FORTINET

2017 GLOBAL ENTERPRISE SECURITY SURVEY

CYBERSECURITY CHALLENGES FACING EVERY IT PROFESSIONAL - HOW ARE ATTITUDES TOWARDS CYBERSECURITY IN BUSINESS CHANGING?

At the time of writing, the dust is just settling on yet another high-profile data breach. A US credit report company experienced a attack between May and July 2017, in which hackers got away with the data of 143 million Americans.

By the time you read this, another equally catastrophic security breach may well have befallen another major business. They're happening all the time. And for every step forward businesses take in their hack defenses, cybercriminals take two.

To avoid more compromised customer data and boardroom casualties, organizations need to ask themselves some hard questions. Is the board truly committed to IT security? Have recent security breaches really changed security focus, spend and culture? Where has investment been and has it been in the right place?

These are the questions which Fortinet aims to answer through its 2017 global survey on the changing attitudes towards cybersecurity in business.

KEY FINDINGS

THE MAJORITY OF BUSINESSES HAVE EXPERIENCED A SECURITY BREACH IN THE PAST TWO YEARS

85% of the businesses surveyed (Figure 1) have been victims of a security breach in the past two years. Malware and ransomware are the most prevalent threats, with 47% of organizations having experienced an attack of that kind (Figure 1), and 50% of respondents still viewing them as one of their top three risks today (Figure 1).

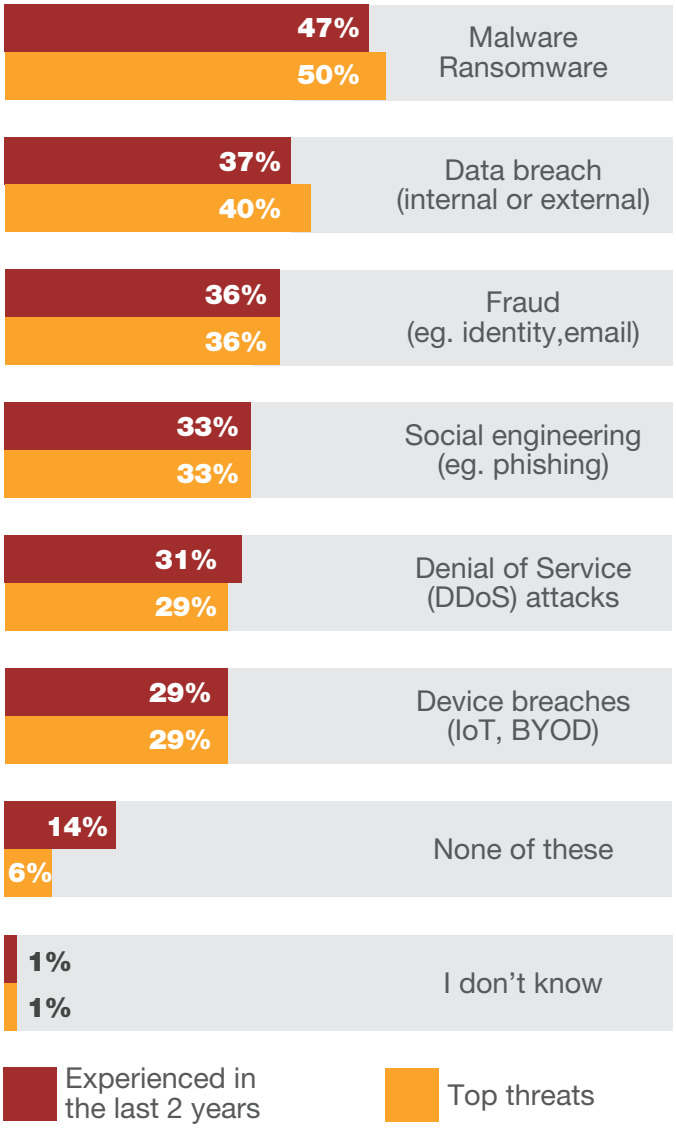

FIGURE 1:
SECURITY BREACHES

CYBERSECURITY HAS BECOME A SIGNIFICANT IT INVESTMENT TO BUSINESSES

Unsurprisingly, given the scale and impact of the cybersecurity threat, IT security has become a key investment to businesses as part of their IT strategy. According to the survey, three out of every five (61% - Figure 2) spend 10% or more of their IT budget on security. And 71% spend more than they did one year ago (Figure 3).

