2017 Security Pressures Report

BASED ON A SURVEY COMMISSIONED BY TRUSTWAVE

Trustwave®

Table of Contents

01 Introduction

02 Key Findings

02 Methodology

04 Overall Security Pressures

05 Human Pressure Exertions

07 Personal Pressures

09 Operational Pressures

11 Security Threats & Responsibilites

13 Cyberattack & Data Breach Worrying Outcomes

15 Cyberattack & Data Breach Repercussions

17 Internal vs External Threats

19 Riskiest Insider Threats

21 Speed vs Security

23 Emerging Technologies

25 Features vs Resources

27 Staffing Levels

29 Internal Resource Pressures

31 In-House vs Managed Services

33 2017 Wish List

35 Conclusion

Introduction

The saying goes that time flies when you are having fun, yet it feels somewhat peculiar and ungainly assigning a lighthearted term to describe the daunting work of IT and security professionals like yourself. But time also does fly when you are busy, and there is certainly no shortage of onerous responsibilities and tasks confronting the information security profession every day. So here we are again, for the fourth year, with our annual investigation into the diverse sources of encumbrance greeting you behind every door.

We officially welcome you to the 2017 Security Pressures Report from Trustwave. Why do we believe it is a worthwhile exercise to conduct this survey and compile a report based on the results each year? Because you are human. You have real emotions, thoughts and feelings, despite how you may be perceived by others: as a gallant solider, operating steadfastly on an unpredictable battlefield, always in control.

But these characteristics are almost impossible to achieve. There is an undertow of distress and panic that virtually all IT and security pros feel in some capacity – and this report brings those to the surface in the form of digestible statistics. But more importantly it helps to provide a critical window into all that is at stake for you and your organization from a security perspective and, most of all, let you know – you are not alone.

As always, our hope is this report will enable you, your team, your bosses and your overall business to better understand where your security program may be falling short, where you are being overwhelmed or where your needs are not being addressed.

For ease of consumption, the report is designed into individual sections of "pressures" each featuring insightful context and convenient data tables, with the results compared against last year's findings as a way of understanding the state of security. In addition, we have broken out the results by country to include the United States, United Kingdom, Canada, Australia, Singapore – and for the first time – Japan. Like in years past, you will find some of the comparison data is particularly intriguing and revealing into the mindset of IT and security professionals based on their region.

We encourage you to enjoy this report as you see fit – a read-through its entirety is certainly an option, as we do our best to connect each distinct section so that it flows naturally. We have also laid out the report so you can pick out certain sections that matter most to you depending on the individual challenges you may be confronting at a given point in the year.

Key Findings

A REAL PRESSURE COOKER: 53% of respondents felt more pressures to secure their organizations in 2016 compared to 2015.

COMPUTER KIDNAPPING: Data or system access restricted by ransomware is the second-most worrying outcome of an attack or breach, behind customer data theft, but outpacing intellectual property theft.

THE TOP TWO: Advanced security threats rank as the top operational security pressure for respondents, followed by shortage of security skills.

NEED SKILLS NOT STAFF: Just under one quarter of respondents say their staffing size is ideal, up 11 percentage points year over year.

PREVENTION AND DETECTION: Identifying vulnerabilities and hindering malware rank as the top two security responsibilities facing respondents.

IN HARM'S WAY: 35% of respondents do not believe their organization is safe from security threats, up nine percentage points year over year.

GETTING IT RIGHT, FIRST: The pressures respondents feel to rush out IT projects before they are security ready declined by 12 percentage points.

REACHING OUT FOR HELP: Extending security coverage against advanced threats and compensating for internal skills shortages are top two reasons for partnering with a managed security services provider.

YOU ARE NOT ALONE: For another year, the percentage of respondents who turn entirely to internal staff to install and maintain security solutions dropped.

GOING OLD SCHOOL: The pressures to select security technologies containing "all of the latest features" decreased from 74% to 64% this year.

EVENLY MATCHED: Respondents are nearly split – 51% to 49% – over who poses the greatest threat: external adversaries versus trusted insiders.

HEADS IN THE CLOUDS: Of emerging technologies, the cloud overwhelmingly presents the most pressure to adopt and deploy, but the Internet of Things (IoT) and social media gained ground this year.

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, which included 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 and professional services. Respondents work at organizations that employ a mean of 4,267 people. The survey was deployed through emails sent in January 2017. Survey results have a margin of error of +/- 4% in the United States and +/- 6.9% in all other countries.

Overall Security Pressures

Each year since this annual report was first published, a majority of respondents have reported that the amount of pressure they experienced in regard to their security increased from the prior 12 months. That outcome did not change in this year's installment, where 53% of respondents express that they faced increased pressure trying to secure their organization in 2016 compared to 2015.

While the ascent is not as drastic compared to last year's report – when 63% of respondents reported dialed-up security pressure – the fact is staggering nonetheless. More often than not, IT and security professionals are feeling the heat when it comes to protecting their organization against a wide range of adversaries and threats. Like last year, the struggle is most conspicuous in the United States, where pressure expanded year over year for 60% of respondents. The majority of respondents from the other countries polled also acknowledge increasing pressure – except in Singapore, where just 37% share such a sentiment.

Thirty percent of overall respondents believe pressure stayed level in 2016, compared to 2015. Meanwhile, 17% of respondents compose an optimistic group who experienced decreasing pressure year over year.

Looking ahead, 58% of respondents expect to experience added pressure to secure their organizations in 2017, while 31% foresee it to remain stable and 12% anticipate a drop in pressure is on the horizon.

Amount of Pressure Felt in 2016 (Compared to the Prior Year)

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Up	**63%**	▼	**53%**	60%	53%	53%	55%	37%	51%
Same	**21%**	▲	**30%**	24%	32%	35%	33%	27%	42%
Down	**16%**	▲	**17%**	16%	16%	13%	13%	37%	8%

Amount of Pressure Expected to Feel in 2017 (Compared to 2016)

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Up	**65%**	▼	**58%**	62%	60%	53%	57%	48%	57%
Same	**24%**	▲	**31%**	24%	32%	36%	35%	33%	37%
Down	**11%**	▲	**12%**	14%	8%	12%	8%	20%	7%

* Throughout the report, percentages may not add to 100 due to rounding.

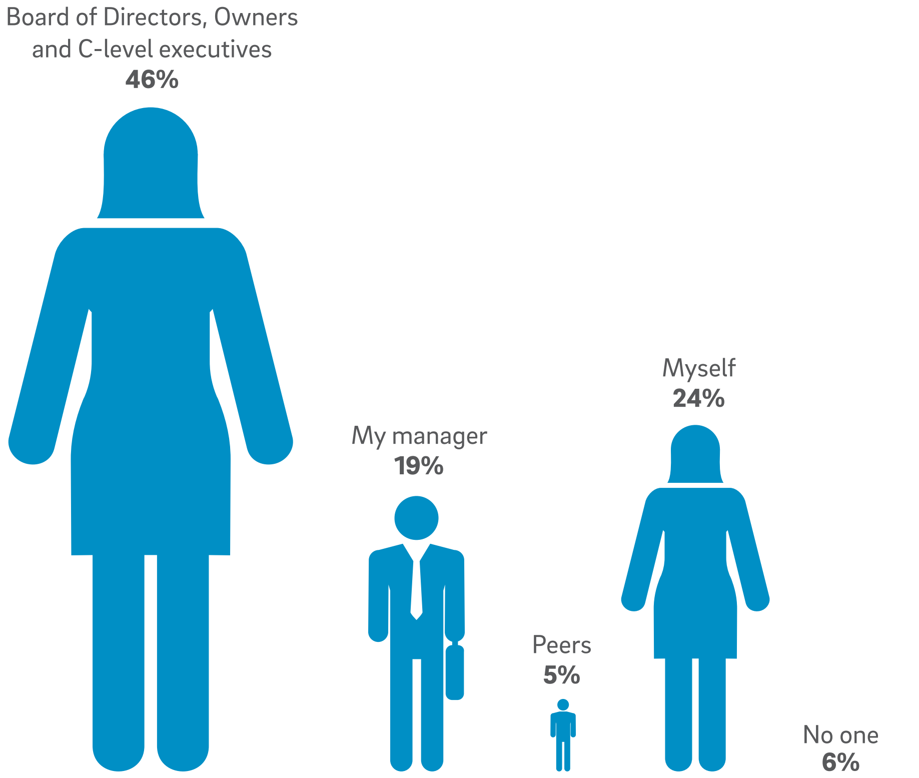
Human Pressure Exertions

The success of a security program has far-flung implications on the overall business. After all, a data breach can result in a back-breaking experience for any organization and derail its financial objectives. On the flip side, robust security can drive business and serve as a competitive differentiator.

This is part of the reason why the job of IT and security professional has become so transcendental, cutting across business lines and departments on its ascent to the corner offices and board rooms. More than ever, senior leadership and boards of directors are interrogating security teams on their plans, and expecting information and insight in return.

As to which individuals exert the most pressure on respondents, the highest ratio of respondents (46%) choose boards, owners and C-level executives. However, that percentage drastically fell year over year because the pressure exerted by oneself soared 13 points to become the second-biggest human pressure pusher among respondents at 24%. Next come direct managers (19%), nobody (6%) and peers (5%).

