21%
To handle routine tasks	26%	↓	23%	19%	26%	21%	26%	29%	27%
To stretch budgets	28%	↓	21%	21%	24%	17%	18%	24%	25%
To free up time to work on IT projects that got delayed by unresolved security issues	18%	↓	16%	16%	16%	16%	19%	24%	8%
To gain more visibility into the IT environment	10%	⊘	10%	9%	9%	8%	9%	15%	12%

REASONS FOR PARTNERING WITH AN MSSP (BY COUNTRY)

IN-HOUSE VS MANAGED SERVICES

Momentum for managed security services is an indication of a maturing market well positioned for continued growth. It also signifies that organizations have become shoehorned due to a host of factors, from pernicious threats to device proliferation to resource shortages, and consider managed security their best option to discover breathing room.

Seventy-eight percent of respondents are likely to or already do partner with an MSSP – and the number of organizations that exclusively install and maintain security solutions themselves dipped five percentage points in this year's report to 62%. Much of the remainder of respondents (35%) now use managed security providers either in conjunction with their in-house team or as the sole handler of their security program.

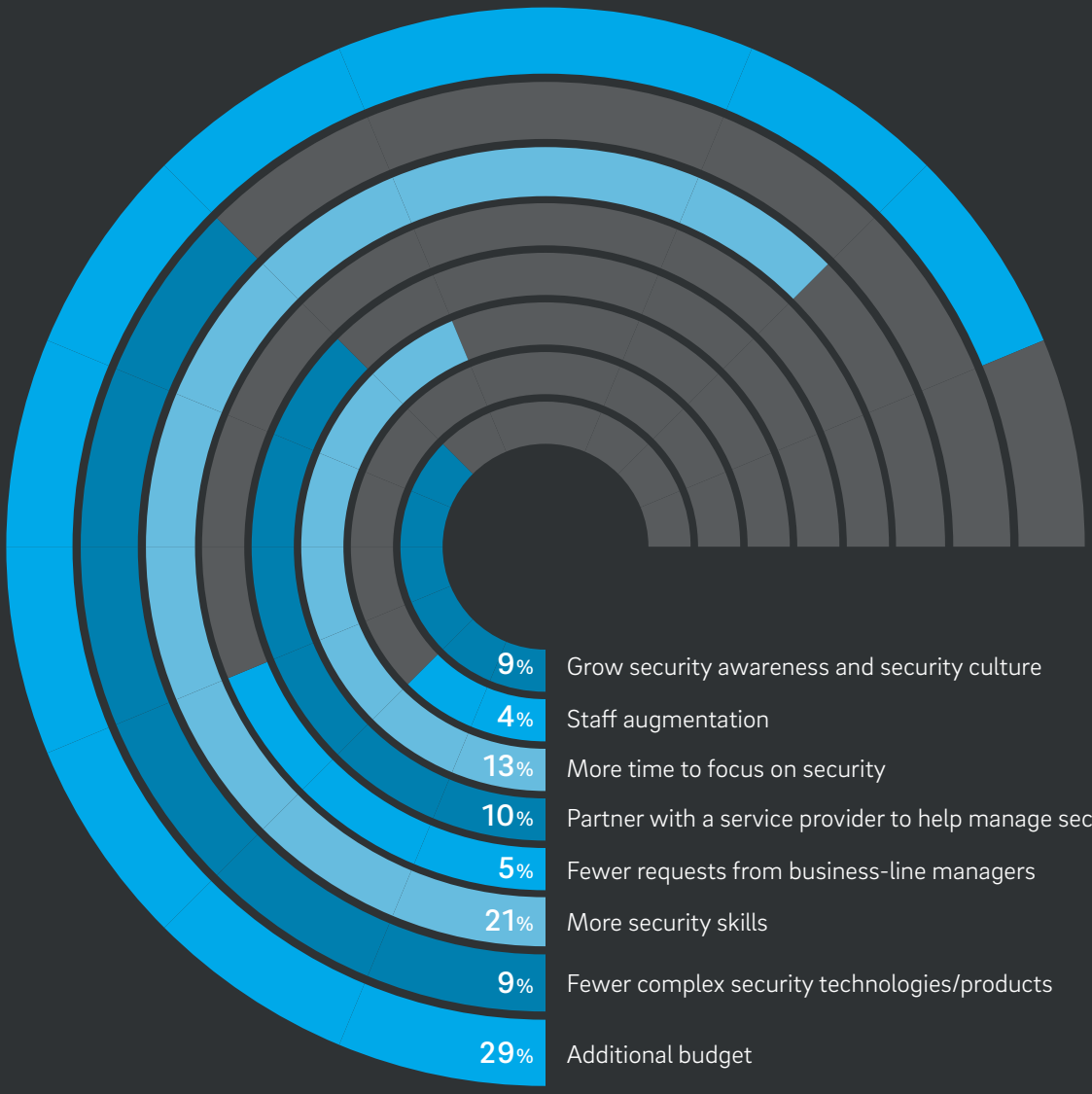
How likely are you to partner with a managed security services provider to relieve some of the security pressures you face?

