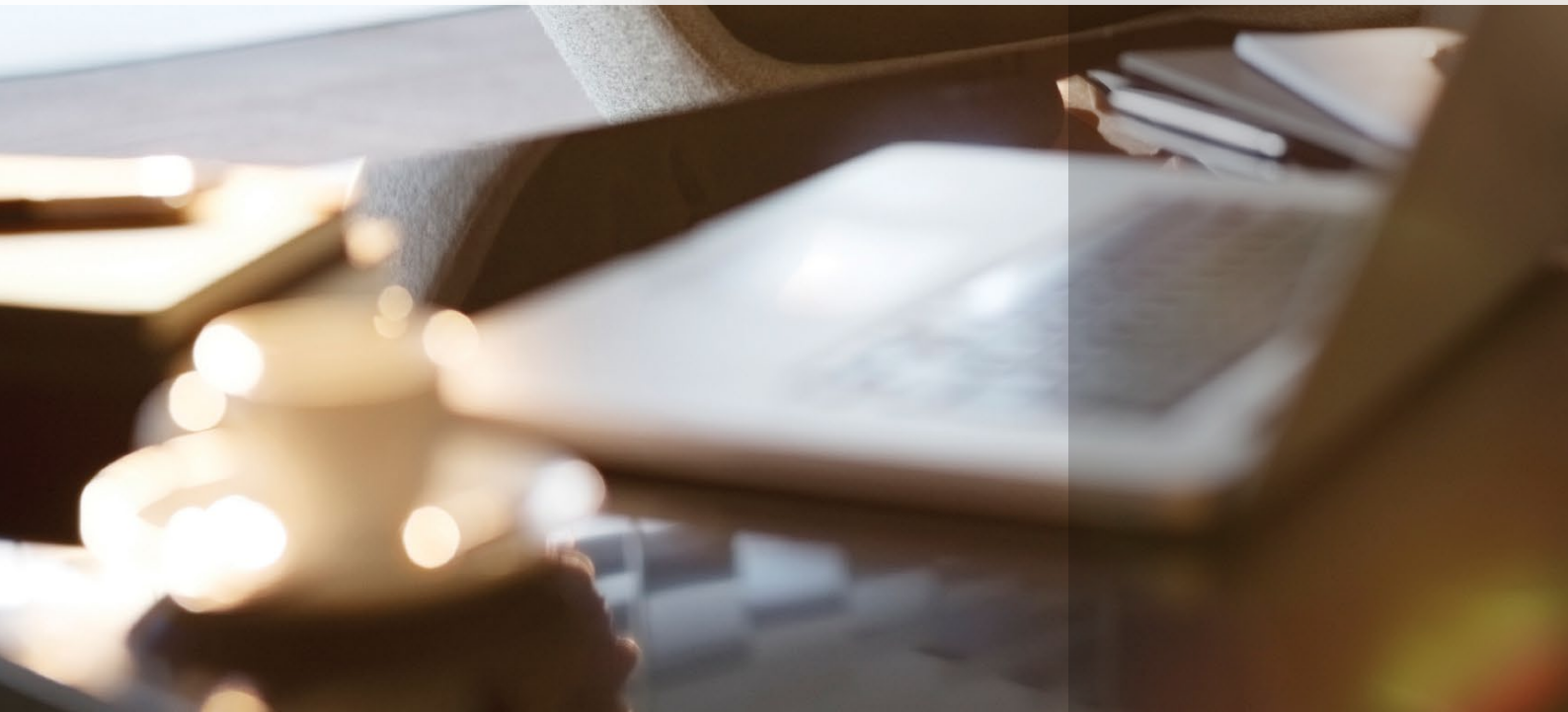
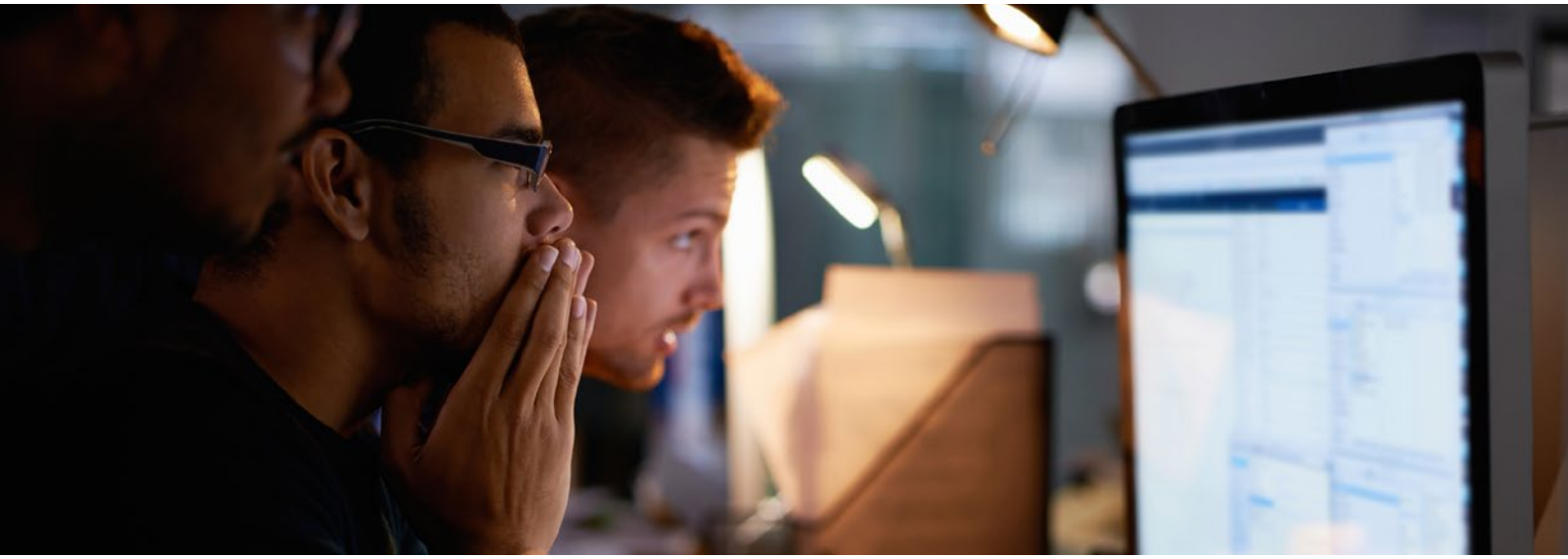
FORTINET

FORTINET SURVEY

The Fortinet Security Census 2014

Lightspeed GMI





Executive Summary

The Fortinet Security Census 2014 has uncovered the harsh realities of protecting businesses from the unpredictable and increasingly problematic challenges of cyber attack, data theft and other IT security concerns.

This research exercise was undertaken in August 2014 on behalf of Fortinet by the independent market research company Lightspeed GMI[1]. It polled 1,610 qualified IT decision makers (ITDMs) including CIOs, CTOs, IT Directors and Heads of IT working at large organizations from 15 countries around the world.

In this research we learn a great deal from exploring the current perceptions of IT leaders about the challenge of IT security and the changing dynamics within large organizations driven by emerging technologies, increasingly complex and frequent threats, and the quest to use IT to harness innovation. The research also reveals a strong trend for increased pressure and awareness in IT security matters from senior boardroom executives, exploring some of the resulting impact.

Top IT professionals have a tough job capitalizing on the opportunities to develop new services, drive improved efficiencies and exploit the value of their data assets, and it seems it's made even tougher with security concerns adding to the burden. Amid a perfect storm of tightening compliance pressures, new technologies to embrace, and an increasingly challenging threat landscape to contend with, the analysis explores how these businesses are approaching big data analytics, data privacy and biometrics in this context, and closely examines the current and future demand drivers pushing them to respond with new approaches to strategy, investment plans and even new consumption models for IT security services.

[1] See 'Note on Methodology' on page 15 for more details on how and with who the research was undertaken

Key Findings

- **Increasing Boardroom Pressure for IT Security:** The pressure coming from senior executives about IT security had risen markedly from one year ago, when 49 percent of respondents reported a high or very high rating of pressure, to today when the figure is 63 percent.

- **Conflicting Views on the Value of Reputation:** ITDMs perceive differences between what they and senior business executives deem signs of a successful IT security strategy, especially when it comes to the objective of 'avoiding getting a reputation for poor data security'. ITDMs believe this is senior executives' second highest critical success factor (21 percent) while placing it firmly at the bottom of their own list with only 12 percent.

