2015 Security Pressures Report

BASED ON A SURVEY COMMISSIONED BY TRUSTWAVE

Trustwave®

Smart security on demand

Table of Contents

Introduction

In science, pressure is defined as the continuous physical force exerted on the per-unit area of a surface. There is an official formula, in case you were wondering: Pressure equals force divided by area. We interact with pressure from the moment we stretch in the morning to the moment we set our heads down at night. It ranges from the mundane and routine, like poking at our smartphones or scratching an itch, to the irritable, such as trying to undo a nettlesome jar of peanut butter or wearily finish a workout.

In most cases, we apply pressure to something, complete the task and move on. Nearly all of the time, we don't consciously register we are even doing it. But pressure is not as forgettable when it is the cerebral kind. That is the type that confounds us, that enrages us, that spurs on sleepless nights, that sticks with us and that, figuratively and mentally, can feel like the weight of the world pushing down on us.

No matter the security maturity level at a given organization, the pressure is on.

Few white-collar professions face as much mounting pressure as the information security trade. It is a discipline that, due to the widely publicized data breach epidemic, has suddenly crept out from behind the shadows of the mysterious, isolated and technical — and into the public and business mainstream.

Recognizing this, Trustwave last year unveiled its inaugural edition of the Security Pressures Report to quantify, as best we could, the feeling of tension and hardship facing so many in the information security industry. Our goal was to measure the sources of strain in-house security pros face on a daily basis — from digital threats, to resource shortages, to emerging technologies, to executive demands, to breach fallout — then offer suggestions to mollify them. We have continued this important endeavor with the 2015 Security Pressures Report.

More than 1,000 IT security professionals in the United States, United Kingdom and Canada were polled this time, during an astonishingly active year for security incidents, intrusions and data loss. Their answers differ, of course, depending on how security and risk are perceived within their organizations — from those entities where passing an audit still reigns king to organizations where security is ingrained into the culture, leading to advanced threat modeling, real-time analysis and detection, and incident response.

But one thing is certain: No matter the security maturity level at a given organization, the pressure is on. There is no denying the obvious. Attackers are smart, determined, well-funded and have more data than ever before to target. The security skills gap remains frighteningly large for businesses looking to fill open positions. And organizations are especially exposed due to product complexity and a disintegrating perimeter brought on by an exploding market for consumer-owned devices and a rash of third-party contract agreements.

To make this year's report digestible and useful, we have again broken the common pressures into 13 individual sections — and have juxtaposed this year's results against last year's, as well broken out the results by country. And in some instances, where the findings were noteworthy, we delineate between small and medium-sized business respondents and those who work at enterprises.

So, fasten your seatbelts, and let's begin.

Key Findings

Here are some of the key findings from the 2015 Security Pressures Report:

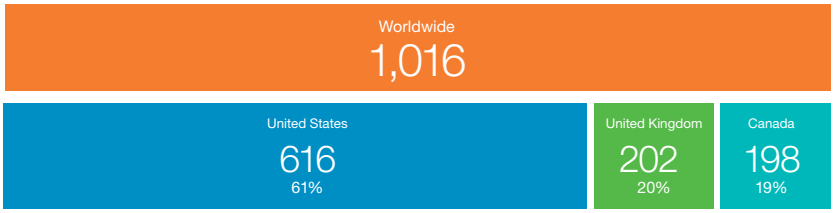
- **Pressure is on:** 54% of security pros felt more pressure to secure their organizations in 2014, and 57% of respondents expect to experience additional pressure to secure their organization in 2015.
- **Differing perspectives:** 64% of enterprise respondents foresee increasing pressure in 2015, compared to 48% at SMBs.
- **False sense of security:** 70% of overall respondents said they are safe from cyberattacks and data compromises.
- **Jumping the gun:** 77% of respondents were pressured to unveil IT projects that weren't security ready.
- **Breaking in:** 62% of respondents were most pressured by external threats, versus ones stemming internally.
- **Reaching out for help:** 78% of respondents said they are likely or plan to partner with a Managed Security Services Provider (MSSP) in the future.
- **"Emerging" concern:** Adoption of emerging technologies, such as the cloud and BYOD, overtook advanced security threats as the top operational pressure facing respondents.
- **Cloudy forecast:** Among emerging technologies, 47% of security pros were most pressured to use or deploy the cloud, up from 25% the previous year.
- **Corner-office commands:** 61% of respondents felt the most "people pressure" was exerted by their owners, board and C-level executives — up from 50% the previous year.
- **Password disconnect:** 9% of security pros cited weak passwords as the insider activity they felt most pressure to fend off, despite previous Trustwave research showing easy-to-crack passwords contributed to nearly one-third of all breaches.
- **Send in the reserves:** 84% of respondents said they wanted the size of their IT security team increased.
- **Fallout phobia:** 84% of respondents cited reputation or financial damage as their biggest fear if their organization is breached.

