Nexia International

Global Cybersecurity Report

2017

Nexia International

Table of Contents

Executive Summary

Our global economies, industries, and competitive markets require that we become progressively more interconnected to one another. On both a personal and commercial level, we are creating deep levels of connectivity between multiple communities and devices via laptops, televisions, thermostats, security systems, appliances, mobile and music devices, commercial equipment, building management systems and the list goes on. This myriad of connected devices is known as the Internet of Things (IoT).

The economic and, in many cases, security benefits of being connected to the Internet and the interconnectivity of systems, customers, employees, trading partners, and equipment are strong drivers of doing business today and remaining competitive. In the words of John Chambers, former CEO of Cisco, "...picture living in a world where everything is connected, and the possibilities that creates is limitless. The industry is on the precipice of an explosion of IoT-related products and services coming to market." The advantages of being connected to the Internet also come with risks that must be managed to insure that the economic and social advantages are not turned into a disadvantage or potentially a disaster.

The increasing interconnectivity of personal, infrastructure, and business systems, and a growing and progressively more open market for stolen data are only a few of the reasons that the landscape of cyber risk and the number of companies and individuals that are vulnerable to attack is growing at an exponential pace. Cybersecurity is big business. For example, only a few years ago the concept and perceived risk of a ransom attack was quite rare and remote; however, according to the Cisco 2017 Annual Cybersecurity Report, ransomware is growing at a yearly rate of 350%. Our interconnectedness establishes a sort of cyber supply chain that links our corporate, home, mobile and interconnected devices with the myriad of others to which we are connected. Just consider for a moment how many individual, corporate, social, shopping, and Internet connections you have on your own. Are you connected to your thermostat, lighting system, security system, garage door, refrigerator? Now imagine how many systems are connected in a business, mall, sporting facility or hospital.

Evidence shows us that organisations such as banks, government agencies, healthcare institutions and large corporations that maintain highly valuable data are more likely to be attacked more frequently than most. The reality is that no industry, location, organisation or individual is safe. As Chamber's puts it, "there are two types of companies: those who have been hacked and those that don't yet know they have been hacked." While we cannot confirm or deny this assertion, we know with certainty that hacking and data breaches are increasing in frequency and impact. This trend spans

industries and company size, and now, even organisations thought to be at low risk for a data breach are finding themselves victims of ransomware or phishing campaigns. Attacks are being carried out on a substantial scale by a myriad of actors such as hacktivists, organized crime, nation states and hobbyists. Some recent attacks of note include the ransomware "Wannacry" of 12 May 2017. Delivered via a phishing email, this attack spread throughout the world within hours, executed by inattentive users and causing damage to insufficiently patched systems. The Petya ransomware attack on 27 June 2017 was another large attack that crippled firms, airports, banks, and government departments worldwide. The reasons to attack are as widely varied as the number of perpetrators and sometimes the motivation is simply "just because we can." There are also deliberate attacks mounted by sophisticated organisations that are designed to find ways into an organisation.

Given the economic impact and potential consequences of cyber-attacks, the lack of attention to and investment in cybersecurity is an area that deserves considerable attention. According to Ponemon Institute, the average cost of a data breach is $3.62 million USD, which equates to an average of $141 USD per lost or stolen record.[1] These are merely the direct costs (i.e., lawyers, notifications, consultants, etc.) and do not reflect the lack of consumer confidence that would arise. When large, publicly traded organisations are breached, their stock price will likely be impacted, but they frequently have the resources to recover. A small or mid-size organisation may not be so lucky.

Nexia International conducted a global survey to assess the current state of cyber preparedness. A core goal of the survey is to provide insight on how organisations view cyber risk and what they are doing about it, and how organisations are providing executive management with the data they need to avoid or at least mitigate a security event.

Our analysis of survey responses indicates that there is still considerable education and investment required to reduce the level of cyber risk and improve organisational preparedness and responsiveness across most industries and geographies. There also appears to be a significant need for many organisations to improve their overall understanding of the cybersecurity risk landscape. The following summarizes our key observations:

- Only 39% of respondents consider cybersecurity a top concern.

[1] 2017 Cost of a Data Breach Study – Global Overview. Benchmark research sponsored by IBM Security and independently conducted by Ponemon Institute LLC, June 2017.

- 46% of respondents across the Americas and 50% of the respondents in EMEA do not have a formal cybersecurity program. 76% of APAC respondents indicated that they have a formal cybersecurity program.
- 50% of respondents indicated that hacktivists, organized crime, and employees – both current and former – are the sources of greatest cyber risk.
- 20% of respondents have not conducted a cybersecurity assessment, and only 25% of respondents provide cybersecurity training to employees at least annually.
- 20% of respondents who are required to have a cybersecurity program based on governmental, industry or customer requirements do not currently have a cybersecurity program.
- Limited time and budget along with a lack of qualified staff were the key reasons cited for not having an effective cybersecurity program.
- More organisations that have a cybersecurity program reported experiencing a breach than those who do not have a formal cybersecurity program. However, it is the organisations that have a cybersecurity program that are more likely to identify a breach. We are unable to report on the number of breaches that go undetected.
- The majority of the respondents indicated underinvestment in advanced cybersecurity initiatives such as a robust security incident response plan to identify, detect, and handle security incidents including data breaches.

The above, taken with the rest of the survey data and responses, highlights an overall lack of intensity and awareness of the need for a comprehensive cybersecurity program. And if the rising cyber threats and increasing fines are not enough for companies to rethink their cyber programs, there are ample new regulations that may provide the needed impetus.

Perhaps the most stringent and prescriptive of these regulations is the EU's General Data Protection Regulation (GDPR), which goes into effect in May of 2018. This rule imposes very specific criteria for organisations holding EU citizens' personal data. Such requirements include appointing a data protection officer, encrypting data, adhering to stringent privacy standards, and much more. Fines in the event of a breach and demonstrated lack of compliance could result in €20 million or 4% of corporate revenues from the prior year, whichever is higher.

The United States has seen a resurgence of cyber requirements. Since 2014, the Securities and Exchange Commission has been stating that cybersecurity is one of its top concerns and has performed various "sweeps" across the financial market. Similarly, the Department of Health and

Human Services has performed site visits of healthcare organisations to assess their compliance with data protection standards and increased investigations into whether organisations are compliant.

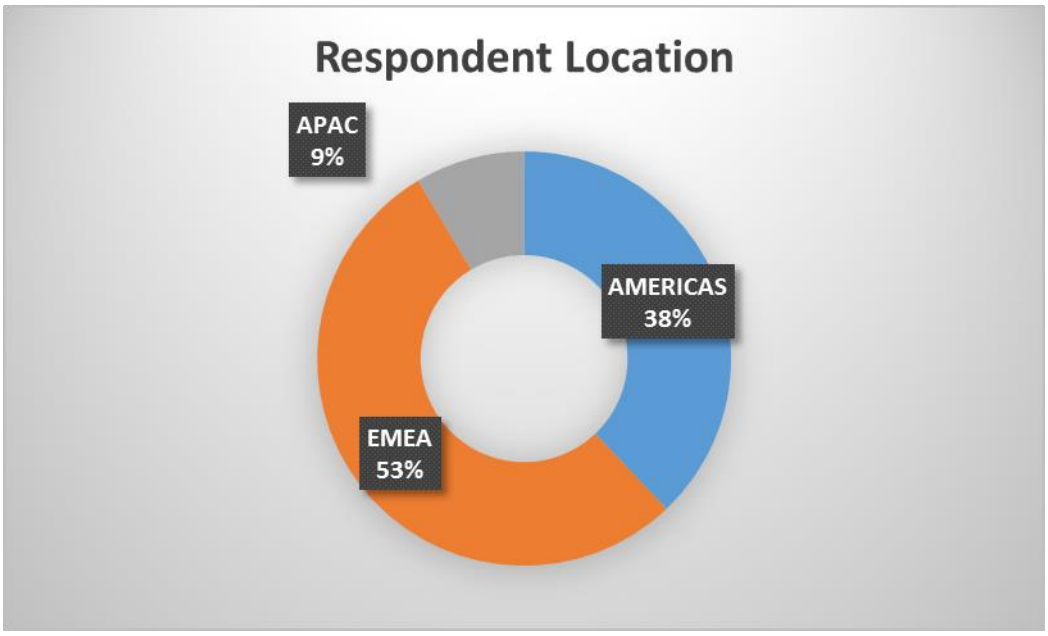
If there is any silver lining in all of this, most security experts would say that it all comes down to some basic controls and that most breaches are preventable. We know from our experience as well as reading numerous breach reports that weak passwords, poor patch and vulnerability management, and a lack of user awareness account for a vast amount of the security incidents in the news. And, regardless of whatever sophisticated tools are used by companies to prevent and detect hacking, knowledgeable security professionals with proper training and governance are still required.

Our hope is that this report will help organisations determine for themselves where they stand in relation to others and motivate them to implement cybersecurity programs that will keep the hackers at bay and their intellectual assets safe.

About the Survey

Nexia International's global cybersecurity survey[2] ("survey") was conducted among organisations across three different regions: the Americas, including North and South America; EMEA, including Europe, the Middle East, and Africa; and APAC, including countries from Asia and Australia.

Figure 1: Respondent Region



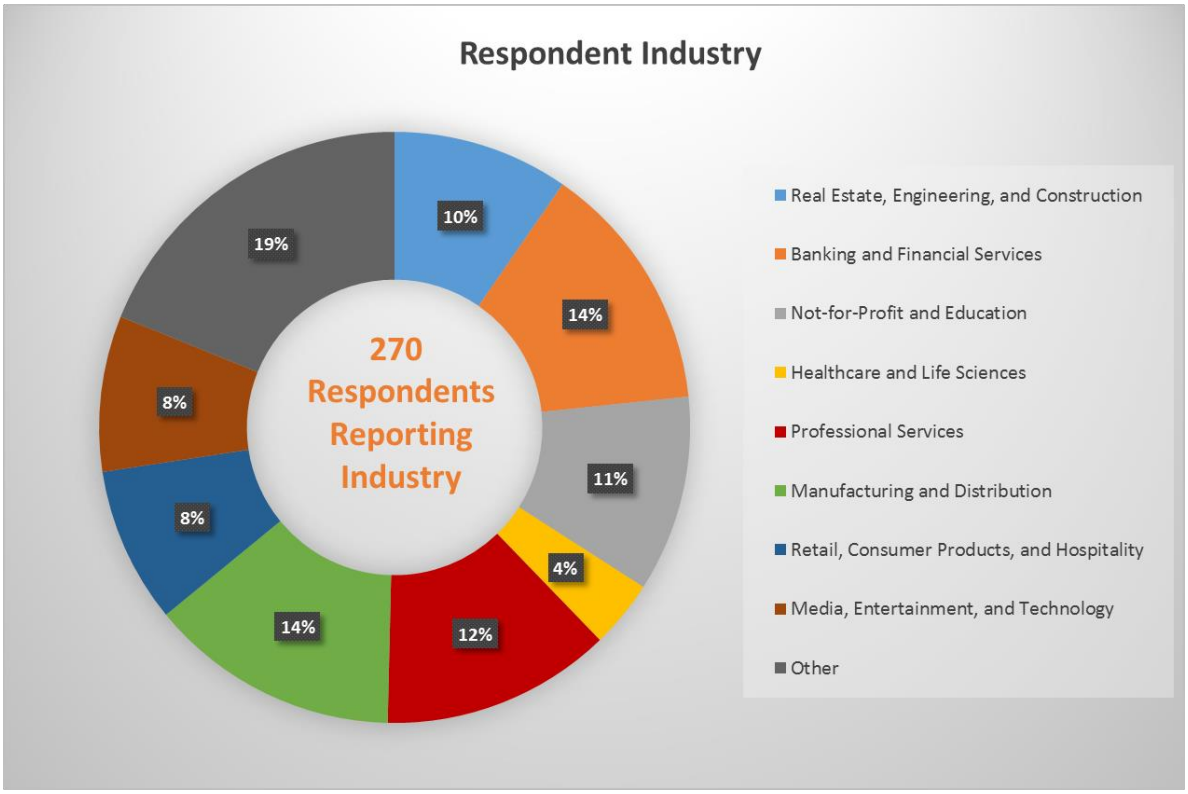
The objectives of the survey were to:

- Create a market understanding of the state of cyber practices across a broad range of organisations and industries
- Gain insight into cybersecurity concerns
- Establish a foundation of cybersecurity thought leadership information
- Increase awareness of concerns and practices related to cybersecurity

The survey was distributed via email to the respondents and was conducted between November 15, 2016, and April 30, 2017. There were more than 350 responses to the survey, but not all respondents answered every question. Respondents represented nine different industry sectors as shown in Figure 2 on the next page.

[2] The Nexia International 2017 Global Cybersecurity Survey consisted of 8 demographic questions, 14 cybersecurity practice and perception questions, 6 optional identified questions, and 1 open ended comment question.

Figure 2: Respondent Industry

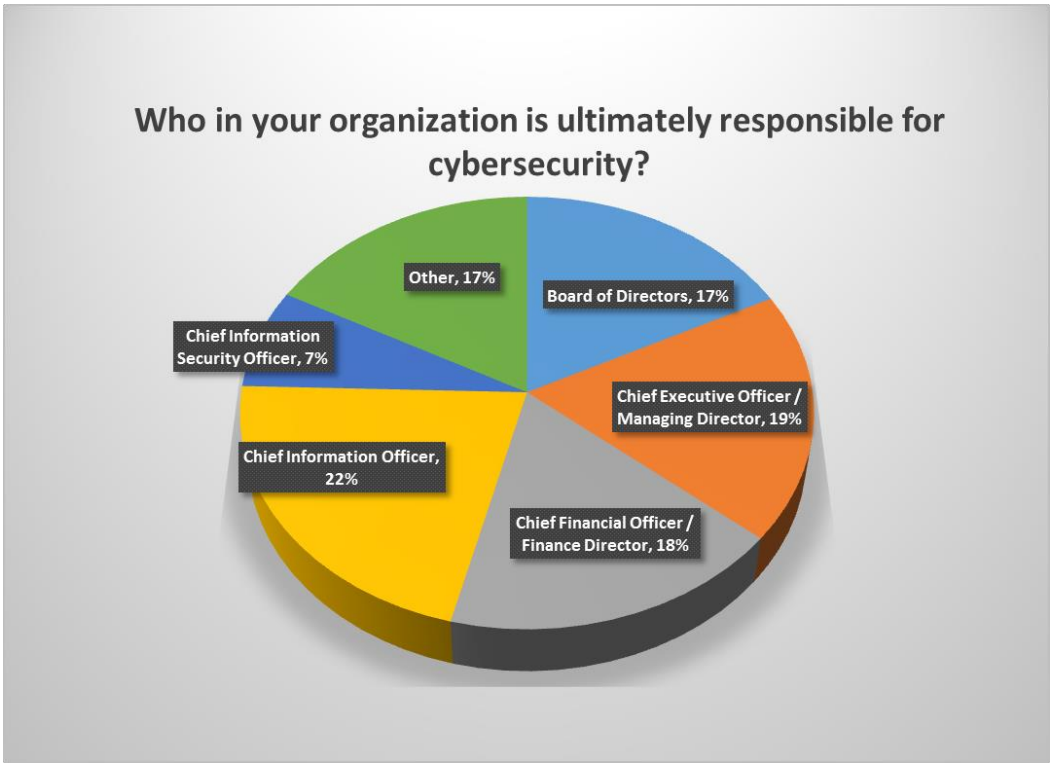


The annual turnover of respondents' organisations ranged from less than $10 million USD to greater than $1 billion USD.

Preparedness

There was no definitive identification regarding who is responsible for cybersecurity across the respondents. Responsibility for cybersecurity was spread among various leaders and included information technology (IT) and business professionals. What we did not see from the results was a high percentage of Chief Information Security Officers (CISOs) identified as having responsibility for cybersecurity programs. This is likely due to the diversity of the size of the organisations responding to the survey. We would expect only very large or even global organisations to have a CISO. It will be interesting to see if the implementation of new regulations in the European Union results in a change in cybersecurity responsibility over the next few years to the Chief Data Officer.

