THE SECURITY TEAM OF 2020

THE
SECURITY
LEADERSHIP
SERIES

TrustedImpact
PROTECTING DIGITAL

"BY 2020, 60% OF DIGITAL BUSINESSES WILL SUFFER MAJOR SERVICE FAILURES DUE TO THE INABILITY OF THE I.T. SECURITY TEAM TO MANAGE DIGITAL RISK..."

-GARTNER

PREFACE/FOREWARD

The Industrial Revolution was recognised as a period of great transformation that radically changed the global economy and influenced nearly every aspect of daily life. However, today, the Digital Age represents an era much more influential and unlike anything seen in the history of mankind.

Today's Digital Age is characterised by multiple, rapidly accelerating changes all occurring simultaneously and causing disruption in ways that few anticipated. Technological changes such as global connectivity, increasing bandwidth, greater technology affordability, faster adoption rates, and increased mobility – each significant in their own right – but when taken together, are rewriting the traditional rules of society and the way whole industries operate within it.

Businesses as we've known them are changing before our eyes. For example, in 2015 "Uber, the world's largest taxi company, owns no vehicles and employs no drivers. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate and has never had to make a bed or serve a meal." On the other hand, it's hard to believe that only a few decades ago, iconic household brands such as Encyclopaedia Britannica, Kodak, or the Yellow Pages would soon be bankrupt because of their inability to respond to these changes.

In the Digital Age, "assets" – which were traditionally physical and tangible in the industrial revolution – have now been replaced with digital manifestations which are both abstract and intangible. While the need to secure one's assets has been essential for centuries, the relatively new concept of "information security" has now taken centre stage because of pervasive global 'actors', all with different motivations find ways to exploit and monetise the value of these information assets.

In the Digital Age, Information Security has the power to make or break business goals. In an era where everything is digitally interconnected, and partners, employees, customers, and even competitors are often collaborators in the process of business innovation, information security can mark the difference between success and failure. Key business objectives such as revenue growth, product quality, time-to-market, customer loyalty, company reputation and shareholder value are all at risk if information security is not interwoven into the fabric of the digital organisation.

Like the Digital Age, the information security industry is also constantly changing and requires innovative approaches to keep pace with the diverse 'actors' motivated to exploit information assets. Therefore, as one of Australia's leading information security consulting firms, we saw value in undertaking an industry survey to collate the latest thinking from a diverse set of Australian industry leaders. The focus was to highlight key industry trends over the next five years (towards the year 2020), and in particular, to correlate how those trends might impact the skills and roles of the security team of 2020 to enable Australian businesses to succeed in the Digital Age.

ABOUT TRUSTEDIMPACT

TrustedImpact has a singular focus in Information Security. We help enterprises achieve their business objectives by protecting the flow of important information from unauthorised access, use, disclosure, disruption, modification, theft, or destruction.

Information security is all we do – we're specialists in information security, not part-time generalists who dabble in this complex discipline. We use seasoned professionals with expertise in information security to position your organisation for growth and success. Our 'business driven context' means recommendations are practical; they reflect your business and integrate well into your day-to-day operations.

We're also independent consultants with no financial affiliation with technology vendors. This means our business model is not about our success in reselling someone else's technology, but is purely focused on your success.

ABOUT THE AUTHOR

A number of TrustedImpact professionals were actively involved in the interviews, collection of data, and synthesis of results including: Steve Judd, Ron Speed, Demetrios Stoupas and Tom Crampton. However, the driving force behind the survey was Ruth Rozario, Principal of TrustedImpact People.

Ruth is an experienced risk executive and has worked in several large Australian financial institutions. She looks after the TrustedImpact "people" division, which seeks to provide contracting resources to organisations. She is committed in building security teams that work and hence is interested in placing people that can work within your team and deliver outcomes on objectives.

Placing anyone in a role is easy, placing people who can complement and work within your team is the challenge.

Ruth can be contacted on (03) 9023-9710 or via email at ruth.rozario@trustedimpact.com.

CONTENTS

THE SURVEY

In late 2014 and early 2015 Trusted**Impact** interviewed thirty (30) influential thought-leaders ("Leaders" or "The Leaders") from the Australian technology, security and risk industries with the aim to gather intelligence on the emerging trends in the security landscape leading up to 2020. In particular, we were keen to understand how these trends would influence the types of skills and roles needed to operate the information security team of 2020.

Survey participants were chosen from a diverse range of Commercial and Government organisations across multiple industry sectors including, for example, the financial services industry through to online and digitally-based organisations. While the Leaders were given an overall structure from which to respond to key questions, an important aspect of the survey involved having an interactive discussion to get their views from their individual and company's perspectives.

EXECUTIVE SUMMARY

Five (5) main conclusions are evident from the synthesis of the survey input and results. These conclusions are:

01. **There are significant changes and trends that are reshaping the information security industry at a rapid pace.**

02. **How one succeeds in the role of the Chief Information Security Officer (or equivalent) is also changing.**

03. **For the security team to be effective in 2020, the composition of skills and roles will change and must become more engaged with their businesses.**

04. **Overall 'demand' for security personnel will undoubtedly outstrip 'supply' in the next five years, however, what is more important is the mix and composition of skills for the successful Security Team of 2020.**

05. **Therefore, success in 2020 requires businesses to start preparing today to keep ahead of these information security trends and to change the composition of skills and roles required to meet these challenges.**

Surviving in a fast-changing environment: The survey Leaders overwhelmingly agreed that the industry is in a period of significant change. Many reflected on the challenges they face dealing with the diversity and complexity of the rapidly emerging threats that their organisations face from a host of external sources. Many also expressed concerns about their abilities to keep pace with such threats.