It is not clear what prompted such a dramatic shift in this year's results, as it was seen across countries, except in Singapore, where this year's results mirror last year's overall findings. One possible explanation is that business managers and executives are more likely to recognize that placing too much pressure on IT and security professionals does not translate to improved performance – and instead may lead to stress and burnout. In an era where security talent is at a premium, organizations can ill afford to lose skilled individuals. Thus, the largest human source of pressure has migrated more to the respondents themselves than their leaders, as they try to cope with all of the challenges on their plate.



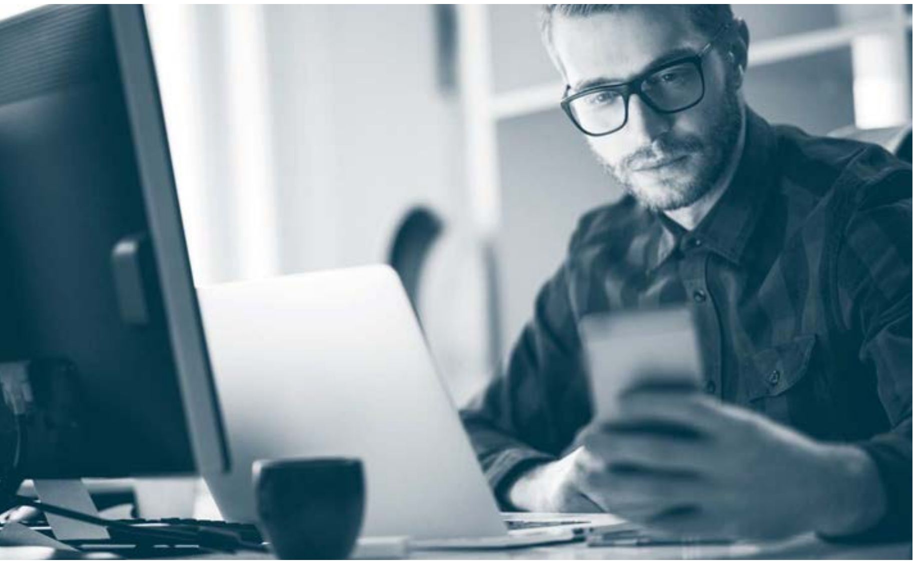
Who exerts the most pressure on you related to IT security?

Human Pressure Exertions by Country

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Board of Directors/Owners/ C-level executives	**59%**	▼	**46%**	51%	40%	47%	35%	57%	39%
Myself	**11%**	▲	**24%**	27%	27%	20%	31%	12%	22%
My manager	**21%**	▼	**19%**	15%	20%	20%	21%	22%	21%
No one	**2%**	▲	**6%**	4%	8%	6%	9%	1%	16%
Peers	**7%**	▼	**5%**	3%	7%	9%	5%	9%	3%

Personal Pressures

There is an old saying in the IT security industry that you do not want to end up on the front page. If you do, it usually means something bad happened – typically a crushing data breach that exposed the sensitive information of your employees and/or customers. And when a business does earn the dubious distinction of front-page placement, it often stirs up pressures (and sympathy pains) from IT and security professionals toiling away at other organizations – either because they are concerned they could be next, or more likely, because they now must answer questions and institute additional safeguards to ensure they are not.

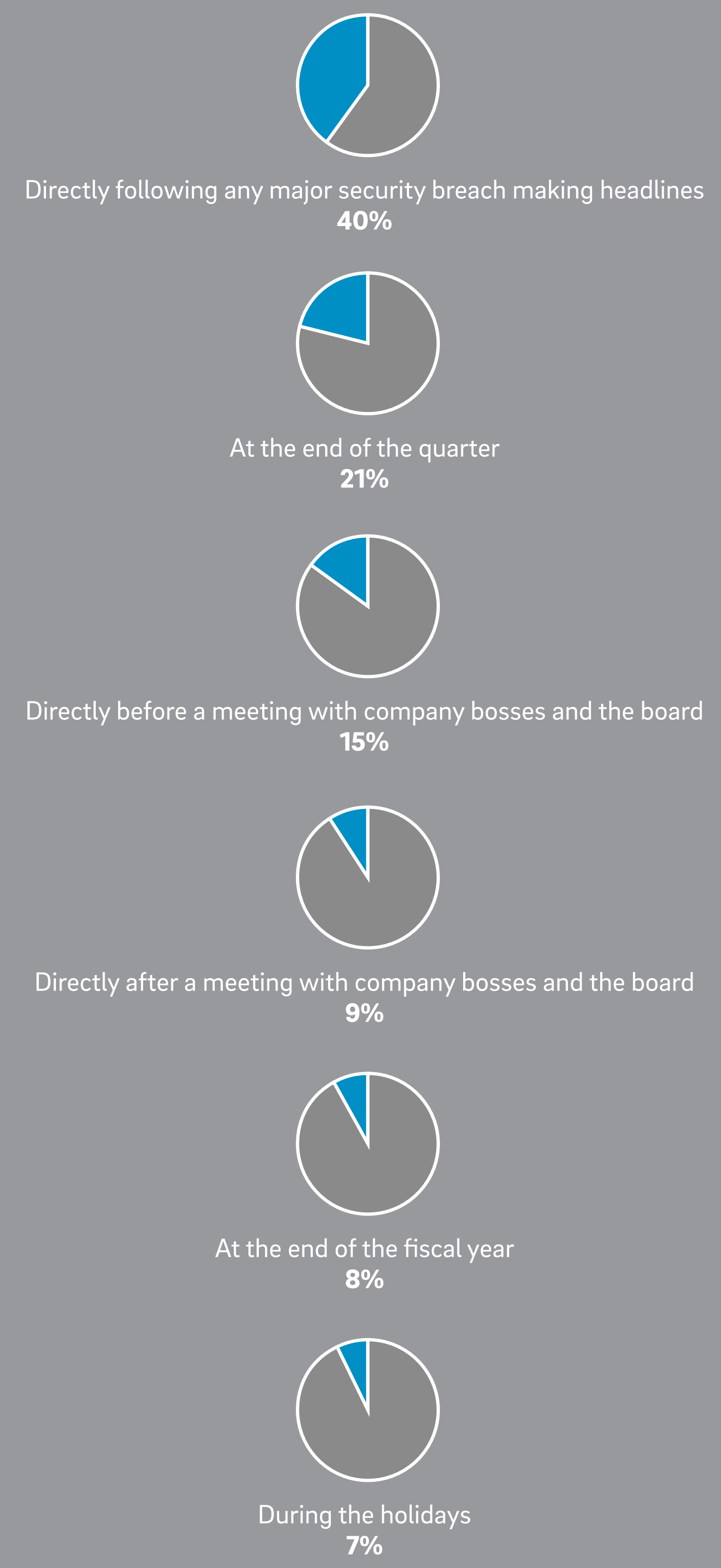


Forty percent of respondents feel the most pressure in relation to their security program directly following any major security breach making headlines. Roughly half as many (21%) experience the most strain at the end of the quarter, while for 15% it comes directly before a meeting with company bosses and the board. Another 9% admit the most pressure comes after the board meeting, while 8% acknowledge the greatest pressures at the end of the fiscal year and 7% say during the holidays.

Personal Pressures by Country

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Directly following any major security breach making headlines	39%	▲	40%	45%	32%	30%	32%	38%	57%
At the end of the quarter	11%	▲	21%	20%	31%	27%	24%	16%	15%
Directly before a meeting with company bosses and the board	17%	▼	15%	15%	11%	17%	19%	19%	11%
Directly after a meeting with company bosses and the board	23%	▼	9%	9%	12%	10%	8%	13%	4%
At the end of the fiscal year	5%	▲	8%	7%	9%	9%	9%	13%	4%
During the holidays	5%	▲	7%	5%	7%	8%	9%	3%	10%

When do you feel the most pressure in relation to your security program?