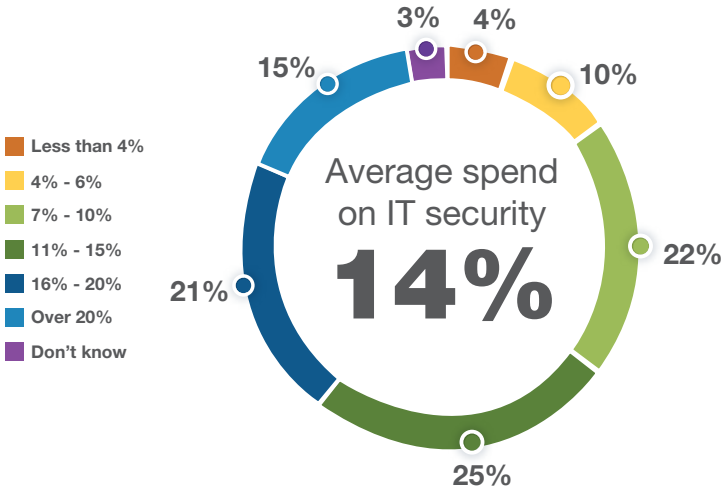

FIGURE 2: % OF IT BUDGET SPENT ON SECURITY

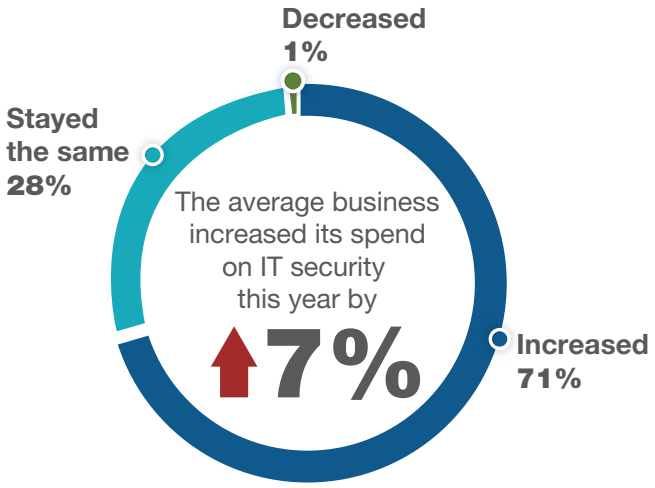

FIGURE 3: CHANGE IN IT BUDGET OVER LAST YEAR

While businesses for the most part invest in keeping solutions up to date (67% in 2017 – Figure 4), there is also more expenditure being made in new security solutions and services, perhaps reflecting the ever changing nature of security threat. 60% invested in new security solutions and services in 2017 and 56% expect to do so in 2018 (Figure 5).