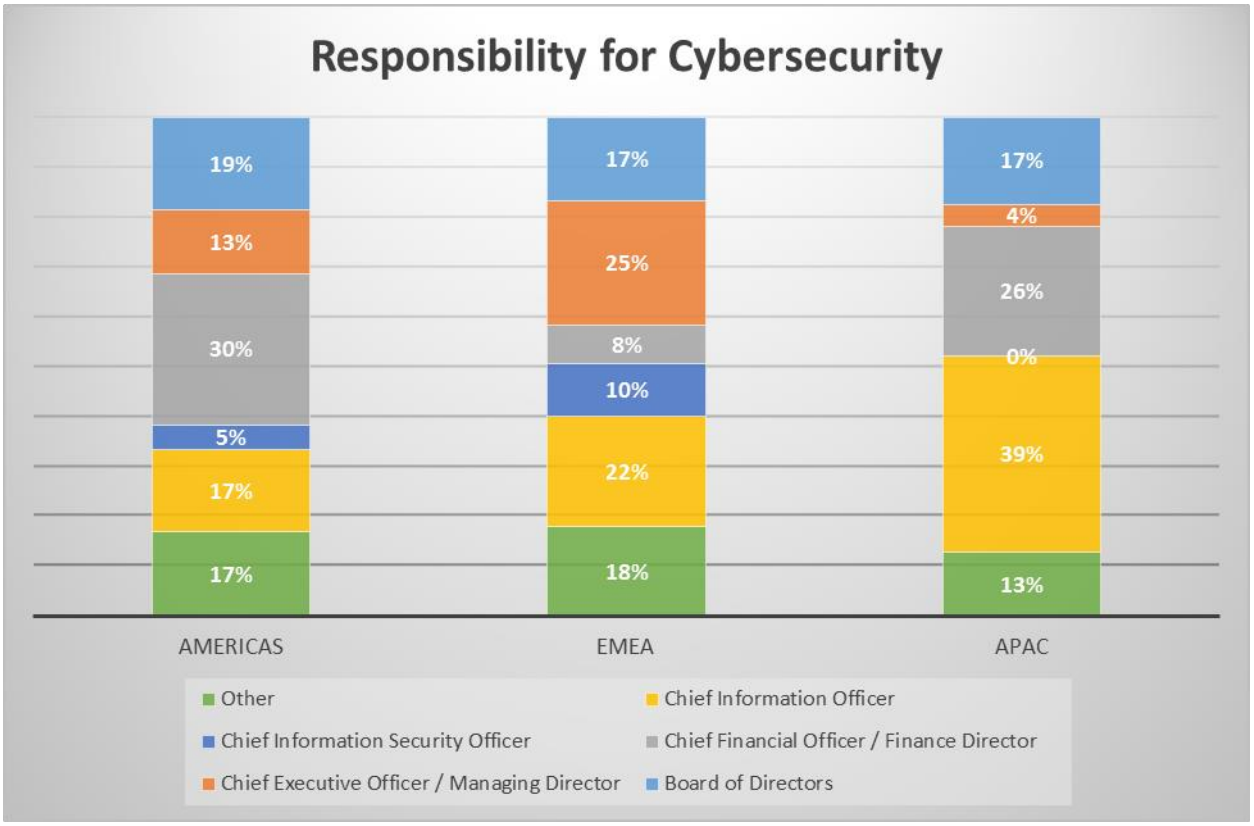
Figure 3: Who in your organisation is ultimately responsible for cybersecurity?



By Region

APAC had the highest percentage of chief information officers (CIOs) having responsibility for the cyber program, while EMEA had the greatest percentage of chief executive officers (CEOs) having responsibility. Respondents from the Americas and APAC indicated that a substantial percentage of chief financial officers/finance directors are responsible for their organisations' cyber programs.

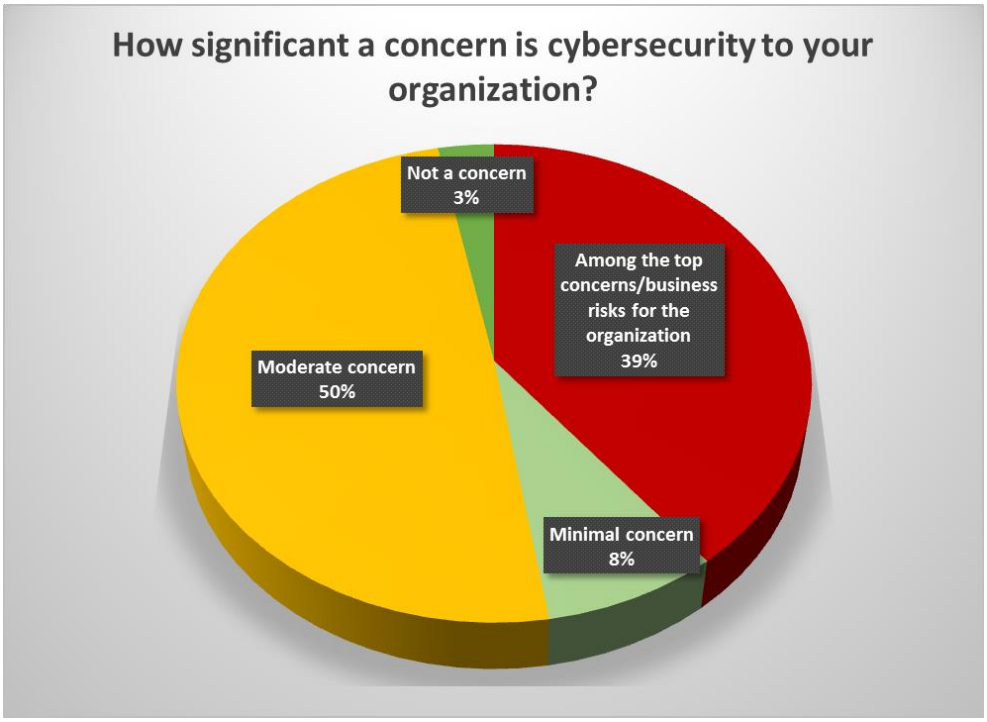
Figure 4: Regional view – Who in your organisation is ultimately responsible for cybersecurity?



Level of Concern

While nearly 90% of all respondents listed cybersecurity as either being a top or moderate concern, it is curious that only 39% listed cybersecurity among their top concerns. This calls into question whether or not there is enough concern shown to drive the development of effective and comprehensive cybersecurity programs. Organisations still need to fund and maintain their cybersecurity programs sufficiently. We will examine where organisations are spending money, as well as constraints towards maintaining or building a cybersecurity program later in this report.

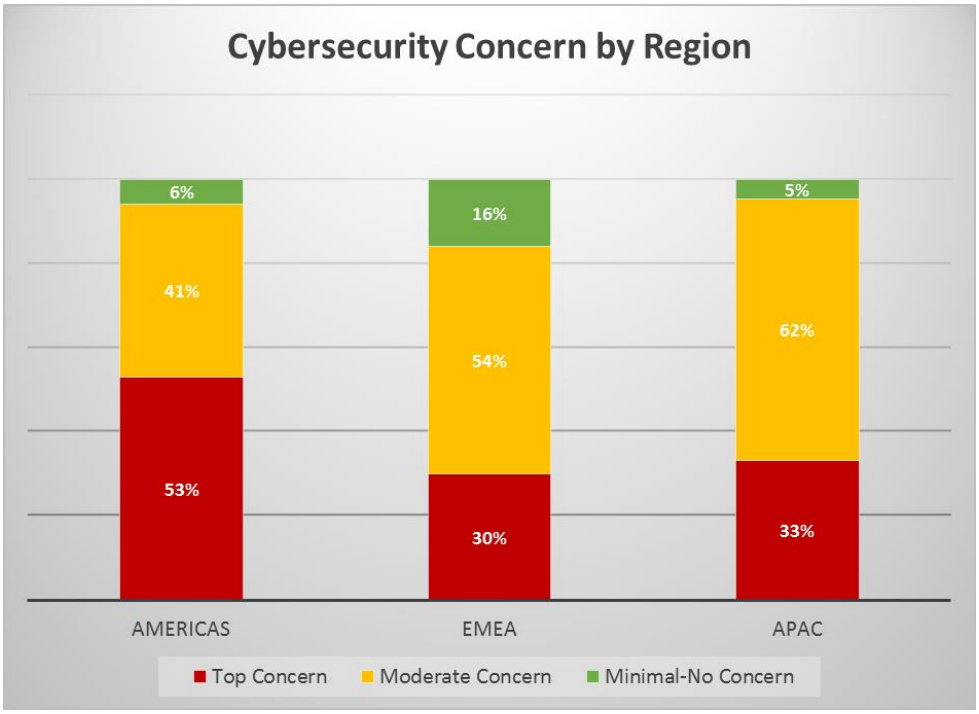
Figure 5: How significant a concern is cybersecurity to your organisation?



By Region

When comparing how much of a concern cybersecurity is by region, the Americas contrast sharply with EMEA. More than half of all respondents from the Americas cited cybersecurity as a top concern. In contrast, only 30% of EMEA respondents felt the same. This may be due to a longer history of strong data protection laws in EMEA.

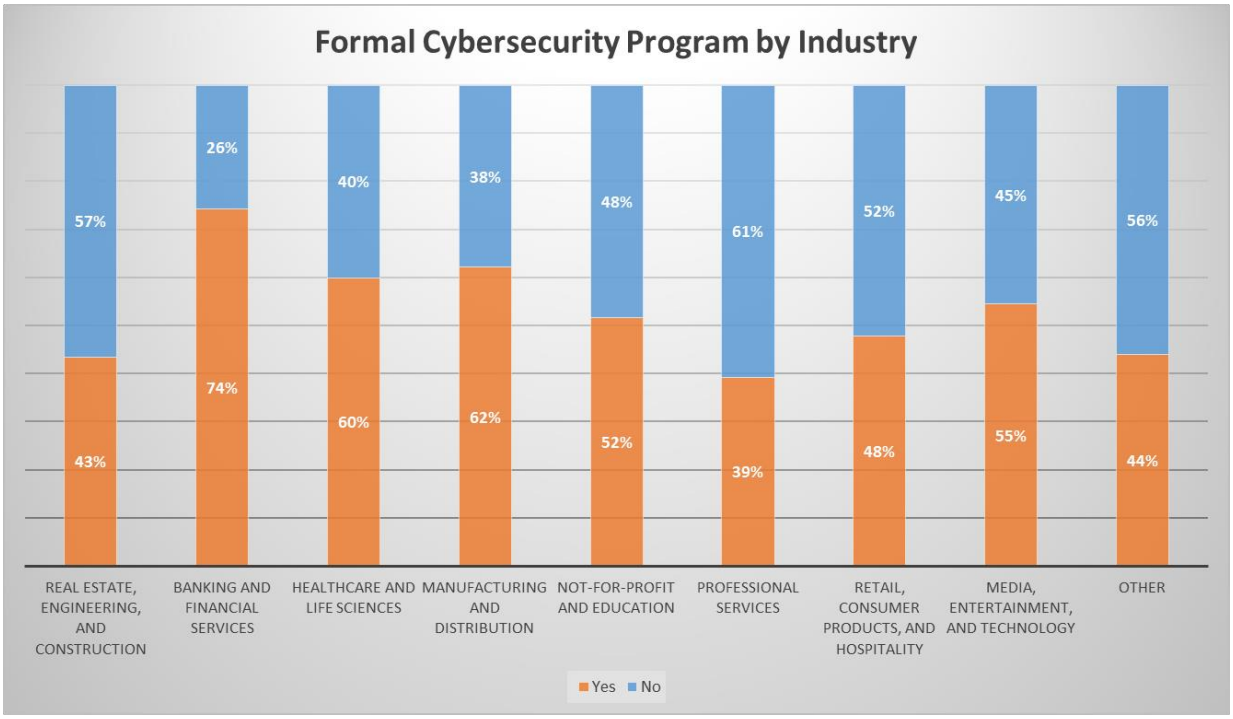
Figure 6: Regional view – How significant a concern is cybersecurity to your organisation?



Formal Program in Place?

For the purposes of our survey, we define a "formal" cybersecurity program as having policies and procedures, defined ownership, and governance in place. The survey shows that 53% of organisations reported having a formal cybersecurity program in place. Given its highly regulated environment, it is no surprise that Banking and Financial Services ranks highest among the industries, with 74% indicating having a formal cyber program in place. Similarly, 60% of Healthcare and Life Sciences organisations, another heavily regulated industry, confirmed the same. We were somewhat surprised that the Manufacturing and Distribution (M&D) industry scored 62% in this regard. Increased customer focus or the recognition that a cyber-attack could significantly harm operations has likely spurred the increased attention in this sector. Professional Services firms scored the lowest in terms of having a formal cybersecurity program: less than 40%. With increasing regulation related to the protection of personal data, it will be interesting to see the trend in this area over the next few years.

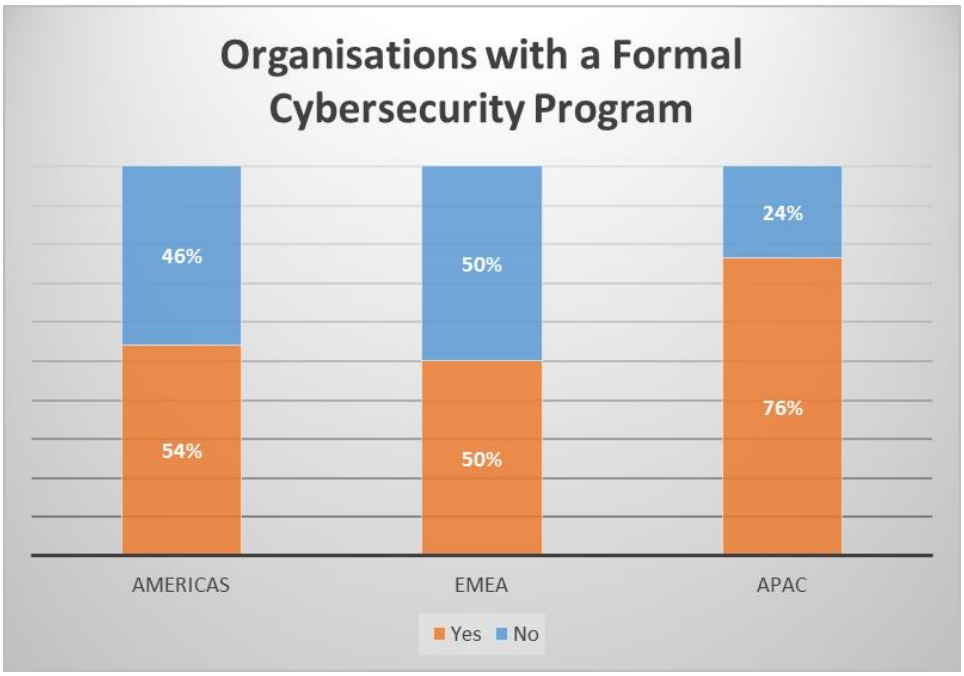
Figure 7: Industry view – Does your organisation have a formal cybersecurity program (i.e., a program that is supported by policies and procedures, periodic cybersecurity risk assessments, and accountability and governance over cyber risks and threats)?



By Region

On a regional basis, the Americas and EMEA were roughly even, with about half of respondents stating they have a formal cybersecurity program in place. 76% of APAC respondents indicated they have a formal cybersecurity program in place.

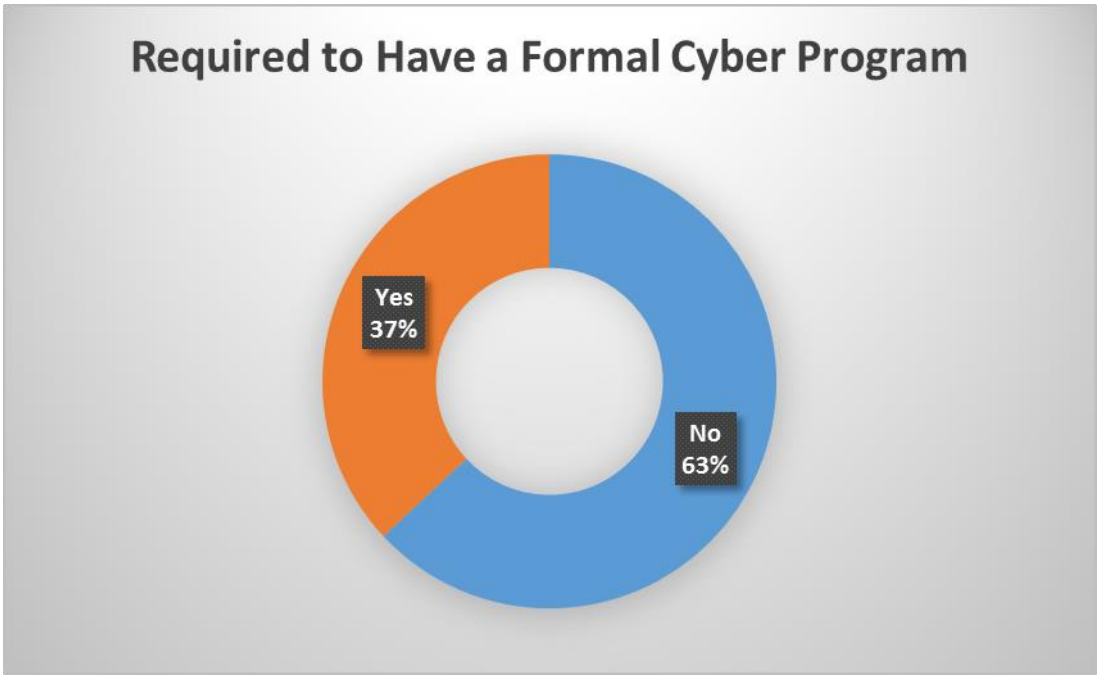
Figure 8: Regional view – Does your organisation have a formal cybersecurity program (i.e., a program that is supported by policies and procedures, periodic cybersecurity risk assessments, and accountability and governance over cyber risks and threats)?



Required to Have a Cyber Program?

Thirty-seven percent (37%) of respondents stated they were required to have a formal cyber program based on government or industry related regulations.