Operational Pressures

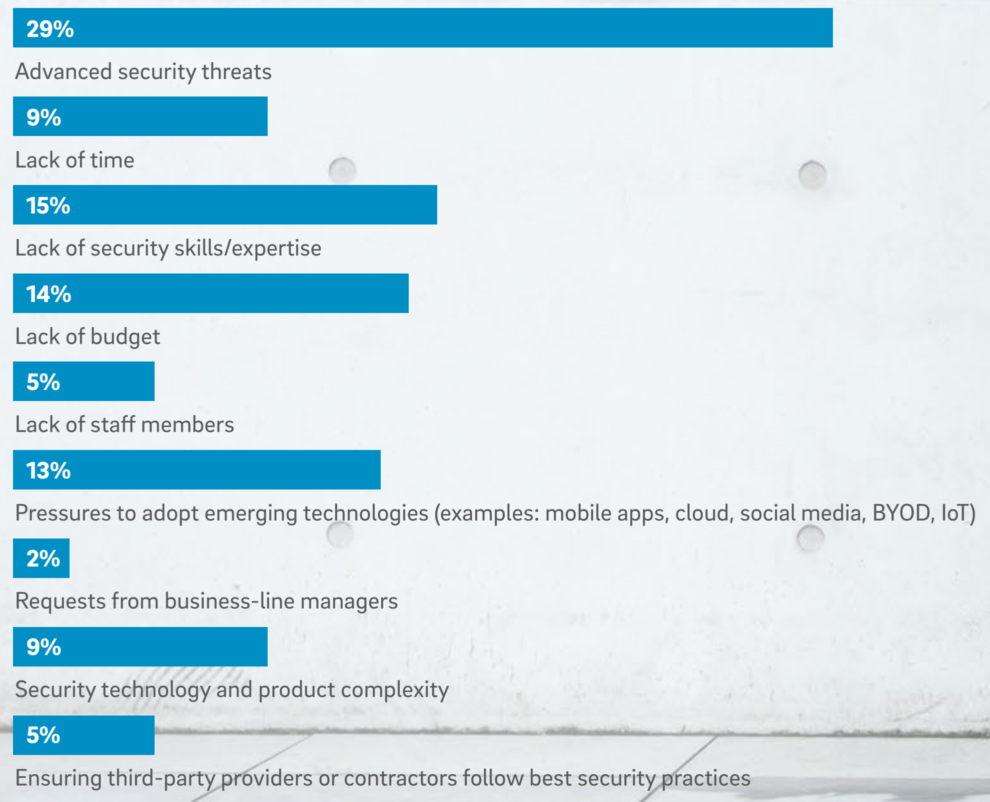
Nearly all workers, no matter their profession, must withstand pressures born out self-pride and the demands of their superiors. But few face as merciless a collection of operational pressures as IT and security professionals.

And above all else – like a cybercrime kingpin ruling over his sprawling syndicate – sits advanced security threats, which for the second year in a row outpaces of all the other operational pressures that respondents face in relation to their security program.

Twenty-nine percent of respondents rank advanced security threats as their top operational pressure, with the highest proportion of the pool coming from Japan and the United States. While the next-closest option on the list – shortage of security skills and expertise – only earns 15% of the top votes, this operational pressure has steadily risen each year and drew especially high marks in Japan and Singapore.

Shortage of skills and expertise remains slightly ahead of lack of budget (14%) and adoption of emerging technologies (13%) to claim second place for the first time. Emerging technology adoption - including cloud, social media and IoT - took a noticeable dip in this year's report compared to last year, when 22% of respondents classified it as their top operational pressure. Rounding out this year's list are security technology and product complexity (9%), lack of time (also 9%), lack of staff members (5%), ensuring third-party contractors follow best practices (also 5%) and requests from business-line managers (2%).

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

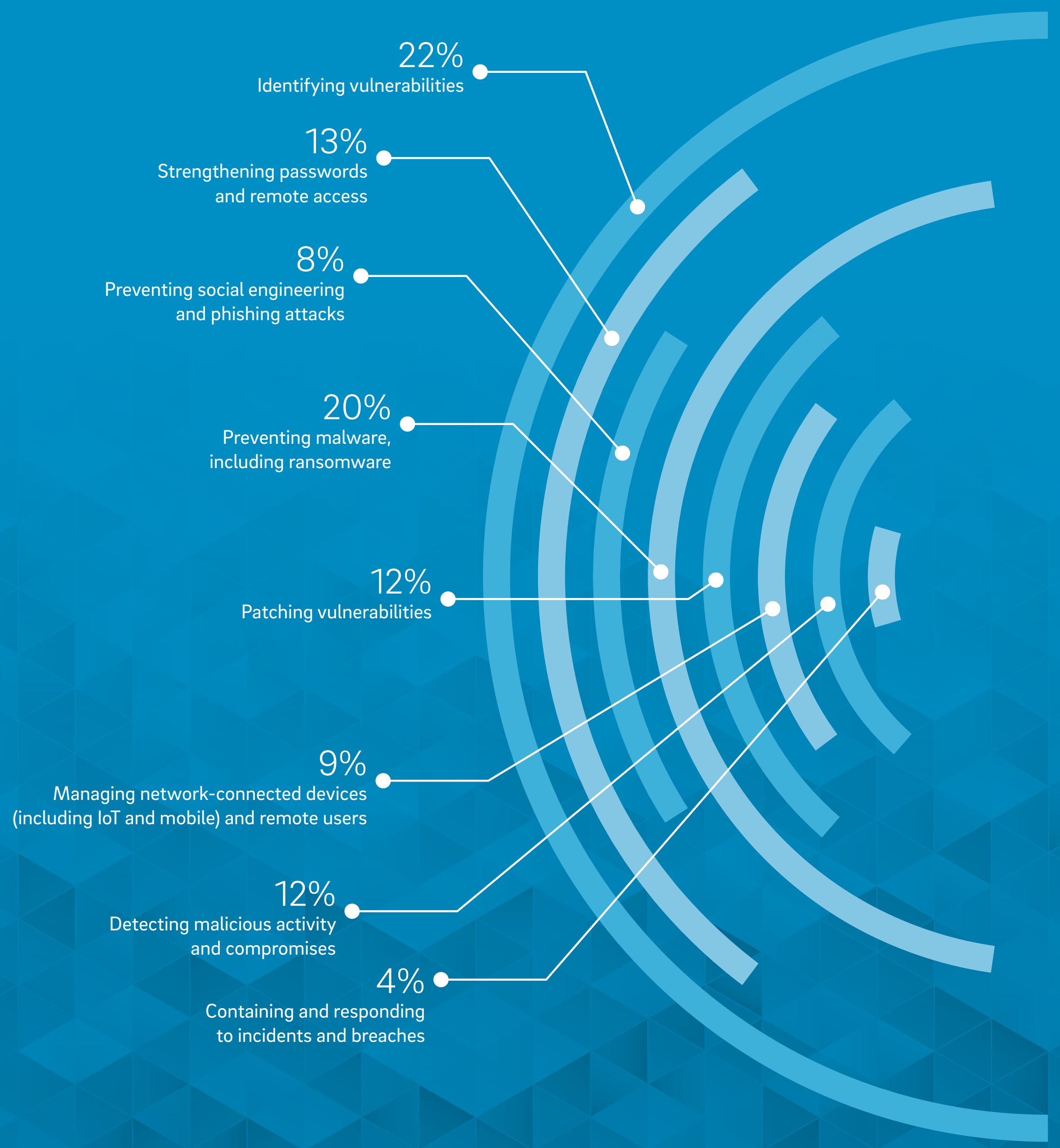


Operational Pressures by Country

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Advanced security threats	**24%**	▲	**29%**	33%	24%	25%	21%	25%	41%
Lack of security skills/ expertise	**14%**	▲	**15%**	11%	17%	9%	13%	24%	21%
Lack of budget	**12%**	▲	**14%**	12%	13%	20%	16%	16%	14%
Adoption of emerging technologies (examples: mobile apps, cloud, social media, BYOD, IoT)	**25%**	▼	**13%**	13%	15%	11%	17%	14%	6%
Lack of time	**6%**	▲	**9%**	8%	10%	13%	14%	4%	7%
Security technology and product complexity	**11%**	▼	**9%**	10%	13%	11%	7%	9%	4%
Lack of staff members	**5%**	=	**5%**	5%	4%	4%	6%	6%	7%
Ensuring third-party providers or contractors follow best security practices	**6%**	▼	**5%**	6%	4%	8%	6%	2%	2%
Requests from business-line managers	**6%**	▼	**2%**	2%	3%	1%	2%	2%	1%

Security Threats & Responsibilities

Which security tasks are you facing the most pressure to address?



As IT environments expand across Security DNA™ (databases, networks and applications) – and the traditional perimeter erodes amid a rapid influx of mobile devices, IoT and remote workers – the exploits of cybercriminals have flourished. And wouldn't you know it? Of the major security responsibilities respondents must confront, identifying vulnerabilities has delivered the most pressure (22%).

A close second is preventing malware, which is the most pressure-filled security responsibility for one-fifth of respondents, a stat that is up six percentage points year over year. Next comes strengthening passwords and remote access (13%), a responsibility that, when failed on, contributes to a disproportionately large share of compromises.[1]

Meanwhile, 12% respondents face the most pressure detecting malicious activity and compromises, which is surprisingly down from 19% in last year's report. Rounding out the list is patching vulnerabilities (also 12%), managing network-connected devices and remote users (9%), preventing social engineering and phishing attacks (8%), and containing and responding to incidents (4%).

Taken as a whole, the results seem to point to a gradual growth in security hygiene and maturity among organizations, from basic prevention-focused blocking and tackling efforts to now more proactive vulnerability and threat identification. Over the next several years, it would not be surprising to see companies advance their programs even further, to more advanced detection and response. Yet sometimes, sadly, it takes a breach to get them to take steps forward.