- **Securing the Enterprise Becoming Harder to Achieve:** Up to 88 percent of respondents believe the job of keeping the organization secure has become more challenging, with the rising volume and complexity of threats the biggest culprit. C-level IT leaders are suffering the most with over 60 percent saying the task is 'significantly' or 'substantially' more challenging according to some factors.

- **Security Takes Priority over Innovation:** A total of 53 percent of all ITDMs surveyed have slowed down or cancelled a new application, service or other initiative because of cyber security fears. The figure spikes to 63 percent among those reporting the highest level of boardroom pressure and scrutiny around IT security.

- **Spending Plans Address Data Privacy & Big Data Security:** The high profile issues surrounding data privacy and big data are provoking action, with up to 90 percent of ITDMs planning to change their outlook on IT security in response. The majority in each case is inclined to spend more money and resources to address the challenge, rather than simply rethink existing strategy. The biggest companies are the most likely to invest.

- **Confidence is High for Introduction of Biometrics:** 46 percent of ITDMs believe biometrics is already a mainstream technology, or will be so in the next 12 months. Two-thirds say they already have the tools to ensure it can be managed securely. A small minority believes they will struggle to secure biometrics in the future.

- **IT Departments Typically Well Resourced:** When asked if they had been provided with sufficient human and financial resources for IT security in the last year, four-out-of-five ITDMs said yes. A total of 83 percent feel they will also have sufficient resources in the next 12 months.

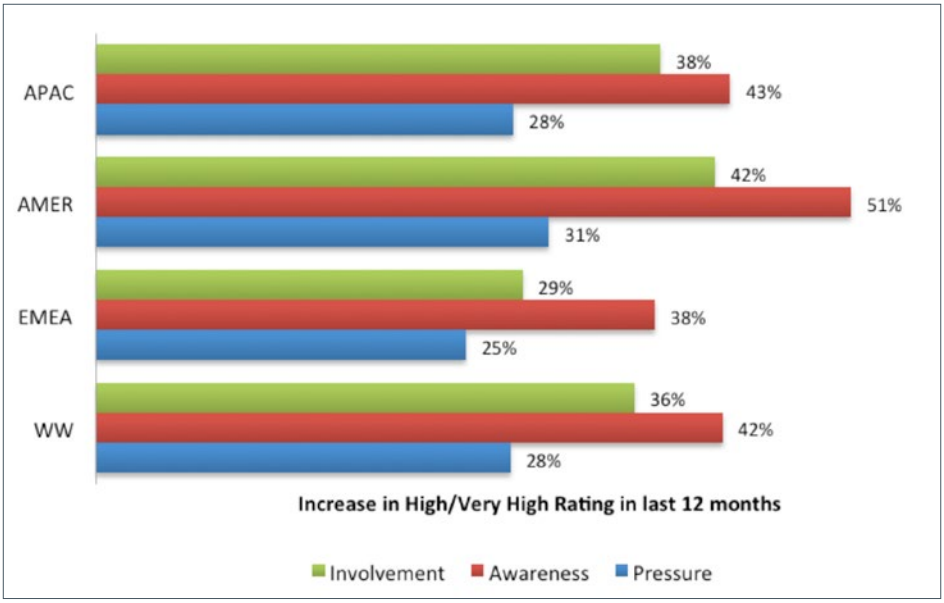
- **Big Appetite for Managed Security Services:** A quarter of ITDMs cited 'outsourcing some or all IT security functions' as the single most important initiative for confronting the rising complexity and volume of cyber threats. Half of all ITDMs agreed that the increasingly challenging threat landscape would be the key driver for potentially adopting managed security services in the future.

The Impact of IT Security as a Boardroom Issue

Rising Levels of Scrutiny from Senior Executives

High profile IT security attacks and national security scandals have been a common feature in the worldwide news reports of the last 12 months, and this is borne out in the dramatic increase in pressure, awareness and involvement in IT security matters coming from the direction of the boardroom. Rising levels are shown in the graph below, with 'high' or 'very high' ratings of pressure (up 28 percent), involvement (up 36 percent) and awareness (up 42 percent) all showing pronounced increases over one year.

FIGURE 1: GLOBAL STATUS OF INCREASED BOARDROOM SCRUTINY ON IT SECURITY



≥63%

Current levels of boardroom scrutiny on IT security at large organizations:

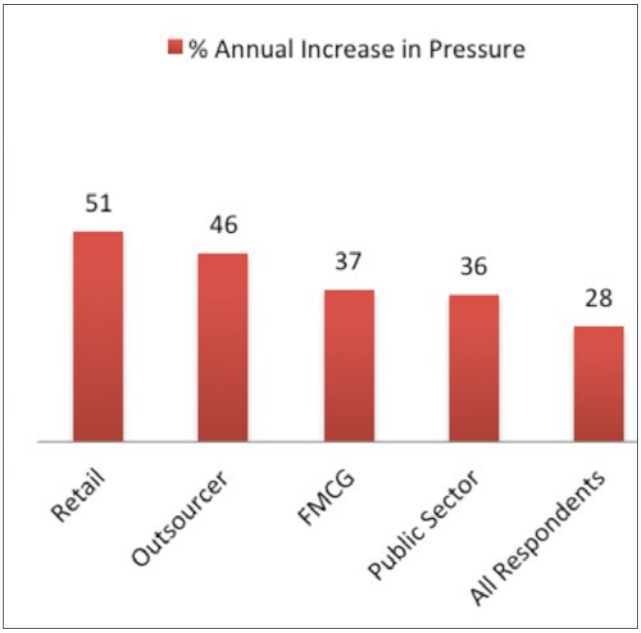
Pressure from boardroom on IT security:
High / Very High – 63%

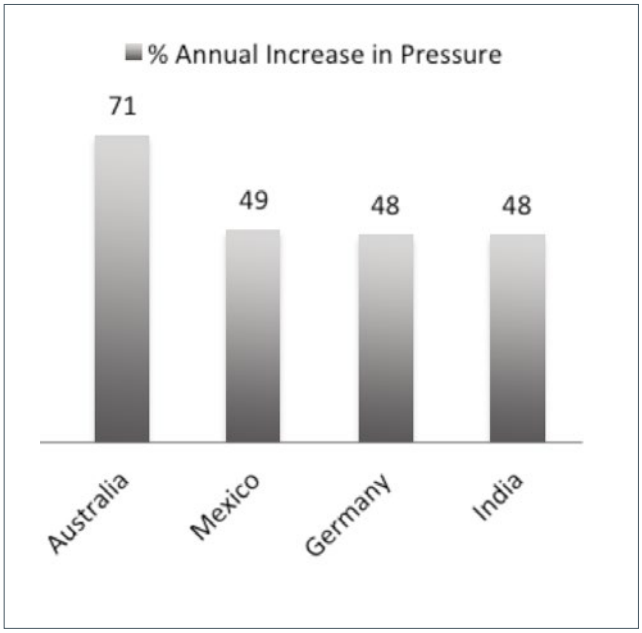
Awareness among boardroom execs about IT security:
High / Very High – 74%

Involvement by execs in IT security strategy:
High / Very High – 75%

Looking specifically at 'pressure', significant changes are visible across a wide range of industries, but are largest in the retail sector where high/very high pressure levels have jumped 51 percent in the last year (going from 43 percent to 65 percent today). Some countries are affected to an even greater extent above trend, as shown in the graph below.