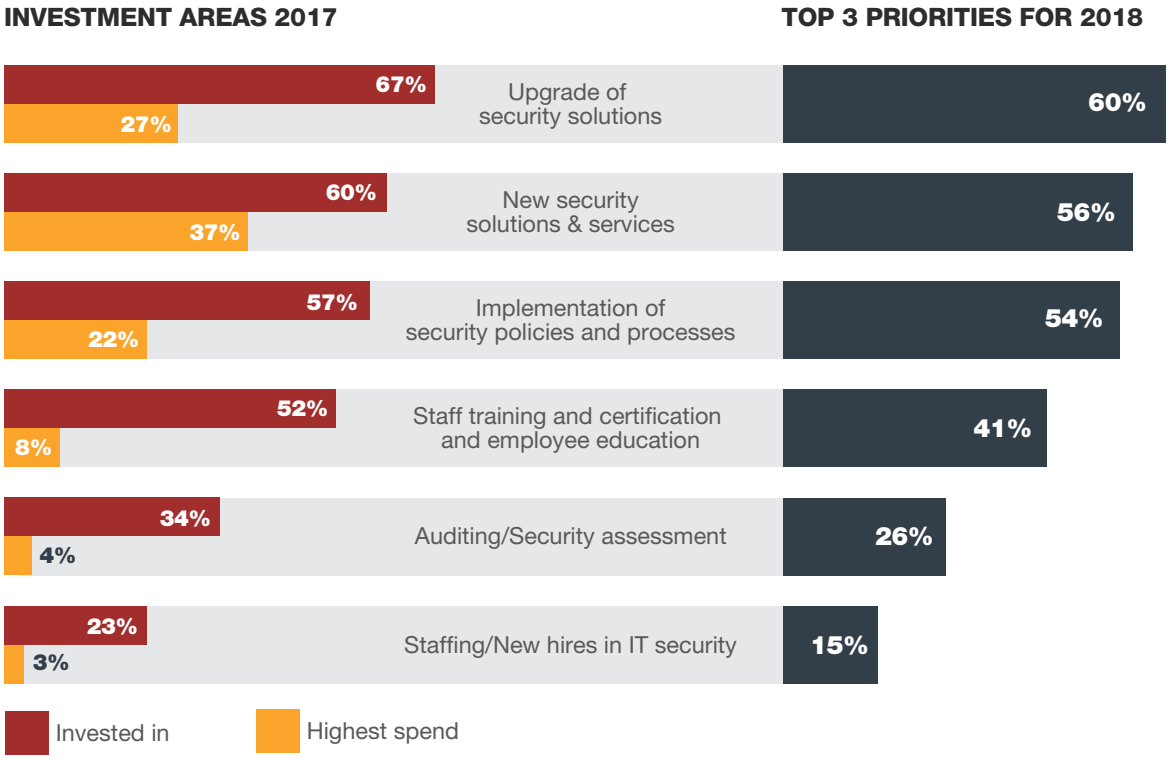

FIGURE 4: INVESTMENT AREAS IN 2017

FIGURE 5: TOP 3 PRIORITIES INVESTMENT IN 2018

BOARD MEMBERS ARE NOT MAKING CYBERSECURITY A SIGNIFICANT ENOUGH PRIORITY

And yet, in spite of a clear and present threat, 48% of IT decision makers believe that cybersecurity is still not a top priority discussion for the board. In fact, the security agenda appears to be essentially reactive. According to the survey, increases in cybersecurity investment comes either in the wake of global cyberattacks like WannaCry (49%) or to comply with government regulations (34%). We can expect that these drivers of board awareness to become more prominent – especially with the passage of the General Data Protection Regulation in the EU, which will go into effect in 2018.

According to respondents, the board appears to be more involved in post-breach management than prevention – only taking action as a result of security breaches in 93% of cases (Figure 6) with the vast majority (77% - Figure 6) wanting to know what happened, i.e. identifying the cause of the breach and reviewing IT security processes while two-thirds (67% - Figure 6) want to review or increase the budget in response.

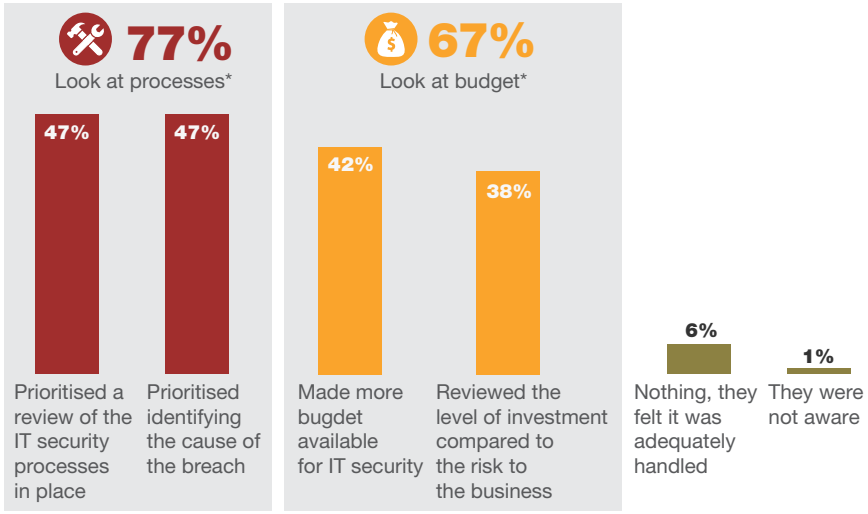

FIGURE 6: BOARD REACTION TO BREACHES

**A net is the total number of people that chose at least one of the answers included in the net. As the question is a multiple choice, nets are different from the sum of the single answers they include (people who chose two or more answers included in the same net are not double-counted).*