Methodology

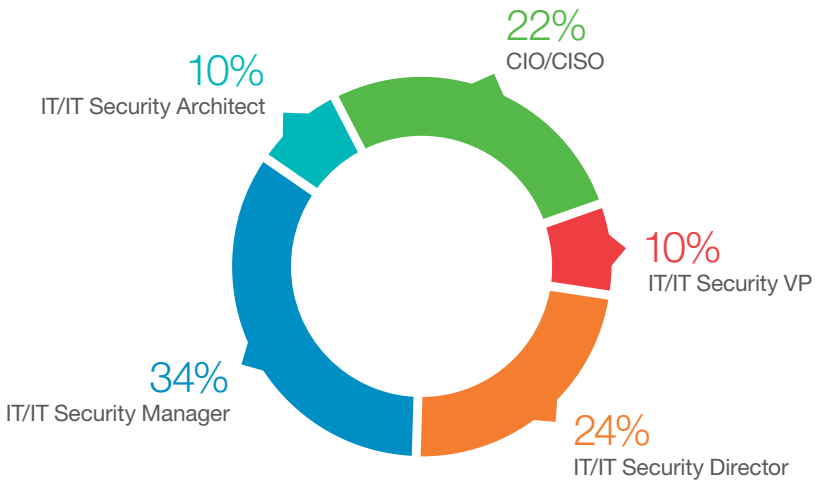
Trustwave commissioned a third-party research firm to survey 1,016 full-time information technology (IT) professionals who are security decision makers or security influencers within their organizations. The objective of the survey was to measure the variety of pressures they face regarding information security. Respondents consisted mainly of chief information officers (CIOs), chief information security officers (CISOs), IT/IT security directors and IT/IT security managers: 1,016 worldwide, which included 616 in the United States, 202 in the United Kingdom and 198 in Canada. More than half of the respondents (55%) work for enterprise businesses, those with 1,000 or more employees. The rest (45%) work for small to medium-sized businesses (SMBs), with less than 1,000 employees. Respondents work in a variety of sectors, with the most frequent being technology service providers (21%) and financial services/banking (17%). The survey was deployed through emails sent between December 2014 and January 2015. Survey results have a margin of error of +/- 2%.

Respondent Demographics

Location



Occupation



Findings

Overall Pressure

All signs point to turbulent times for digital gatekeepers, and our findings back this up. Overall pressures for security professionals increased from 2013 to 2014, and even more apprehension is expected in 2015. 54% of respondents experienced more pressure to secure their organizations in 2014 compared to 2013. 57% expect to experience more pressure to secure their organizations this year, 32% expect it to stay the same and 11% anticipate it to decline.

Security pros in the United States and the U.K. (55%) felt the largest increase in pressure in 2014, compared to respondents in Canada (50%). 62% of security pros in the U.K., 57% in the United States and 48% in Canada expect security pressures to increase in 2015. Just 3% of respondents in the U.K. expect pressures to drop this year, although U.S. respondents were a bit more optimistic, with 15% predicting a drop.

64% of enterprise respondents foresee rising pressure in 2015, compared to fewer than half (48%) at SMBs. Just under a quarter of security pros at enterprises (24%) expect pressures to stay the same, compared to 42% at SMBs.

Amount of Pressure Felt (Compared to Previous Year)

	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
Up	54%	=	54%	55%	55%	50%
Same	32%	^	34%	30%	37%	40%
Down	14%	v	12%	15%	8%	10%

Amount of Pressure Expected to Feel in Upcoming Year (Compared to Current Year)

	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
Up	58%	v	57%	57%	62%	48%
Same	30%	^	32%	28%	35%	44%
Down	12%	v	11%	15%	3%	8%

Cyberattack and Data Breach Worries

Not surprisingly, considering the sheer number of high-profile data breaches affecting businesses in 2014, fears about data loss worried security pros significantly more than reputation damage, website disruptions and fines and legal action.

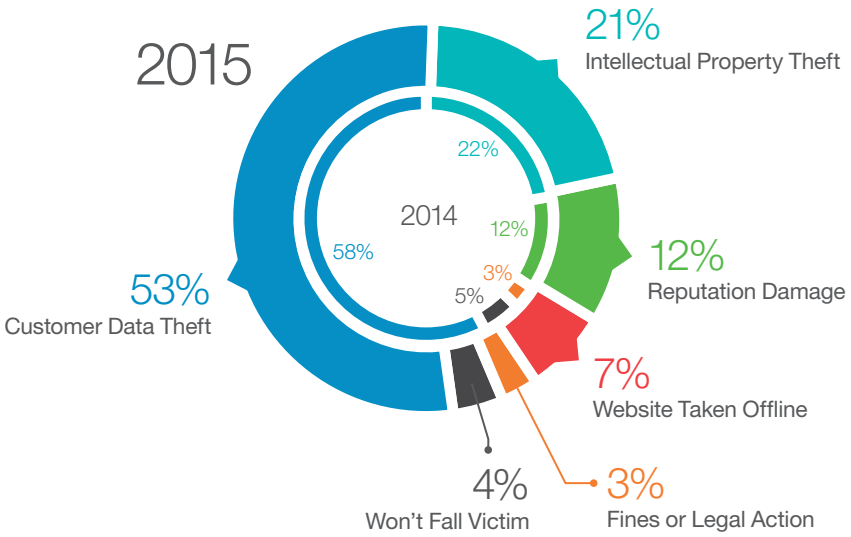
Startling, however, is that 70% of respondents believe their organization is safe from cyberattacks and data compromises, despite a recent Ponemon Institute study indicating that 43% of companies experienced a breach in the past year. The seemingly false sense of security is most pronounced in the U.K., where 80% of security pros believe their organization is safe from threats, versus 68% each in United States and Canada. More enterprise respondents (72%) than SMBs (68%) believe their organization is safe.

Meanwhile, 53% of respondents said customer data theft worried them the most, followed by intellectual property theft at 21%, reputation damage at 12%, website disruption at 7%, and fines or legal action at 2%.