FIGURE 2: COUNTRIES AND INDUSTRY SECTORS SHOWING HIGHEST JUMPS IN IT SECURITY BOARDROOM PRESSURE

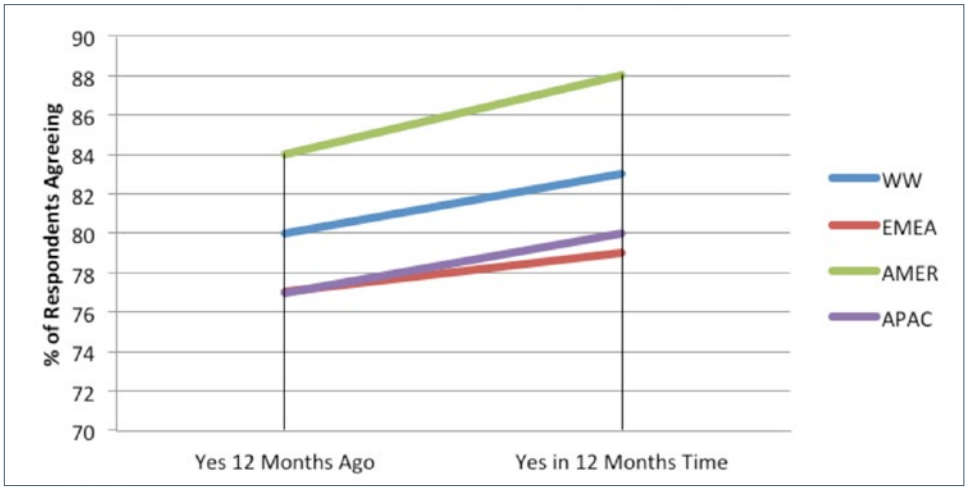




More Resources Available to Address IT Security

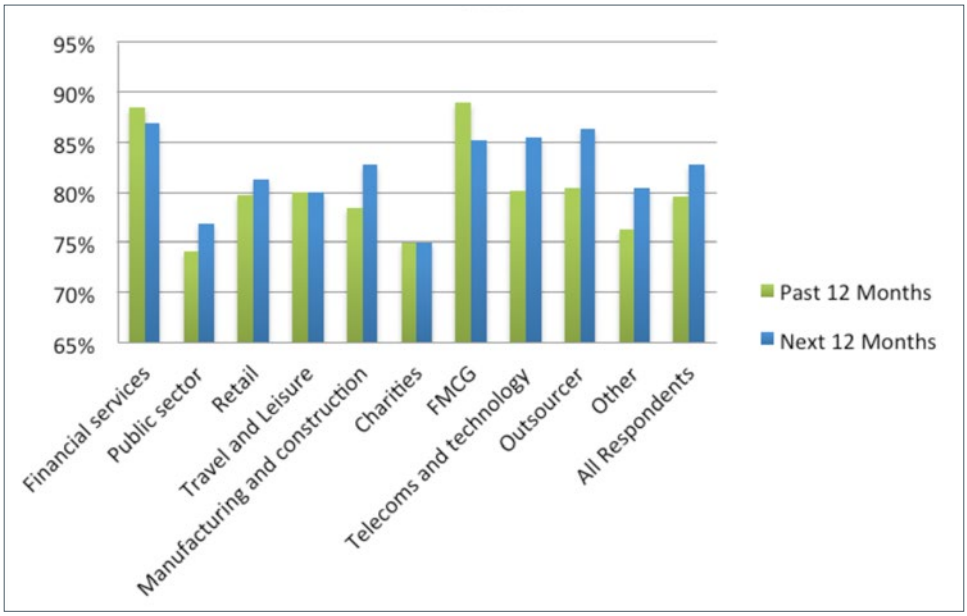
Boardroom influence is having a positive effect in many quarters, with our survey finding that the lion's share of ITDM respondents was not only satisfied with their present resourcing levels for IT security, but also optimistic about those levels increasing. Four out of five ITDMs agreed that they had been provided with sufficient resources for IT security in the last 12 months, and a total of 83 percent believe they will have sufficient resources in the next 12 months.

FIGURE 3: ASSESSMENT OF WHETHER RESOURCING LEVELS ARE SUFFICIENT FOR A SUCCESSFUL IT SECURITY STRATEGY



Most industry sectors carried this trend, for example with public sector going from 74 to 77 percent and retail from 80 to 81 percent. Financial services sector ITDMs feel best equipped (87 percent for the next 12 months), though their trend is downward (89 percent for the past 12 months).

FIGURE 4: INDUSTRY SECTOR ANALYSIS OF RESOURCING SATISFACTION LEVELS



When making a geographic analysis of these results, the four countries in the survey sample taken from the BRIC[2] and MINT[3] blocs of powerful new economies stand out as feeling the most highly equipped to deal with the challenges of implementing their IT security strategy with 89 percent of Brazilian ITDMs bullish about next year's resourcing levels, 90 percent of Indians, 91 percent of Mexicans and 97 percent of Chinese.

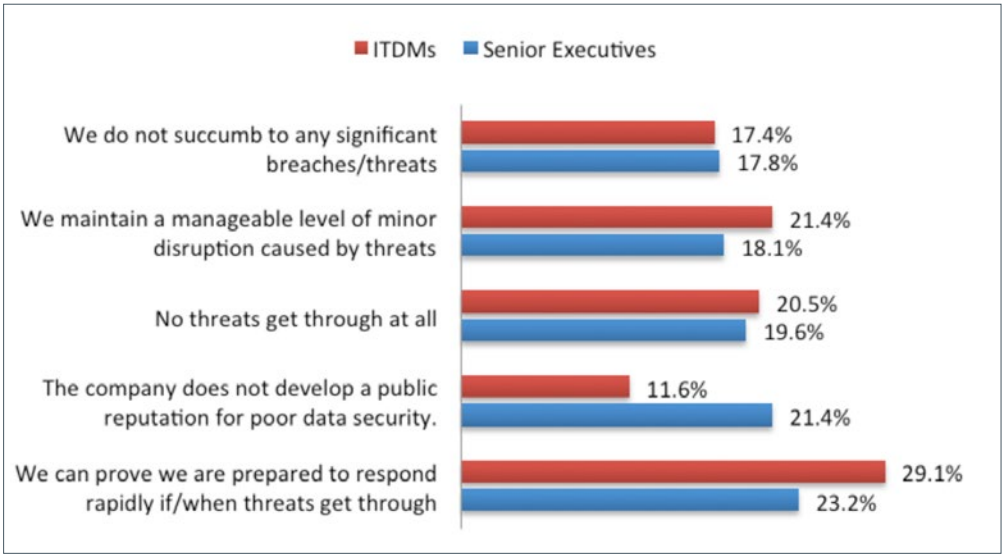
[2] The new economic powerhouses being Brazil, Russia, India and China

[3] The next economic powerhouses being Mexico, Indonesia, Nigeria and Turkey

Opinions Differ Between IT & The Boardroom on Security Success Factors

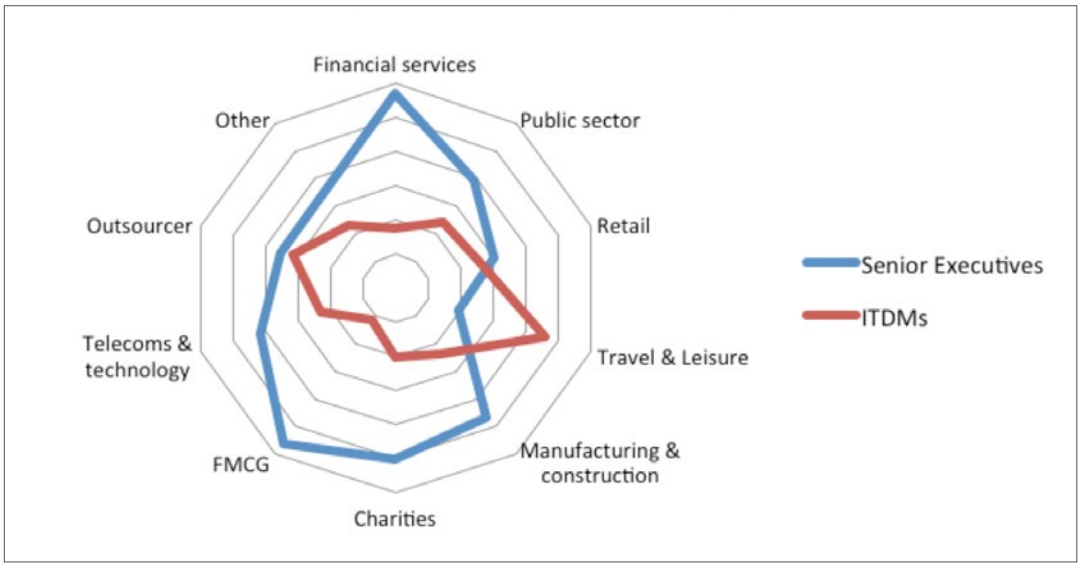
While the research didn't poll senior non-IT business executives themselves, it did collect ITDM's perceptions on the priorities of this group in terms of IT security. ITDMs identified that 'proving we are prepared to respond rapidly if/when threats get through' is the most critical success factor both for themselves (29 percent) and senior executives (23 percent). However, the survey found that business leaders and the IT department disagree over the importance of 'upholding our reputation' as a measurement of a successful IT security strategy.