Figure 9: Is your organisation required to have a cybersecurity program?



A rather alarming fact was that 20% of those companies required to have a formal cybersecurity program do not actually have such a program in place. This statistic brings in further question the effectiveness and robustness of the governance process of those monitoring compliance as well as the level of impact of potential consequences for not abiding by these regulations.

Figure 10: Despite being required to have a cybersecurity program, not all respondents reported having a formal cybersecurity program in place

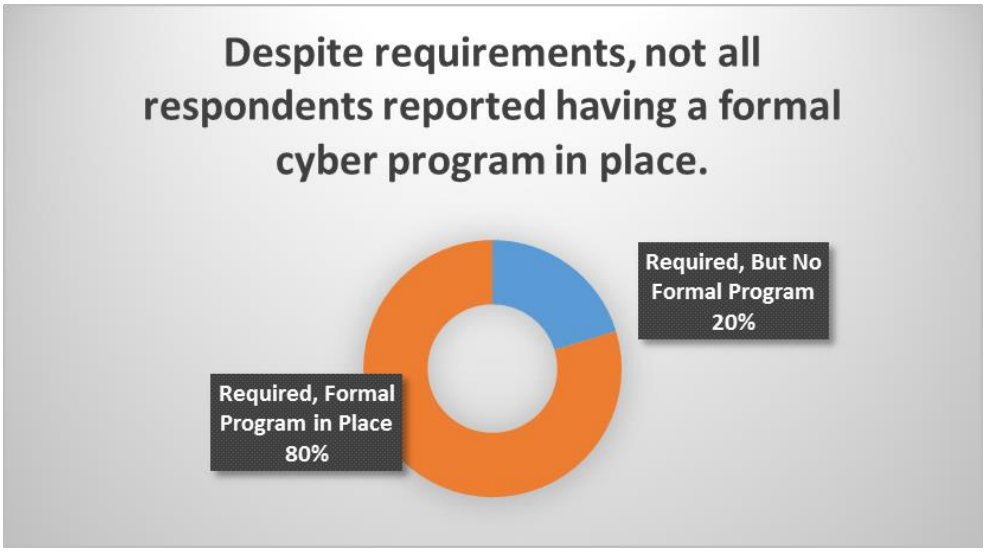
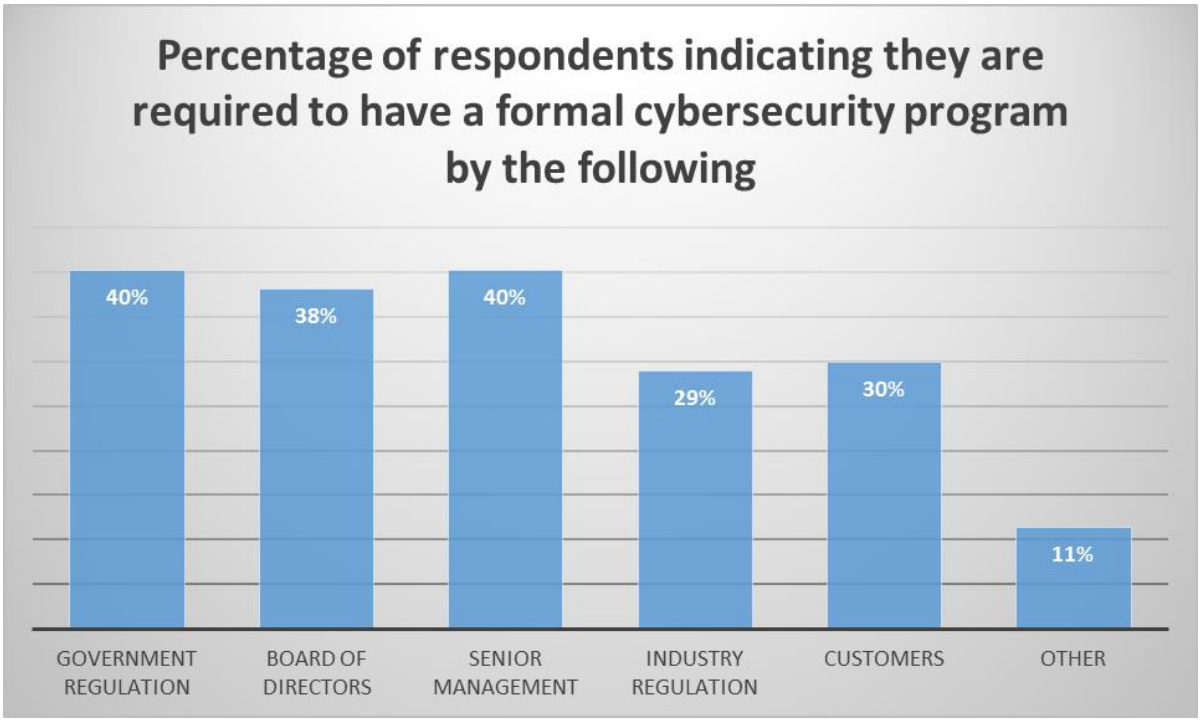


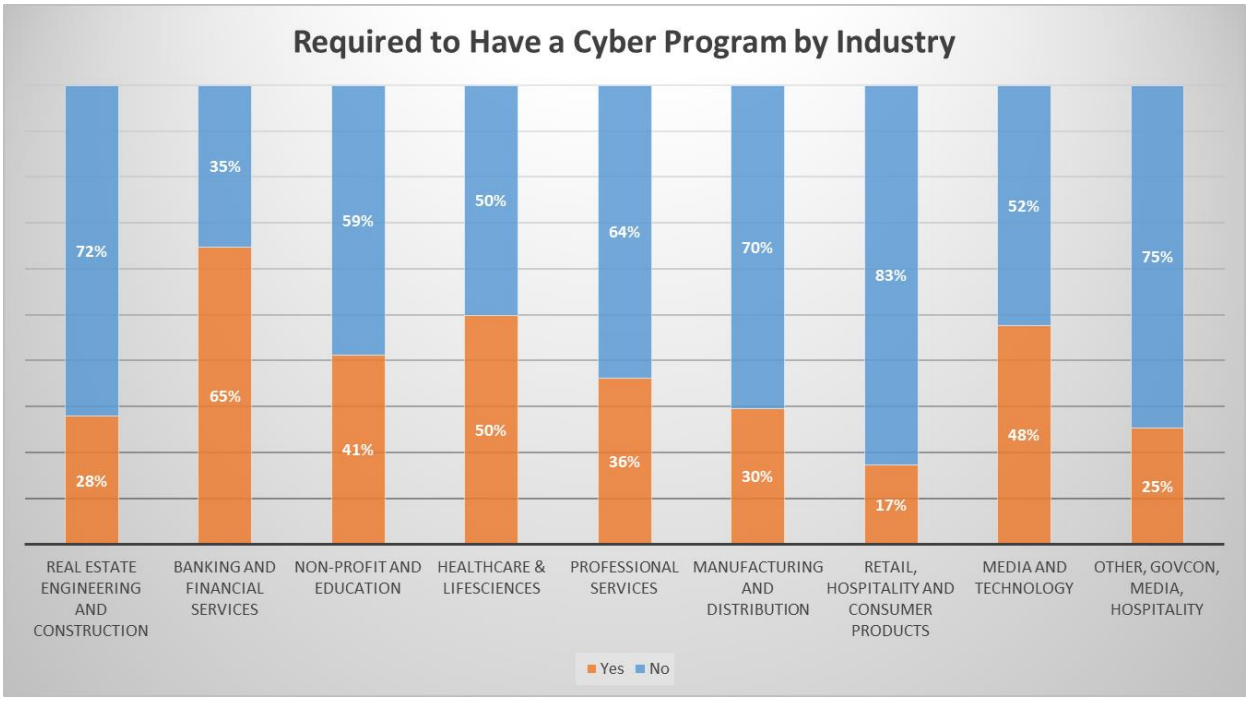
Figure 11: If your organisation is required to have a cybersecurity program, whom requires it?



By Industry

Banking and Financial Services had the largest number of respondents reporting that they are required to have a formal cyber program, followed by Healthcare and Life Sciences.

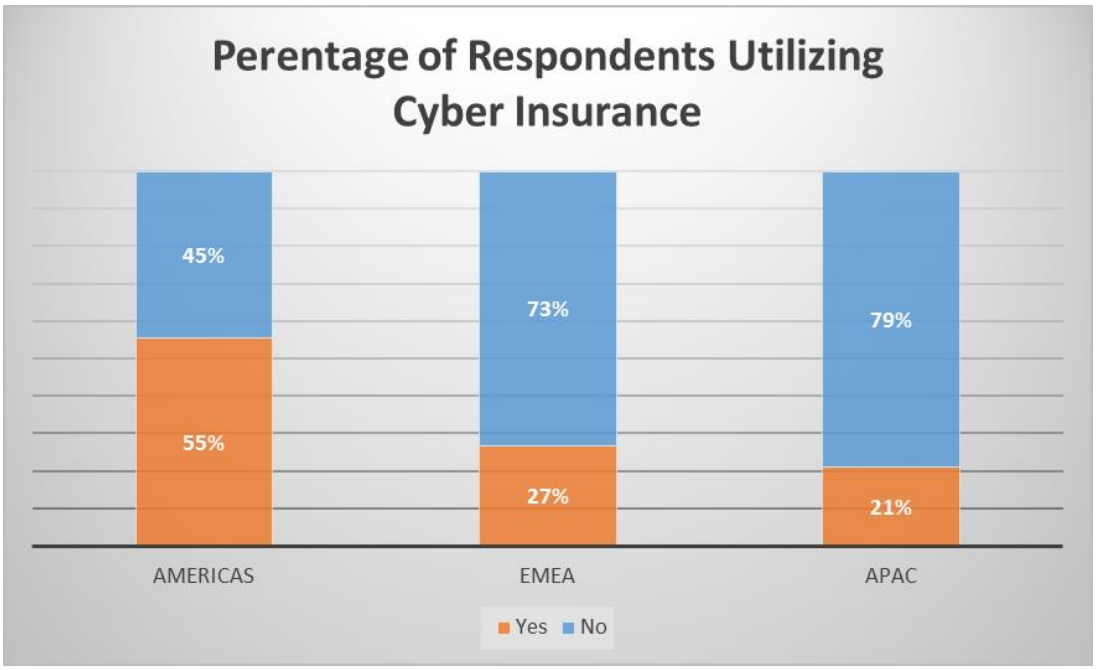
Figure 12: Industry view- Is your organisation required to have a cybersecurity program?



Insurance

Cyber insurance is more prevalent in the Americas than EMEA and APAC. Cyber insurance is a relatively new vehicle for transferring cybersecurity risk and has appeared to have gained considerable traction, at least in the Americas region.

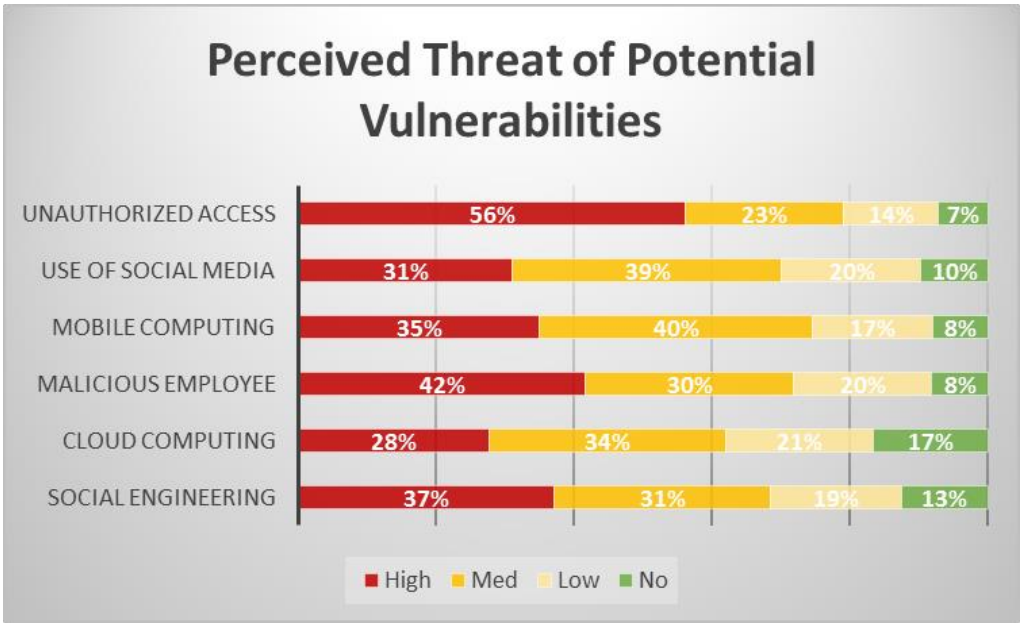
Figure 13: Does your organisation have cybersecurity insurance?



Threat Environment

The results of the survey indicate that the human element poses the greatest perceived risk to organisations: specifically, unauthorized access and malicious employees. The increasing complexity and scale of data, IT, and sources of entry make managing access to sensitive data extremely difficult, particularly for data-intensive organisations. These risks may also be the ones most familiar to organisations. Not all organisations have adopted cloud computing or have a strong social media presence, making risks from these technologies less prevalent. Further, access controls are included in nearly all compliance mandates that address security and privacy, and auditors routinely test internal controls over this area. Hence, it is not surprising that unauthorized access and malicious employees are regarded as the top concerns. It will be interesting to see how the responses to this question change over time as the nature of technology deployment and the cybersecurity risk landscape evolves.

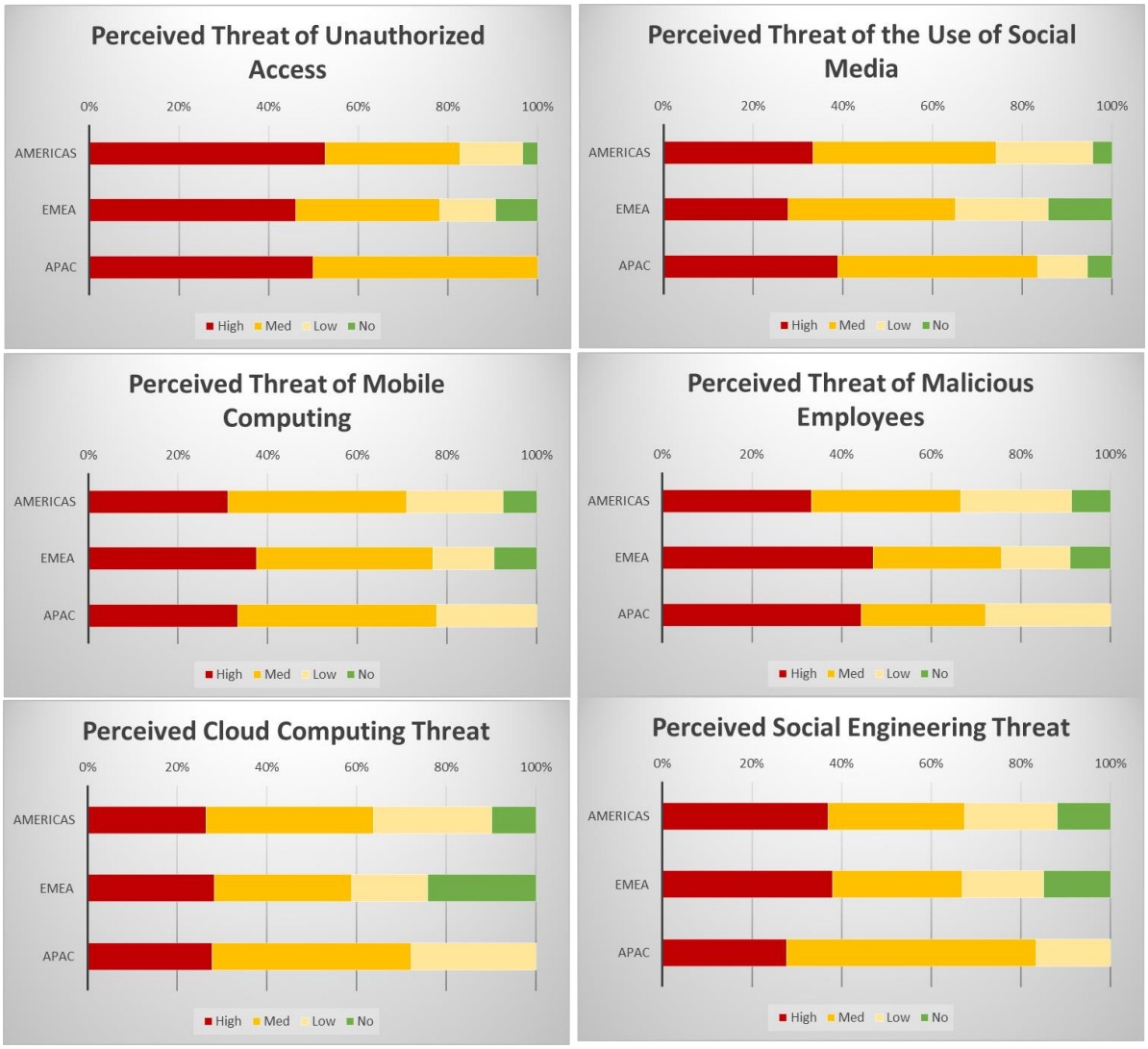
Figure 14: Rank the following potential vulnerabilities according to the perceived level of risk they pose to your organisation



By Region

Regionally the results were fairly consistent.