Feeling safe from attacks is one thing — but it doesn't mean a compromise won't happen. Only 4% of respondents believe their organization will not fall victim to cyberattacks or data breaches.

The United States had the highest number of respondents with customer data theft (58%) as the top worry, compared to 44% in the U.K. and 48% in Canada. Meanwhile, 19% of U.K. respondents rated reputation damage as their top concern, versus 15% in Canada and 8% in the United States.

Top Cyberattack and Data Breach Worries



	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
Customer Data Theft	58%	v	53%	58%	44%	48%
Intellectual Property Theft	22%	v	21%	21%	18%	24%
Reputation Damage	12%	=	12%	8%	19%	15%
Website Taken Offline	N/A		7%	7%	10%	4%
Fines or Legal Action	3%	=	3%	3%	2%	3%
Won't Fall Victim	5%	v	4%	3%	7%	6%

Respondents Who Feel Safe from Security Threats

	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
Customer Data Theft	72%	v	70%	68%	80%	68%
Intellectual Property Theft	28%	^	30%	32%	20%	32%

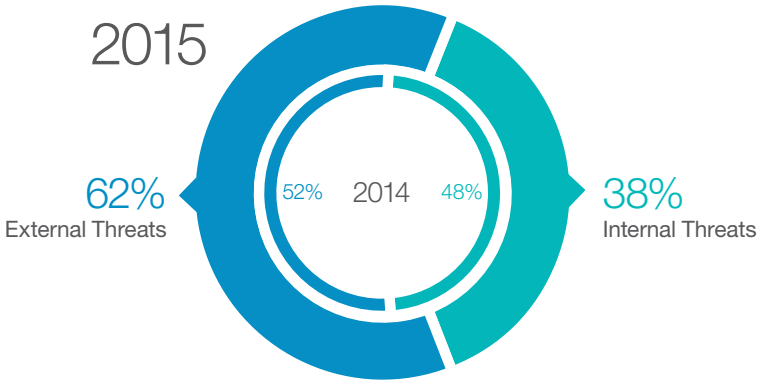
External Versus Internal Threats

For another year in a row, threats originating from outside company walls ignited more pressure than threats posed by insiders. 62% of security pros (up from 52% the previous year) said protecting against external threats, such as hackers and data-stealing malware, exerted the most threat pressure, compared to 38% who cited internal threats (either accidental or malicious) as the largest source of tension. Worries over external threats were most pronounced in Canada, where 69% of respondents graded them as their top threat source to protect against, compared to 61% in the United States and 55% in the U.K.

For internal threats, respondents said employee accidents and non-malicious mishaps (20%) dialed up the pressure more than deliberate malfeasance and/or data leakage (18%).

The results were not surprising, of course, considering the unfortunate procession of breach victims in the headlines. However, the insider threat — which can involve collusion with an outsider — still poses a significant risk to organizations. Late last year, the U.S. government issued an alert warning of a surge in attacks waged by disgruntled insiders. But admonitions such as that one evidently were not enough to sway the feelings of the response pool. In last year's report, 48% of respondents considered internal threats more pressure-inducing than external threats, but that number fell by a whopping 10 percentage points in this year's report.

Top Security Threat Sources



	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
External Threats	52%	^	62%	61%	55%	69%
Non-Malicious Internal Threats	28%	v	20%	19%	22%	20%
Malicious Internal Threats	20%	v	18%	20%	23%	11%

Riskiest Insider Threats

NEW FOR 2015

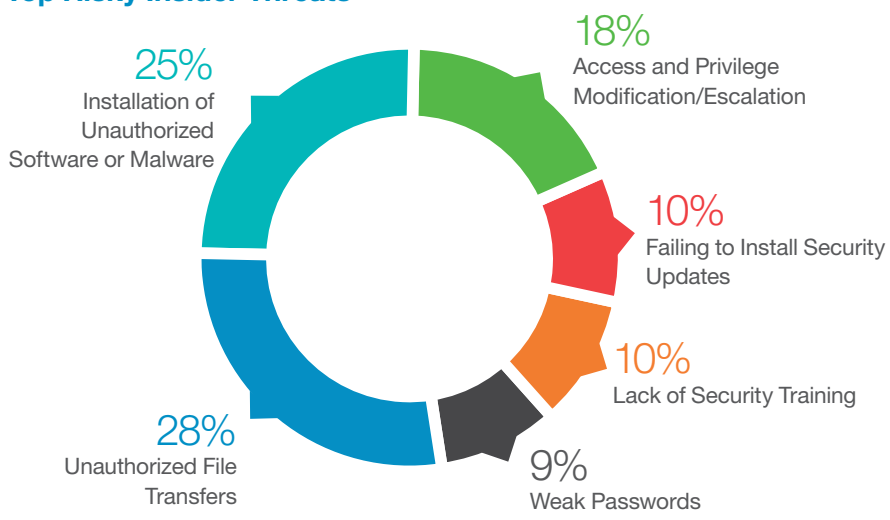
Insider threats do continue to wreak havoc at organizations of all sizes. Unauthorized file transfers, such as those initiated through the cloud or email, ranked as the top internal activity (28%) that security pros felt pressured to protect against. One-quarter of respondents said they were most strained by installation of unauthorized software or malware. Another 18% graded access and privilege modification as their top insider pressure point.