FIGURE 5: DIFFERING CRITICAL SUCCESS FACTORS FOR IT SECURITY



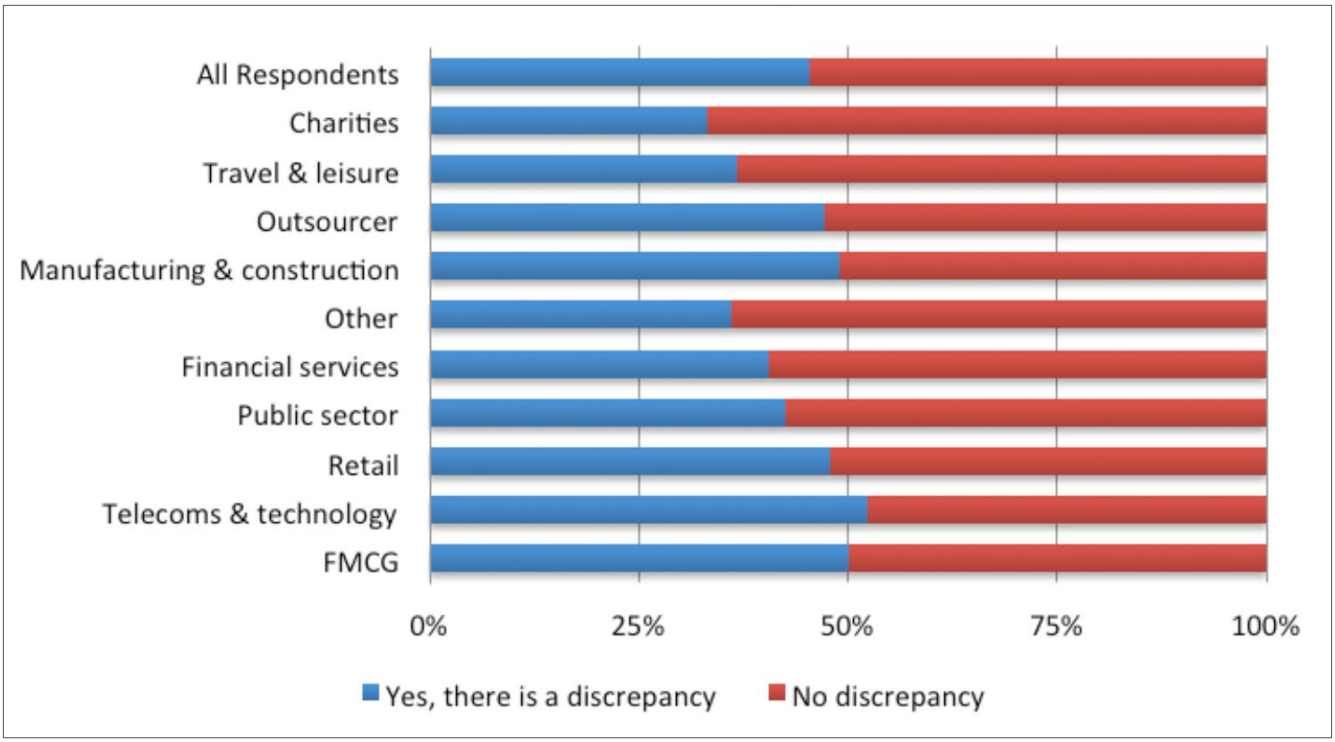
Looking more closely at respondents by industry sector, the divergence of opinion on the question of 'reputation' could not be starker. Here, the highest senior executive scores were given by financial services (29 percent), FMCG (28 percent) and charities (25 percent). However, ITDMs scored 'reputation' the lowest as regards their own priorities, with charities at 10 percent, financial services at 9 percent and FMCG at only 6 percent.

FIGURE 6: PERCEPTIONS ON THE IMPORTANCE OF AVOIDING "A PUBLIC REPUTATION FOR POOR DATA SECURITY"



The survey also discovered a large share of ITDMs (46 percent) who felt there was a discrepancy between their organization's public stance about its resilience against cyber attack and what it invests financially in its security strategy. One could conclude that these organizations were talking tougher on IT security than they were actually delivering.

FIGURE 7: DISCREPENCIES BETWEEN WHAT ORGANIZATIONS SAY AND DO ABOUT IT SECURTY

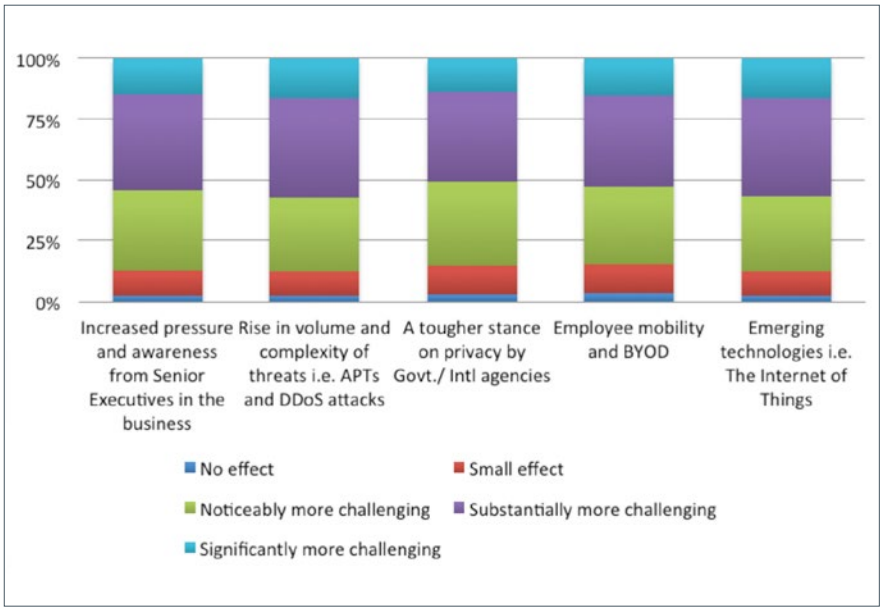


It's Getting Harder to Combine Security with Business Innovation

The Perfect Storm with Rising Volume and Complexity of Threats at its Centre

The growing pressure on ITDMs from the boardroom is having a direct impact on the increasingly challenging job they have keeping their organizations secure. In fact, increased pressure and awareness from the boardroom is making 87 percent of ITDMs' jobs 'noticeably', 'significantly' or 'substantially' more challenging. However, the trend having the biggest impression on the challenging nature of the IT security objective (at 88 percent) is the rising volume and complexity of threats. Other converging factors are contributing to an extremely challenging set of responsibilities for ITDMs.

FIGURE 8: A PERFECT STORM OF FACTORS MAKES ENTERPRISE SECURITY MORE CHALLENGING



88%

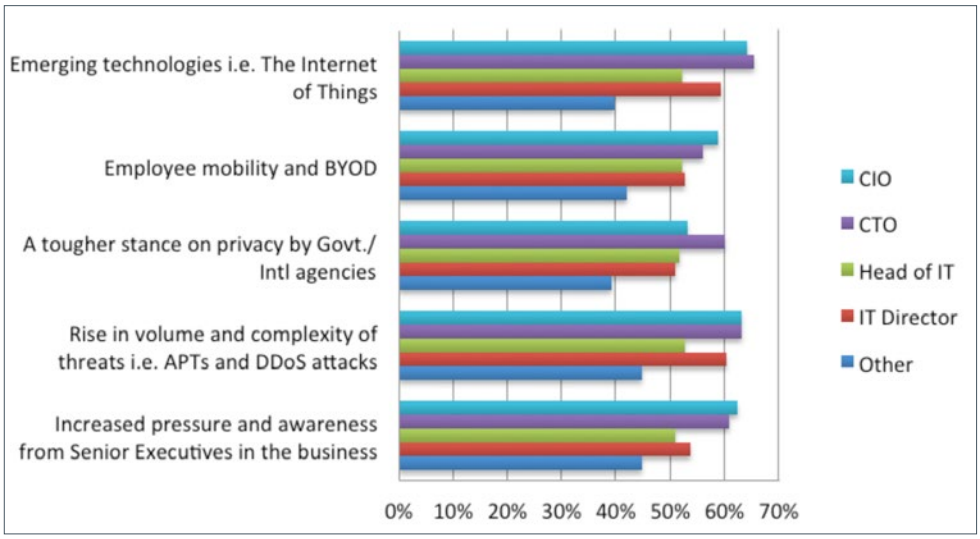
ITDMs say the job of securing the business is getting noticeably to significantly more challenging.

Top ranked reasons:

1. Rise in volume and complexity of attacks
2. Coping with emerging technologies (like IoT and biometrics)
3. Increased pressure and awareness from board execs
4. A tougher stance on privacy by Government/international agencies
5. Issues caused by employee mobility and BYOD

Within the IT profession, the individuals finding things more challenging than any other group are the C-level IT professionals; CIOs and CTOs. Compared to their colleagues, they consistently report greater instances of these factors making their job 'significantly' or 'substantially' more challenging.