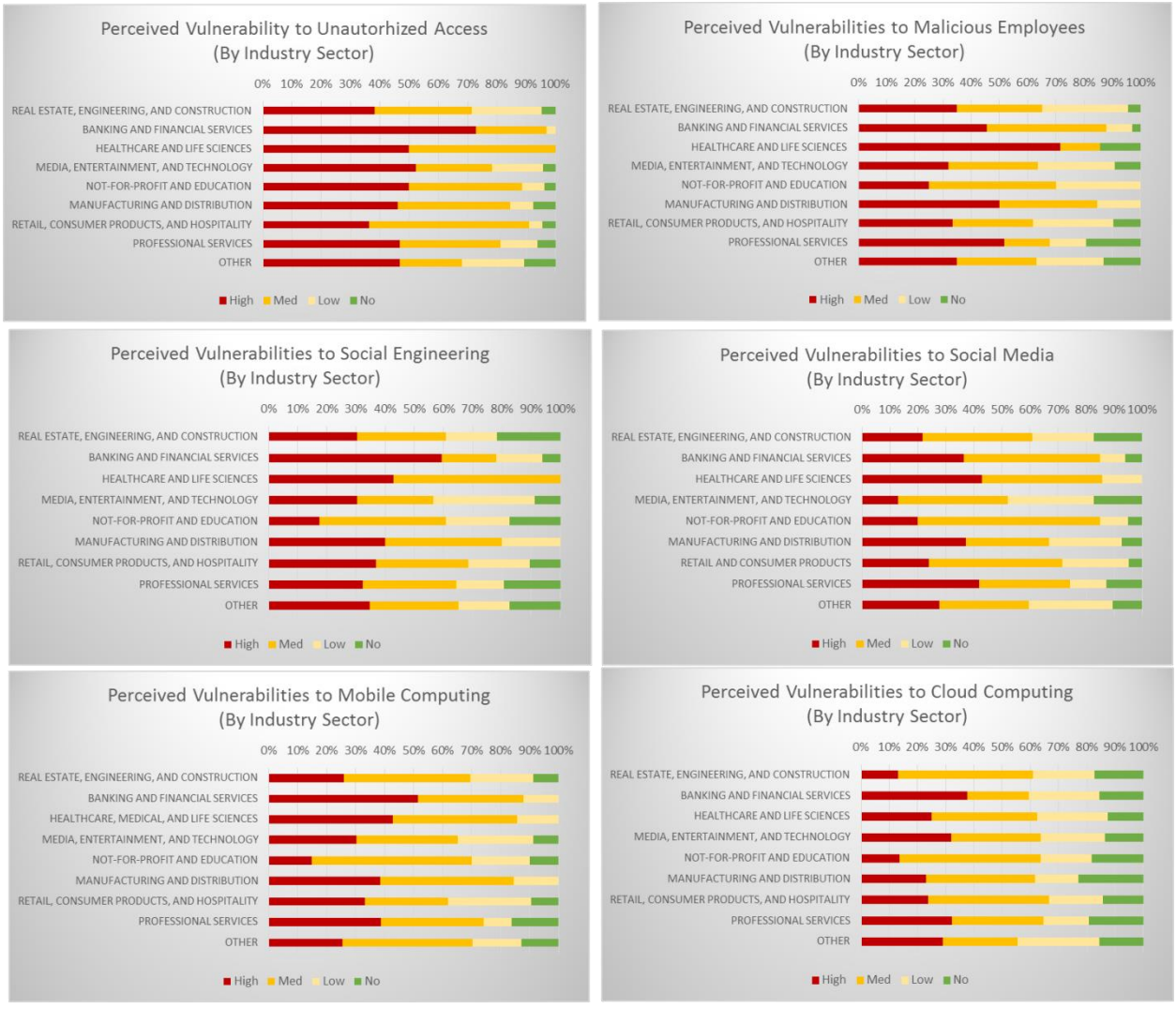
Figure 15: Regional view – Rank the following potential vulnerabilities according to the perceived level of risk they pose to your organisation



By Industry

Healthcare and Life Sciences and Banking and Financial Services scored the highest in perceived threats across all potential vulnerabilities. Given the highly publicized breaches as well as increased attacks in these sectors, this is consistent with expectations.

Figure 16: Industry view – Rank the following potential vulnerabilities according to the perceived level of risk they pose to your organisation

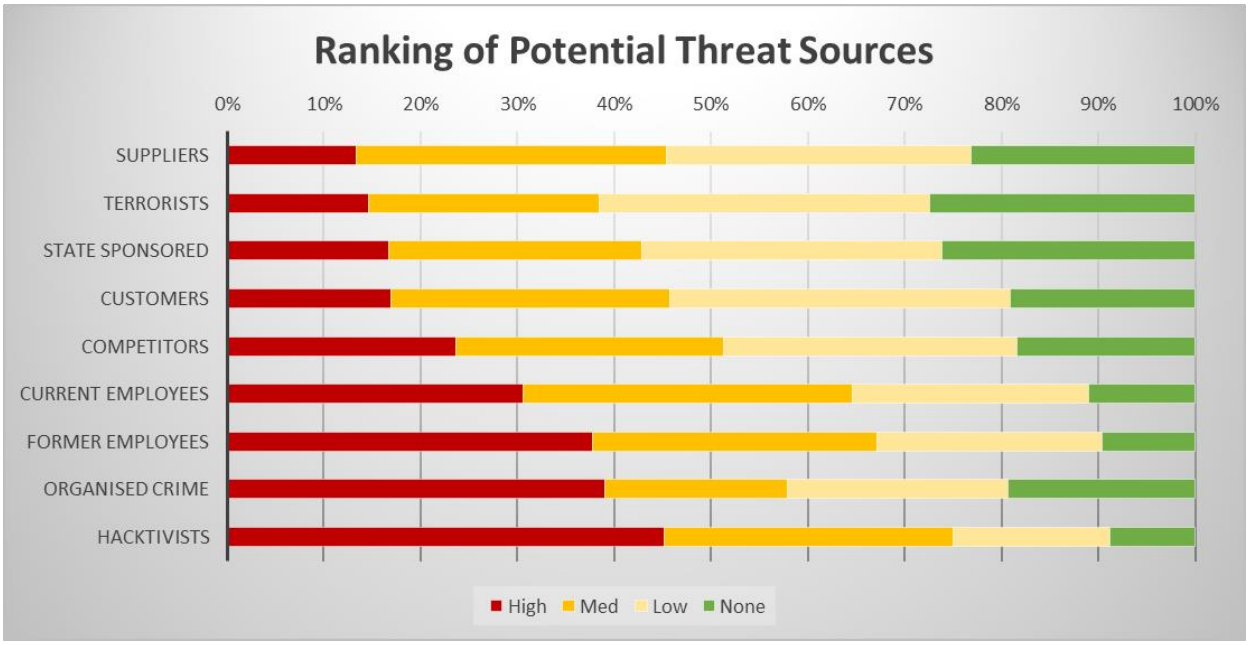


Profiling the Risk of Potential Threat Sources

Overall

The landscape of cyber threat sources is very broad, covering the gamut of opportunistic, relatively unsophisticated lone hackers to organized crime and state-sponsored cyber terrorism. Hacktivists ranked as the highest perceived threat, followed by nearly identical survey results for both organized crime and former employees. The fact that the perceived threat of a former employee was considered to be nearly equal to that of professionally organized crime rings emphasizes the need for formalized and swift access termination procedures for employees.

Figure 17: Rank the following threats according to the perceived level of risk they pose to your organisation

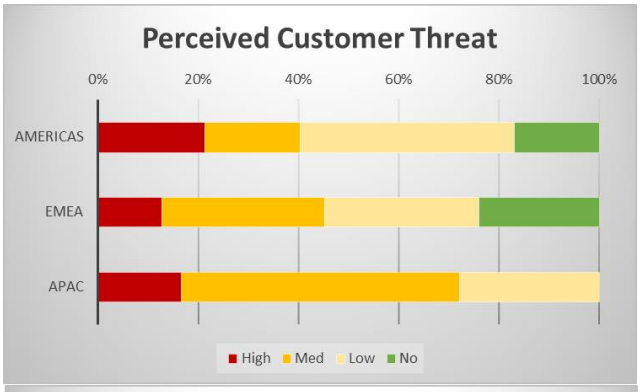


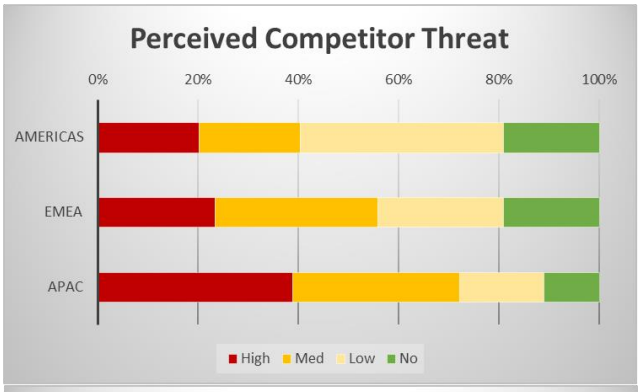
By Region

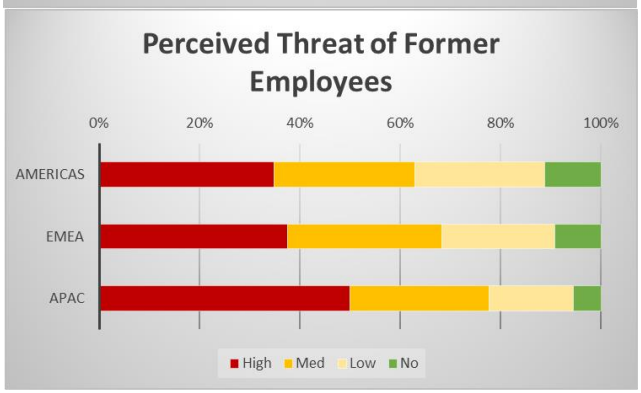
From a regional perspective, the results were consistent with current global trends in cybersecurity. EMEA showed the greatest percentage of respondents ranking organized crime as a high-risk. This may in part be due to the large hacking-related organized crime rings in countries such as Russia and Ukraine. With the well-publicized hacking and ransomware attacks stemming from these countries and the geographical proximity to EMEA, it does not seem surprising. Similarly, the perceived risk of competitor threat is the highest in APAC.

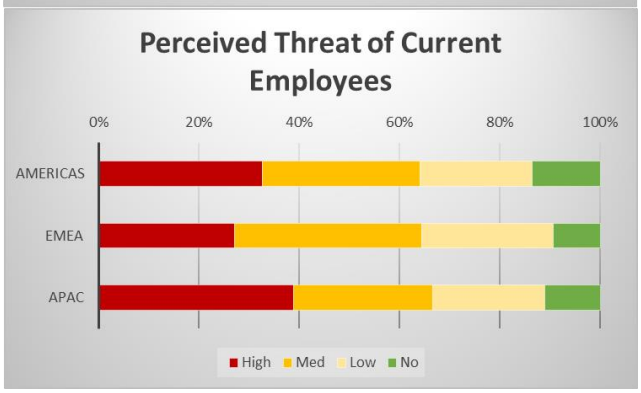
Figure 18: Regional view - Rank the following threats according to the perceived level of risk they pose to your organisation

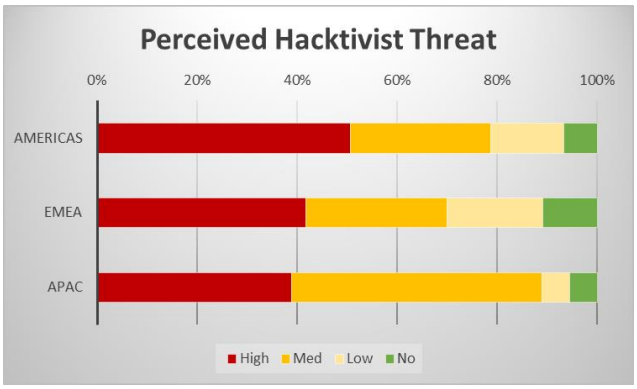
Figure 18 (continued): Regional view - Rank the following threats according to the perceived level of risk they pose to your organisation







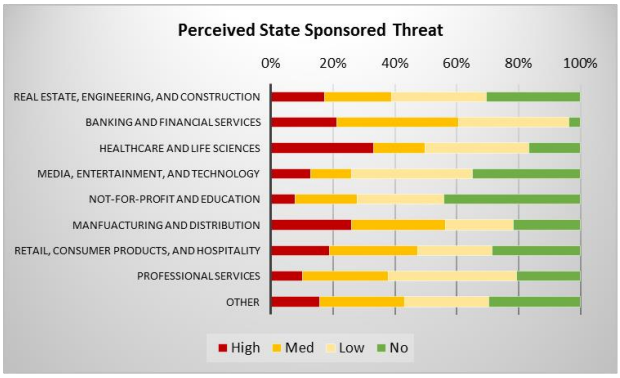


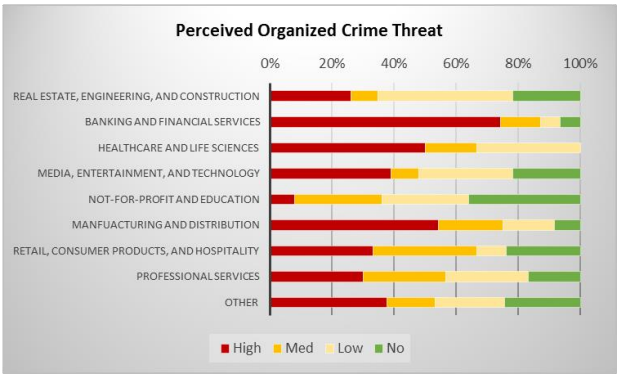


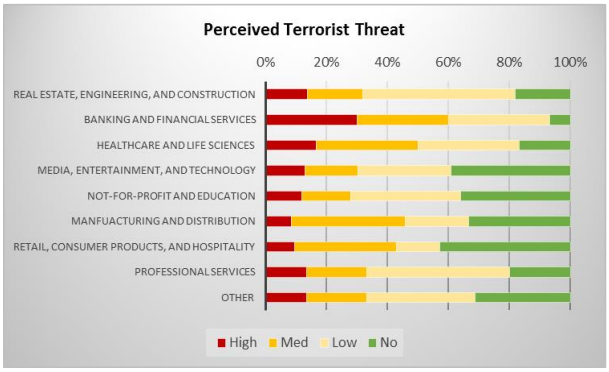
By Industry

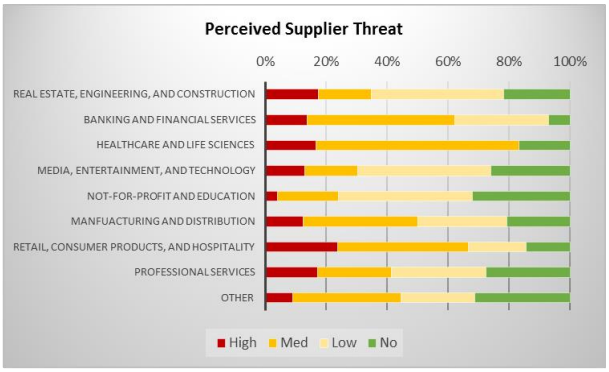
Organisations in the Banking and Financial Services industry led the responses to perceived organized crime threat, which also correlates with current trends faced by companies within that industry. Organisations in the Healthcare and Life Sciences industry had the highest overall concern for several categories: threats from former employees, competitors, and state-sponsored attacks, while also scoring in the top three for organized crime.