Security Threats & Responsibilities by Country

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Identifying vulnerabilities	**21%**	▲	**22%**	26%	18%	25%	19%	20%	16%
Preventing malware, including ransomware	**14%**	▲	**20%**	18%	23%	19%	24%	24%	14%
Strengthening passwords and remote access	**12%**	▲	**13%**	14%	16%	11%	12%	8%	15%
Patching vulnerabilities	**8%**	▲	**12%**	10%	11%	10%	8%	12%	22%
Detecting malicious activity and compromises	**19%**	▼	**12%**	12%	12%	11%	9%	16%	15%
Managing network-connected devices (including IoT and mobile) and remote users	**10%**	▼	**9%**	9%	11%	10%	11%	9%	9%
Preventing social engineering and phishing attacks	**12%**	▼	**8%**	7%	8%	11%	12%	10%	6%
Containing and responding to incidents and breaches	**4%**	=	**4%**	3%	4%	5%	6%	3%	5%

[1] "2016 Trustwave Global Security Report", Trustwave, 2016

Cyberattack & Data Breach Worrying Outcomes

Even for those with great thresholds for frustration, 2016 was a trying year. And that extended to the world of security, where last year drew the dubious honor of having the most reported breaches ever in the United States.[2] Worldwide, one study placed the amount of exposed records in 2016 at a stunning 4.2 billion.[3]

Considering the continually advancing probability of succumbing to a successful cyberattack or data breach, many security practitioners have shifted their anxiety from the possibility of being compromised to what such an incident may look like not if – but when – it occurs.

Thirty percent of respondents rank customer data theft as the top worrying outcome of a cyberattack or data breach. That number dropped 13 percentage points from last year's report, but the fall is mostly due to the introduction of a new option in the survey question this year – "data or system access restricted due to ransomware" – which is the most worrying outcome of an attack or breach for 18% of respondents. In the United States, 21% of respondents view ransomware as their most unsettling post-incident consequence.

4.2
BILLION
amount of exposed records in 2016[3]

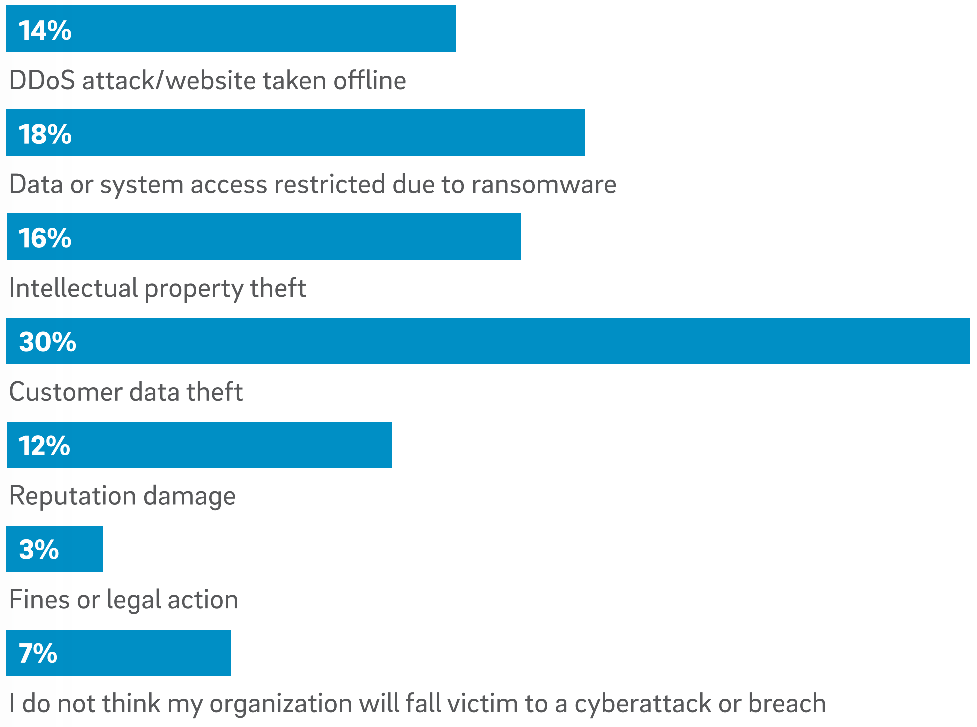
Concerns over ransomware even outpace intellectual property theft, which was the most troubling attack or breach outcome for 16% of respondents. Rounding out the list is a DDoS attack/website being taken offline (14%), reputation damage (12%), and fines or legal action (3%).

Seven percent of respondents do not believe their organization will fall victim to an attack or breach, which surprisingly has risen for the past three years, albeit only three percentage points overall. This trend contradicts, however, a more telling finding which asks respondents whether they feel safe from security threats – 65% report they do, whereas 35% do not. The number of respondents who feel protected plummeted nine percentage points from last year, an indicator of how prolific the threat landscape (and the inability to defend within it) has become. Concerns over one's ability to stave off threats is most pronounced in the U.K. and Singapore. Most notably, in Japan, a whopping 91% of respondents do not feel safe from threats, the most lopsided result in this report.

Meanwhile, 35% of respondents confess their organization has experienced a data breach, compared to 61% who say their business has not been breached, and 4% who are unsure. While the overall number of respondents who report having been breached declined year over year, it rose two percentage points in the United States.

[2] Identity Theft Resource Center, "ITRC Data Breach Report", 2016
[3] Risk Based Security, "Year End Data Branch QuickView Report", 2016

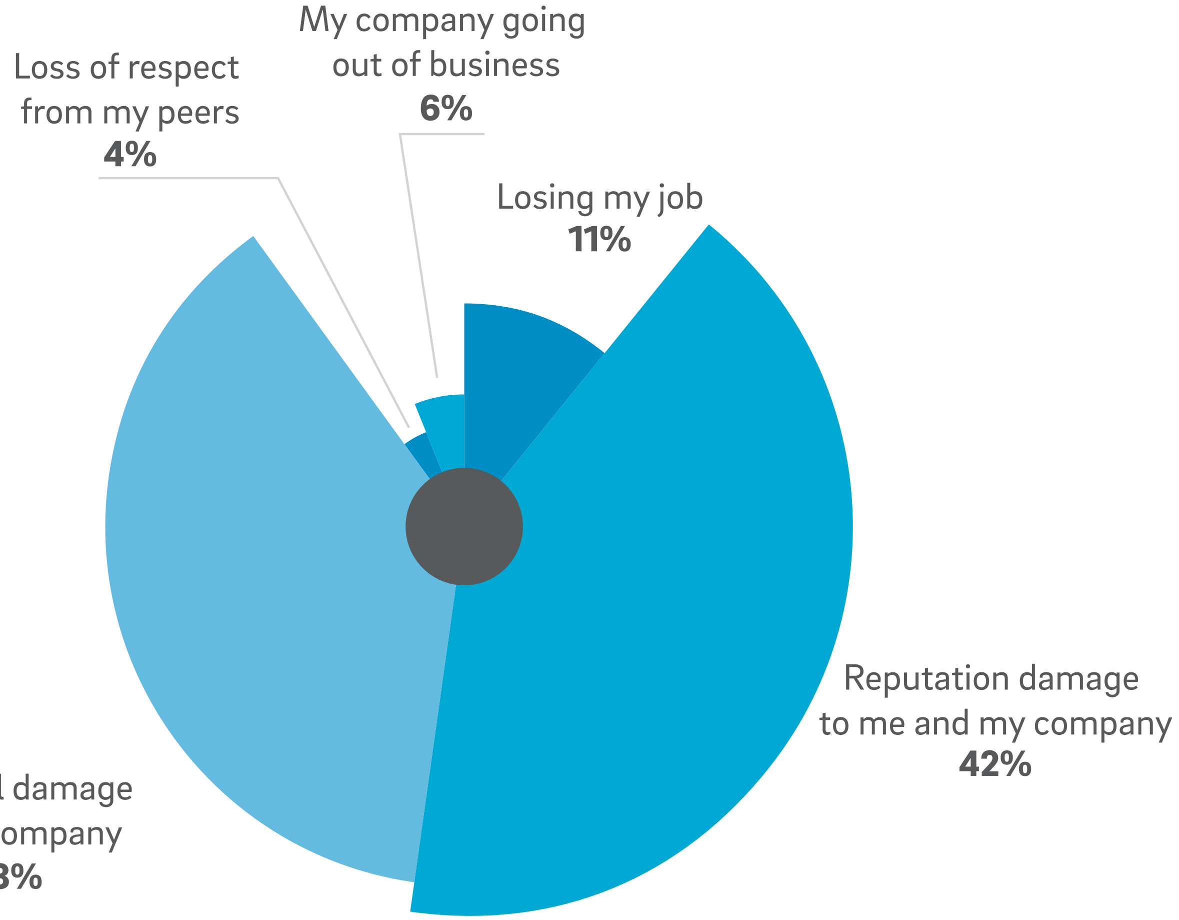
What outcome worries you most about cyberattacks and data breaches?



	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Customer data theft	43%	▼	30%	28%	35%	36%	20%	27%	41%
Data or system access restricted due to ransomware	N/A		18%	21%	15%	15%	20%	18%	12%
Intellectual property theft	22%	▼	16%	13%	15%	17%	18%	23%	12%
DDoS attack/website taken offline	13%	▲	14%	18%	10%	13%	14%	9%	16%
Reputation damage	13%	▼	12%	11%	16%	9%	14%	14%	15%
I do not think my organization will fall victim to a cyberattack or breach	5%	▲	7%	6%	7%	9%	13%	5%	3%
Fines or legal action	4%	▼	3%	3%	3%	3%	3%	6%	3%

Cyberattack & Data Breach Repercussions

What repercussion do you fear most if your organization is breached?