FIGURE 9: iNFLUENCERS ON THE 'SIGNIFICANTLY' AND 'SUBSTANTIALLY' MORE CHALLENGING ROLES OF IT PROFESSIONALS

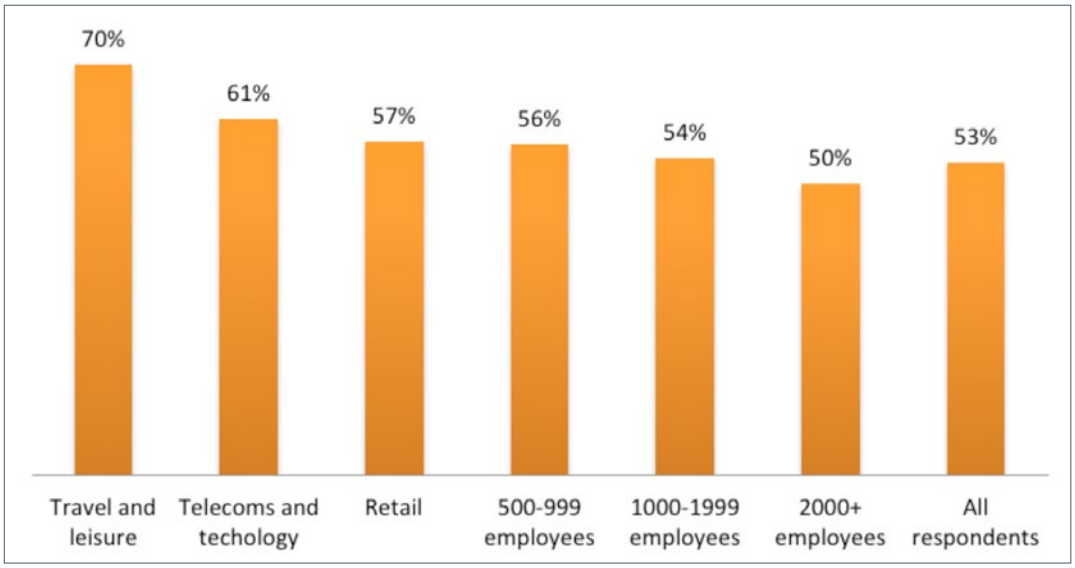


Security Takes Priority Over Innovation

One of the most troubling findings from the research is that so many ITDMs clearly find it difficult to pursue their innovation objectives because of security concerns. A total of 53 percent of respondents have paused or abandoned at least one new application, service or other business initiative because of concerns that IT security could not manage the risk. The figure is 63 percent among those reporting a high or very high level of boardroom pressure around IT security.

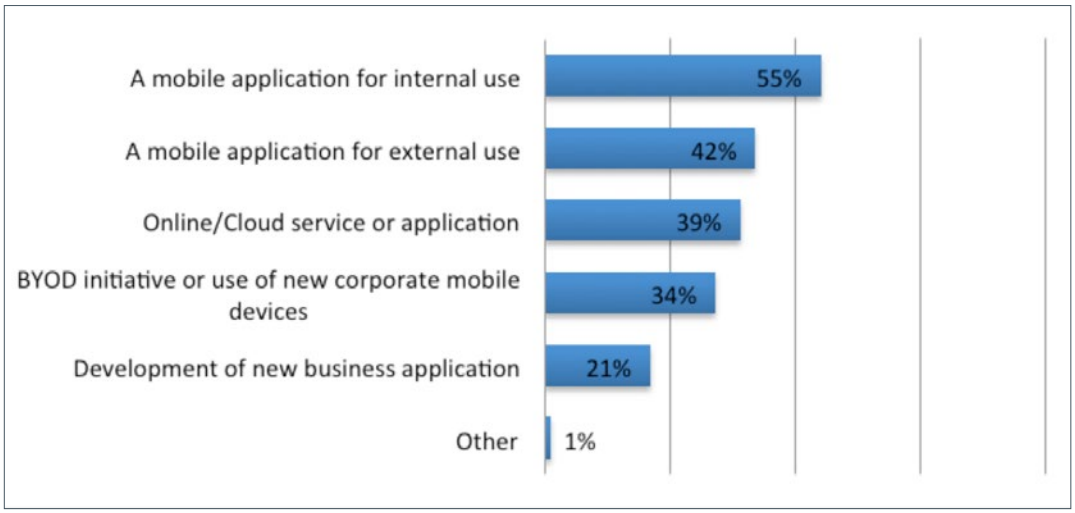
The results also highlighted how the smaller organizations involved in the survey (from 500 employees and above) were more prone to adhere to this trend.

FIGURE 10: INDUSTRY SECTORS MOST PRONE TO STOPPING INNOVATION BECAUSE OF IT SECURITY



The types of services, applications and initiatives involved in these instances where security scares off innovation, appear to be dominated by mobility related initiatives and applications. These include internal mobile apps (identified by 55 percent of those pausing/abandoning a new IT Initiative or business application/service because of concerns their security at the time would not sufficiently cope with enabling it), external mobile apps (42 percent) and the introduction of new corporate devices/BYOD (34 percent).

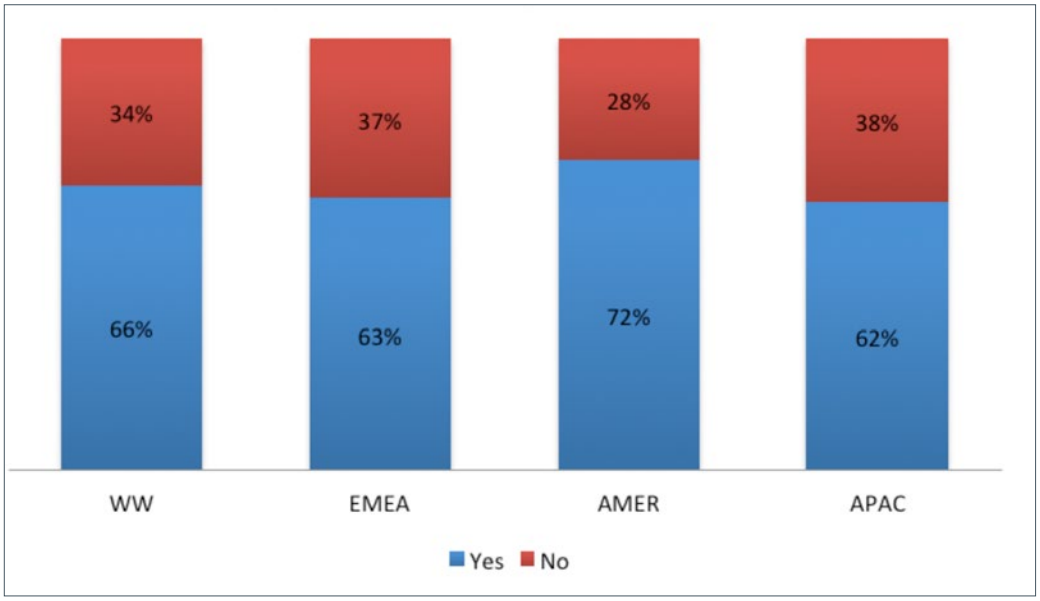
FIGURE 11: THE KINDS OF INNOVATION WHERE SECURITY SAYS 'NO'



IT Decision Makers Brace Themselves for Biometrics

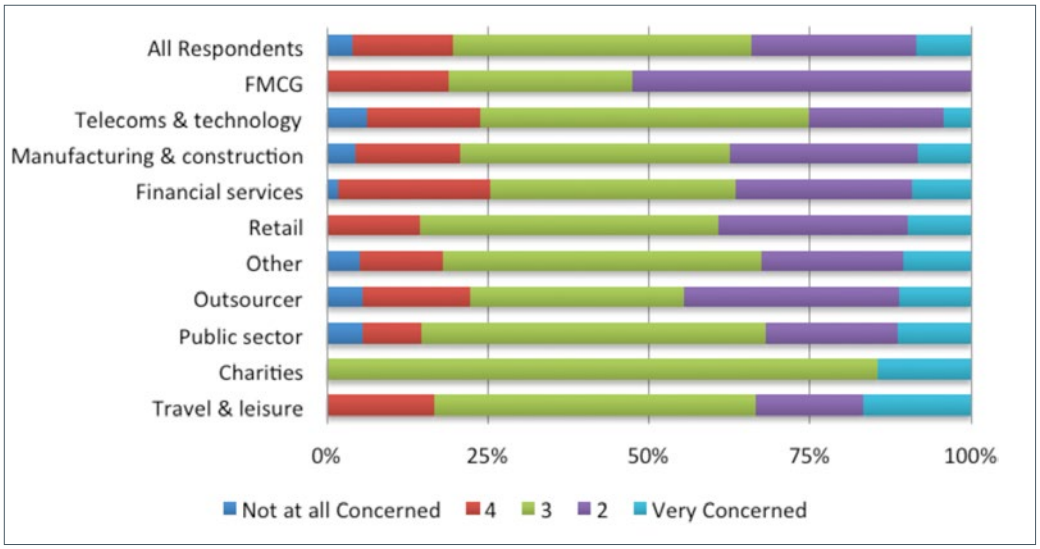
46 percent of the ITDMs asked believe biometrics has already arrived or will arrive in their industry sector in the next 12 months. Two-thirds of ITDMs think they have the tools today to make sure that biometrics and biometric data are secure in their organization. However, that leaves a sizeable minority who are anxious about its ability to keep biometrics secure right now, and in the future.