In addition, many organisations find themselves simultaneously faced with the need to be more actively and effectively engaged internally with their broader business populations, (both company employees and contractors) to raise awareness of security threats and proactively manage the prevalent impact of 'clickjacking' and other employee-related security issues they faced. On this topic, many Leaders felt that they had been successful in engaging with senior management on the risks and issues of information security, the majority felt they didn't have the resources to adequately engage the much larger population of middle management or customer-facing staff.

INDUSTRY PARADIGM SHIFTS (From – **To**)

Product knowledge	**Vendor knowledge**
Firewalls / Perimeter	**Information Flows**
Ivory Tower / Policy	**Company-wide / Pervasive**
Business Intelligence	**Big Data Analytics**
Anti-virus	**Social engineering**
Internet capacity	**Mobility / IoT**

Finally, the increasing role of third parties, outsourcing, and "the cloud" is clearly an area that has, and will continue to shift attention. The traditional approach to 'protect the perimeter' is becoming difficult at best (and at worst, obsolete) when a majority of an organisation's data resides outside of the traditional perimeter. One Leader adeptly noted "a few years ago, it was all about firewalls and the perimeter. It's now about the cloud, and soon it will all be about information flows". In addition, the concept of a simple "third party" is changing as another Leader explained their efforts to analyse the use of certain 'domain credentials' and uncovered three "levels" of third parties (i.e. the use of 'sub' and 'sub-sub' contractors) residing across three different countries.

The CISO as a marketer and leader: The Chief Information Security Officer (CISO, or equivalent) will become less focused on technology and security tools, and become considerably more focused on marketing. This is not only focused 'upwards' to the Executive team and

Board but also across the organisation to all staff and even involve end customers. The main challenge in this role is to engage the "hearts and minds" of the organisation so they are more empowered to become the protectors of the business's and sensitive data.

The role is also becoming more of an overall business leadership role. Many Leaders are trying creative ways to better depict and describe the role (e.g. "digital protection team"), as it shifts from a more traditional "gatekeeper role" to an "enabler of the business role". We noted nevertheless, that our Leaders felt that these skills are "additional" requirements, as a number strongly believe an effective CISO must maintain a very high degree of technical proficiency due to the complex technical nature of many threats.

The successful security team of 2020 must become more "well rounded": Communication, negotiation, analytical and business engagement skills were all, on average, identified as large gaps leading up to 2020. We believe the shift towards 'softer' people skills is consistent with the industry trends around business engagement and the use of third parties for a majority of a company's IT systems. In these circumstances, skills such as negotiation and communication will be become more important to protect the company's sensitive data. In fact, one Leader noted that their team would need to shift from having 'product knowledge' to having 'vendor knowledge'. This is an interesting shift as not too long ago, nearly all skills recruited for in the information security space were technical skills. We also noted that one skill, Product-Focused expertise actually had a 'negative gap', or in other words, will become less important in 2020 than it is today.

Security roles – less island mentality, more eco-system interconnected: In 2020, information security will no longer work effectively as just an "island" function residing somewhere in the organisation. Instead, it must become an interconnected matrix of roles working collaboratively and cohesively across departments and third parties to adequately protect the organisation's information. Four of the roles identified as becoming significantly more important in 2020 are Privacy, Risk Management, Security Architecture and Security Operations – all roles that are not necessarily part of a traditional security function but will play a critical part of its success. We feel that this is an indication that information security is projected to encompass or impact on a broader range of organisational roles and functions by 2020.

In terms of the role 'gap' between today and 2020, Business Analysis roles report the largest difference. This is consistent with trends and skills, where business engagement is now growing to be an important skill and trend.

The future is here today: If you wait to build the Security Team of 2020, you'll have missed the boat. The information security industry is changing, as well as the skills and roles required to meet the challenges of 2020. A wealth of industry data (in addition to input from our Leaders), see the overall 'demand' for information security personnel far outstripping today's 'supply' or existing labour pool.

In this type of environment, "prices" for quality security personnel will likely rise, and organisations will likely find that qualified company employees may be able to find higher paid, external contractor roles. Thus, the organisation's challenge to attract and retain qualified personnel will likely increase and will require well-thought-through plans that encompass thoughtful personnel strategies to address key requirements such as skill development, company loyalty, recognition and reward mechanisms, work satisfaction objectives, and remuneration options, etc.