In the previous section, we examined the worries that result from the possibility of a cyberattack or breach. In this section, we ask respondents to consider the most perceptible repercussions they and their organization would experience following an incident, specifically which ones they fear the most.

Reputation damage (42%) and financial damage (38%) easily outstrip the others, with job loss (11%) holding its tertiary standing for another year – an indication that IT and security pros remain distressed by the possibility of being fired following a major incident. Going out of business, an extreme type of fallout but one which has happened in the past to breached organizations, is the fourth-largest potential repercussion (6%) with loss of peer respect (4%) rounding out the list.

Cyberattack and Breach Repercussions by Country

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Reputation damage to me and my company	43%	▼	42%	37%	47%	45%	36%	48%	48%
Financial damage to my company	37%	▲	38%	39%	36%	39%	39%	36%	36%
Losing my job	11%	=	11%	14%	10%	5%	12%	12%	6%
My company going out of business	5%	▲	6%	6%	5%	5%	10%	4%	9%
Loss of respect from my peers	4%	=	4%	4%	3%	7%	4%	2%	3%

Internal VS External Threats

49%

51%

Because data breaches that typically draw headlines are ones carried out by outside hackers, the average computer user would likely assume that external adversaries pose a far graver threat to the security of a business than an internal employee or contractor. But IT and security professionals are less extreme in this viewpoint, given what they know about all of the data under their watch – and who has access to it.

In the age-old debate of who poses the greater risk – insiders or outsiders – both earn prominent placing, according to respondents. External intruders are often well-financed, professional, resourceful and committed to finding weaknesses so they can become threats on the inside. On the other hand, insiders are already in – in many cases having approved and privileged access to sensitive data, knowing how it is secured and flying under the radar because it is difficult to determine whether their actions are illegitimate. (The two subsets of the insider threat are either rogue and vengeful, or negligent and accidental.)

Respondents are nearly evenly split on who they are more pressured to protect against, with 51% citing external threats (a drop of 7% from last year) and 49% naming internal threats. Of the latter, 27% are most bothered by non-malicious individuals who may commit unintended and naïve security policy violations, while 22% are more worried about malicious individuals, typically motivated by greed, frustration or basic fraud to steal data and misuse or destroy systems. Research has shown that historically organizations have chosen to underinvest in countering the deliberate insider threat and have avoided seriously addressing it[4] – so it is no surprise this threat source remains least pressure-inducing of the three.

Which type of threat pressures you the most?

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
External threats (malicious hackers, data-stealing malware, etc.)	58%	▼	51%	49%	55%	51%	48%	55%	56%
Internal threats (employee accidents, non-malicious mishaps, etc.)	24%	▲	27%	32%	23%	25%	26%	19%	29%
Internal threats (employee malfeasance, deliberate leakage of data, etc.)	18%	▲	22%	19%	22%	24%	27%	27%	16%

[4] Chuvakin, Anton, "Threats Inside vs Insider Threats.", Gartner.com, 2016

Riskiest Insider Threats

For a second year in a row, the list of riskiest insider threats went unchanged. Unauthorized file transfers (29%) rank first among respondents, with installation of unauthorized software or malware coming in second (21%). The latter references a common outcome of phishing attacks, which remains among the biggest security threats facing organizations and the most common way cybercriminals gain an initial foothold in companies.[5]

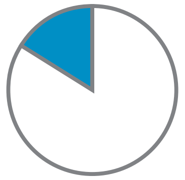
The next riskiest insider threat is access and privilege modification/escalation (17%) – which speaks to deliberate insider maliciousness more than any of the other survey options in this section. That is followed by weak passwords (16%), notably up five percentage points this year. Insecure and exploitable passwords are a common way hackers breach systems and laterally advance through the network, so one can expect them to continue to draw alarm from respondents. Rounding out the list of riskiest insider threats is failure to install security and application updates (10%) and general lack of security training (7%).

By country, unauthorized file transfers saw the largest delta, with 36% of U.K. respondents citing it as the insider activity they feel the most pressure to defend against compared to just 19% in Japan. Respondents from the Japan say access and privilege modification/escalation is their largest insider concern.

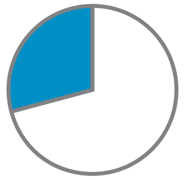
[5] Verizon, "Data Breach Investigation Report", 2016

Which type of threat pressures you the most?

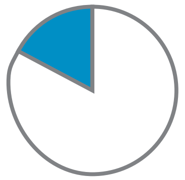
	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Unauthorized file transfers, such as via email or cloud storage services	**31%**	▼	**29%**	29%	36%	31%	24%	34%	19%
Installation of unauthorized software or malware	**24%**	▼	**21%**	24%	18%	22%	22%	19%	19%
Access and privilege modification or escalation	**18%**	▼	**17%**	14%	16%	19%	22%	16%	23%
Weak passwords	**11%**	▲	**16%**	18%	15%	18%	18%	12%	12%
Lack of installation of security updates and application updates	**9%**	▲	**10%**	11%	9%	4%	9%	12%	14%
General lack of security training	**7%**	=	**7%**	5%	7%	8%	7%	8%	15%



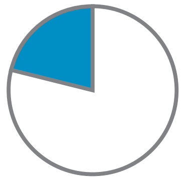
Weak passwords
16%



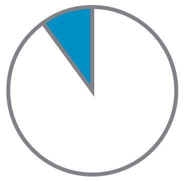
Unauthorized file transfers, such as via email or cloud storage services
29%



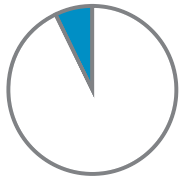
Access and privilege modification or escalation
17%



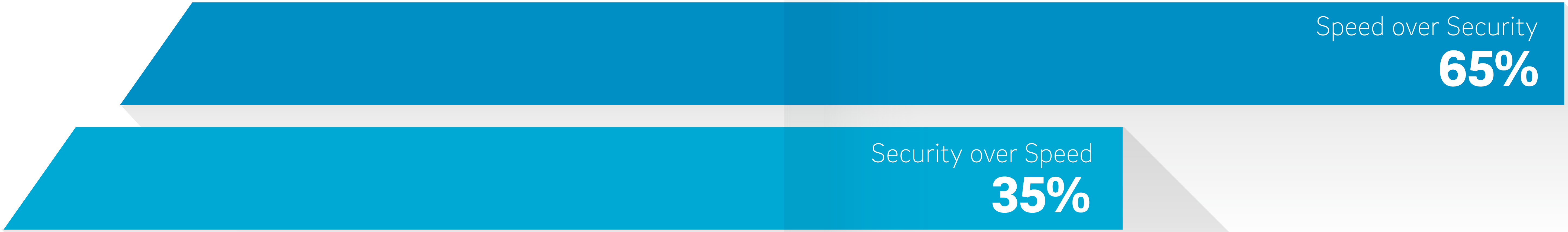
Installation of unauthorized software or malware
21%



Lack of installation of security updates and application updates
10%



General lack of security training
7%



Speed vs Security

Despite the somber tone of this report, there are bright spots. After all, optimism and success help keep us going. For instance, over the past several years, one of the most commonly quoted statistics of this report has been the high frequency by which practitioners are forced to roll out IT projects before they are security ready. But this year we learn that this specific pressure has finally slowed down somewhat.

Only 65% of respondents feel pressure to roll out IT projects before they have undergone the necessary security checks and repairs, compared to 77% in the previous two versions of the report. This speaks to improved software and application secure development, as well as growing organization wide recognition that catching vulnerabilities early is far less costly than dealing with them later. On the flip side, 35% of respondents are not pressured to deploy new technology too quickly. However, improvement on this front only saw gradual gains in the United States and Singapore, where 71% and 74% of respondents, respectively, are still being pressured to push out IT projects in haste.

Throughout 2016, were you pressured to roll out IT projects despite your concerns the projects weren't ready due to security issues?

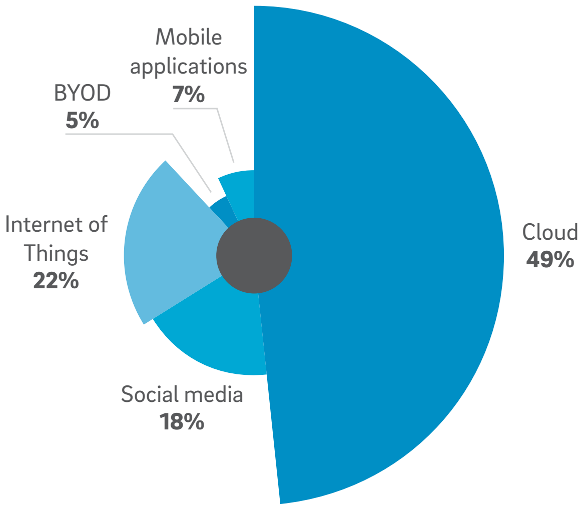
	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Yes - once or twice	**60%**	▼	**50%**	56%	41%	44%	47%	56%	43%
No	**23%**	▲	**35%**	29%	43%	41%	41%	26%	43%
Yes - frequently	**17%**	▼	**15%**	15%	16%	16%	13%	18%	14%

Emerging Technologies

Earlier in the report, we learned that, despite a decrease, adoption of emerging technologies still ranks in the top half of operational pressures. Drilling deeper into the data, the findings point to a fast-moving shakeup within this area of responsibility for IT and security professionals.