The stats lead to the conclusion that boards only take action when things go wrong, and that there might be a blame culture around IT security. Indeed, in 70% of breach incidents (Figure 7), the board blames IT – either a specific individual or the department as a whole – while only 60% recognize inadequate investments (Figure 7).

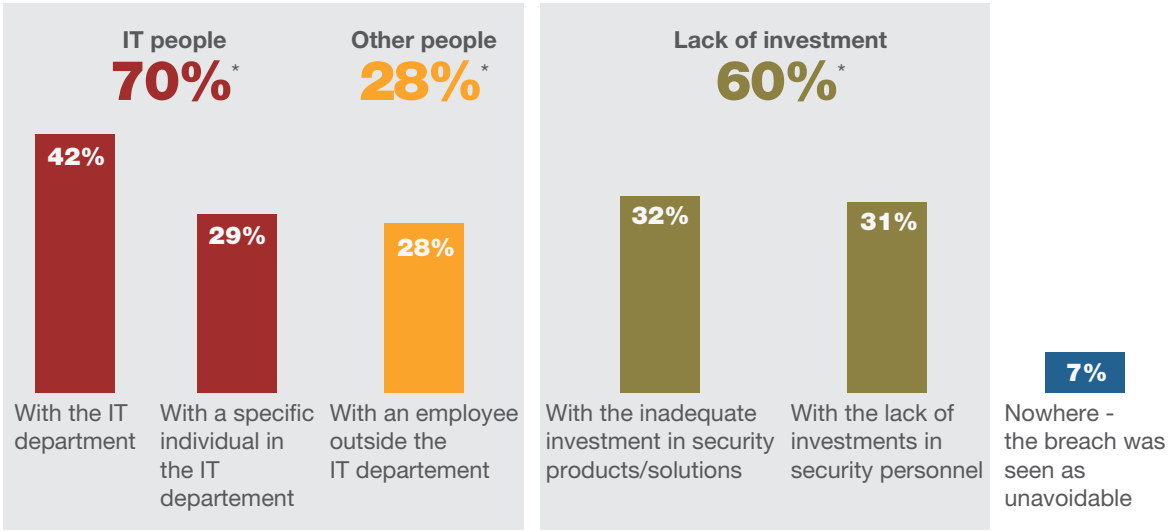

FIGURE 7: PERCEIVED RESPONSIBILITY FOR BREACH

**A net is the total number of people that chose at least one of the answers included in the net. As the question is a multiple choice, nets are different from the sum of the single answers they include (people who chose two or more answers included in the same net are not double-counted).*

As a result, IT decision makers feel strongly that cybersecurity should become a top management priority with 77% of the respondents saying that the board should actually put IT security under greater scrutiny.

TRANSITION TO THE CLOUD IS GETTING BOARD'S ATTENTION

Fortunately, the future isn't all doom and gloom. In fact, the digital transformation journey that so many businesses are on may eventually result in a greater focus on cybersecurity.

A key driver behind this is that the business benefits of migrating key applications and data to the cloud are so clear that 77% of IT professionals believe the transition to the cloud is a priority for the board. The end result is that 74% of respondents believe that migration to the cloud will make cloud security a growing priority in the future. This trend is actually supported by the fact that, today, only 37% of respondents (Figure 8) say the cloud security emerges as the most disregarded area when it comes time and/or resource allocation. As a result, half of businesses (50%) surveyed are already planning investment in cloud security over the next 12 months.

This is a clear call to arms for IT professionals everywhere. The cloud already has the board's attention – this is opportune moment to ensure that cybersecurity in general is on the agenda as well.