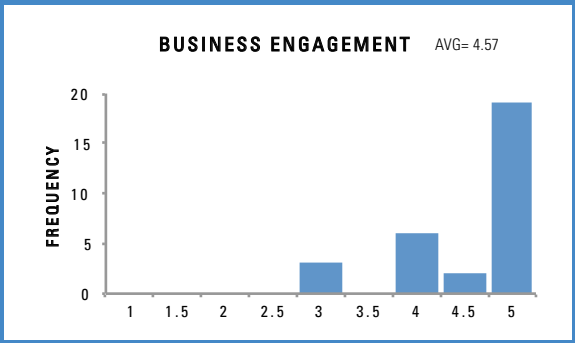
Furthermore, the company's approach to utilising employees versus contractors, external partners, vendors, and/or managed service organisations will become a necessary piece of the puzzle. For example, if internal acquisition and retention strategies to obtain the right security skills or resources is ineffective, the company's external risks and threats will not simply 'hold off' until the company's resourcing problem is solved. One prudent approach will be to build strategic partnerships with capable organisations that can complement a company's internal resources (or lack thereof).

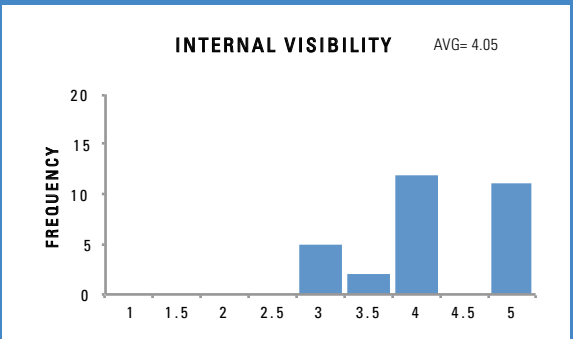
Regardless of approach, if an organisation does not consider the important strategic implications of these issues TODAY and begin to put actions into play, waiting until 2020 to respond will be too late. The adage of 'a stitch in time, saves nine' was always relevant in information security, but with the changes facing the industry, it's an absolute necessity if your organisation wants to succeed in 2020.

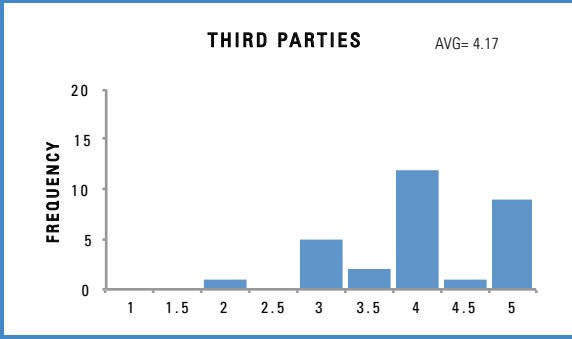
TRENDS

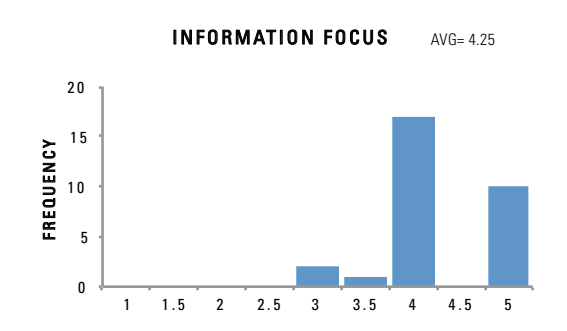
STATISTICAL ANALYSIS

The following graphs illustrate the numerical results relating to the preselected industry trends. Participants ranked their responses on a nine point scale ranging between "significantly disagree" (score of 1), "disagree" (score of 2), "neutral" (score of 3), "agree" (score of 4) to "significantly agree" (score of 5). Participants could also score half way between those ratings (thus 0.5 ratings). (AVG= Average)









SURVEY RESULTS TRENDS

To understand what skills and roles will be needed by 2020, we began the survey exploring the issues and industry trends that participants were facing. The objective of this approach was to ensure that participants had an appropriate future perspective in mind.

Indeed, history is littered with unfortunate examples where major shifts in technology have been the demise in old thinking. It is said that "military men are always preparing to fight the last war, rather than the next one". Thus, the objective of beginning the survey within the context of major industry trends, was intended to ensure that the participants are not falling into the trap of old thinking.

The survey, specifically highlighted four key trends that Trusted**Impact** saw as relevant to the industry. The objective of highlighting these trends was to not only ascertain the significance of these issues, but also to get the participants thinking of other key trends that they may be facing and which would be relevant in regards to the security team of 2020.

The four (4) trends that were initially highlighted to participants were:

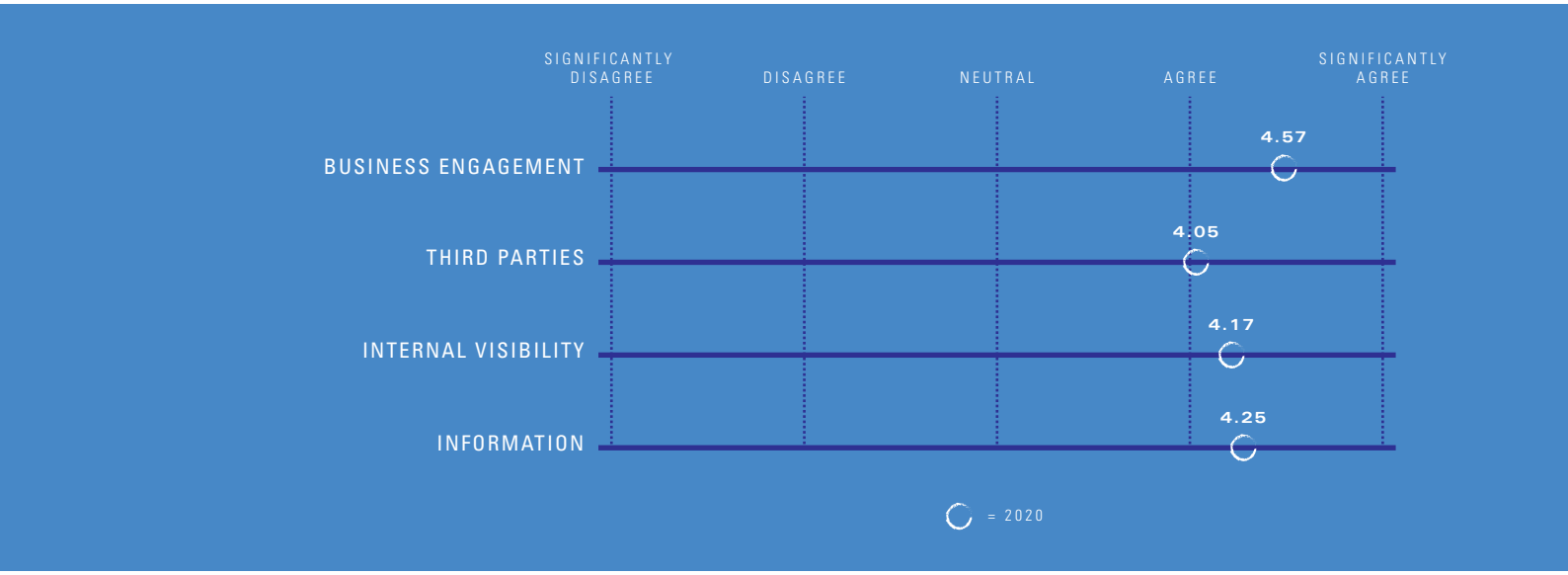
01. **Business Engagement:** By 2020, an effective security program will require members focused on more actively engaging company personnel outside of the IT Department and at all levels from entry to senior executives.

02. **Third Parties:** By 2020, external third parties will gather, store or process more than half of the company's systems or data.

03. **Internal Visibility:** By 2020, the security program will need better tools and skills to monitor 'internal' activity and data flows.

04. **Information Focus:** By 2020, the organisation must have a much better understanding of "sensitive information"; what it is and where it resides.

Overall, the participants of the survey ranked each of these four trends, on average between agree and significantly agree. The following graphic illustrates the average results of the responses.



"WE NEED TO EMBED SECURITY INTO BUSINESS OPERATIONS"

Business engagement was noted as the most significant trend facing the security team of 2020. Our Leaders ranked "Business Engagement" the highest with an average score of 4.57. This implies that the effective security team will need to be focused on more actively engaging company personnel outside of the IT Department and at all levels from entry-level to senior executives. Information security is clearly not simply an Information Technology issue, but is a much broader issue that permeates an entire organisation. For example, front-line staff who deal directly with customer requests are typically best suited to determine whether a customer is 'genuine' in the event they cannot provide all of the 'factors of authentication' required for account enquiries.

"SECURITY MUST BE DRIVEN FROM THE TOP. WE RECENTLY CREATED A JOINT COMMUNIQUE WITH THE CEO TO STAFF ABOUT THE IMPORTANCE OF SECURITY."

A large number of participants noted that their engagement with senior executives and the Board of Directors had improved significantly over the previous few years. They felt that there was a healthy level of interaction with senior management to keep them abreast of the key risks that their organisations faced. However, their team or budget was not yet large enough to actively engage with middle-management or lower staff levels. We also found it interesting that several participants used the same word to describe the challenges they faced with respect to business engagement, as they noted the need to continue to "demystify" security, so that it was more meaningful and practical to other company employees who may not appreciate the unique idiosyncrasies of the information security discipline.

The team of 2020 must have a greater "Information Focus". The second highest trend rating was discussions with participants that "sensitive information" means diversely different things to different types of companies and within disparate industries. For example, in consumer-intensive organisations sensitive information is typically "personally identifying information" on credit and debit card details. In other organisations, it may comprise intellectual property. While we did not specifically focus on what information was considered to be 'sensitive' participant's understood the approach and provided some interesting perspectives.

Irrespective of the definition, it was clear from our Leaders that organisations are taking strides to improve their information focus. For example, one organisation saw "security" as one piece of the "information" challenge. In fact, this organisation went against traditional convention and expanded the remit of the Security Manager to a more exacting definition of the Chief "Information" Officer. The previous "CIO" was now considered the Chief Technology Officer, or CTO, to connote a role to apply technology to transform and improve the business. This 'new' role was all about information from data quality, data lifecycle, big data analytics, etc. Indeed, security from their perspective was simply one part of information. "Once you know what data you have, securing the valuable information becomes much easier". One other organisation undertook a global initiative (lead by the CEO, rather than a CIO or CISO) to clearly identify the intellectual property that resided across the company. What was unique, was the business driven nature of this program, which recognised, and broadly quantified the value of their intellectual property to ensure that additional protections were put into place to keep it safe from its competitors.

One key trend for the security team of 2020 is the need to have a better understanding of 'sensitive information' – what it is and everywhere it resides.