FIGURE 12: ARE SECURITY SOLUTIONS TODAY ROBUST ENOUGH TO ENABLE YOU TO TAKE ADVANTAGE OF BIOMETRICS?



Of the one-third that doesn't believe that their current IT security is sufficiently prepared to secure biometric data, 34 percent are placed high on the spectrum of concern that they will struggle to enable secure biometrics in the future. ITDMs in some sectors are especially concerned, such as in FMCG where 52 percent share this same level of apprehension.

FIGURE 13: HOW CONCERNED ARE THOSE ITDMs WHO CAN'T PROTECT BIOMETRICS TODAY ABOUT PROTECTING BIOMETRICS IN THE FUTURE?



What's on the agenda for ITDMs?

9/10 ITDMs plan to change their outlook on security strategy in response to Big Data & Data Privacy concerns.

46% Say biometrics is already here or will be in next 12 months

Strategic Outlook on Investment Priorities and Consumption Models

IT Security Investments Triggered by Data Privacy and Big Data Challenges

With so much industry discussion surrounding the specific challenges of data privacy and securing big data, the survey took the opportunity to validate the assumption that ITDMs were busy planning their response. The result was a resounding 'yes', with only a small minority (around 10 percent, respectively) claiming they had no such plans. For data privacy in particular, respondents were more bullish toward making investments to address the issue than to rethink existing strategy.

FIGURE 14A: REACTIONS TO THE BIG DATA / DATA ANALYTICS TREND (BY REGION)

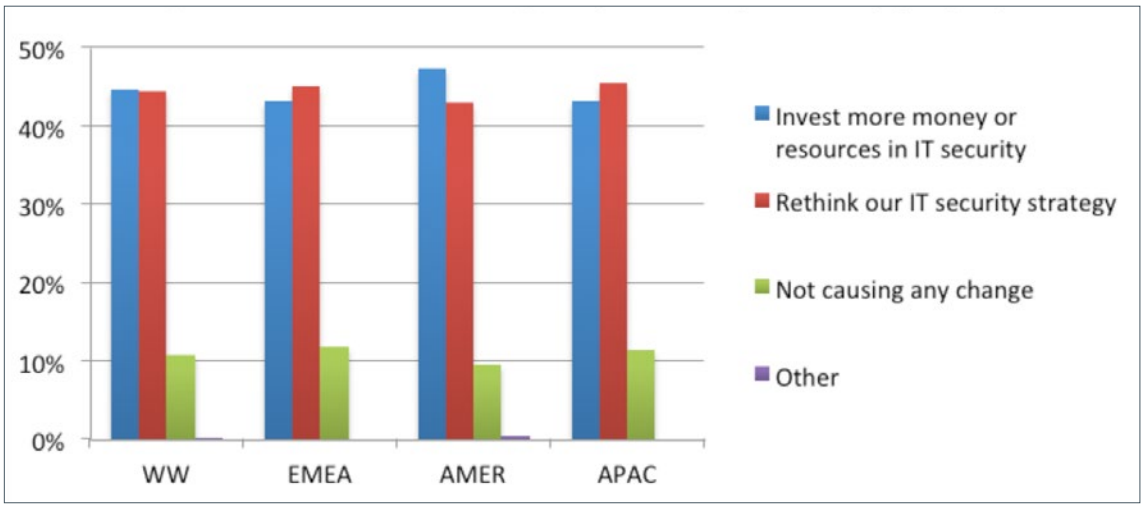
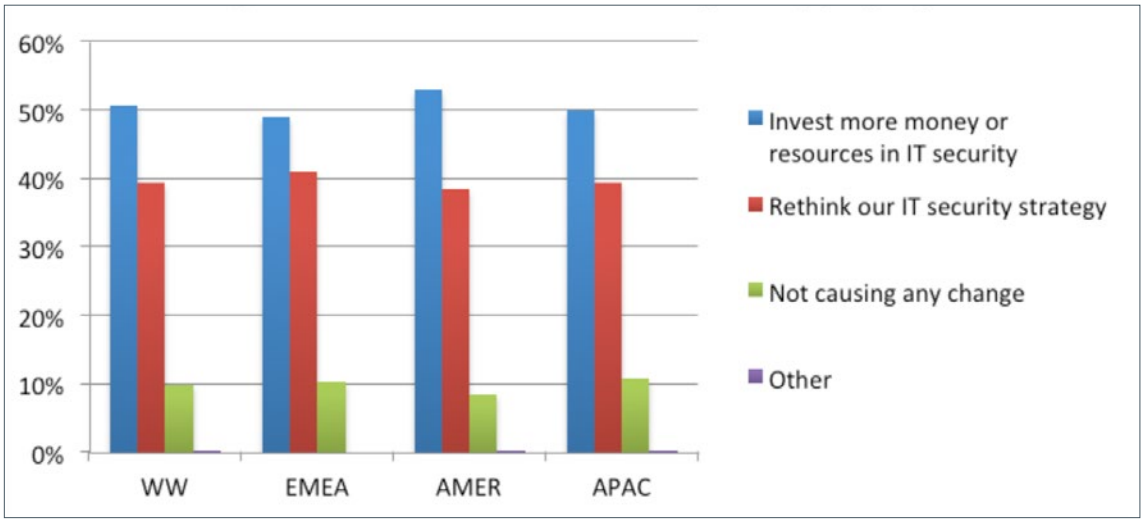


FIGURE 14B: REACTIONS TO THE DATA PRIVACY TREND (BY REGION)

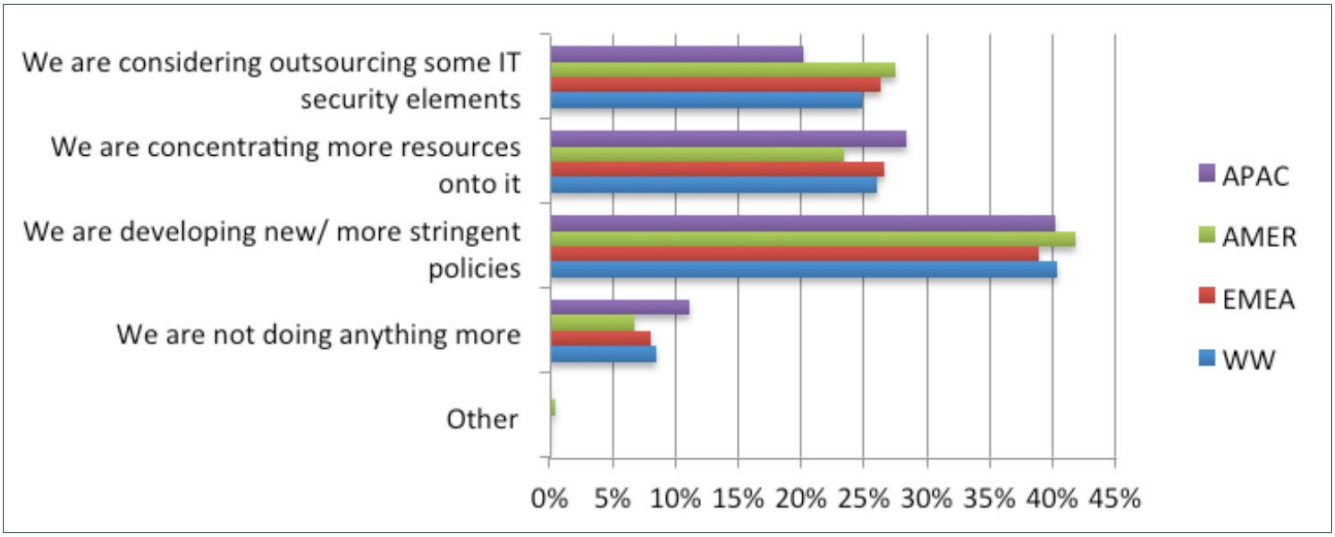


The largest companies were more inclined to invest more money and human resources than smaller counterparts. Taking the example of Big Data, 47 percent of 2000+ employee organizations agreed with the investment approach and 40 percent preferred instead to rethink strategy. For organizations in the 500-999 employee bracket, it was 42 percent for investment and 47 percent for strategy rethink.