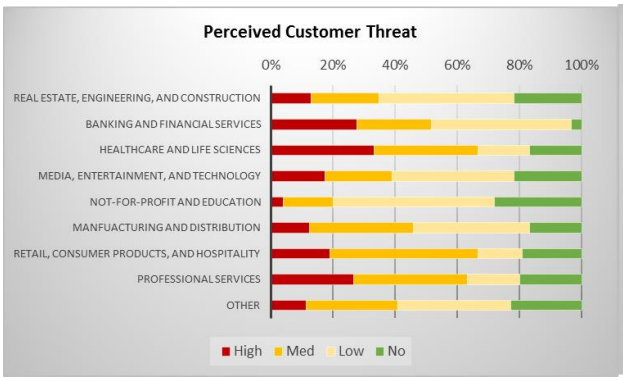
Figure 19: Industry view - Rank the following threats according to the perceived level of risk they pose to your organisation











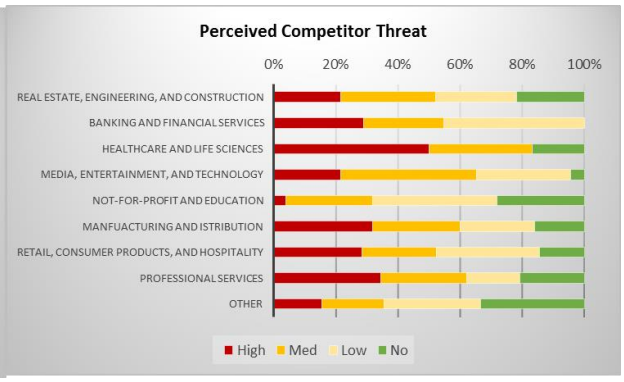
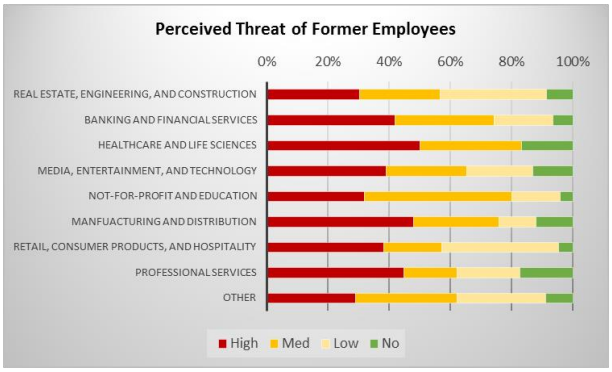
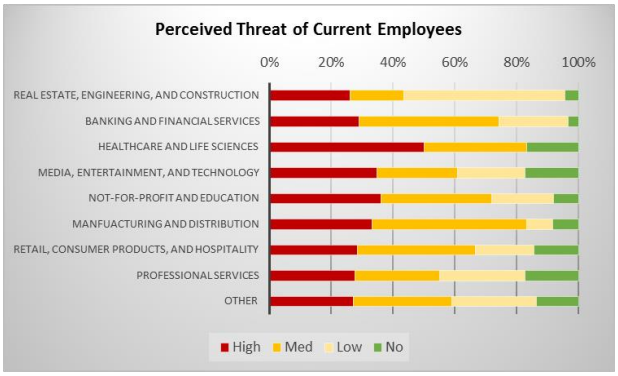
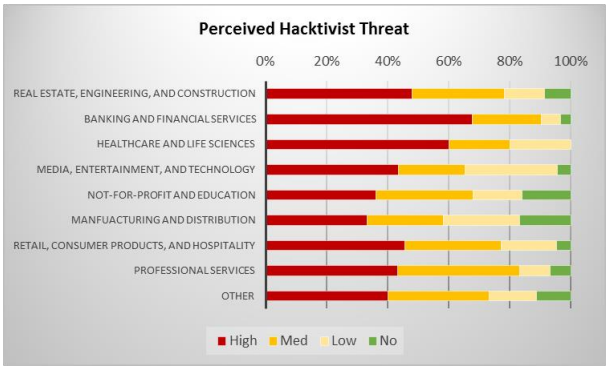


Figure 19 (continued): Industry view - Rank the following threats according to the perceived level of risk they pose to your organisation





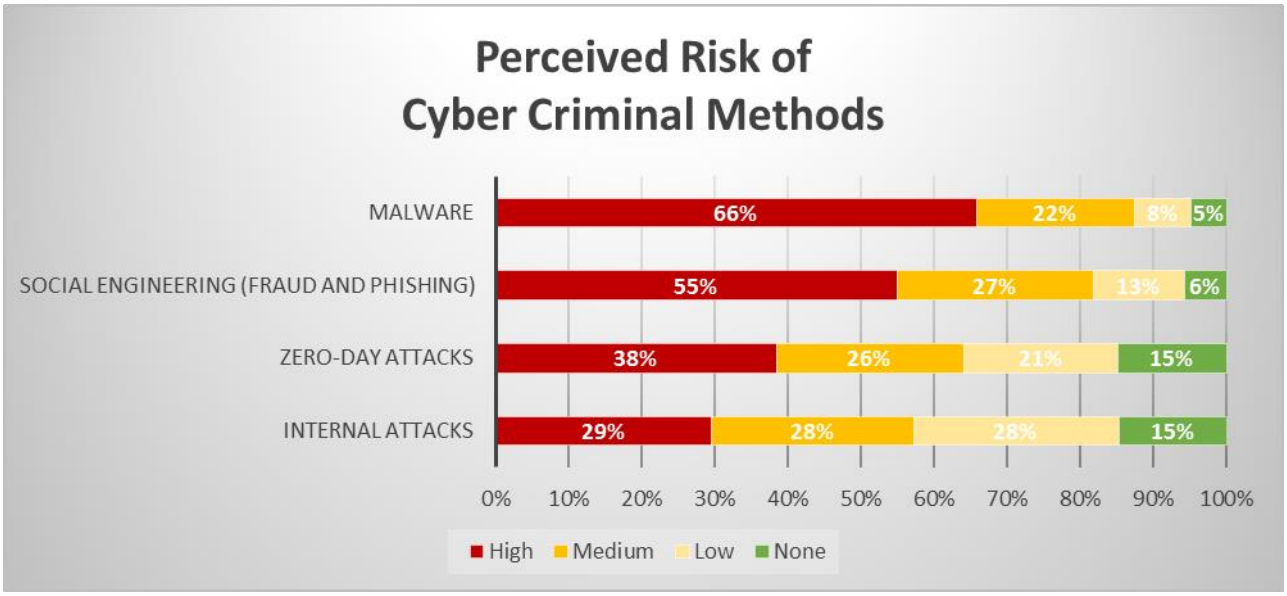


Cyber Criminal Methods

Overall

The greatest perceived risk of cyber-attack methods is malware, followed by social engineering. A malware attack is a piece of malicious software that takes over a person's computer in order spread to other devices and gain access to user profiles. Phishing and social engineering attacks are attempts to steal a user's login and password information, gain access to other sensitive data, or to deliver malware. Both have become a global epidemic.

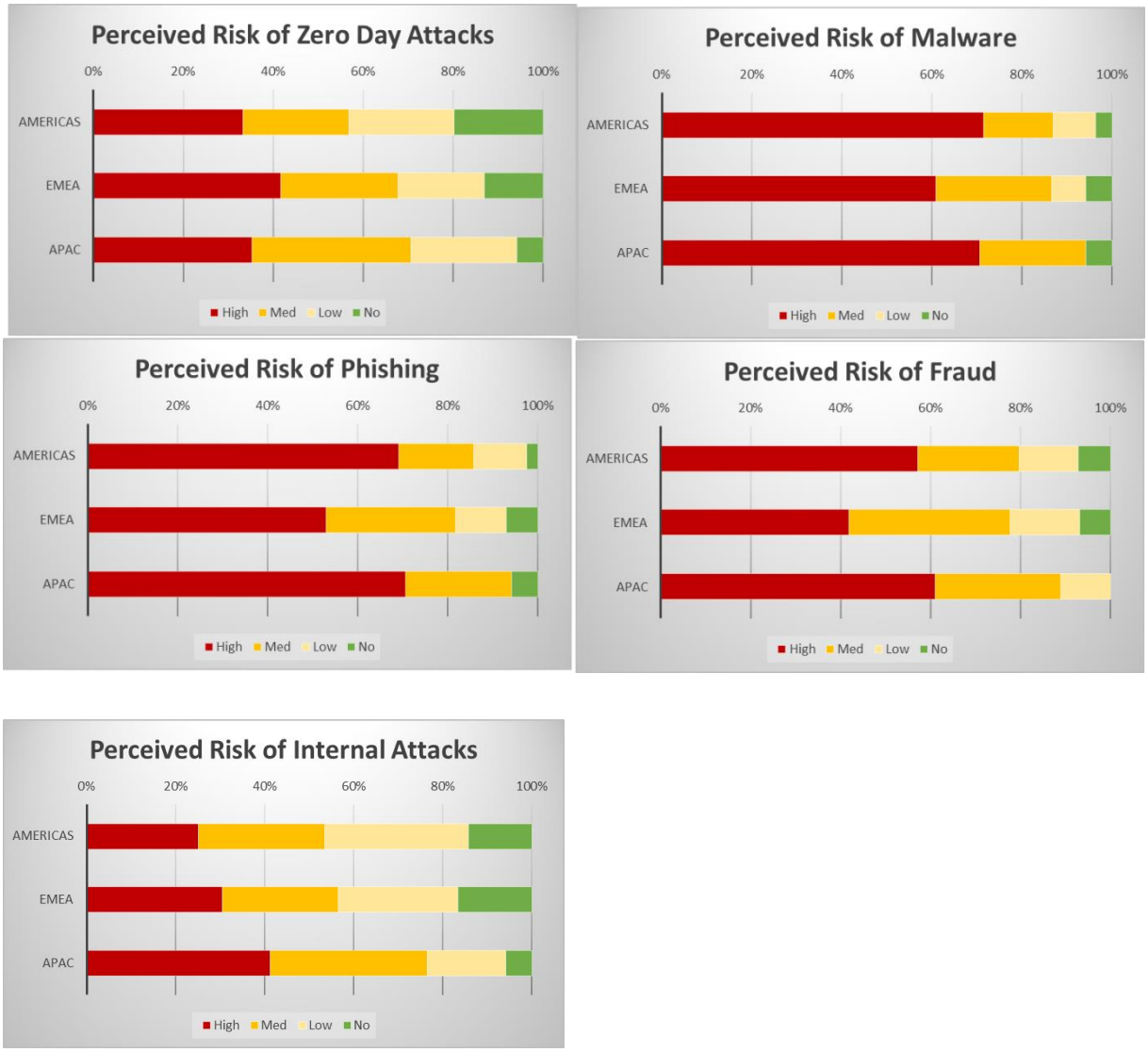
Figure 20: Rank the following methods used by cyber criminals according to the perceived level of risk they pose to your organisation



By Region

Regionally, the perceived risk of fraud was highest in APAC, which also had the lowest score for perceived risk of zero-day attacks (e.g., a new attack for which there is currently no known patch or signature to effectively identify and remediate). The other responses were generally consistent among regions, with the Americas and APAC showing fairly even responses. The exception was the risk of internal attacks where the Americas scored significantly lower than the other regions in terms of viewing this as a high risk.

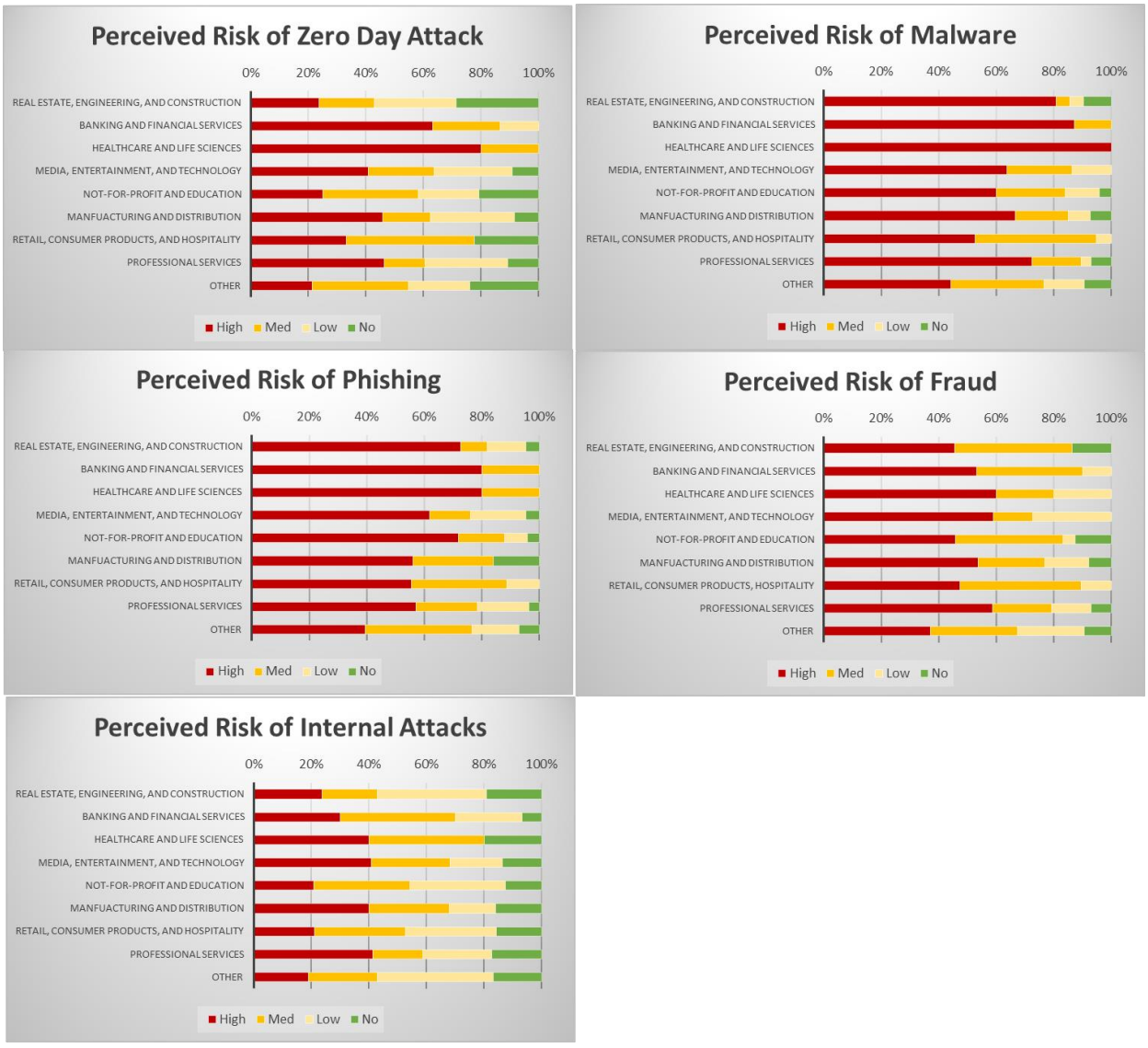
Figure 21: Regional view — Rank the following methods used by cyber criminals according to the perceived level of risk they pose to your organisation



By Industry

With the exception of fraud risk, Healthcare and Life Sciences topped every category of perceived risks for all forms of attack methods. As stated previously, this industry segment has become a prime target given the richness of data these organisations maintain. We found it interesting that Media, Entertainment, and Technology ranked among the highest in their perceived risk of fraud. Not-for-Profit and Education showed little concern for a zero day attack. While Manufacturing and Distribution showed a fairly consistent level of concern over zero day and phishing attacks, the sector was most concerned about malware.

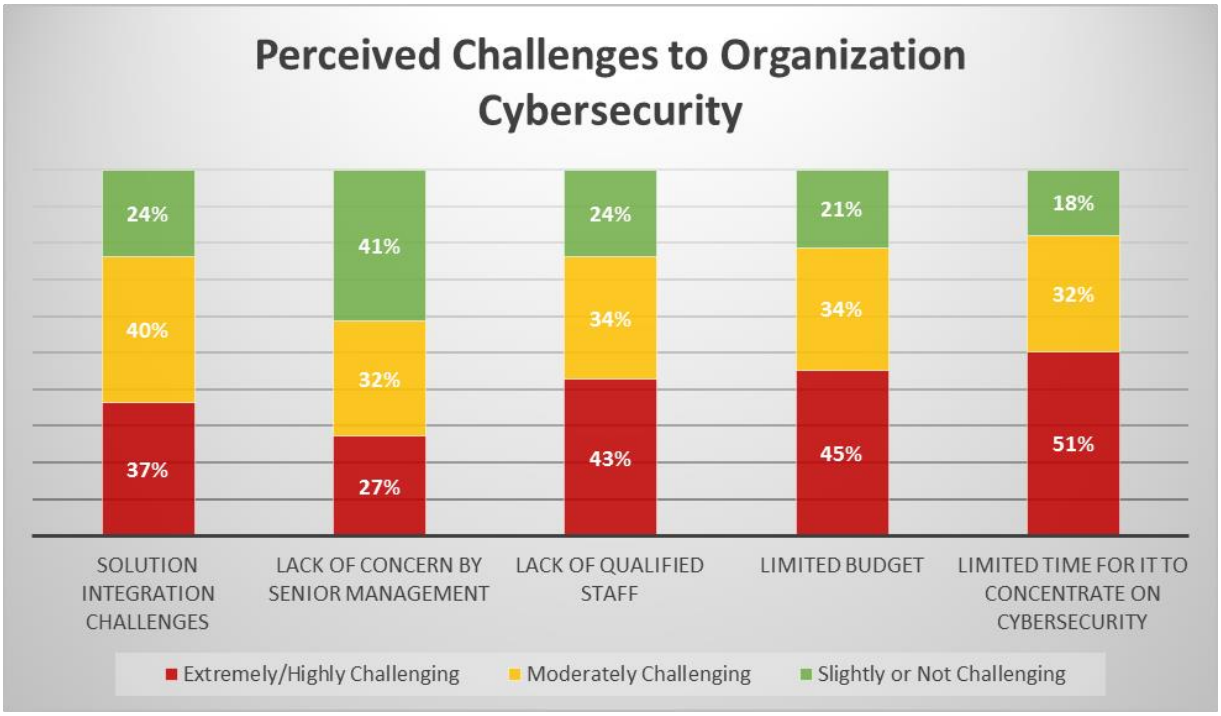
Figure 22: Industry view – Rank the following methods used by cyber criminals according to the perceived level of risk they pose to your organisation



Internal Challenges to Cybersecurity Efforts

Limited time and budget, followed closely by lack of qualified staff, are the top challenges to managing cybersecurity cited across all industries and regions. This is not surprising given the ever-changing landscape of cybersecurity threats. It is interesting that only 27% of organisations indicated a lack of concern by senior management as a challenge given the small number of respondents who ranked cybersecurity as a top concern.