Somewhat surprisingly, despite previous Trustwave research showing that easy-to-crack passwords contributed to nearly one-third of all breaches, just 9% of security pros overall (7% in the United States) cited weak passwords as the insider activity they felt the most pressure to fend off.

The overall results varied by country, with 31% of security pros in the United States and 26% in Canada ranking unauthorized file transfers as their top risky insider threat. 26% of respondents in the U.K. rated their top internal pressure as access and privilege modification or escalation, compared to only 17% in the United States and 12% in Canada.

Other interesting country-by-country data: 17% of Canadian respondents viewed a lack of security training as their leading pressure, versus just 9% in the U.K. and 8% in the United States — a sign that employee awareness programs may be more mature in those two nations.

Top Risky Insider Threats



	2015 Report Overall	United States	United Kingdom	Canada
Unauthorized File Transfers	28%	31%	22%	26%
Installation of Unauthorized Software or Malware	25%	27%	21%	24%
Access and Privilege Modification/Escalation	18%	17%	26%	12%
Failing to Install Security Updates	10%	10%	9%	12%
Lack of Security Training	10%	8%	9%	17%
Weak Passwords	9%	7%	13%	9%

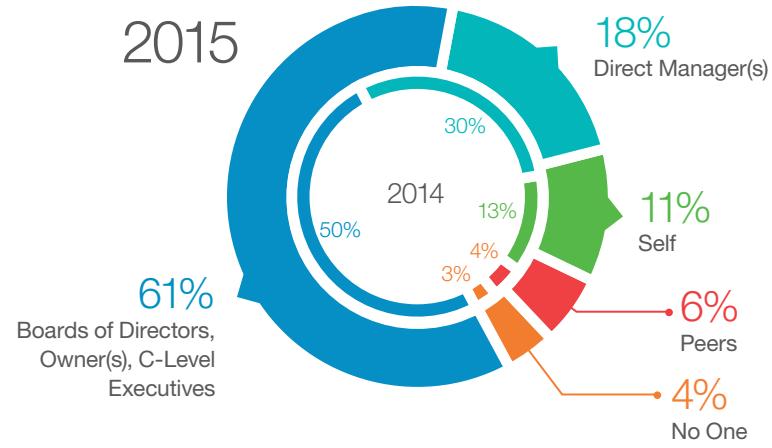
Pressure Exertion

Data protection and overall attack resilience have quickly become primary business priorities, and it's no surprise that the people in charge are taking notice of the many risks that security weaknesses pose — from the reputational to the fiduciary — and are impelling their IT leaders to act. 61% of survey respondents felt the most pressure from their organization's owners, board or C-level executives when it came to security. 18% reported the most people pressure from their direct manager, 11% from themselves and 6% from their peers. Only 4% said they don't receive pressure from anyone.

Pressure from the top drastically increased from the findings in last year's report, where only 50% of respondents reported that their boards/owners/chief executives exerted the most pressure. Also last year, 30% of security pros reported they felt the most security-related pressure from their direct manager, but that number plummeted to 18% this year.

Not surprisingly, the numbers diverge somewhat when comparing enterprise versus SMBs. 66% of enterprise security pros in this year's report said their boards of directors, owners and C-level executives exert the most security pressure, versus 55% at SMBs.

Who Exerts the Most Pressure?

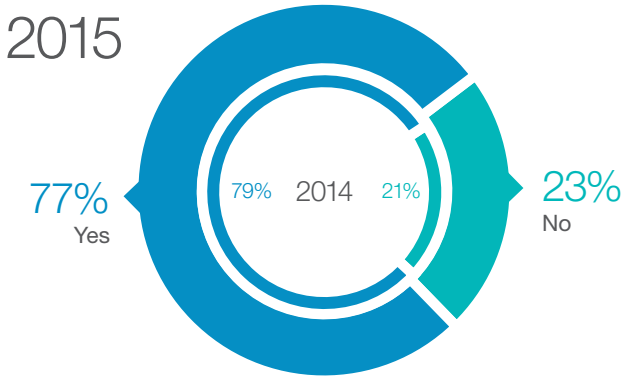


	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
Boards of Directors, Owner(s), C-Level Executives	50%	^	61%	62%	63%	55%
Direct Manager(s)	30%	v	18%	18%	16%	21%
Self	13%	v	11%	11%	11%	11%
Peers	4%	^	6%	6%	7%	9%
No One	3%	^	4%	3%	3%	4%

Speed Versus Security

Attackers love to take advantage of software and applications that contain coding deficiencies through which they can launch exploits — and many companies are lending them a helping hand. For another year, nearly four out of five security pros were pressured to prematurely roll out IT projects, including applications, despite security concerns. Specifically, 77% of respondents were pressured to unveil the projects too soon. 61% said this happened “once or twice” in the year, and 16% said it happened frequently. Clearly feeling higher rush-to-market demands, enterprise respondents (84% yes) faced more pressure to hastily deliver IT projects than their counterparts at SMBs (69% yes).

Pressure to Roll Out IT Projects Despite Security Issues



	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
Yes, Once or Twice	63%	^	61%	61%	65%	57%
Yes, Frequently	16%	=	16%	19%	13%	12%
No	21%	^	23%	20%	22%	31%

Top Operational Pressures

Emerging technology adoption, advanced security threats and budgetary constraints were the top three operational pressures facing security pros. When asked about the top operational pressures they faced related to their information security programs, respondents cited the adoption of emerging technologies (25%), advanced security threats (24%) and budgetary constraints (12%). Just behind was security product complexity at 11%. Rounding out the top operational pressures were: lack of time (6%), ensuring third-parties follow best security practices (6%), requests from business-line managers (6%), shortage of security expertise (5%) and personnel constraints (5%).