More Resources Not Always Best for Combating Worsening Threat Landscape

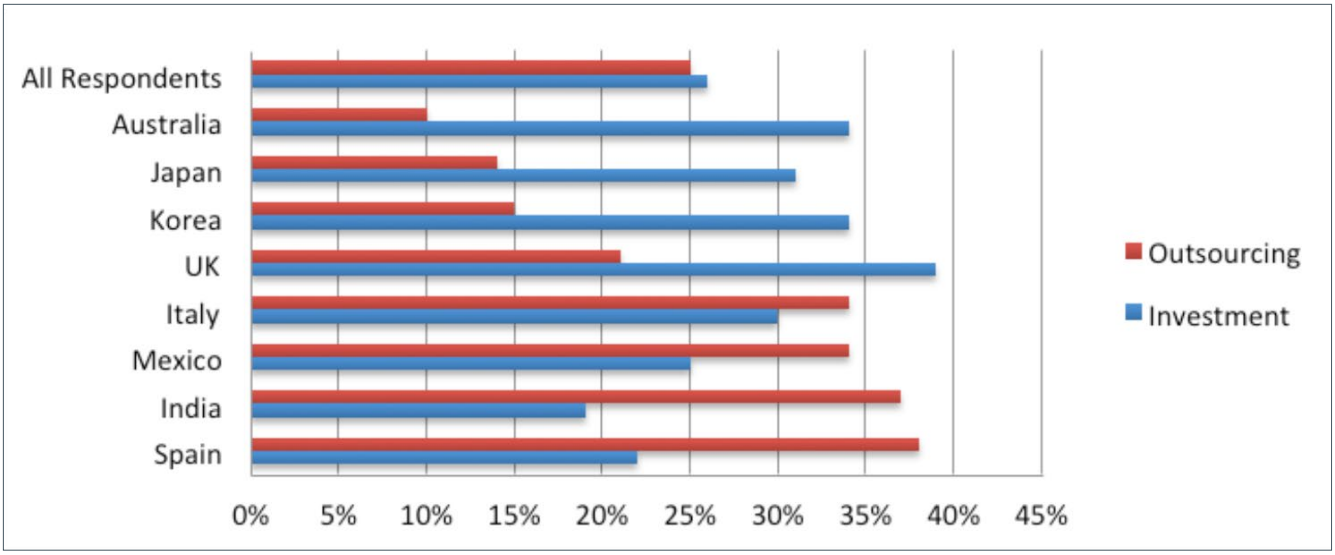
When asked to identify the single most important initiative for confronting rising threat volume/complexity, only 26 percent said that they would concentrate more financial and human resources on it. The figure is particularly compelling given we have already established that the overwhelming majority of ITDMs concur with the view that they have sufficient financial and human resources available to them to address their IT security challenges. Almost the same proportion (25 percent) argued for outsourcing some if not all IT security functions to a third party managed security service provider (MSSP). 40 percent were in favor of developing new/more stringent policies as their choice.

FIGURE 15: VIEWS DIFFER ON THE BEST APPROACH TO COMBATING THE WORSENING THREAT LANDSCAPE



The predisposition toward managed security services is greatest in Spain (38 percent) where ITDMs rank it their number one option. By contrast in Australia, where respondents were overwhelmingly in favor of investing more resources, only 10 percent opted for the MSSP route.

FIGURE 16: TOP COUNTRIES CHOOSING THIRD PARTY SECURITY OUTSOURCING / INVESTMENT AS THE BEST WAY TO COMBAT WORSENING THREATS

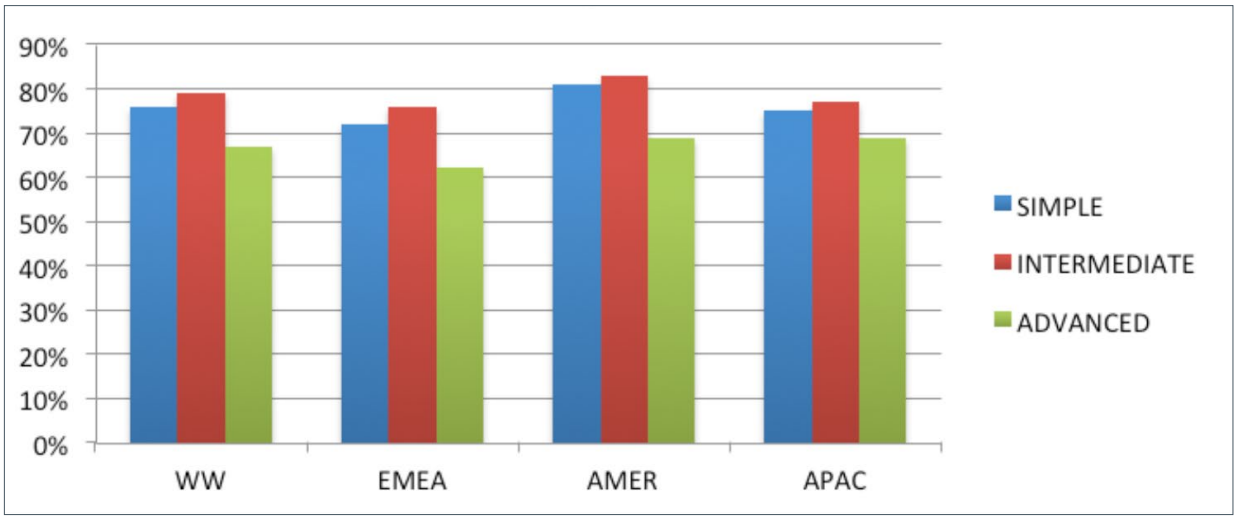


Outsourcing Trends Embrace Complex Security Capabilities

Our survey found that only a minority of ITDMs believes that even the most advanced IT security functions are unsuitable for outsourcing to a managed security service provider. That's the conclusion from having asked each respondent to qualify the suitability of individual security functions for their organization. In the figure below we've placed these functions into three groups appropriate to their complexity of operation:

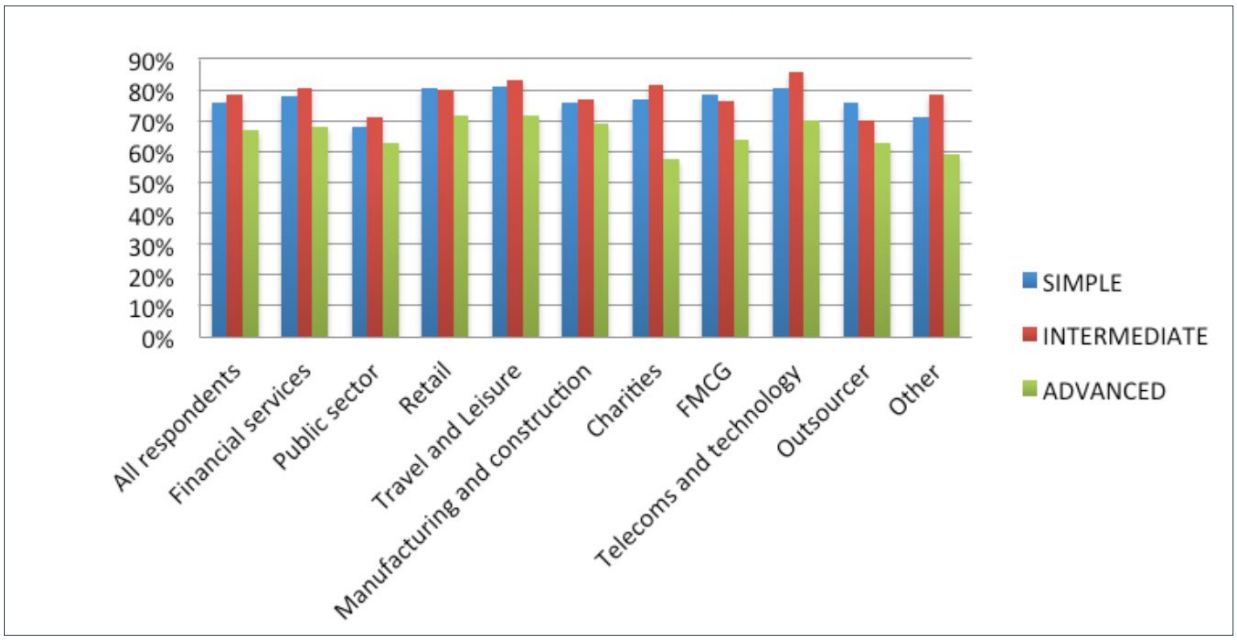
- Simple (stateful firewall, email AV/antispam, IPS)
- Intermediate (web application firewall, authentication, wireless security)
- Advanced (ATA sandboxing, DDoS mitigation).