The cloud overwhelmingly presents the emerging technology respondents are under most pressure to adopt and deploy (49%), up five percentage points from last year's report. Companies continue to invest in the cloud, which can include infrastructure, platform and software-as-a-service implementations. The biggest growth area in cloud is now coming from enterprise-level businesses which plan to scale back their reliance on traditional, on-premises computing environments and transition to a hybrid model.[6] Larger size companies have traditionally been slower to migrate to off-premises workloads, but are increasingly drawn to the time-to-market, quality, productivity and cost benefits of the cloud.

Meanwhile, as businesses hurdle toward the mainstream adoption of connected devices, the Internet of Things (IoT) has taken over a clear second place (22%) of emerging technologies that respondents face the most pressure to adopt and deploy. But social media (18%) is coming on strong – rising eight percentage points year over year. One possible explanation for this are concerns over the phenomenon of "fake news" across social media sites, in addition to reported growing evidence of a rise in impersonator social media accounts that could be used to launch phishing attacks and conduct fraud.[7]



Name the top 'emerging technology' you feel the most pressure to use or deploy.

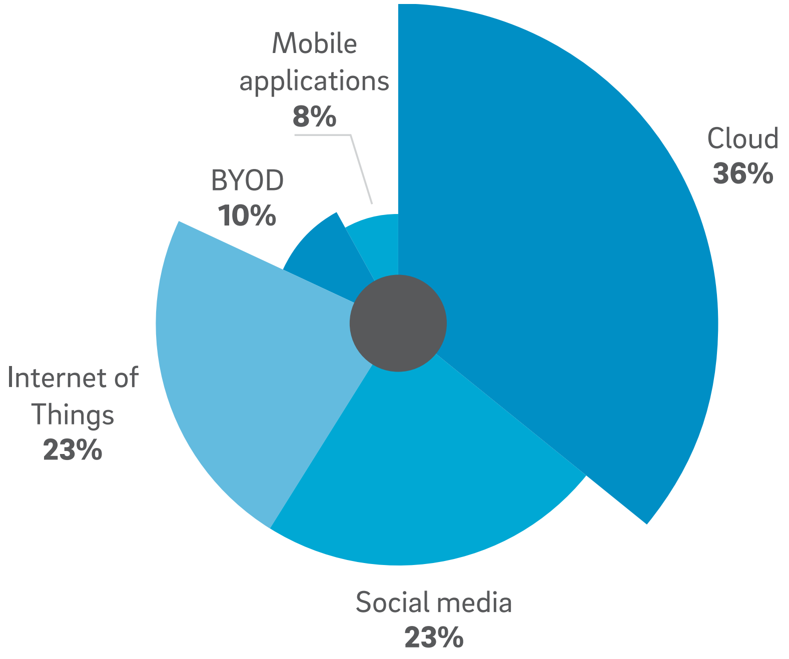
	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Cloud (includes public cloud and SaaS applications)	44%	▲	49%	52%	47%	52%	40%	46%	53%
Internet of Things (IoT)	17%	▲	22%	20%	23%	18%	23%	27%	25%
Social media	10%	▲	18%	20%	19%	18%	23%	16%	12%
Mobile applications	7%	=	7%	6%	7%	8%	8%	8%	6%
BYOD	16%	▼	5%	3%	6%	5%	8%	5%	5%

[6] McKinsey and Co., "McKinsey's ITaaS Cloud Survey", 2016
[7] ZeroFox, "Social Engineering in the Social Media Age", 2017

Next on the list comes mobile applications, which hold steady at 7% of respondents. Interestingly, bring-your-own-device (BYOD) has considerably backtracked, falling from the top pressure-breeding emerging technology for 16% of respondents to just 5% in this year's report. Based on the results, businesses appear to be doing a better job of balancing the risks and rewards of employee-owned devices permeating the workplace, whether it is through security solutions or more stringent and adhered-to policies and standards.

In terms of which emerging technology poses the greatest risk, the cloud reigns king (36%, up four percentage points). This means that despite increased adoption rates of the cloud, security and compliance concerns still abound. Next is social media and IoT (both 23%), followed by BYOD (10%) and mobile apps (8%).

Name the top 'emerging technology' you feel poses the greatest security risk to your organization.



	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Cloud (includes public cloud and SaaS applications)	32%	▲	36%	41%	30%	32%	31%	29%	40%
Social media	15%	▲	23%	23%	23%	25%	26%	24%	21%
Internet of Things (IoT)	19%	▲	23%	20%	23%	25%	23%	31%	19%
BYOD	19%	▼	10%	9%	16%	11%	13%	9%	10%
Mobile applications	10%	▼	8%	7%	9%	8%	8%	8%	11%

Features **VS** Resources

27% feel they do not have the proper resources to deploy the latest technologies

Businesses often want to acquire security solutions that will not only help them check off the compliance boxes, but also fulfill their desire to discover a "silver bullet" technology. The problem is that while such a product may contain the latest bells and whistles, it often neither lives up to expectations nor adds value to the business. In some cases, it ends up never being utilized and is exiled to the shelf, where it collects dust indefinitely. This is especially problematic when you consider the large number of disparate point solutions that organizations tend to purchase.

64% are pressured to select security technologies with the latest features

Thankfully companies appear to be scaling back their penchant for software and hardware that they may not necessarily have the internal staff and skills to properly install, deploy and manage. The pressure to select security technologies containing "all of the latest features" dropped from 74% in last year's report to 64% this year, the lowest in the four years of this report. Still, that means just under two-thirds of respondents are still feeling pressure to implement these technologies despite 27% of them believing they lack the proper in-house resources to effectively use them. That number, however, did drop from 31% in last year's report.

Investigating the country-by-country data, the United States carries the torch in terms of respondents who feel pressure to choose the latest security technologies (70%), but contained the greatest number of respondents who believe their organization has the proper resources to use such technologies (81%). Japanese respondents, meanwhile, have nearly an even split on their confidence to use these technologies.

Are you pressured to select/purchase security technologies that contain all of the latest features?

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Yes	**74%**	▼	**64%**	70%	61%	58%	56%	62%	63%
No	**26%**	▲	**36%**	30%	39%	42%	45%	39%	38%

Do you feel you have the proper resources to deploy/maintain security technologies that contain all of the latest features?

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Yes	**69%**	▲	**73%**	81%	75%	76%	71%	66%	51%
No	**31%**	▼	**27%**	19%	26%	24%	30%	35%	49%

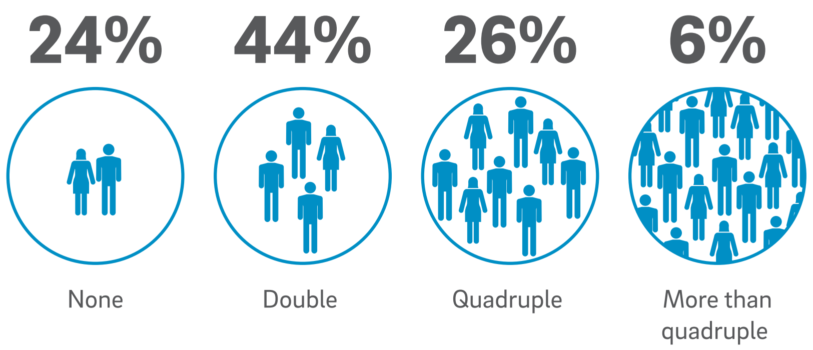
Staffing Levels

We have already discovered that a lack of personnel exerts far less pressure on respondents than operating with a scarcity of security skills at their disposal, and the dichotomy is only further affirmed in this section.

Respondents were asked to reveal their ideal staffing sizes and nearly one-quarter (24%) admit they are already at the optimal level – an 11-point hike from last year's report. One-third of Australian respondents are operating at the perfect level.

In terms of respondents who seek headcount expansion, 44% want to double their size (down eight points from the previous year) and 29% desire to quadruple it. Meanwhile, 6% thirst for a staff increase of more than quadruple the current size.

How much more does your IT team need to grow?



How much bigger do you think your IT security team should be to reduce the pressures on your team and to more effectively do its job?