A shining example of a 'leader' was the CEO (not CIO or CISO) who initiated a global project to identify the company's 'Crown Jewels'... intellectual property that, if taken or lost, would reduce revenues by a defined amount.

This was a great example and unique because it was: a) driven from the top – not just an "IT project", b) about identifying & segregating valuable data, and c) quantified value – a challenge most organisations struggle with.

The security team of 2020 must have better tools and skills to provide "Internal Visibility" of activity and data flows. Our leader's ranked greater 'visibility' of data flows and electronic activity as a top trend – in particular, identifying anomalies or abnormal data flows that might signal a breach or nefarious activity. Many organisations and Leaders did not have rudimentary capability today. The scoring of this trend reached an average of 4.2 (slightly higher than 'Agree').

However, we noted that several leaders expressed some important variations or potential exceptions to this trend. For example, one noted that their organisation had set specific targets to outsource a large percentage of their systems and data to third parties. This leader paradoxically noted, "when we put our data into the cloud, we lost all visibility of who had access to it... for example, how do you do 'incident management' in the cloud?" Another leader coined the interesting term of "Black Data", which in their mind was the result of their organisation encrypting a large number of links and outside of volume information, they had little to no visibility into what data was flowing or whether it was of value.

"HOW DO YOU DO 'INCIDENT MANAGEMENT' IN THE CLOUD?"

When discussing the security challenges of using 3rd parties for company data and systems, one leader noted that they explicitly tracked the 'domain credentials' (aka "superuser" credentials) and found that they were physically located across 3 different companies (suppliers of suppliers of suppliers) and residing in 3 different countries. With growth in the use of 3rd parties (and their own 3rd parties), will these numbers grow exponentially by 2020?

"FIVE YEARS AGO, A LARGE FOCUS ON SECURITY WAS ON 'PRODUCT KNOWLEDGE', WHEREBY BY 2020 'VENDOR KNOWLEDGE' WILL BECOME CONSIDERABLY MORE NECESSARY"

In 2020, "third parties" will gather, store or process more than half of a company's data. Our Leaders agreed (score of 4.1) with this trend. Several said they were either beyond this or close to it today. In fact, one even shared an explicit goal of "70/70/70", which in this context meant they aimed to have 70% of their systems out-sourced, 70% would be offshore, and 70% would be with one major provider.

We also should highlight that there was little definitional difference between third parties and "the cloud". Some interesting perspectives were highlighted in regards to 'the cloud' and the often used term "Shadow IT". For example, a few organisations had conducted in-depth analysis on the 'outbound' or 'exfiltrated' data from the organisation and the technology services/providers that employees were using for various reasons. While these Leaders intuitively felt that the use of unsanctioned third party system (aka "shadow IT") was extensive, it had never been quantified. These organisations were astounded to learn the amount of data that was flowing to unknown third parties. One participant noted that there were 17 'formally sanctioned' providers, yet learned that employees over a period of approximately one month had accessed over 275 unique data storage locations and providers. While they thought it may be two or three times larger, they never anticipated a factor of 16x.

NOTABLE INSIGHTS

Our industry leaders also provided us with constructive input to a diverse range of trends that they were experiencing from either their individual or company's perspectives. These trends often took the form of challenges they faced or saw occurring in the upcoming 5 years, and are summarised in the following:

» With the exponential growth in data and "Internet of Things" (IoT), we'll need to have Artificial Intelligence and "cognitive secuirty".

» Having a deep understanding of technology is now just the ticket to play – one will need business acumen to succeed.

» We must "build in" security. With application development – ensuring secure architecture and coding is applied at the start – and we need to 'help' the developers rather then just beat them up.

» We need better ways to identify and understand vulnerabilities. Today there is no consistent way on a larger scale across organisations to compare vulnerabilities on an 'apples to apples' basis. We need to build common languages about threats and vulnerabilities and develop consistent approaches to resolve these vulnerabilities.

» Information security awareness – we must learn from WWII propaganda 'loose lips sink ships'… the ability to win the hearts and minds of the masses to be aware of info security issues.

» Ethics – where does surveillance stop? – an ethical position and philosophical issue. I'm concerned that security professionals may lack ethics or morals.

» Originally security was left to IT and they'd make the decision. Then we devolved it to become the responsibility of the business units – but have now recognised that there needs to be an overall view of baseline set of requirements to ensure that individual business units think security across the organisation - particularly in environments with lots of disruptive change.

» We must be able to respond to a breach or incident – there's not much difference between organisations that have breaches. However, there is a large gap between those who respond WELL, versus those that respond POORLY.

» Running tin is expensive – the issues therefore are moving from the bottom of the IT stack to higher and more about applications.

» A shift to 'customer focus' – that's external customers, not just users. The next generation may value security less (Facebook), so it's tough to build in security for someone who can't visualise the risks, or may not value the issues.

» Big Data started off as a way to identify how to cross sell products to likely customers. However, there become broader issues when the big data starts to connect the dots behind someone's behaviour. For example, is it okay to connect someone's dietary habits from their grocery store purchases and connect information to their health insurance rates?

» It's about Enterprise Information Management - where security is only one part. Information is about lifecycle, quality, duplication, data mining/ analytics, and security is only one part of information – unlocking the value of information and protecting that value.