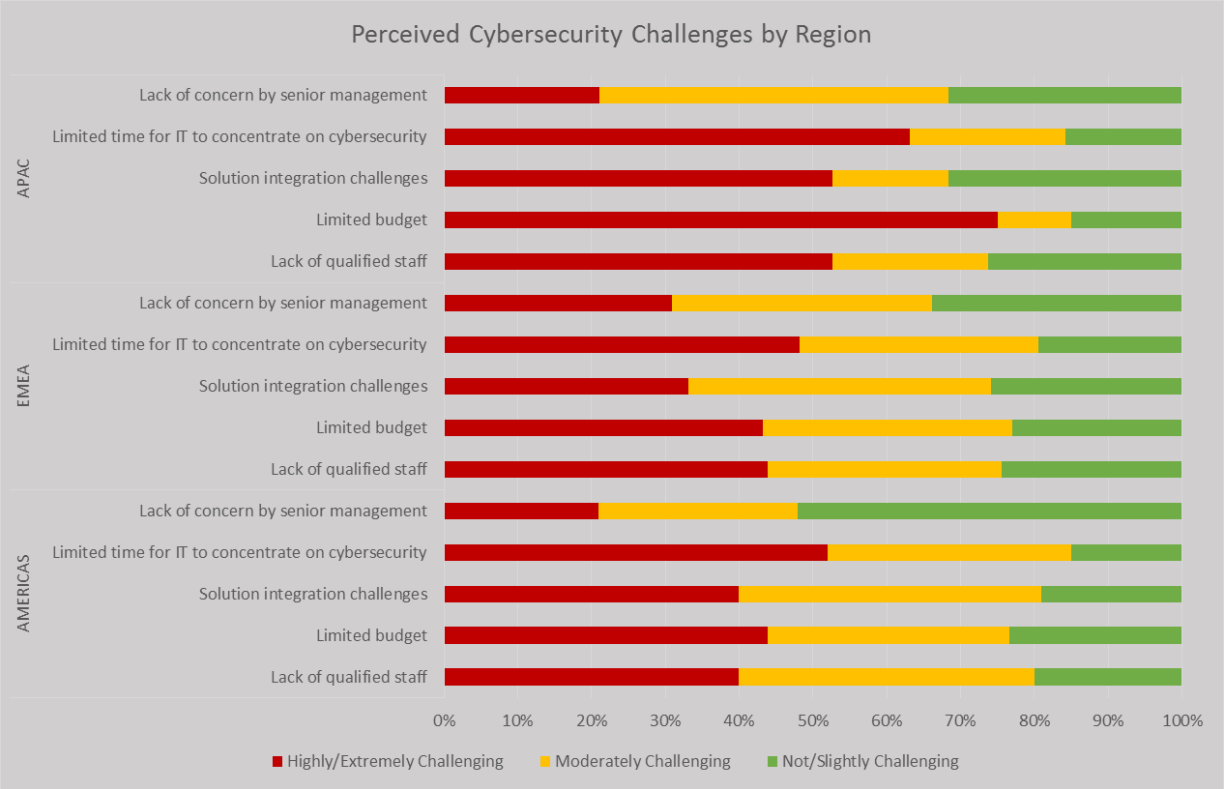
Figure 23: Rank the following issues according to the level of challenge they pose to your organisation's cybersecurity



By Region

Regional results seemed to be fairly well aligned with the overall results on this question.

Figure 24: Regional view – Rank the following issues according to the level of challenge they pose to your organisation's cybersecurity



By Industry

Not-for-Profit organisations are most challenged by budget constraints. Any cyber-specific enhancement opportunity for organisations in this sector competes directly with even the most basic technology spending such as upgrading computers. This contrasts with industries with a greater technology adoption and maturity, such as Banking and Financial Services and Healthcare and Life Sciences, where time constraints were cited as the primary challenge.

Figure 25: Industry view – Limited budget for cybersecurity challenge

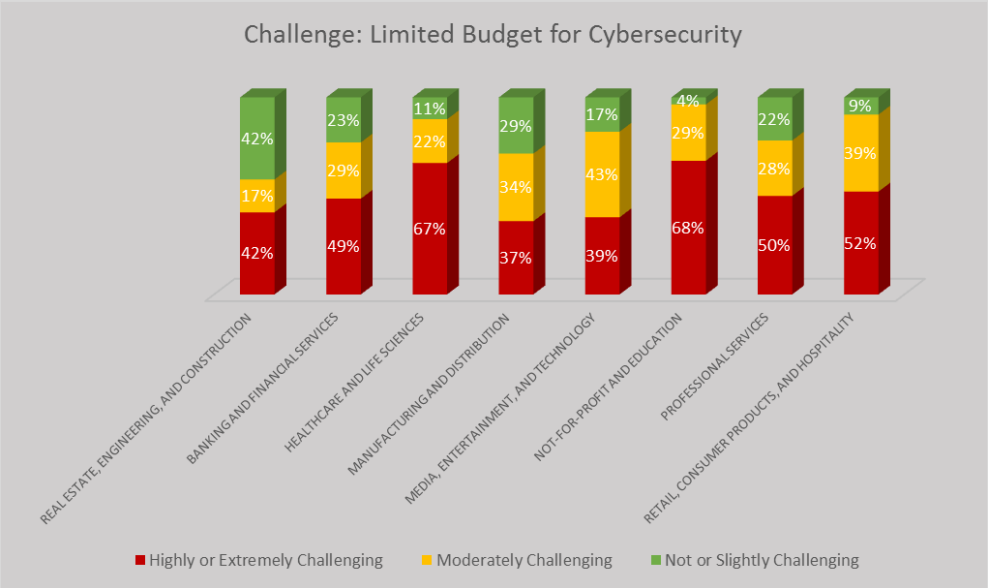
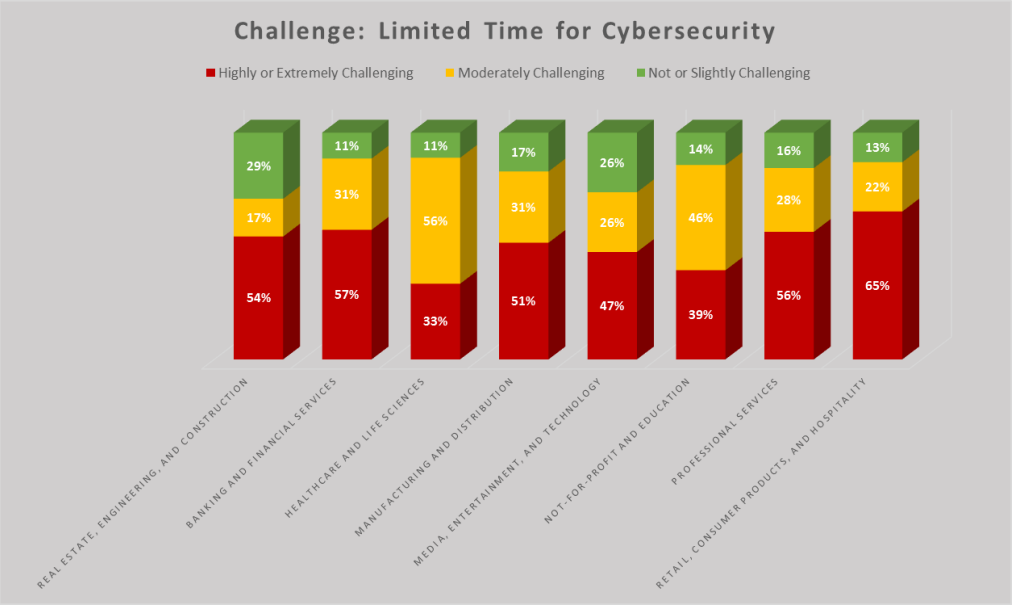


Figure 26: Industry view – Limited time for cybersecurity challenge



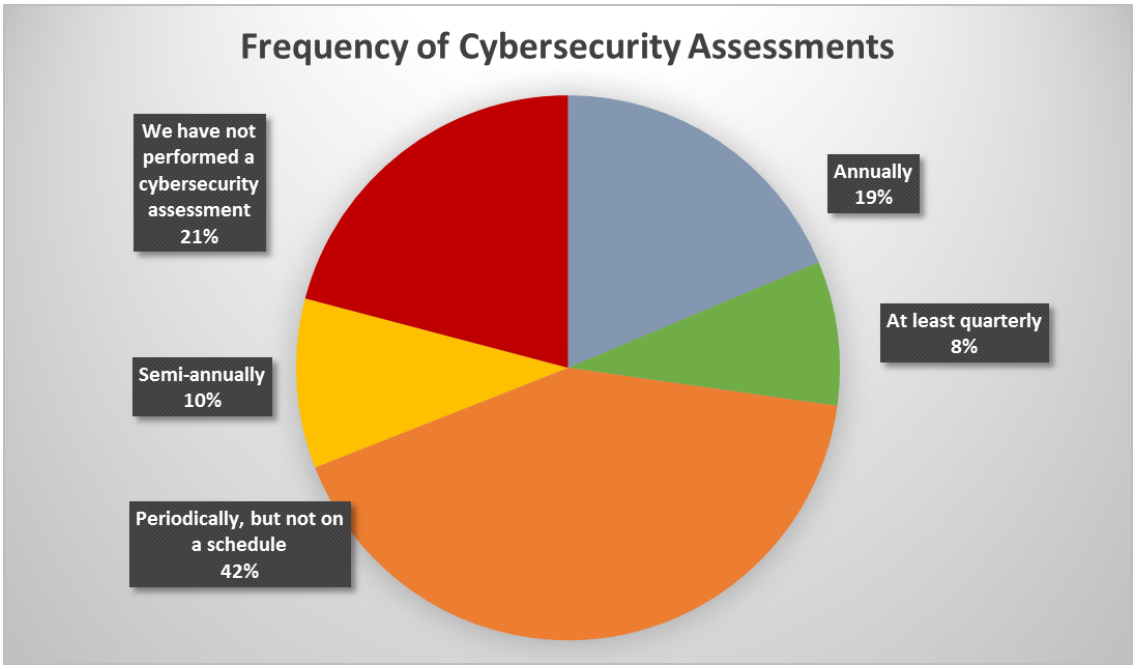
Cybersecurity Program Measures and Investment

In this section, we asked the respondents to answer questions regarding investments in cybersecurity programs, including cybersecurity assessments; security awareness training; and tools and technologies related to cybersecurity domains such as security operations, identity and access management, threat detection, monitoring and response, data privacy, and data loss prevention. In addition, we asked the respondents to rank their overall level of satisfaction with their current cybersecurity posture and capabilities within their organisations.

Assessment Frequency

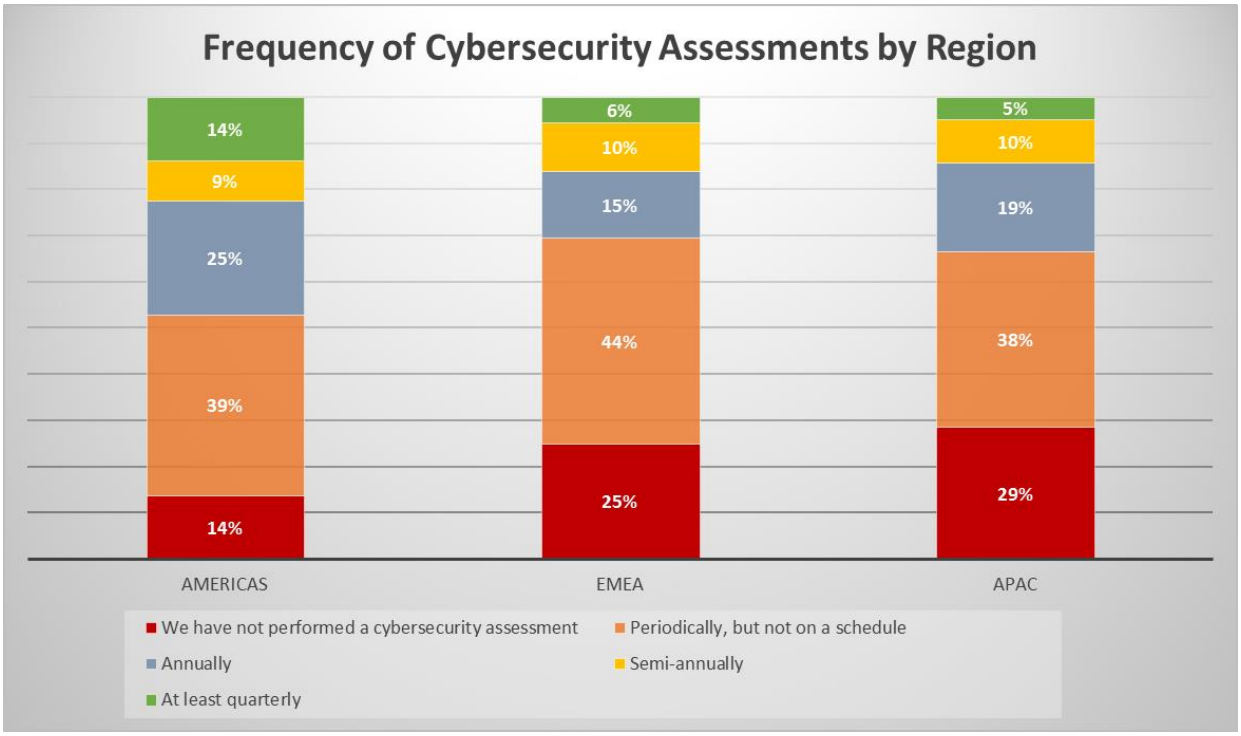
As shown in the graph, 19% of respondents indicated that they undergo a cybersecurity assessment once a year; 42% responded that they do conduct a cybersecurity assessment on their environment but it is ad-hoc and not routinely scheduled; and 20% of the respondents have not performed a cybersecurity assessment. A rather alarming statistic is that, depending on the region, anywhere between 50% and nearly 70% of organisations have either not performed an assessment or perform them in an ad-hoc manner.

Figure 27: How often does your organisation perform a cybersecurity assessment?



By Region

Figure 28: Regional view – How often does your organisation perform a cybersecurity assessment?

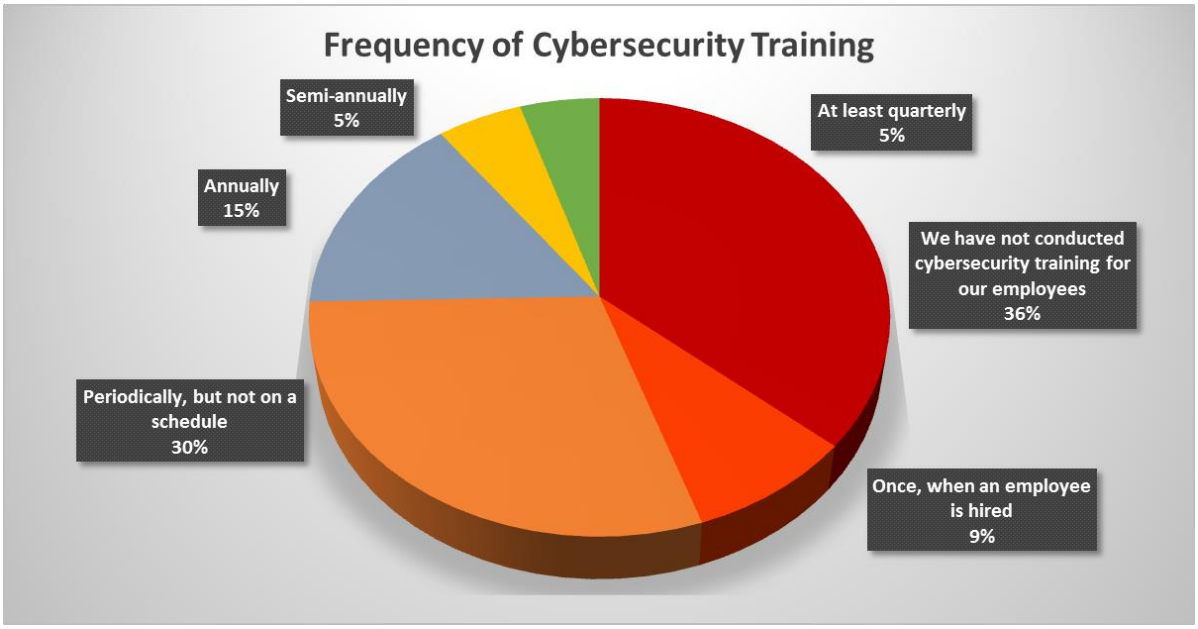


It is concerning that so many organisations do not engage in periodic and formal cybersecurity assessments of their environments. This may lead to unknown threats and attacks that go unnoticed and potentially may have a negative impact on these organisations. The lack of push for formal cybersecurity assessments may indicate that the leadership and boards within these organisations do not consider the threats and concerns related to cybersecurity to be a substantial enough risk to make the investment worthwhile.