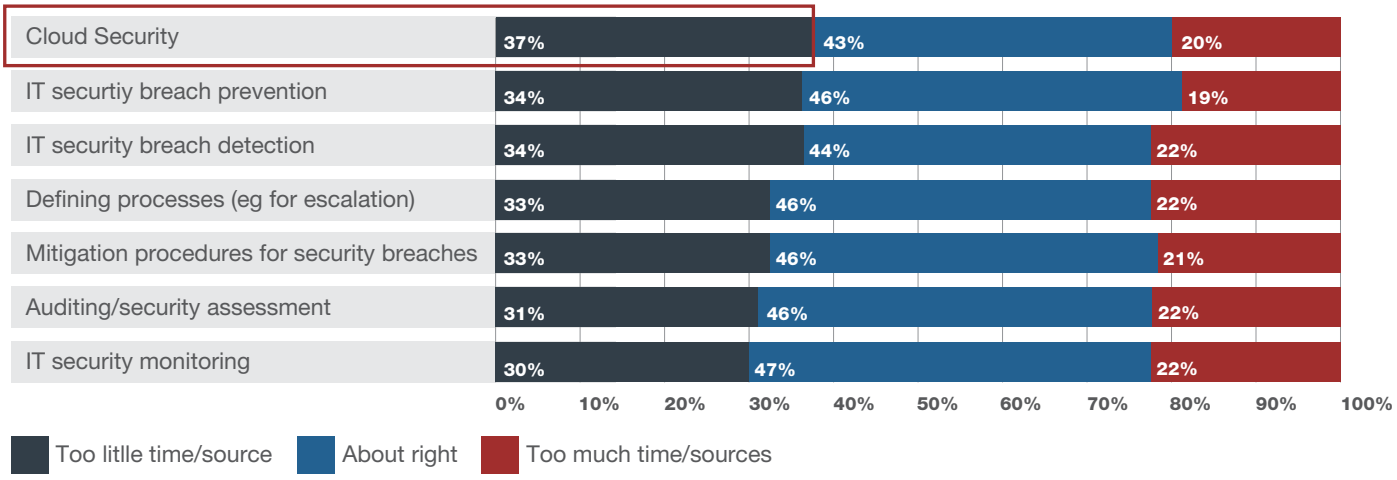

FIGURE 8: ORGANIZATION'S COMMITMENT

ORGANIZATIONS ARE COMPLACENT ABOUT THEIR CYBERSECURITY POSTURE

Over half (53% - Figure 9) of organizations surveyed rate their current IT security as either good or excellent. Nearly three-quarters (72% - Figure 9) believe they are doing better than their peers. Barely one in twenty (6% - Figure 9) cybersecurity professionals believes they are lagging behind.

That can't be right, can it?

With so many organizations experiencing security breaches, some of these organizations must be overestimating how protected they are. Major attacks such as WannaCry and NotPetya targeted existing weaknesses that, for most, could have easily been secured. Yet, whether due to overconfidence or complacency, they weren't.