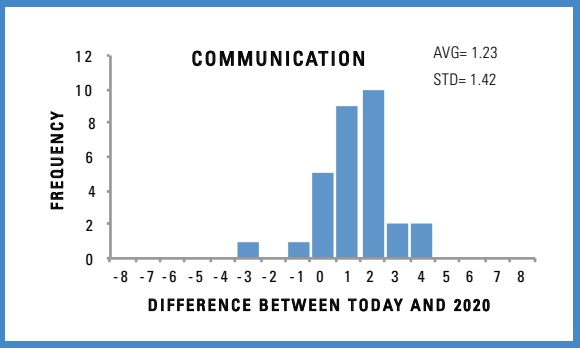
» The 'human factor' – insider threat – people are the weakest links.

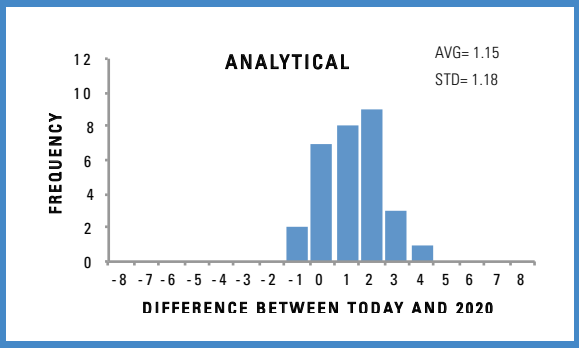
» We need to get smarter about design – developing a 'secure process' versus expecting users to understand security – focusing on design from the start – car airbag example – don't make them drive safer, give them ways to protect themselves from an incident.

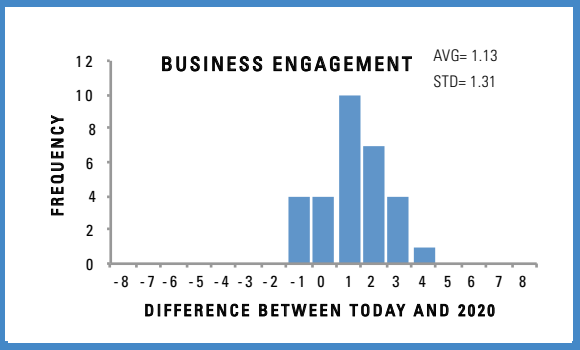
SKILLS

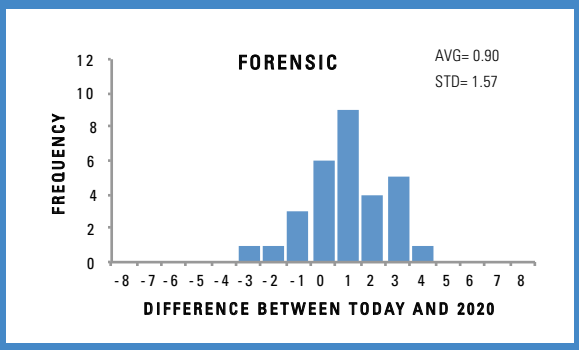
STATISTICAL ANALYSIS

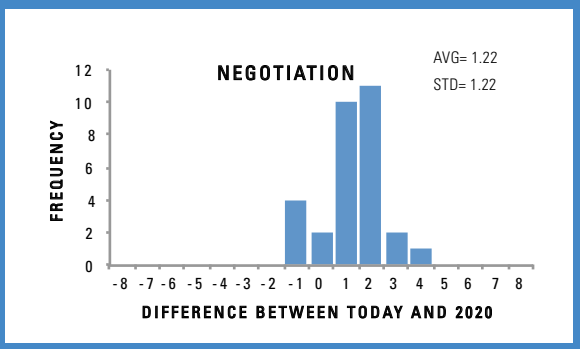
These graphs illustrate analysis conducted of the skills section of the survey. For each skill, the numerical difference between the "today" score and the "2020" score was calculated. This numbers below are the 'gap' between today's skill position and what is required by 2020. These graphs illustrate the frequency of respondent gaps. (AVG = Average, STD = Standard Deviation)