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Double (2 times the current size)	52%	▼	44%	45%	45%	45%	36%	50%	46%
Quadruple (4 times the current size)	29%	▼	26%	29%	28%	24%	28%	23%	20%
None - current size is ideal	13%	▲	24%	20%	25%	26%	33%	21%	26%
More than quadruple the current size	6%	=	6%	6%	4%	6%	5%	7%	9%

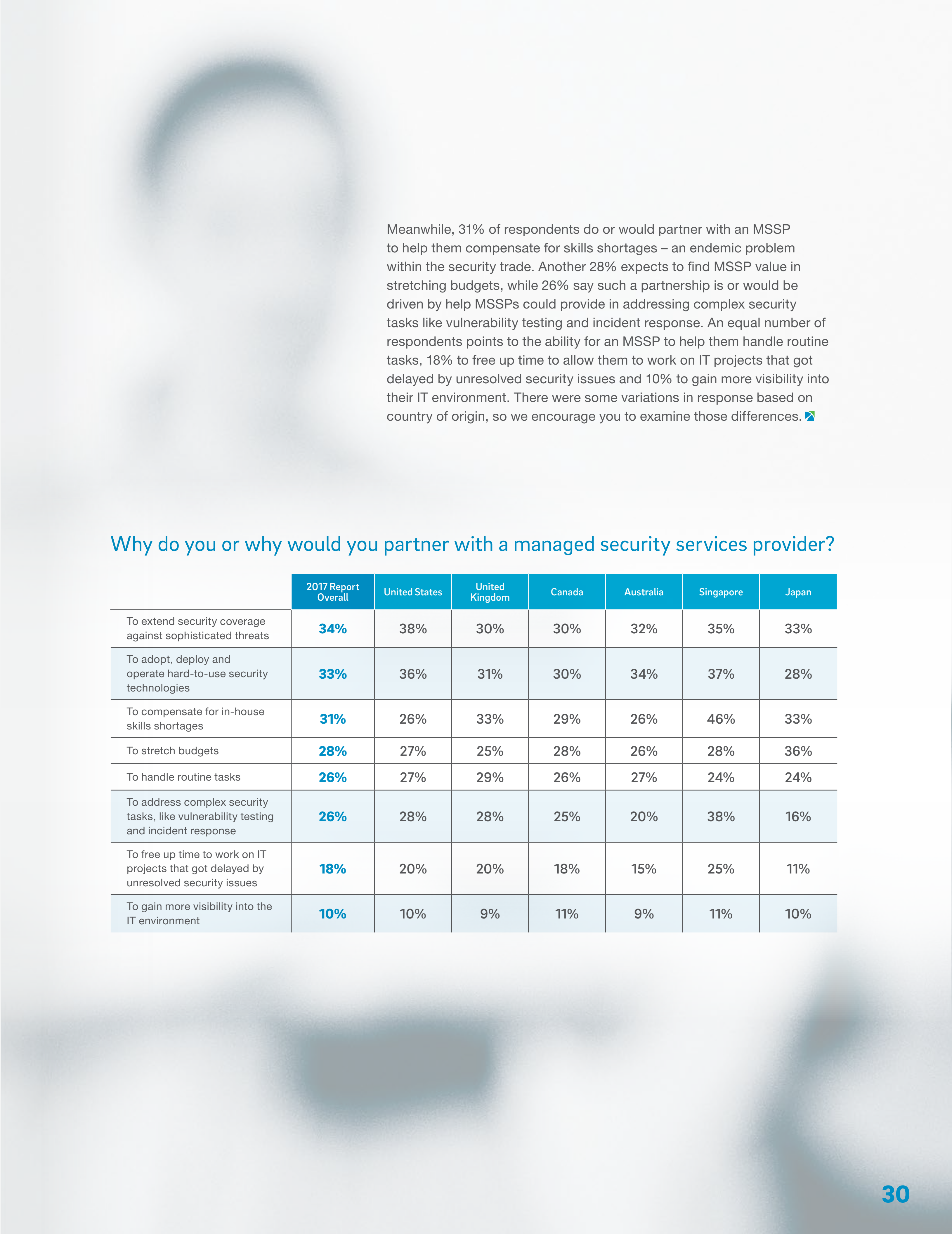
Internal Resource Pressures

The managed security services market is projected to be worth $34 billion by 2021.[8] As our report has so far documented, IT and security professionals must endure mounting pressures to address the complexity that cybercrime defense, data protection and risk reduction present to internal teams. Thus, they are looking outside their walls for help alleviating their sources of strain, while amplifying their security postures beyond what their core competencies and existing resources can currently offer.

But exactly what have they or what would they hope to get out a relationship with a managed security services provider (MSSP)? In our only survey question which allowed respondents to choose multiple options a – functionality we added because organizations typically turn to MSSPs for multiple reasons – the most-selected response (34%) is the capability to extend security coverage against sophisticated threats. Thirty-three percent say the decision is or would be to help them adopt, deploy and operate hard-to-use security technologies (which speaks to the “shelfware” problem we discussed earlier in this report).

$34 billion

managed security services market by 2021[7]



Meanwhile, 31% of respondents do or would partner with an MSSP to help them compensate for skills shortages – an endemic problem within the security trade. Another 28% expects to find MSSP value in stretching budgets, while 26% say such a partnership is or would be driven by help MSSPs could provide in addressing complex security tasks like vulnerability testing and incident response. An equal number of respondents points to the ability for an MSSP to help them handle routine tasks, 18% to free up time to allow them to work on IT projects that got delayed by unresolved security issues and 10% to gain more visibility into their IT environment. There were some variations in response based on country of origin, so we encourage you to examine those differences.

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

	2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
To extend security coverage against sophisticated threats	**34%**	38%	30%	30%	32%	35%	33%
To adopt, deploy and operate hard-to-use security technologies	**33%**	36%	31%	30%	34%	37%	28%
To compensate for in-house skills shortages	**31%**	26%	33%	29%	26%	46%	33%
To stretch budgets	**28%**	27%	25%	28%	26%	28%	36%
To handle routine tasks	**26%**	27%	29%	26%	27%	24%	24%
To address complex security tasks, like vulnerability testing and incident response	**26%**	28%	28%	25%	20%	38%	16%
To free up time to work on IT projects that got delayed by unresolved security issues	**18%**	20%	20%	18%	15%	25%	11%
To gain more visibility into the IT environment	**10%**	10%	9%	11%	9%	11%	10%

[8] MarketsAndMarkets, “Managed Security Service Market by Services, Deployment Type (Hosted or Cloud, Hybrid Cloud, and On-Premises), Organization Size (SMES and Enterprises), Vertical, and Region - Global Forecast to 2021”, 2017

In-House **VS** Managed Services

For the reasons suggested in the previous section, partnering with a managed security services provider (MSSP) has become almost an imperative for organizations strained by internal resource struggles and forced to cope with worries over data theft and the proliferation of mobile devices entering the workplace, among other threats.

And statistics reflect this fundamental shift is underway. For a second consecutive year, the number of respondents reporting that their security is installed and maintained entirely by their in-house IT staff and security teams dropped – this year to 67%. Twenty-six percent of respondent organizations are involved in a partnership between in-house teams and an MSSP, and in Singapore alone that number rises to 36%. Another 5% delegate the entirety of their security solution set to an MSSP, and 2% answered “other.”

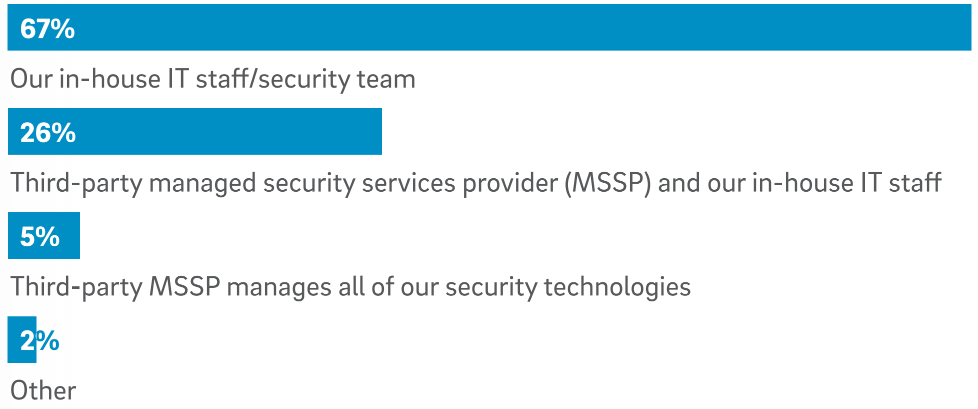
As to their plans to partner with an MSSP, 43% already do, which rose from 39% in last year’s report. That stat is considerably more pronounced in the United States, where 53% of respondents already use managed security services – a 14% leap from last year. Another 40% overall plan to partner with an MSSP in the future, with 17% indicating such an arrangement appears unlikely.

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

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Likely - we already do	**39%**	▲	**43%**	53%	36%	39%	43%	38%	30%
Likely - we plan to in the future	**47%**	▼	**40%**	36%	42%	41%	28%	50%	51%
Not likely	**14%**	▲	**17%**	11%	23%	21%	29%	13%	19%

Who is currently responsible for installing and maintaining your security solutions?