Training Frequency

People are often considered to be the weakest link in the information security chain, which includes cybersecurity. Yet only 10% of respondents indicated that their organisations provide mandatory security awareness training to their new and existing employees more than once a year and 15% provide training annually. Thirty percent indicated that they provide training periodically but not on a schedule and not on set frequency. Forty-five percent provide no training or provide training once during the new hire orientation, potentially leaving existing employees vulnerable to phishing attacks or cyber scams and falling prey to divulging valuable information to malicious actors. As indicated earlier, budget constraints may be a strong contributor to the lack of training. Post mortems conducted on many recent breaches have indicated that human error and lack of awareness played a role in the security breach.

Figure 29: How often does your organisation conduct cybersecurity training for employees?

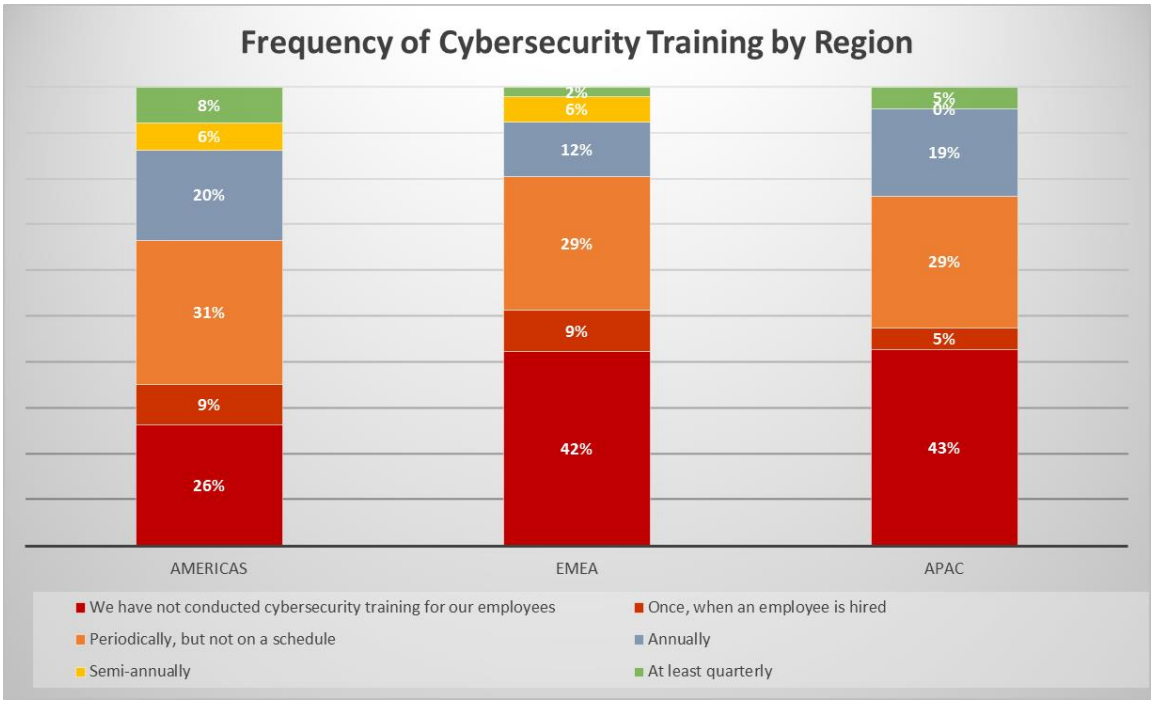


By Region

Organisations in the Americas seem to be more disciplined in providing frequent and regular training to their employees compared to organisations in EMEA. Thirty-four percent of respondents from the Americas provide training either annually, semi-annually, or quarterly. Fifty-one percent of respondents from EMEA and 48% of APAC respondents indicated that they either do not provide any training or provide training only during new hire orientation. The discipline of organisations in the Americas could be a result of the number of high-profile attacks that have occurred, spurring organisations in this region to be more proactive and increase employee awareness. That said, we

believe the General Data Protection Regulation (GDPR) introduced by the European Union will prompt organisations to provide more frequent security awareness training to their employees across the world. Intended to standardize data security, retention, and governance across the European Union countries, GDPR requires stringent oversight of where and how sensitive data — including personal, credit card, banking, and health information — is stored and transferred, and how access to it is governed. In all regions, regulations over security and privacy are increasing, which may drive increased training and awareness.

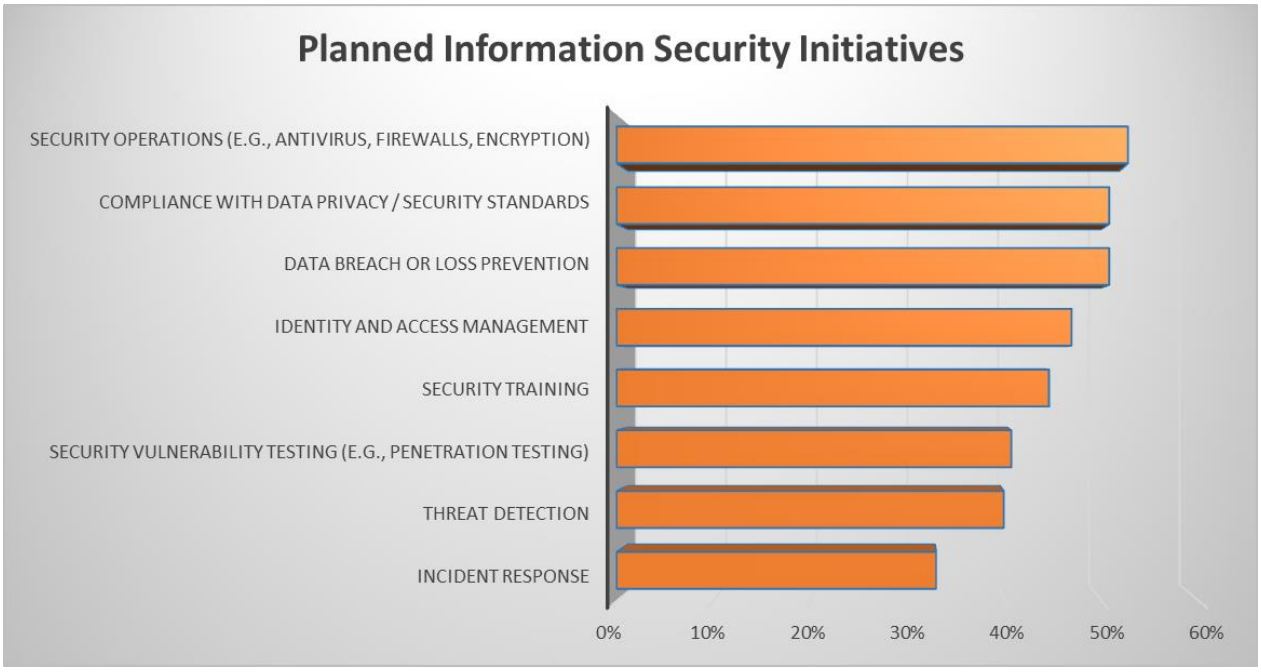
Figure 30: Regional view – How often does your organisation conduct cybersecurity training for employees?



Planned Initiatives

When we asked questions of our survey respondents in relation to their planned investments and initiatives in cybersecurity, it was not surprising to see that the largest proportion of cybersecurity budgets is allocated towards easily implementable security operations solutions and procedures such as antivirus and firewalls. Compliance-driven spending such as data privacy and alignment with security standards came in a close second, with data loss prevention and identity and access management rounding the top four priorities for respondents. What was surprising from the survey results was the lack of prioritization and hence an underinvestment in the establishment of an incident response plan and threat detection capabilities. Without adequate investment in monitoring, detecting, and handling of security incidents, organisations can spend approximately $3.62 million dollars, on average, after being a victim of a security incident, or roughly $141 per compromised record[3]. In some industries such as Healthcare and Life Sciences and Banking and Financial Services, it can run as high as $380 and $245 per record respectively, while the public sector may spend just $71 per breached record to recover from the security incident[2]. The message is that detection and response are equally important as preventive technologies.

Figure 31: Which of the following information security initiatives does your organisation plan to address in the next 12 months?

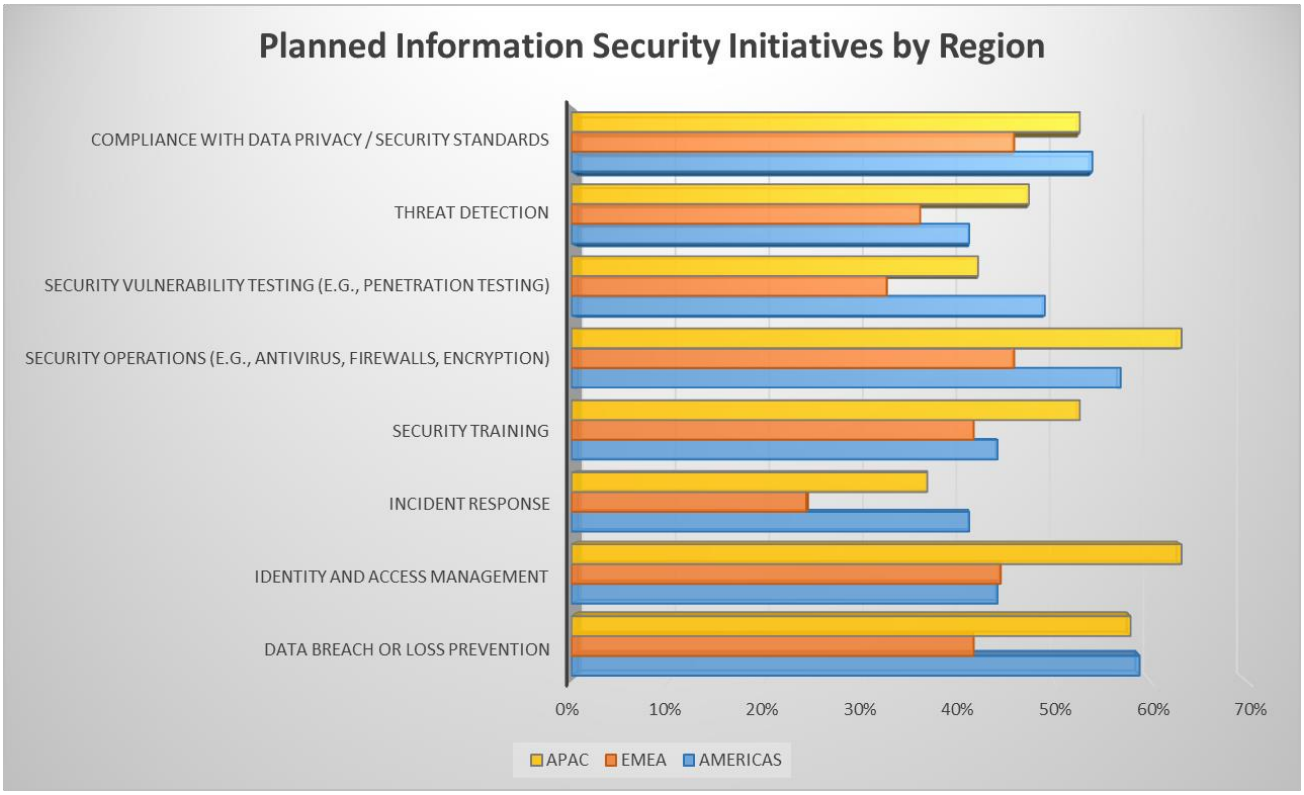


[3] 2017 Cost of a Data Breach Study – Global Overview. Benchmark research sponsored by IBM Security and independently conducted by Ponemon Institute LLC, June 2017.

By Region

Overall, participants from EMEA indicated they have not prioritized and do not plan to invest as heavily in information security initiatives as the other regions. We find this result interesting in the context of the substantial regulatory framework being implemented in Europe.

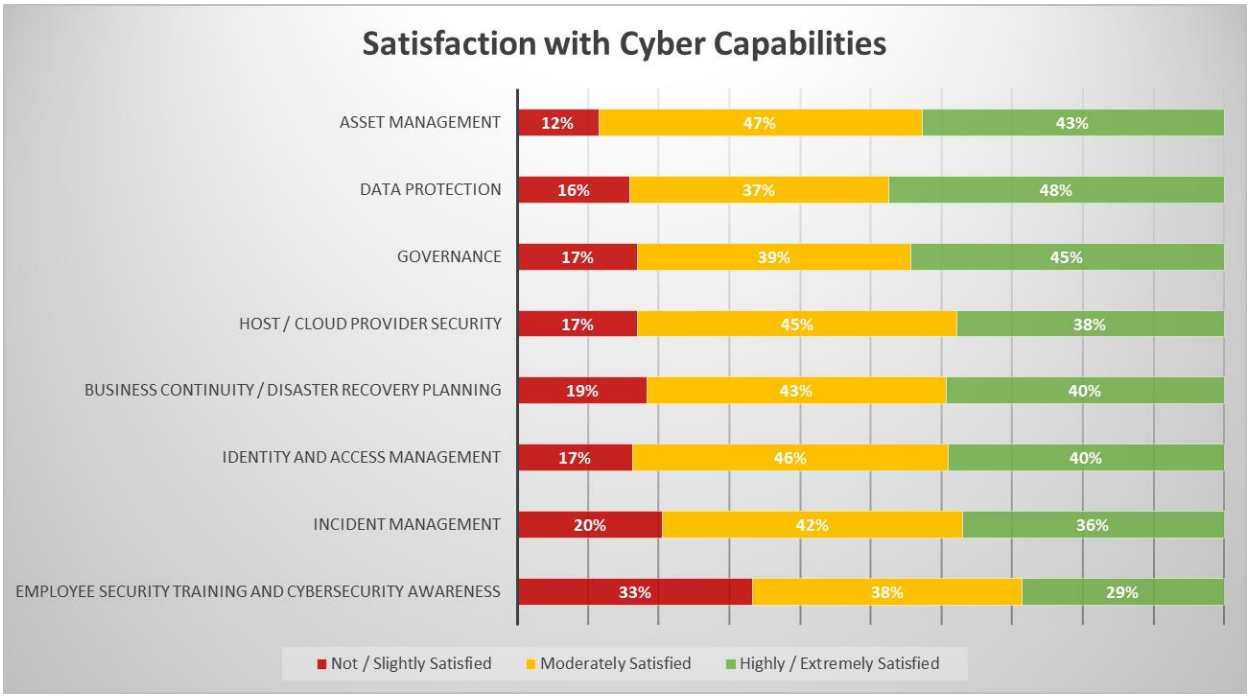
Figure 32: Regional view – Which of the following information security initiatives does your organisation plan to address in the next 12 months?



Satisfaction Level

More than 35% of respondents indicated that they are highly or extremely satisfied with their current cybersecurity capabilities, which include asset management, data protection, governance, cloud security, business continuity and disaster recovery planning, identity and access management, incident management, and security awareness training. This is somewhat surprising considering the other responses throughout the survey indicating a relative lack of investment and frequency of assessments. Perhaps over confidence or lack of awareness and knowledge of the ever-changing threat environment may have contributed to the results.

Figure 33: How satisfied are you with your organisation's capabilities in the following areas?



By Region

Some interesting trends were noted across different regions which correlate with results from previous sections, whereby approximately 40% of respondents in APAC are not satisfied with their current cybersecurity awareness capability and employee security awareness training programs, but 80% of respondents are at least moderately satisfied with their asset management and identity and access management capabilities.

Figure 34: Regional view – How satisfied are you with your organisation's capabilities in the following areas?

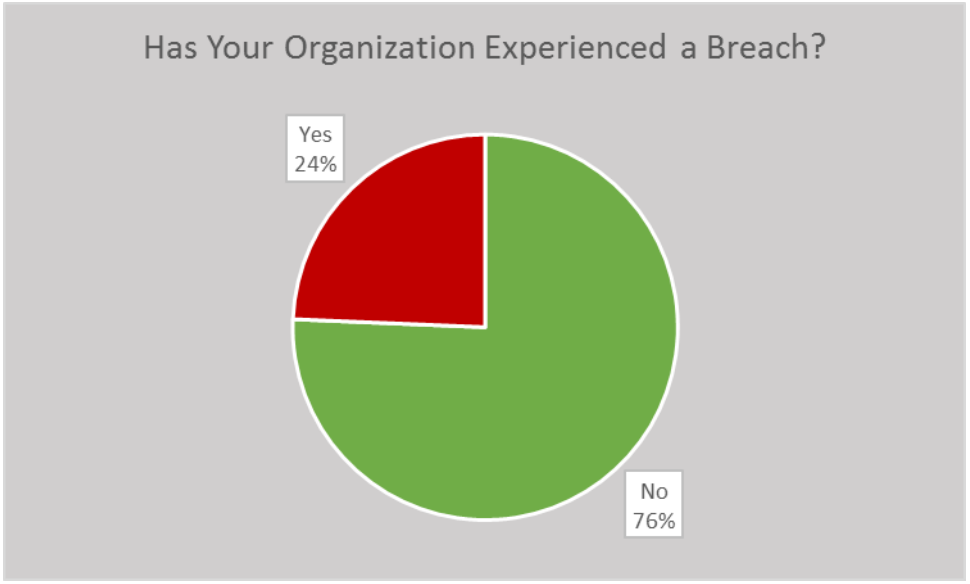
Figure 34 (continued): Regional view – How satisfied are you with your organisation's capabilities in the following areas?