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Likely - we already do	43%	↓	33%	38%	31%	31%	30%	31%	32%
Likely - we plan to in the future	40%	↑	45%	43%	40%	47%	36%	60%	45%
Not likely	17%	↑	22%	19%	29%	22%	34%	9%	22%

LIKELIHOOD OF PARTNERING WITH AN MSSP (BY COUNTRY)

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Our in-house IT staff/ security team	67%	↓	62%	66%	68%	59%	62%	52%	61%
Third-party managed security services provider (MSSP) and our in-house IT staff	26%	↑	28%	24%	25%	31%	26%	38%	32%
Third-party MSSP manages all of our security technologies	5%	↑	7%	7%	3%	7%	6%	9%	3%
Other	2%	↑	3%	3%	4%	3%	5%	1%	4%

RESPONSIBLE FOR INSTALLING AND MAINTAINING SECURITY SOLUTIONS (BY COUNTRY)



Top 8 wishes for 2018

2018 WISH LIST

The traditional way we like to conclude this report is on a hopeful tone. This section will jettison you, even for an ever-so-brief period, into a utopian world where your wishes can come true.

If such a place existed, 29% of respondents would receive additional budget, while 21% would acquire additional security skills for their organization. Many of the wishes sought by respondents in last year's report line up with this year's, although an additional wish list option was added this year that drew abundant interest: growing security awareness and a security culture (9%) – a concept that addresses the importance of permeating the message of security across all departments and from the corner offices down to the cubicles.

Additional time to focus on security and the formation of a partnership with an MSSP were also popular wishes in this year's report.

Name the top item on your wish list to help alleviate the pressures you face related to security.

	2017 Report Overall		2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Additional budget	30%	↓	29%	26%	35%	33%	32%	33%	25%
More security skills	24%	↓	21%	21%	17%	16%	23%	17%	30%
More time to focus on security	9%	↑	13%	14%	9%	16%	12%	10%	11%
Partner with a service provider to help manage security program	11%	↓	10%	10%	10%	6%	8%	17%	8%
Fewer complex security technologies/products	14%	↓	9%	10%	9%	9%	9%	9%	9%
Grow security awareness and security culture	--	--	9%	10%	11%	8%	8%	7%	9%
Fewer requests from business-line managers	9%	↓	5%	7%	4%	6%	2%	5%	2%
Staff augmentation	3%	↑	4%	3%	4%	6%	3%	1%	4%

SECURITY WISH LIST ITEMS (BY COUNTRY)

CONCLUSION

"Pressures can either burst a pipe or make a diamond."

Athletes have used this phrase to describe the intense duress that teams can find themselves in – and, depending on how they confront the pressures, the result can be famine or feast. It might wise to consider this phrase the next time your hardships seem too much to bear, and how you can throttle your stresses to make diamonds.