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Our in-house IT staff/security team	**69%**	▼	**67%**	73%	70%	66%	71%	50%	63%
Third-party managed security services provider (MSSP) and our in-house IT staff	**26%**	=	**26%**	23%	27%	31%	21%	36%	25%
Third-party MSSP manages all of our security technologies	**4%**	▲	**5%**	3%	4%	3%	5%	12%	5%
Other	**1%**	▲	**2%**	1%	0%	1%	4%	3%	8%



83% plan to or already partner with a managed security provider

2017 Wish List

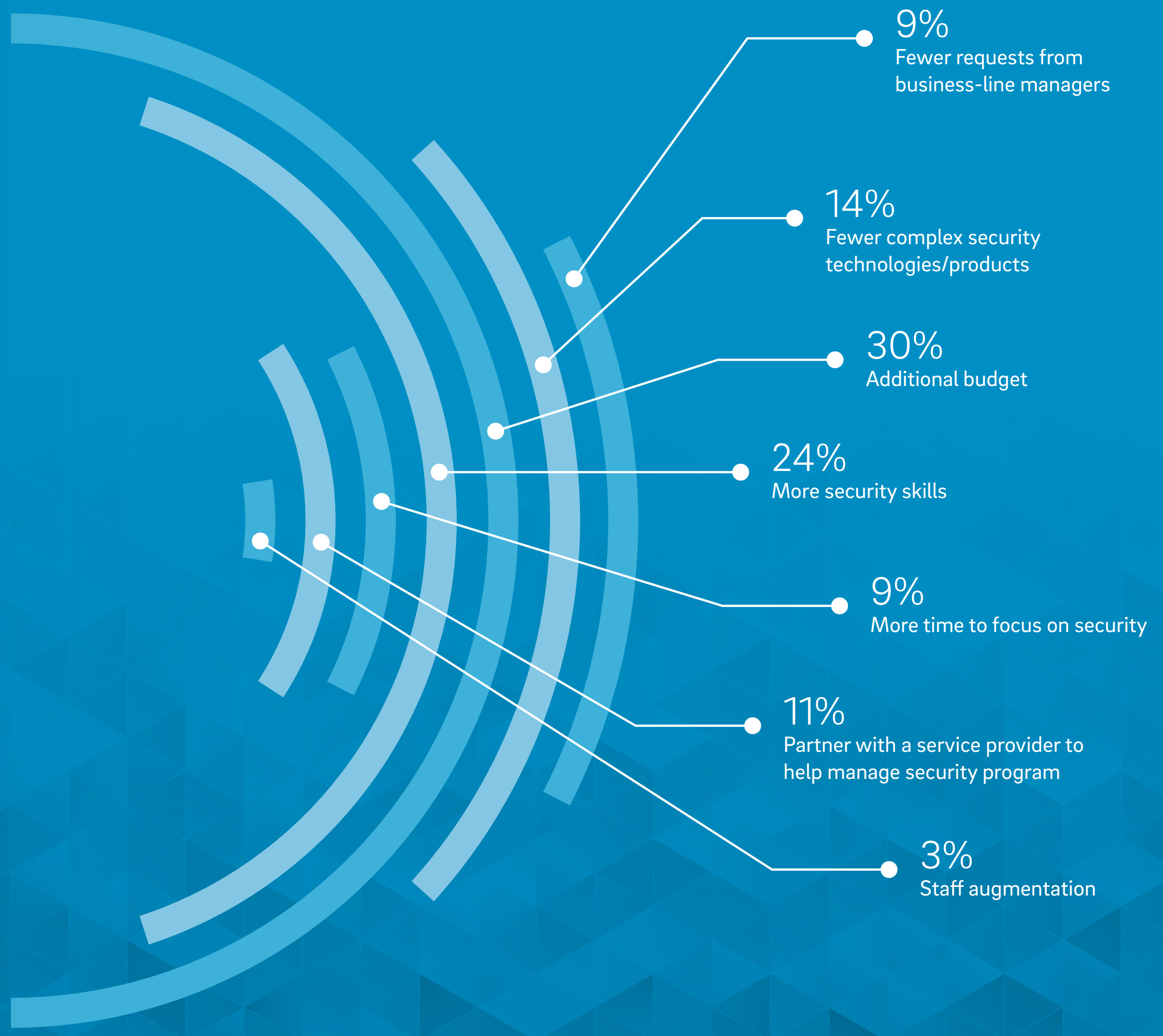
We all secretly long for a personal genie, and for IT and security professionals, it may sometimes feel like magic is required to fulfill your ambitions and objectives. But even if genies do not exist, you are free to wish and set intentions. Thirty percent of respondents say obtaining more budget tops their list of 2017 desires – topping the rankings for the fourth year in a row. Coming in second position again on the wish list is the yearning for more security skills (24%) among staff members.

Another 14% are channeling the universe for fewer complex technologies and products, followed by the aspiration to partner with a service provider to help manage security (11%) – which, based on the previous two sections in this report, took an unsurprising jump of three percentage points from last year's report. Rounding out the wish list is getting more time to focus on security (9%) and fewer requests from business-line managers (also 9%). Staff augmentation (3%) again brought up the rear, which confirms that respondents would much prefer to grow their skills versus merely throwing bodies at the pressures they face.

Name the top item on your wish list for 2017 to help alleviate the pressures you face related to IT security.

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Additional budget	**33%**	▼	**30%**	23%	34%	43%	31%	36%	29%
More security skills	**20%**	▲	**24%**	26%	25%	21%	21%	22%	30%
Fewer complex security technologies/products	**15%**	▼	**14%**	14%	16%	12%	17%	13%	15%
Partner with a service provider to help manage security program	**8%**	▲	**11%**	13%	8%	11%	10%	13%	7%
Fewer requests from business-line managers	**7%**	▲	**9%**	12%	5%	6%	10%	5%	8%
More time to focus on security	**14%**	▼	**9%**	11%	11%	8%	8%	10%	7%
Staff augmentation	**3%**	=	**3%**	2%	3%	1%	6%	2%	5%

Top 7 wishes for 2017



Conclusion

If you were not yet aware of all of the diverse security pressures that confront and exasperate IT security decision makers and influencers, you certainly are now. And while they may seem overwhelming, your ability to tolerate and endure these mechanisms of force should not be considered unachievable. After all, pressures are not necessarily bad things – in fact, they are par for the course for those operating in a highly complex and fast-moving industry like information security. Having pressures is a promising sign that you care about your job and are not willing to accept an equation in which your adversaries hold the advantage.

Security pressures, however, do become problematic and destructive when they get the best of you. If you allow your thoughts to obsess on the negative – by losing sight of the present and what needs to be done now to instead stew over prior events or drown in fear over the future – pressures can easily morph into a mindset that is unmistakably corrosive.

That is why this year we wanted to not only leave you with practical advice that will help you fight cybercrime, protect data and reduce risk, but also recommendations that are more mindful and personal in scope in hopes you can apply more conscience thought to your day to day. Let us begin with the latter and then move over to more traditional security guidance.

Keep Things in Perspective

Because of the nature of the job – defending against attacks with varying motivations – you need be right 100 percent of the time. We all know this is not only impossible, but foolish to even consider trying to accomplish. Instead, the better approach is to work to mitigate security risk as best as possible by investing in what will have the largest impact, all with the recognition that mistakes will happen. You need to learn from them and try to avoid sweating the small stuff. Short-term results may not always fall your way, but if you are problem solving and decision making with the long term in mind, you will net the biggest and most strategic security wins for your organization.

Remain Optimistic

Few people work in an industry in which rarely a day goes by that one of your peers is not addressing some major incident that leaves their competence in question. Gone are the days when ensuring anti-virus updates and maintaining firewalls were your sole responsibilities. It is important to, as best you can, ignore the headlines and remember that things like threats, cyberattacks and board room lectures are all part of the job (as pressure-inducing as they may be).

Follow this Five-Point Framework

The U.S.-based National Institute of Standards and Technology offers a five-point security framework[9] that is an optimal starting point for increasing security maturity: identify, protect, detect, respond and recover. This may sound simple and not particularly ground-breaking, but you would be surprised how many organizations are failing to do some – or all – of it well. To help accomplish each, consider: 1) risk assessments to understand your environment; 2) web application firewalls and email and web security gateways to protect against infiltration; 3) regular security testing across your DNA (databases, networks and applications) to discover exposure points; 4) security monitoring and threat detection to uncover malicious activity as fast as possible; and 5) incident readiness and response to mitigate damage caused by a compromise and quickly get back to normal operations. But that is just the technology piece: You also need to have a testable plan in place to ensure your security program is meeting – and exceeding – expectations.

Get on the Offensive

The above framework offers a solid baseline, but you also should consider pushing the needle forward. While hacking back may not be advisable for all organizations, you still need to be aggressive and offensive. As a corollary to security monitoring, threat hunting involves the manual act of collecting and analyzing data. With the help of Big Data analytics and machine learning, trained and experienced analysis – like a gumshoe on a cold case – can comb through intelligence to look past automated alerts, filter out the noise and identify shady patterns, unauthorized access and malicious actions.

Establish Internal and External Allies

Security can no longer be considered a siloed discipline. You must seek and win support from both senior leadership and other departments if security is to become part of the company culture. Demonstrate for them the value of infosec to their parts of the business and customize the message for them. But while support is one thing, action is an entirely separate beast. Outside of your organization, consider turning to a managed security services provider, which can help powerfully compensate for and amplify areas of your security program that you find too complex or lack the adequate internal resources to personally address.

[9] NIST Cybersecurity Framework, https://www.us-cert.gov/ccubedvp/cybersecurity-framework

Trustwave®

trustwave.com