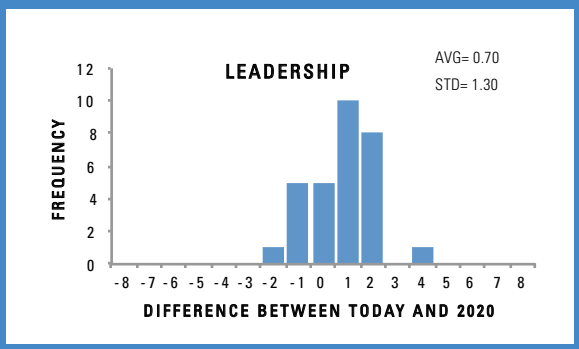


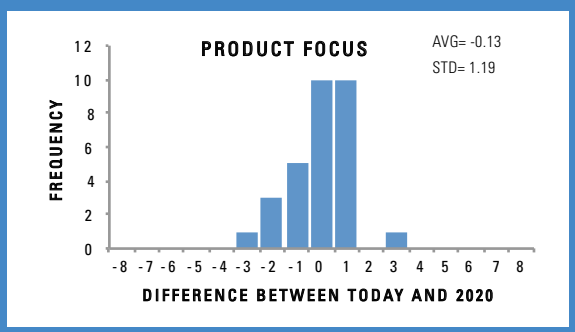


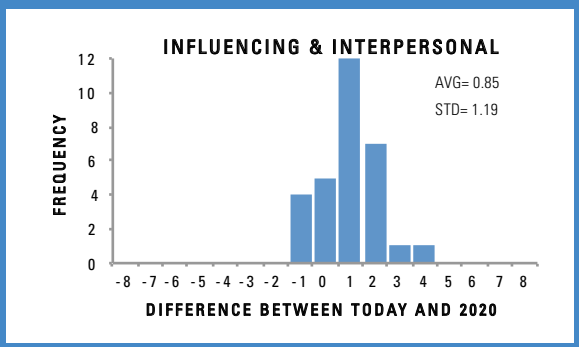












SURVEY RESULTS SKILLS

After understanding the trends, the '2020 Security Team' Leadership series collected the views on a range of different skills that will be required to meet the fast changing trends and also the challenges in sourcing the skills. We looked at eight (8) key skills and asked the question where it is today and how important will it be in 2020.

The eight (8) different skills defined were as follows:

01. **Communication** – the ability to convey security advice (written and verbal) in easily understood, non-technical jargon to both executive and staff levels from different disciplines in the broader business.

02. **Business Engagement and Understanding of the Business** – the ability to translate complex security and risk issues to non-security personal and to constructively engage with different business disciplines (i.e. marketing, legal, operations, etc.) in a context that is relevant to their roles and responsibilities.

03. **Negotiation/Contractor/Partner Management** – the ability to collaboratively and constructively liaise and/or negotiate with external parties who may not share the same operational objectives or demands as your organisation. This involves identifying opportunities where there may be 'common ground' to achieve desired outcomes for all parties involved.

04. **Product Focussed Expertise** – the ability to have a deep understanding of the unique idiosyncrasies, constraints and capabilities of a particular technology product(s) to maximise the effectiveness of its purpose.

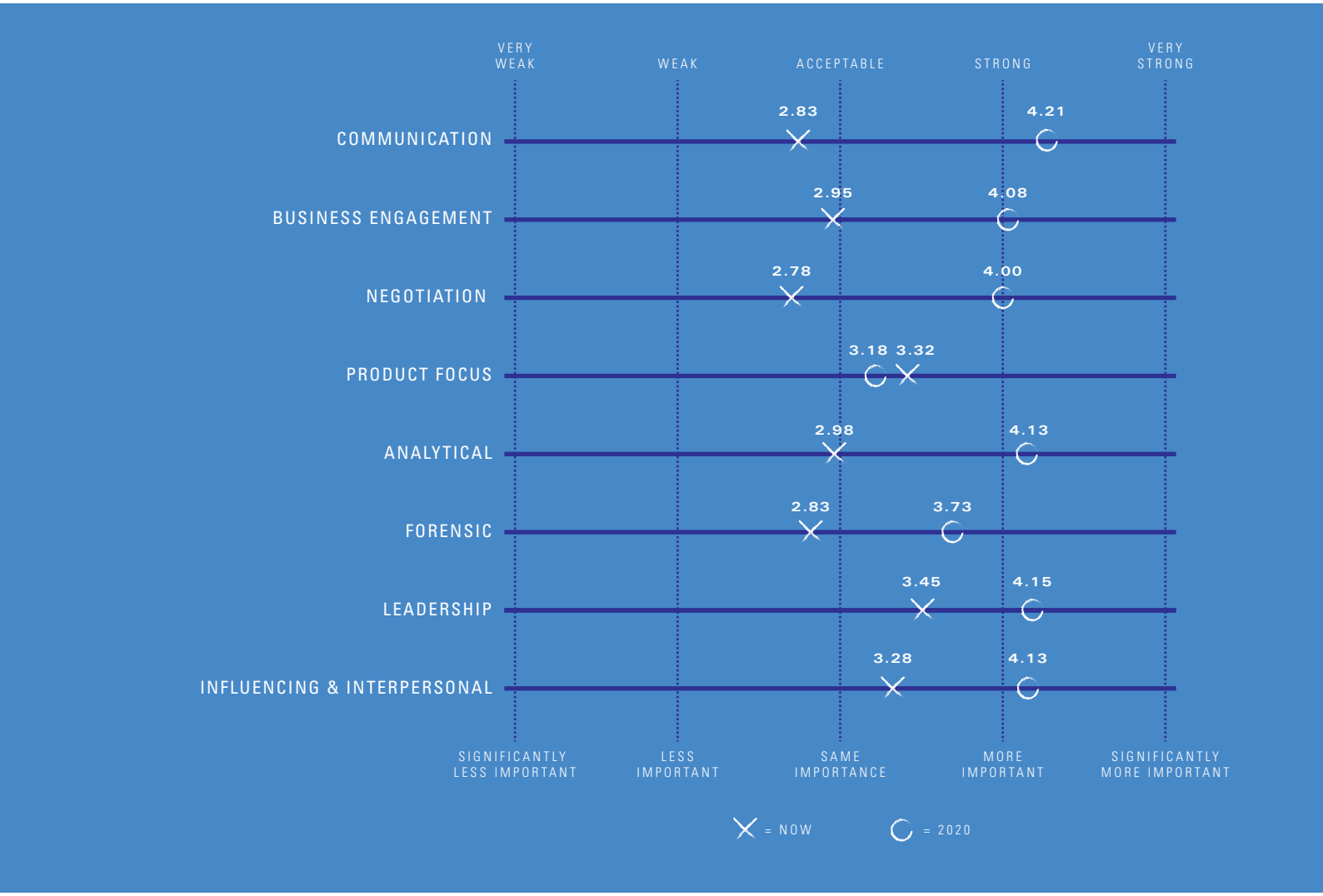
05. **Broad Analytical Expertise** – the ability to apply logical thinking and analytical skill on complex issues. To identify and separate 'cause and effect', to interrogate data to confirm or disprove hypotheses and make logical connections between apparently disparate data.