There were contrasts in response, depending on country. The top operational pressure for practitioners polled in the United States was advanced security threats (27%), but only 16% of respondents in the U.K. felt similarly. Meanwhile, double the percentage number of respondents in Canada (20%) than in the United States (10%) ranked budgetary constraints as their largest pressure.

In last year's report, respondents deemed advanced security threats as their No. 1 operational pressure (22%), followed by adoption of emerging technologies (17%) and budgetary constraints (13%).

Top Operational Pressures Facing Security Pros

1. **Adoption of Emerging Technologies**
2. **Advanced Security Threats**
3. **Budgetary Constraints**

	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
Adoption of Emerging Technologies	17%	^	25%	26%	24%	24%
Advanced Security Threats	22%	^	24%	27%	16%	22%
Budgetary Constraints	13%	v	12%	10%	13%	20%
Security Product Complexity	15%	v	11%	12%	13%	8%
Time Constraints	9%	v	6%	6%	6%	5%
Ensuring Third-Party Contractor Security	N/A		6%	5%	6%	6%
Requests from Business-Line Managers	7%	v	6%	5%	10%	3%
Shortage of Expertise	7%	v	5%	5%	6%	5%
Personnel Constraints	10%	v	5%	4%	6%	7%

Emerging Technologies

As the previous section revealed, security pros viewed the adoption of emerging technologies as their largest source of operational pressure. This begs the question: Exactly which emerging technologies were causing them such grief?

By a considerable margin, security pros were most pressured to adopt or deploy the cloud. 47% of security practitioners ranked the cloud first, followed by bring-your-own-device (BYOD) (22%). Coming in third were mobile applications (15%), then social media (9%) and big data (7%).

Respondents also rated the emerging technologies they felt posed the greatest security risk to their organization. The cloud again took top honors (40%), followed by BYOD (27%), mobile applications (14%), social media (13%) and big data (6%).

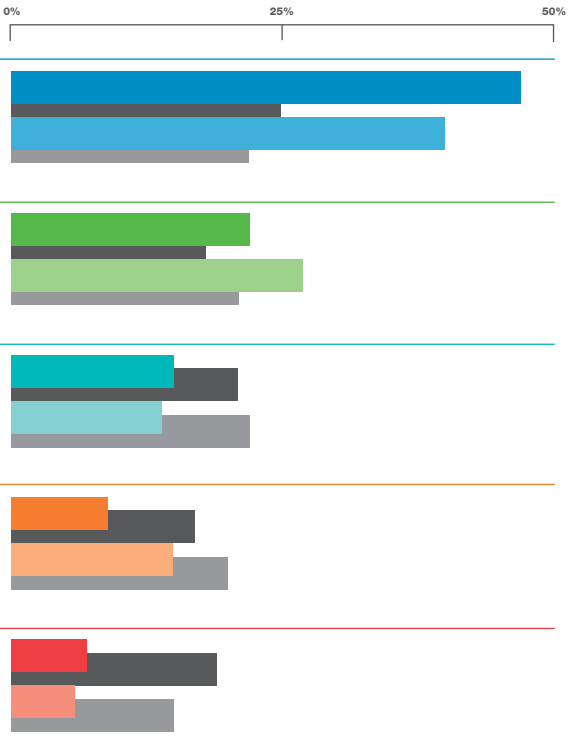
This was a notable contrast to the findings from last year's report, where the results were more bunched. In the 2014 report, far fewer respondents viewed the cloud as the emerging technology that poses the greatest adoption/deploy pressure and security risk to their organization (25% and 22%, respectively).

Meanwhile, despite more organizations than ever buying into the potential productivity and morale gains of permitting employees to connect their personal devices to corporate networks, great strain is being placed on security pros. As the smartphone and tablet market experiences rapid growth, these endpoints essentially have become no different than desktops and laptops. As such, 22% of respondents view BYOD as the top pressure-inducing emerging technology, and 27% as the greatest emerging technology risk.

But as the cloud and BYOD ratchet up anxiety in the IT department, security practitioners seemingly have warmed up to other emerging technologies. For instance, big data took a big dip this year compared to last year, when 19% of respondents perceived it as the top emerging technology to adopt/deploy and 15% as the largest emerging technology risk. In this year's report, those numbers fell to 7% and 6%, respectively. Social media and mobile applications also experienced similar big drops.

Among enterprise and SMB respondents, they viewed adoption/use pressures and security risks somewhat similarly when it came to emerging technologies. However, more SMB respondents (43%) viewed the cloud as the greatest emerging technology risk than enterprise respondents (38%). Meanwhile, more enterprise security pros (30%) viewed BYOD as the greatest emerging technology risk than SMB respondents (24%).