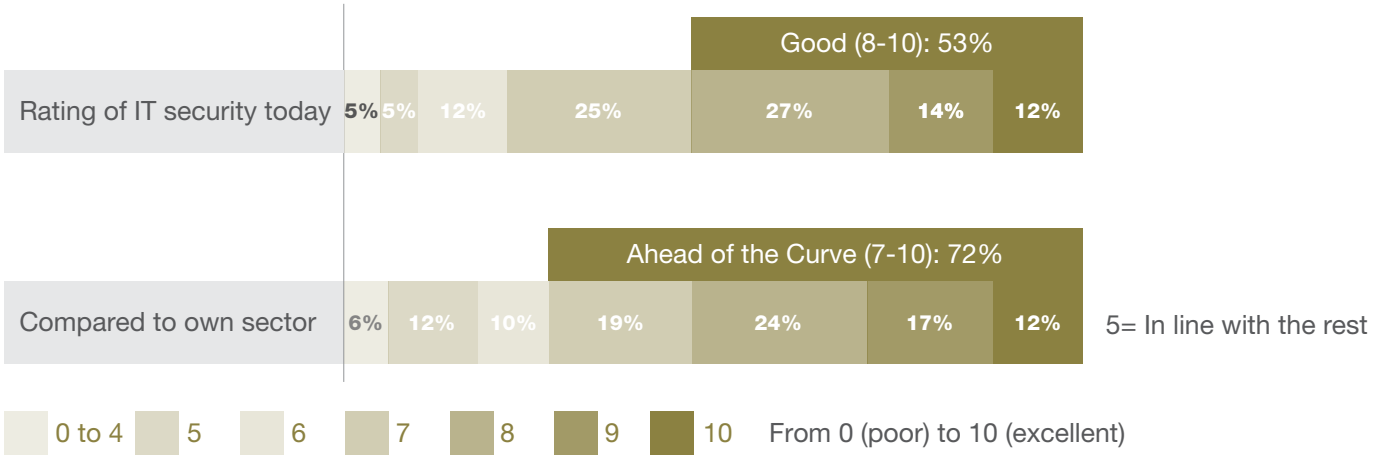

FIGURE 9: RATING OF THEIR ORGANIZATIONS'S IT SECURITY

Worryingly, the research shows that this complacency appears in other areas as well. As organizations adopt more and more technology, for whatever reason, the security implications associated with them seems to be treated as an afterthought. For example, through wireless, cloud and IoT there are more ways than ever to hack into a network. In this light, it's surprising to see that only 24% of IT professionals are planning to segment their network in 2018. Effective internal segmentation can limit lateral movement across a network during an attack, confining the breach to a specific area and minimizing potential data loss. In the upcoming General Data Protection Regulation (GDPR), minimizing data loss in the case of a data breach will be critical to minimize or avoid its substantial fines.

Managing access to the network is another area where organizations have fallen into complacency. Only 54% feel confident that they have adequate control and visibility over whom is allowed in the network and what resources can be accessed (Figure 10). Being able to track and manage network access policy is a fundamental aspect of cybersecurity, especially in conjunction with the use of internal segmentation, but it appears that nearly half don't have a handle on it.

FIGURE 10: ITDMS CONFIDENCE LEVEL

MORE NEEDS TO BE DONE ABOUT EMPLOYEE EDUCATION

When asked about what they would have done differently over their career in security (Figure 11), 42% of IT decision makers responded (Figure 11) that they would have invested more in employee security awareness training to prevent a security breach (43% - Figure 11) and better position their organization to deal with the current IT security threat (41% - Figure 11).

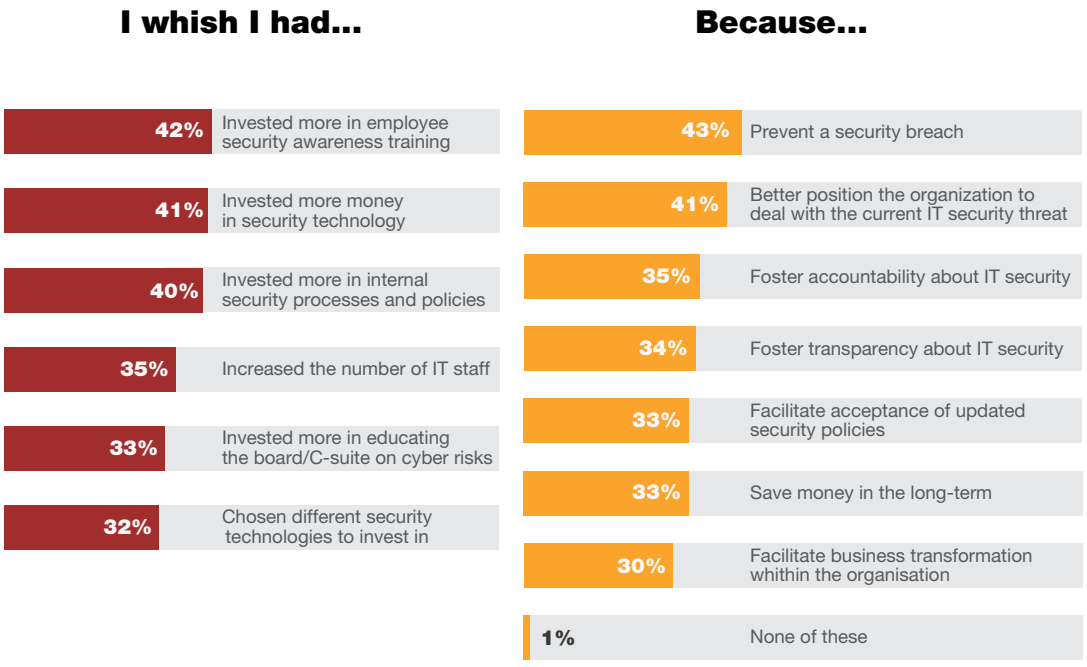

FIGURE 11: HINDSIGHT

This year, over half of organizations (52%) have invested in employee security awareness training. On a positive note, over two-thirds (67% - Figure 12) are now planning programs to educate employees about IT security.