Athletes in team sports have the added benefit of being able to lean on their teammates during the most challenging times. While athletes in individual sports bear no such luxury, if a player on a team is, say, having a subpar outing, the coach can substitute him or her out until they sort things out. Ultimately, though, someone will have to step up when the game is on the line – and make a diamond or burst a pipe.

In security, there is a lot on the line too. And it takes a team to maturate a security program. Unfortunately for many reading this report, teams are hard to come by internally due to skills and resource shortages. That is why more and more organizations are looking externally for support.

We have referenced managed security services providers (MSSPs) multiple times in this report. If you are considering going that route to help ease your burden and ensure your wish list items get fulfilled, here is what you should be looking for:

Global Reach: True global MSSPs have unrivaled visibility and intelligence into advanced threats and continuity of operations that no regional or smaller providers can match.

Security Expertise: With today's worldwide shortage of security expertise, there is no substitute for MSSPs that employ the industry's best and brightest security minds.

Lifecycle Portfolio: Partnering with an MSSP that is effectively a "one-stop shop" for all your security needs is critical in the selection process.

Actionable Security Portal: Even if you delegate responsibilities to an outside vendor, you may still want to retain some control – and certainly will want to keep tabs on your activities and operations. MSSPs should offer a single pane-of-glass that provides an intuitive window into your security world.

Advanced Threat Detection and Response: Support for real-time visibility into endpoint operations is an essential given the growing number of devices and workstations, and attackers' preference for targeting these assets. Security operations centers – especially if globally connected – can extend these capabilities and cover the lifecycle of a security incident, form detection all the way through containment and remediation.

Customer Focus: In the end, it's all about you, the pressure-filled IT security professional. A top-tier MSSP should be highly qualified in all areas of security, but above all should want to listen closely to understand your business and all its needs. The finished product should be a customized and flexible solution set – and a more relaxed security practitioner.

A FIVE-YEAR RETROSPECT

A lot can change in five years, especially in such a dynamic and fluid industry like cybersecurity. In honor of this report's five-year anniversary, we asked respondents to compare their experiences as a security practitioner in present day with how they perceived what they could have accomplished five years ago.

Still pressured? Absolutely. Throwing in the towel? Not a chance. When the going gets tough – as it unquestionably has over the previous 60 months for security professionals due to the many reasons documented in this report – the tough get going. Indeed, 54% of respondents are more confident than they were five years ago in their ability to secure an organization. Another 32% consider themselves similarly confident, while only 15% are less confident.

During a time that feels significantly easier to fail than succeed at deterring cyberattacks, information leaks and breaches, and keeping sensitive data shielded from malicious hackers and spiteful insiders, the undaunted, optimistic and resolute nature of security practitioners – even if they may not exhibit such traits on the surface – is refreshing and, frankly, thrilling to see.

The findings of this section may be driven any number of factors, from respondents' increasing confidence in new security tools for identifying and responding to malicious activity, to increasing comfort partnering with managed security services providers, to flourishing support from senior leaders, to old-fashioned hubris. Whatever the reason, though, one thing is certain: A hopeful security professional is a happier security professional.

Compared to five years ago, do you have more or less faith in your ability to secure an organization?

	2018 Report Overall	United States	Canada	United Kingdom	Australia	Singapore	Japan
Dramatically more	15%	22%	10%	9%	11%	7%	13%
Slightly more	39%	36%	31%	34%	35%	42%	59%
Same	31%	25%	43%	43%	34%	32%	25%
Slightly less	13%	14%	15%	13%	16%	18%	3%
Dramatically less	2%	3%	1%	0%	2%	1%	0%

CONFIDENCE CHANGE IN ABILITY TO SECURE AN ORGANIZATION (BY COUNTRY)

Trustwave® | Singtel

TRUSTWAVE.COM