Year-Over-Year: Emerging Technology



	2014 Report	2015 Report
Cloud		
Most Pressured to Adopt/Deploy	25%	47%
Posed the Greatest Risk	22%	40%
Bring-Your-Own-Device (BYOD)		
Most Pressured to Adopt/Deploy	18%	22%
Posed the Greatest Risk	21%	27%
Mobile Applications		
Most Pressured to Adopt/Deploy	21%	15%
Posed the Greatest Risk	22%	14%
Social Media		
Most Pressured to Adopt/Deploy	17%	9%
Posed the Greatest Risk	20%	13%
Big Data		
Most Pressured to Adopt/Deploy	19%	7%
Posed the Greatest Risk	15%	6%

Emerging Technology: Most Pressured to Adopt/Deploy

	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
Cloud	25%	^	47%	48%	44%	48%
BYOD	18%	^	22%	22%	21%	22%
Mobile Applications	21%	v	15%	14%	16%	15%
Social Media	17%	v	9%	7%	15%	10%
Big Data	19%	v	7%	9%	4%	5%

Emerging Technology: Posed the Greatest Risk

	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
Cloud	22%	^	40%	41%	32%	45%
BYOD	21%	^	27%	28%	32%	23%
Mobile Applications	22%	v	14%	14%	15%	13%
Social Media	20%	v	13%	12%	14%	15%
Big Data	15%	v	6%	5%	7%	4%

Breach Repercussions

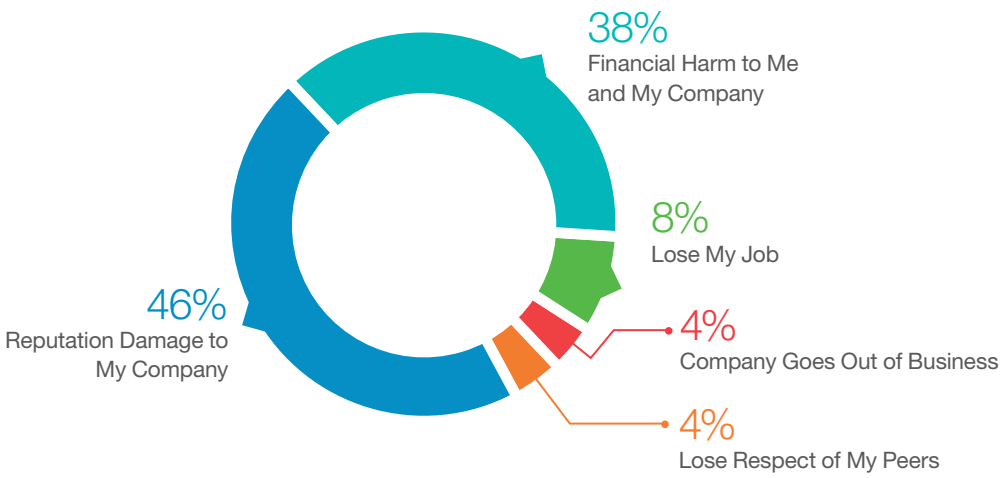
NEW FOR 2015

Data breaches are raining down like confetti — except nobody's having any fun (bad guys not included). So one can hardly blame security professionals for visualizing their business falling victim, and then contemplating how serious the fallout could get.

46% of respondents cited reputation damage to their company as the most-feared repercussion. Another 38% said financial harm to their company is the most-worrying consequence, while 8% were wary about job loss and 4% each fretted about the loss of respect from peers and their company going under.

Companies of varying sizes answered similarly, but there was more concern at the SMB level (10%) than at the enterprise level (6%) about getting fired. Respondents working at the latter (41%) were more fearful of financial damage than at an SMB (35%).

Which post-breach repercussion do you fear the most?



	2015 Report Overall	United States	United Kingdom	Canada
Reputation Damage	46%	48%	40%	47%
Financial Harm	38%	39%	39%	36%
Job Loss	8%	7%	11%	8%
Out of Business	4%	3%	5%	5%
Loss of Peer Respect	4%	3%	5%	4%

Features Versus Resources

As learned in childhood, the hottest new toy isn't always as satisfying as it is cracked up to be. That can apply to adulthood in the security world as well.

Roughly two-thirds of security pros faced pressure to use security technology containing all of the latest features, despite nearly three out of 10 not having the resources to do so effectively.

Specifically 67% of respondents were pressured to select and purchase security technologies with all of the proverbial bells and whistles, despite the fact that 29% did not have the proper resources to effectively use all of those features.

Respondents at SMBs felt less pressured (57%) than enterprises (75%) to obtain feature-filled technologies, but when they did, a whopping 37% don't bear the necessary resources to manage these solutions.

Meanwhile, security pros in Canada felt the least pressure (55%) to acquire technologies with the latest features — possibly because when they did, they were the ones most lacking the adequate resources to properly use them (40%).

Pressure to Select the Latest Security Technologies

Lack the Proper Resources to Use Technologies

Face Pressure to Select the Latest Security Technologies

	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
Yes	65%	^	67%	72%	64%	55%
No	35%	v	33%	28%	36%	45%

Have the Proper Resources to Use These Technologies

	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
Yes	65%	^	71%	72%	77%	60%
No	35%	v	29%	28%	23%	40%

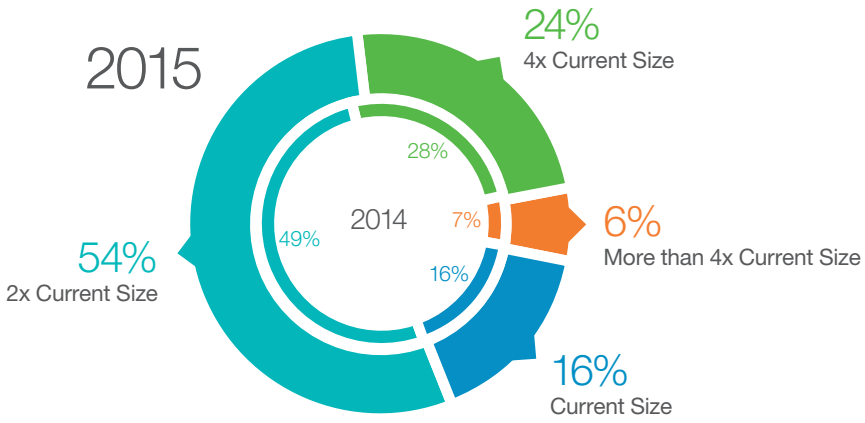
Staffing Levels

What is a surefire way to lighten the load facing a pressured security professional? Provide relief in the form of additional staff.