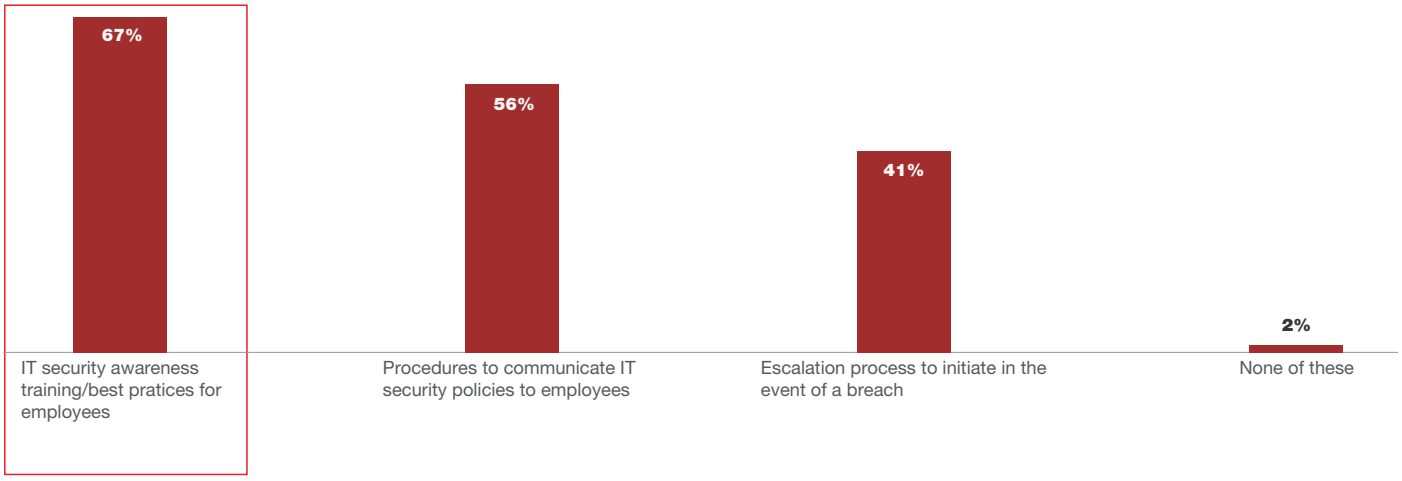

FIGURE 12: PROCEDURES AND EDUCATIONAL ACTIVITIES PLANNED FOR 2018

CYBERSECURITY IS AN ONGOING JOURNEY

According to the research, 76% of IT decision makers consider their organization is on a security journey (Figure 13), an often seemingly endless journey due to the challenges associated with securing today's enterprise network. Whether struggling to secure an ever faster network – 52% of IT professionals (Figure 13) say they have difficulty finding solutions that can keep up with the performance demands of the network – or trying to simplify the network to improve security efficacy - 54% of IT decision makers (Figure 13) say that they will need to significantly reduce the number of vendors in the network - it is clear that the challenges will multiply as the number of high profile data breaches continue to make headlines.