FIGURE 17: PERCEIVED SUITABILITY FOR OUTSOURCING OF CRITICAL IT SECURITY FUNCTIONS



Perceptions differed across vertical sectors, with ITDMs from the financial services and retail sectors more likely to agree with the suitability of functions for managed security services than those from the public sector by around 10 percentage points in each case.

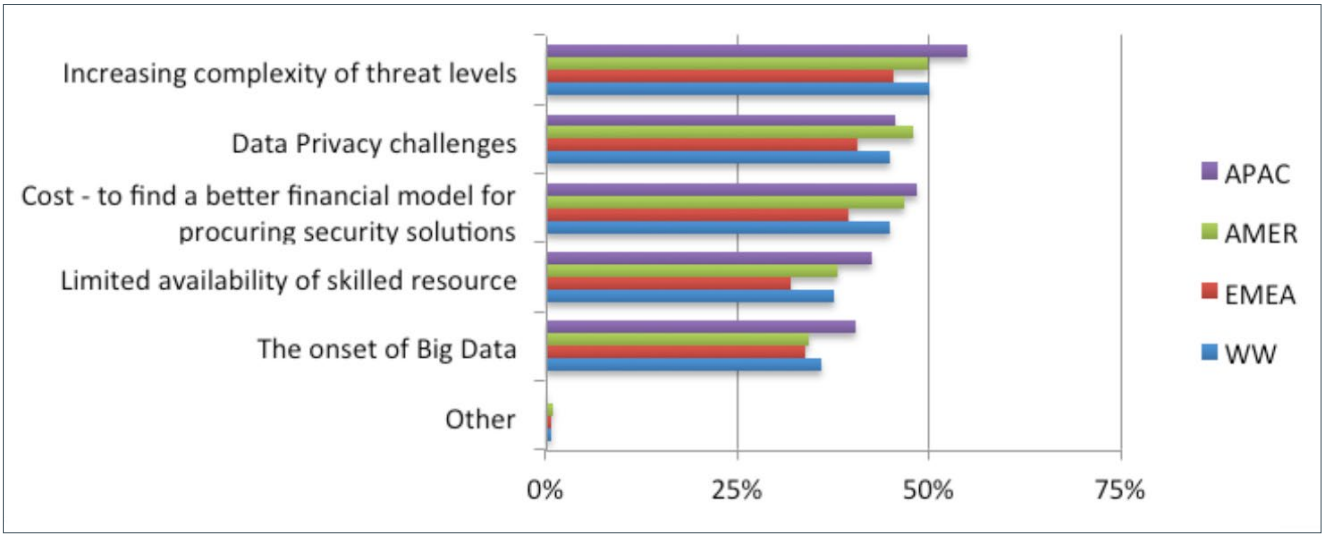
FIGURE 18: PERCEIVED OUTSOURCING SUITABILITY OF IT SECURITY FUNCTIONS (BY SECTOR)



ITDMs Reveal Potential Drivers to Outsourcing and MSSP Selection Criteria

Respondents chose a variety of influencing factors for future decisions around managed security services, with the increase in threat complexity measuring the largest with half of all respondents selecting this as a factor. This was closely followed by data privacy challenges (45 percent), better financial models for procuring security (45 percent), a lack of sufficiently skilled internal resources (38 percent), and the onset of Big Data (36 percent).

FIGURE 19: TOP DRIVERS FOR FUTURE DECISION TO ADOPT MANAGED SECURITY SERVICES



The picture was less uniform geographically speaking, with examples of each factor being chosen as the top driver in individual countries. For example, Australian ITDMs made better financial models (49 percent) their top driver; Brazilian ITDMs put lack of internal resources (44 percent) first; German ITDMs said data privacy challenges (50 percent) were the biggest reason; while respondents in the UK (42 percent) and the US (57 percent) chose 'the onset of big data' and 'increasing complexity of threat levels', respectively.

The harsh reality of IT security

53% ITDMs have paused innovative initiative due to cybersecurity fears

25% consider outsourcing security to an MSSP the optimum initiative to combat growing threats

Despite the lack of emphasis ITDMs put on their own organization's reputation/s (see Figure 6), they appear to greatly value the reputation of potential security outsourcers. Respondents called out 'reputation in the enterprise market' as the attribute of highest-ranking importance for selecting a MSSP with a mean score of 2.15 when asked to rate 1-5 (no.1 being the highest rank).

FIGURE 20: MOST ATTRACTIVE ATTRIBUTES OF A POTENTIAL MSSP

Attribute	Mean Rank 1-5 (1 Highest, 5 Lowest)
Reputation in the enterprise market	2.15
Portfolio of services offered	2.56
Global scale of organization	2.67
Reliance on the SLA offered	2.67
Other	4.41

Conclusion

Where once the topic of IT security was technically obscure, and of little interest to the running of a large organization's business operations, today we know that boardroom executives are very interested, involved and concerned about providing sufficient resources to their IT people to keep the business secure.

While survey findings indicated that these interventions could have a counterproductive effect in overcoming the IT challenges, this is counterbalanced by the positive benefits of boardroom executives' involvement into IT security. The vast majority of ITDMs in our research were seemingly content with the resource levels that they are being provided with to address IT security needs both now and in the future.

What exactly to do with these resources was not fully interrogated by this research, but what was made consistently clear were the major priorities of data privacy and big data as well as coping with the increasingly complex and aggressive threat landscape. Investment will be a significant part of addressing their objectives – particularly in respect of data privacy.

One emerging strategy appears to be the outsourcing of security capabilities to managed security service providers. Perhaps emboldened by their adoption of many other cloud services, ITDMs implied a positive acceptance that many kinds of security function – included advanced level functions – were suitable for outsourcing. This will be an interesting trend to track, with all indications pointing to its upward trajectory.

Another finding for closer examination in the future is the worrying response to our question about stalling innovation because of security worries. While the process of testing boundaries is a natural and positive part of innovation, the fact that more than half of respondents said they paused or even abandoned important business initiatives is not good news. It was not surprising to see that those ITDMs seeing the biggest internal pressure from boardroom bosses were the most likely to be scared off innovation.

IT professionals are valuable because they drive innovation into the business, not merely because they supervise the machinery of data and communications technology. IT security should be flexible, intelligent and resilient enough to always say 'yes' to innovation, rather than 'no'.

Such resilience only comes through commitment to a cohesive lifecycle approach that confronts all the many facets of today's cyber threats. This allows enterprises to grow, take advantage of new technologies, be compliant to regulatory requirements and forever remain trustworthy in the eyes of their market.

Note on Methodology

The Fortinet Security Census 2014 was a research exercise undertaken in August 2014 on behalf of Fortinet by the independent market research company Lightspeed GMI. The survey polled 1,610 qualified IT decision makers (ITDMs) including CIOs, CTOs, IT Directors and Heads of IT working at organizations with *500+ employees around the world.

Fifteen countries participated in the survey: Australia, Brazil, Canada, China, Colombia, France, Germany, India, Italy, Japan, South Korea, Mexico, Spain, UK and USA. Specifically, 100+ participated in each country except for the US where there were 201 respondents. Respondents were recorded from across industry sectors.

Respondents were sourced from Lightspeed GMI's online panel; recruited, managed and validated with stringent checkpoints throughout the respondent lifecycle to ensure valid, high-quality responses. Screening included job title, role within business, earnings, responsibilities and purchase decision-making of respondents, and the industry sector and number of employees of the organizations they work for.

* 92 percent of respondents were from this sized group of organizations, the rest from the 100-500 employees bracket.

About Fortinet

Fortinet (NASDAQ: FTNT) protects networks, users and data from continually evolving threats. As a global leader in high-performance network security, we enable businesses and governments to consolidate and integrate stand-alone technologies without suffering performance penalties. Unlike costly, inflexible and low performance alternatives, Fortinet solutions empower customers to embrace new technologies and business opportunities while protecting essential systems and content.

www.fortinet.com

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480