84% of respondents reported the need for additional staff. 54% of security professionals wanted the size of their team doubled and 30% wanted it quadrupled (or more than quadrupled), while 16% of respondents indicated the current size of their team was ideal. Among countries, Canada seemed most satisfied, with a quarter of respondents deeming their current staffing size ideal.

It's important to note: Meager security teams aren't necessarily the consequence of a lack of dollars to fill headcounts. The issue also stems from the reality that it's difficult for businesses to find enough qualified personnel — those with security expertise who can help fulfill the wide swath of security demands, from deploying products to assessing threats in real time to responding to breaches.

Ideal Staffing Sizes



	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
Current Size	16%	=	16%	14%	14%	25%
2x Current Size	49%	^	54%	50%	57%	61%
4x Current Size	28%	v	24%	29%	23%	12%
More than 4x Current Size	7%	v	6%	7%	6%	2%

In-House Versus Managed Services

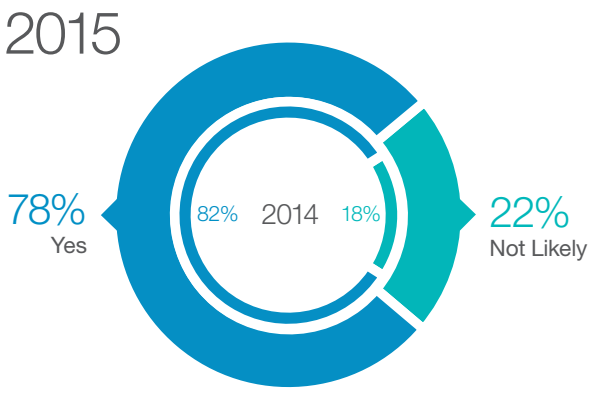
The managed security services market is exploding and steamrolling into the second part of the decade carrying an estimated market value in the tens of billions of dollars, according to independent research estimates. Depending on their size, organizations can turn to managed security for different reasons. In many cases, smaller businesses seek to delegate their entire security workload to a trusted partner who will handle their data protection soup-to-nuts. Larger businesses, meanwhile, often opt for an MSSP to help amplify their security coverage, oftentimes around things like anti-malware and threat management.

According to respondents, around three-quarters of IT teams manage security in house, but nearly four out of five use or will use managed security services in the future. Specifically, 78% of security pros already partner or are likely to partner with a managed security services provider to relieve some IT security pressures. Among those, 43% said they plan to use managed security services in the future, 35% already do and 22% are not likely to use managed security services.

However, just 19% of U.S. and 17% of U.K. respondents are unlikely to utilize managed security services. That number rises to 37% in Canada. Broken down by business size, 70% of SMBs and 84% of enterprises already do or are likely to partner with an MSSP.

For those that work or intend to work with an MSSP, 89% said the partnership will include its in-house staff, while 11% expect to delegate all of their security needs to the MSSP.

Plans to Partner with Managed Security Services Provider



	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
Plan to in Future	46%	V	43%	45%	43%	38%
Already Do	36%	V	35%	36%	40%	25%
Not Likely	18%	^	22%	19%	17%	37%

Extent of Managed Security Services Provider Partnership

NEW FOR 2015

89%
Partnership Between MSSP and In-House Staff

11%
Outsource All Security Needs to MSSP

	2015 Report Overall	United States	United Kingdom	Canada
Partnership Between MSSP and In-House Staff	89%	89%	90%	90%
Outsource All Security Needs to MSSP	11%	11%	10%	10%

2015 Wish List

As this report has documented, security professionals are under pressure. To ease that tension, they need things to happen. So…if they could write a list of desired things or occurrences, what would it include?

Topping their 2015 wish list, 29% of respondents want to be shown the money — through additional budget — followed by 24% who long for more staff security expertise and 21% who would fancy additional time to focus on security. Another 11% would seek the services of a managed security provider, while 7% thirst for less complex security technologies and products. Staff augmentation and fewer requests from business-line managers (both 4%) round out the wish list.

The top three wishes this year didn't change from last year, but they became more clear-cut, painting an obvious picture that security teams sorely are in need of key resources to navigate today's complex threat environment. Last year, respondents yearned for more budget (21%), more security skills (20%) and more time (19%). Meanwhile, SMB and enterprise respondents had the same top three wishes this year, although the former desired additional budget (31%) more than the latter (26%).