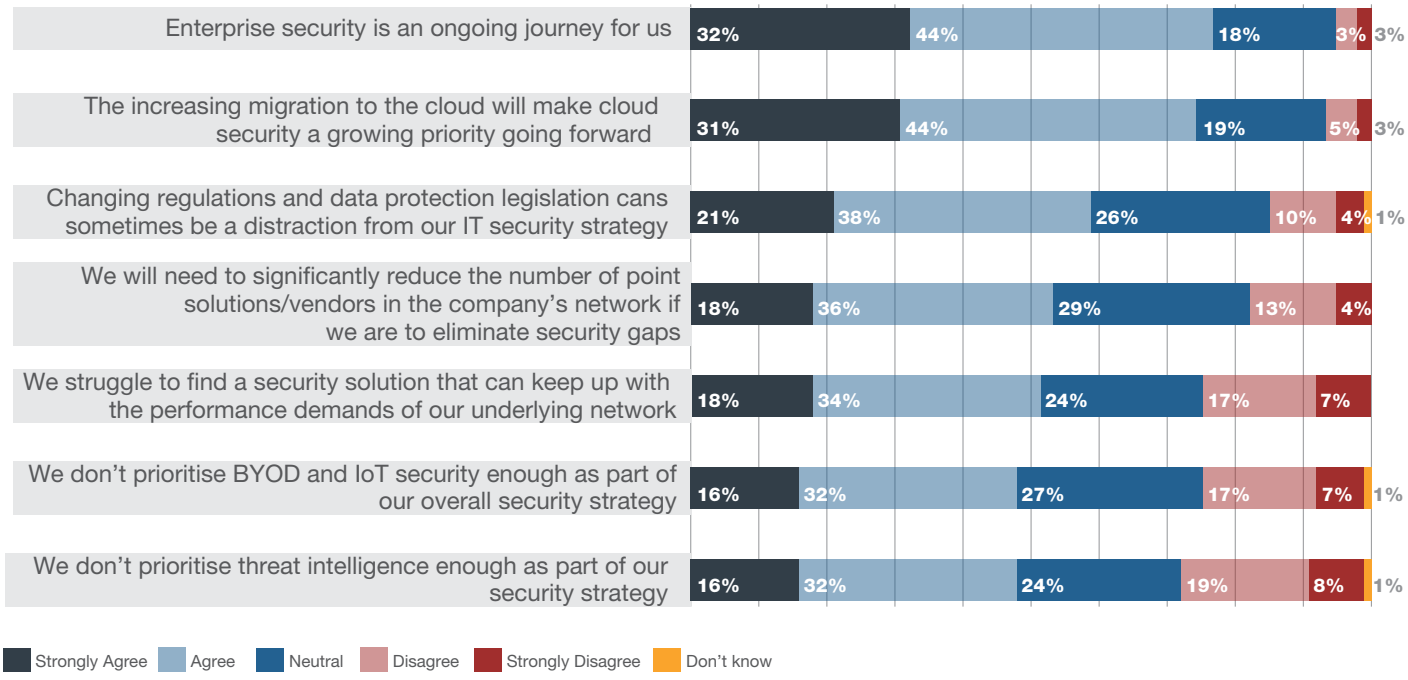

FIGURE 13: ONGOING AND FUTURE CHALLENGES

CONCLUSION

As organizations embark on their digital transformation journey, they need to rethink their business and operating models to maintain their competitive advantage. Digital transformation means businesses are embracing technologies such as the cloud, Internet of Things, big data analytics, which all increase the cybersecurity risk level and make the business environment more complex to protect.

To succeed in their digital transformation efforts, board members must make cybersecurity a strategic issue, within their broader risk management strategy, rather than a simple IT investment. And IT leaders must rethink their cybersecurity approach with a view to the following: extend visibility across the entire attack surface, control network access, segment the network to minimize potential data loss, shorten the windows for time to detection and mitigation, deliver robust performance, and automate security intelligence and management. All those aspects must be addressed to allow the organization take full advantage of its digital transformation.

RESEARCH METHODOLOGY

The Fortinet Global Enterprise Security Survey was commissioned by Fortinet and conducted in July and August 2017 by Loudhouse, an independent research consultancy headquartered in London. 1,801 IT decision makers with responsibility for cybersecurity completed an online survey on the changing attitudes towards cybersecurity in business. Respondents were sourced from 16 countries (US, Canada, France, UK, Germany, Spain, Italy, Middle East, South Africa, Poland, Korea, Australia, Singapore, India, Hong Kong, Indonesia) across a variety of sectors and industries.

ABOUT FORTINET

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 320,000 customers trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

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

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

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

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

126750 0 1 EN