No interesting trend emerged from either the EMEA or the Americas respondents regarding the level of satisfaction in any specific cyber capability surveyed. However, a higher percentage of EMEA respondents reported dissatisfaction across the different cybersecurity capabilities. It will be interesting to see the impact when GDPR enforcement starts in May 2018.

Anatomy of a Breach

Security experts like to say that there are now only two types of organisations: those that know they have been hacked and those that don't know they have been hacked. Our survey shows that 24% of all respondents had a confirmed security breach, (i.e., data was actually stolen). The most serious risks often are the breaches that remain undetected. Unfortunately, this is not possible to measure through a survey. Additionally, the ability to detect a breach depends greatly on the nature of the attack, how much data was actually taken, and the sophistication of the organisation's cybersecurity program. Breaches caused by phishing attacks (e.g., an email seemingly sent by a CFO asking Human Resources for employee tax statements) are identifiable almost immediately after the incidents occur. Conversely, more sophisticated attacks in which hackers probe networks over weeks or months and then slowly siphon off data are notoriously hard to detect without advanced security measures.

Figure 35: Has your organisation experienced a breach?



We find it interesting that 21% of survey respondents who did not have a cybersecurity program reported having a data breach while 28% of companies who have a formal cyber program reported having sustained a breach.

Figure 36: Percentage of respondents reporting a breach that have no formal cybersecurity program in place

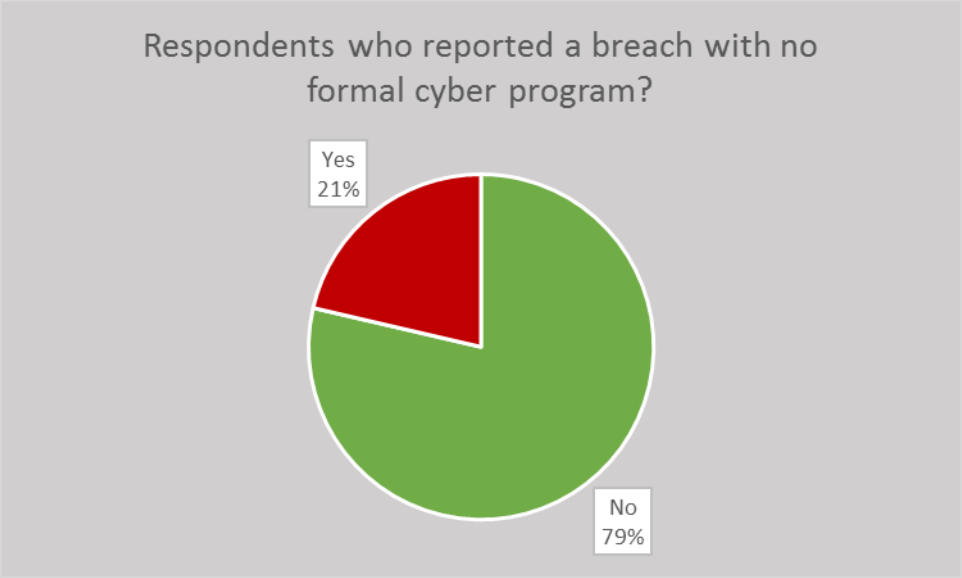
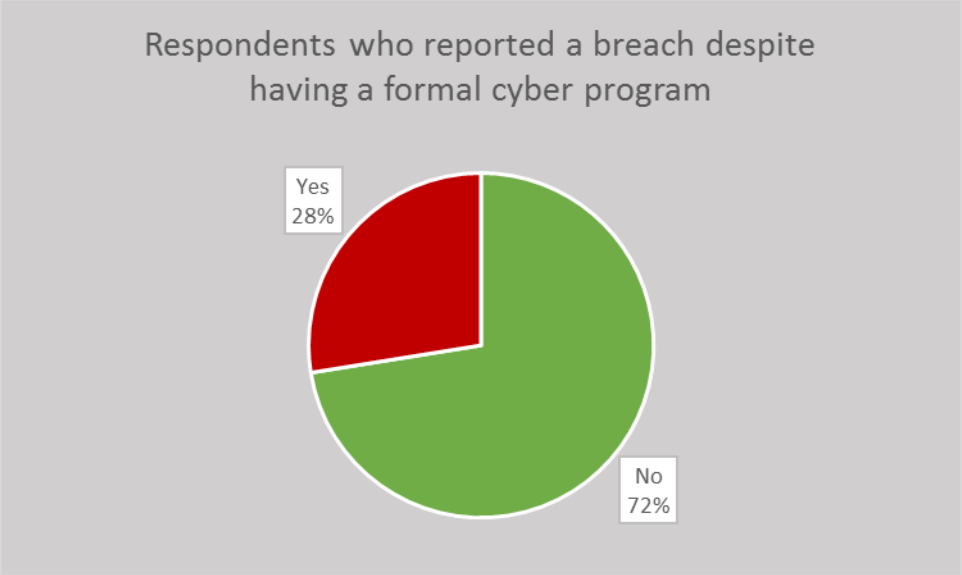


Figure 37: Percentage of respondents reporting a breach despite having a formal cybersecurity program in place



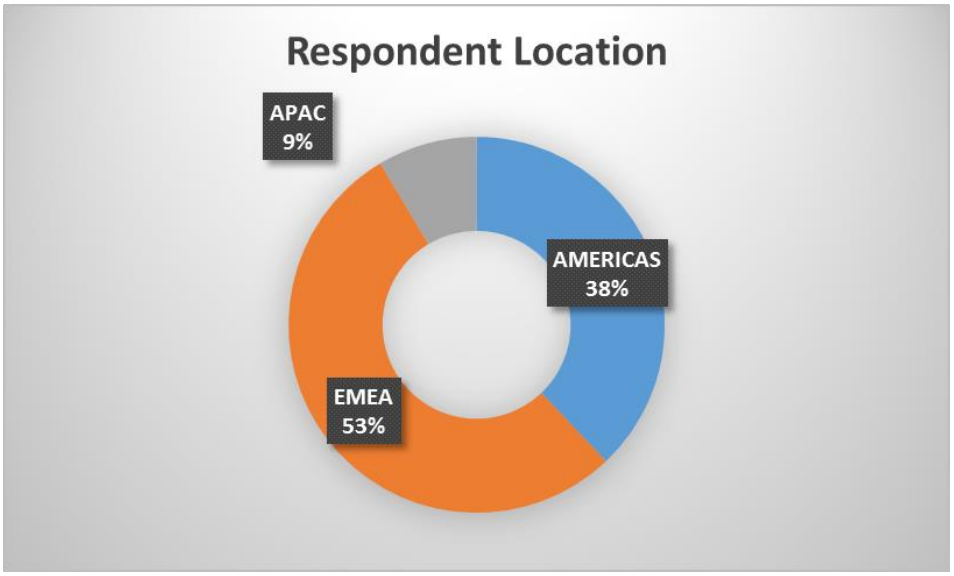
Unfortunately, we do not have additional data needed to determine the reason for the discrepancy. One would hope that having a cyber program would make breaches less likely. Two reasons come to mind: 1) the cyber program was not sufficient or 2) organisations having a cyber program were more likely to identify a breach. One of our previous charts may hold the clue to the answer. From the earlier graph showing the Frequency of Cyber Assessments, we know that the majority of organisations have either never performed an assessment, or perform one on an ad-hoc /

unscheduled basis. Therefore, it seems probable that the organisations may not have adequately assessed the effectiveness of their programs. Cybersecurity, like many risk management initiatives, requires more than a "set it and forget it' approach. Threats continually change, systems grow stale, and new vulnerabilities are introduced. Without evaluating the existing identification, protection, detection, response and recovery capabilities in light of emerging cyber threats, organisations may not even fare better than not having a program at all.

Demographics

The survey was sent to thousands of organisations across different continents – North and South America, combined as the Americas; Europe, Middle East, and Africa, combined as EMEA; and Asia, Australia, and New Zealand; combined as APAC. Based on the responses received, 38% survey participants were from the Americas, 53% from EMEA, and 9% from APAC.

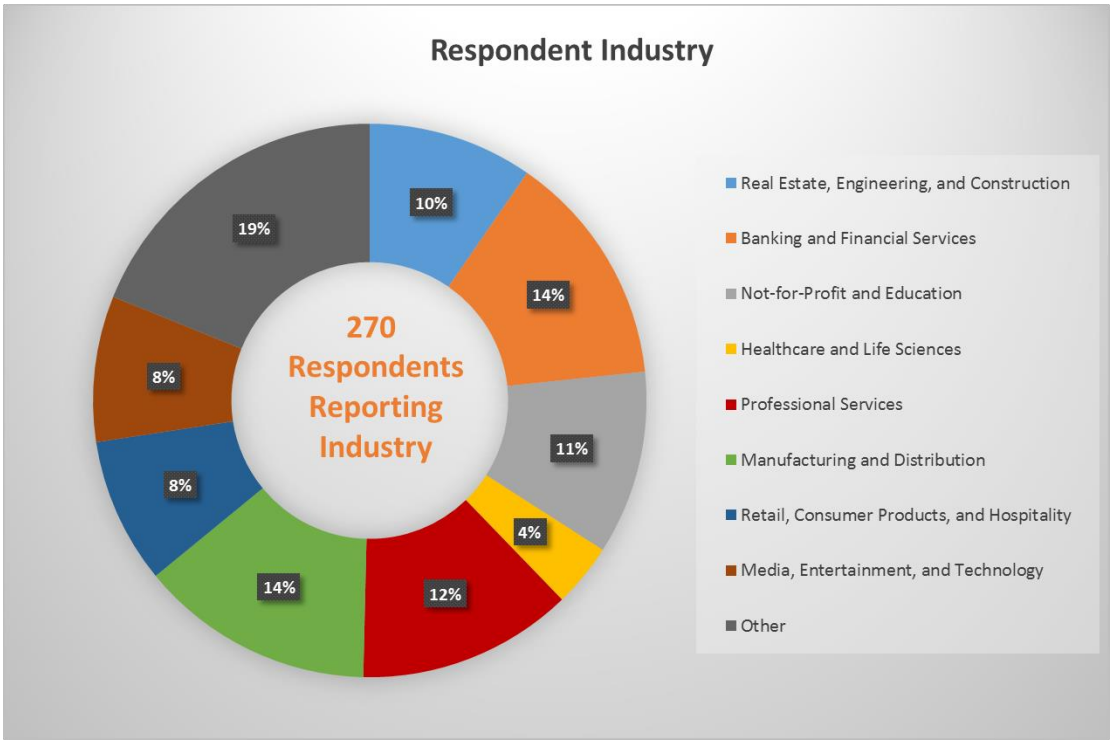
Figure 38: Respondent location



More than 350 participants responded to the survey, and 322 responded to the majority of the survey questions. The respondents were segmented into nine different industries:

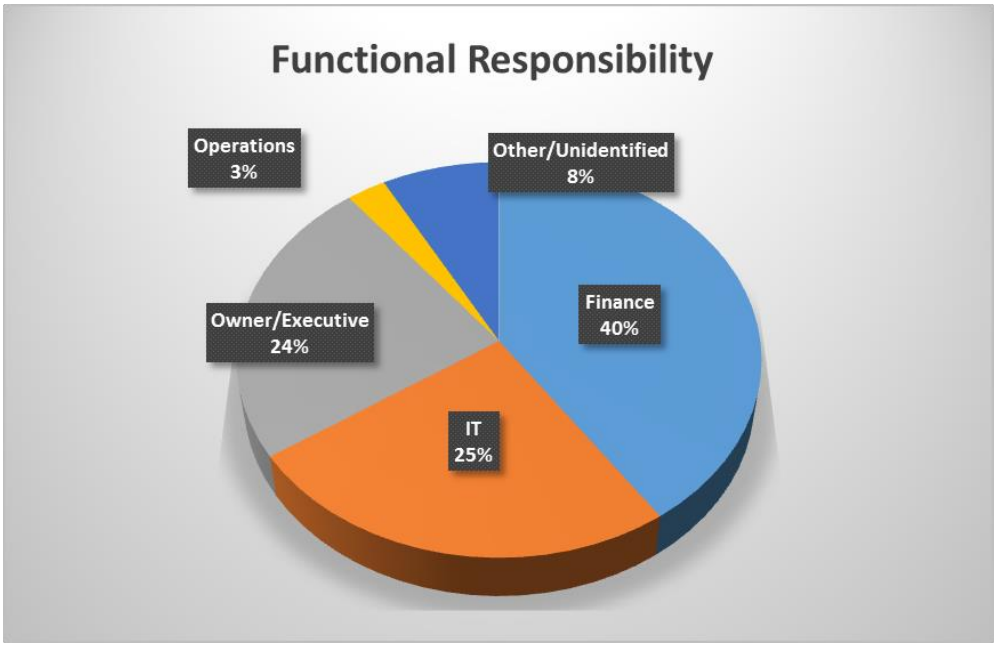
1. Real Estate, Engineering, and Construction
2. Banking and Financial Services
3. Not-for-Profit and Education
4. Healthcare and Life Sciences
5. Professional Services
6. Manufacturing and Distribution
7. Retail, Hospitality, and Consumer Products
8. Media, Entertainment, and Technology
9. Other

Figure 39: Respondent industry



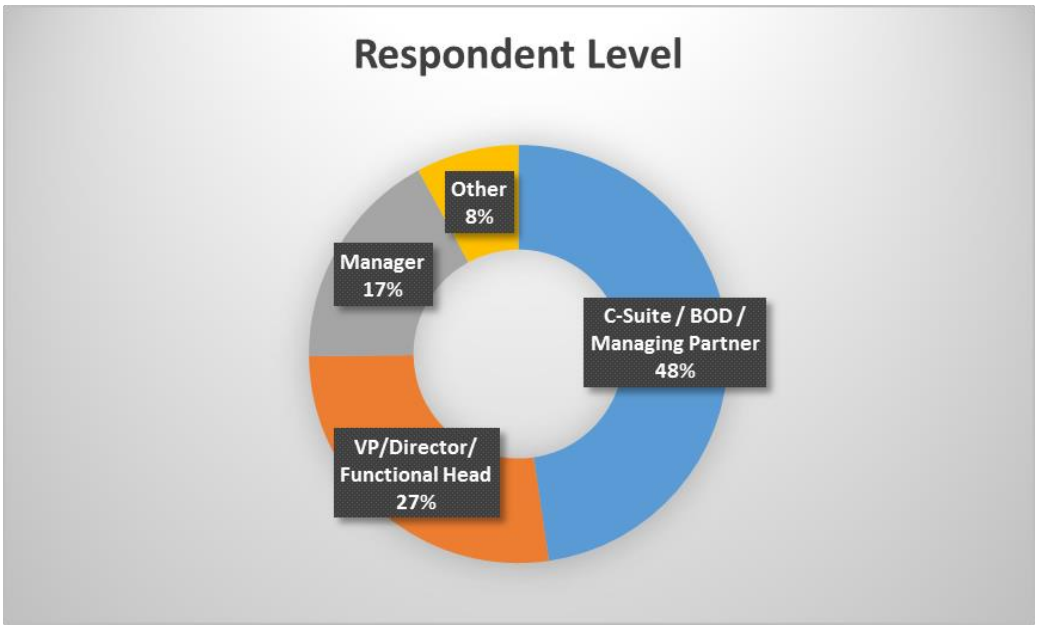
Based on the review of the functional responsibilities indicated by the survey respondents, it was noted that 25% were responsible for IT; 40% for Finance; 24% identified themselves as owners or in executive roles; 3% were part of Operations, and 8% were other or unidentified.

Figure 40: Functional responsibility of respondent



Of the 257 responses received to the question regarding respondent title, 47% self-identified themselves as C-level executives, board directors, or managing partners; 28% self-identified as senior executives such as vice presidents, directors, or functional heads; 17% self-identified as management-level; and 8% indicated that they were in another role.

Figure 41: Title of respondent



Conclusion

As cybersecurity attacks keep increasing in number and have varied levels of negative impact on a large number of organisations globally, it is critical that organisations of all sizes and across all industries acknowledge the ever-changing cybersecurity landscape and the different threats, and be proactive in addressing the concerns. Based on the survey responses, it seems that there are significant opportunities for improvement in the areas of cyber assessment frequency, awareness of threats, and investments. Progress is certainly being made, but organisations have a long way to go in terms of having a strong cyber program in place that can provide robust and repeatable measures to guard against cyber-attacks.

Contact us

For further information, please contact:

Greg Vosper

E greg.vosper@nexia.com
T +44 (0) 2074361114
W nexia.com

David Rubin

E David.Rubin@CohnReznick.com
T +1 201 370 2417
W cohnreznick.com