Security Professional's Wish List for 2015

29% **MORE BUDGET**

24% **MORE SECURITY STAFF EXPERTISE**

21% **MORE TIME**

	2014 Report Overall		2015 Report Overall	United States	United Kingdom	Canada
More Budget	21%	^	29%	27%	26%	34%
More Security Staff Expertise	20%	^	24%	23%	23%	29%
More Time to Focus on Security	19%	^	21%	22%	25%	15%
Service Provider to Help Manage Security Program	10%	^	11%	13%	10%	4%
Less Complex Technologies	12%	v	7%	7%	8%	7%
More Staff	8%	v	4%	5%	2%	7%
Fewer Requests from Business-Line Managers	10%	v	4%	3%	6%	4%

Conclusion and Recommendations

If you are an IT professional focused on security, you don't need a report to inform you that your job is pressure-packed. In fact, you likely already are inured to the unrelenting tension and worriment that comes with a role trusted to protect an organization's vital assets and save it from the costly result of a data breach.

The bases you must cover are plentiful, resulting in the need to navigate an increasingly complex field containing many moving parts and fresh challenges unabashedly greeting you on a daily basis. As a result, you are attending to a dizzying array of threat sources, mired in countless individual projects and trying to make all of your security purchases work for you. You're stretched thin and you're overwhelmed. It's unsustainable. Adding insult, you are unable to see the forest for the trees.

It is our sincere hope that the 2015 Security Pressures Report from Trustwave — by isolating common and key pressure sources facing security professionals worldwide and across business sizes — provides you the ability to step back and gain a clearer perspective on the rigorous duties that stand before you. A more salient understanding of these problems can result in stronger decision-making and the implementation of a more effective, security-first strategy that takes some of the burden off of you and your team.

The report also is a valuable resource to share within your organization to shed light on where you may be feeling the most pressure, ideally resulting in the awareness and action that you require to alleviate these pain points.

In the spirit of leaving you with concrete takeaways and practical advice, here are seven recommendations that should get the ball rolling on the road toward pressure reduction.

1. **Accept that everyone, including you, is at risk:** Perhaps our respondents merely are stricken with an excessive case of denial or hubris, but the fact that 70% believe they are safe from cyberattacks and data breaches, no matter the size of one's company, is an unacceptable way to fashion a security architecture. Operating under the belief that breaches are inevitable allows security pros to better prepare their strategy. Going further, the world's most security-mature organizations are ones that are just as focused on incident response as they are on prevention and detection.
2. **Acknowledge that outsiders and insiders can equally hurt you:** The report notes that 62% of respondents were most pressured by external threats, versus 38% who were most pressured by internal threats. Attacks waged by outside adversaries garner the manifold of headlines, but threats posed by insiders can be as destructive (and perhaps take more time to discover). Align your security strategy to consider the reality of negligent employees and third-party contractors, as well as those workers who purposefully seek to fleece your organization of sensitive data. To keep network users trained in keeping the company and themselves protected, conduct a regular security awareness education program and measure its success. Our next recommendation suggests some other solutions.
3. **Turn to advanced solutions:** Traditional, perimeter-focused security technologies simply aren't cutting it anymore to handle today's zero-day exploits and advanced persistent and blended threats, as well as risks posed by insiders. As a result, companies must turn to more advanced threat management solutions, such as next-generation SIEMs, file integrity monitoring and anti-malware gateways. These provide network visibility and monitoring, glean critically important intelligence and help detect and prevent threats in real time.

4. **Think security first:** For another year, the overwhelming majority of respondents (77%) reported feeling rushed to push out IT projects, such as applications, that weren't security ready. This is a big reason why vulnerabilities are commonplace in applications and other IT rollouts. Automated vulnerability scanning, ongoing and in-depth penetration testing and web application firewall deployment can help keep the bad guys out. Meanwhile, databases connected to these apps also must be monitored and protected to prevent improper access, and leakage or disclosure of sensitive data.

5. **Narrow the disconnect between the security group and senior management:** The most mature businesses are built around a certain culture, where security is viewed as an investment and an enabler, not a cost and an inhibitor. At these organizations, security is not looked at as a necessary evil, nor does it exist merely as a consequence of satisfying compliance requirements. The most forward-thinking owners, boards and C-level executives are well aware of today's potent threat landscape, as well as the many resource challenges facing the IT and security department. They recognize security as a key component of overall business risk. The organizations that deploy strong IT governance, in which security-conscious leaders regularly communicate and collaborate with those responsible for security and ensure priorities are being met, are less likely to have their names slapped across the front pages because of a breach.

6. **Embrace the revolution:** Trends such as the cloud and BYOD — and the latter's "Internet of Things" companion — are here to stay. Respondents to this survey graded the cloud and BYOD as the two emerging technologies applying the most pressure on them. Companies must recognize the exploding risk potential of these technologies, assess them for vulnerabilities and deploy security controls like network access control, data loss prevention and encryption.

7. **Accept a helping hand:** Security is an exhaustive — and exhausting — exercise. Few organizations, no matter their size, are equipped to handle all of the pressing requirements that go into the endeavor. The need to meet a plethora of ever-evolving compliance requirements also is real. Complicating factors is that 84% of respondents said they want the size of their security teams increased, a wish that may go unfulfilled due to budget strains and the lack of a skilled candidate pool from which to choose. There is no shame in turning to an outside partner for help on threat, vulnerability and compliance management. 78% of security pros said they are likely to or already do partner with a managed security services provider. MSSPs can help businesses struggling to meet security and compliance demands simplify their programs through packaged solution bundles, expert management and automated tools. For those organizations with advanced needs, MSSPs can help augment key areas that may be getting short shrift, such as threat and vulnerability management.