06. **Forensic Expertise** – the ability to apply a deep level of technical skill to uncover and clearly understand the events which might lead to the potential misuse of an organisation's computers or data.

07. **Leadership** – the ability, skill, experience and traits in which to apply a process of social influence in which a person can enlist the aid and support of others in the accomplishment of common objectives.

08. **Influencing & Interpersonal** – the ability and skill used by a person to properly interact with others. In the business domain, the term generally refers to an employee's ability to get along with others while getting the job done. Interpersonal skills include everything from communication and listening to attitude and deportment.

An illustration of the average results for each of the skills is below:



Key observations noted from these results include:

» The results revealed that communication, negotiation, analytical and business engagement skills are all close to or below 'acceptable' today and the results of the survey indicate that they will become 'more important' in 2020. This move towards 'softer' people skills is consistent with where the information security function is moving.

"COMMUNICATION IS ALL ABOUT 'PEOPLE' AND THERE IS A NEED TO DEMYSTIFY SECURITY"

» More information technology is expected to be outsourced, hence negotiation and communication skills are important. We saw earlier that business engagement was one of the 'Trends' where participants 'significantly agree' that it will be more important. This is consistent with 'Skills' like business engagement and analytical skill will also be 'more important' in 2020. This is interesting, as not too long ago, most skills required in the information security space were technically focused.

» The survey also found that in-depth product-focused expertise moves backwards in terms of importance. An interesting trend and consistent as organisations look to outsourcing functions. Understanding products in the information security space will diminish while there will be an increased focus on vendors. Vendor knowledge will become more important.

» The survey also found that there was a slight movement in forensic expertise skills. A large number of organisations that took part in the survey outsourced this function and indicated that they will continue to do so leading up to 2020. Hence if there was a skill gap, some of the organisations did not see it as an issue.

» With leadership – we found the gap very small as most of the leaders that took part in the survey agreed that it is strong now and will continue to play an important role. Many of the respondents agreed that the leadership skill set is changing and this is consistent with the changing role of the CISO – a question we asked later in the survey.

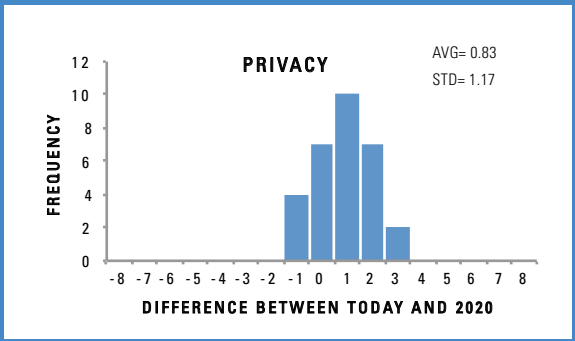
One Leader was working in an organisation with a large number of 'legacy' systems that were tightly interwoven, and often relatively fragile. They expressed their frustration as "our executives always get distracted about the latest and coolest sounding cyber trends, and don't understand just how hard simple patching and maintaining is. It often takes us two weeks to patch a system and then confirm that it hasn't broken something along the way".

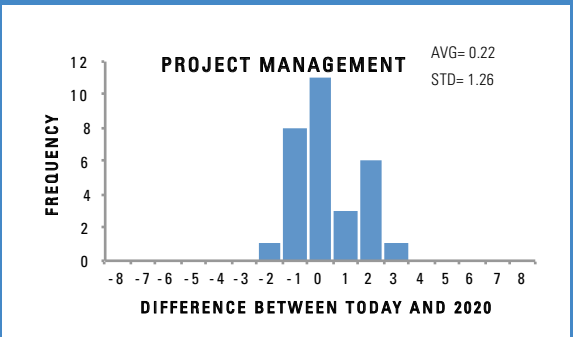
"THERE'S A SKILLS SHORTAGE – WE'RE ALREADY THERE AND ONLY A HEARTBEAT AWAY FROM A CRISIS."

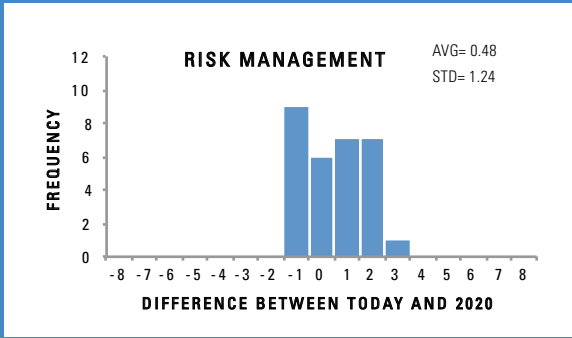
ROLES

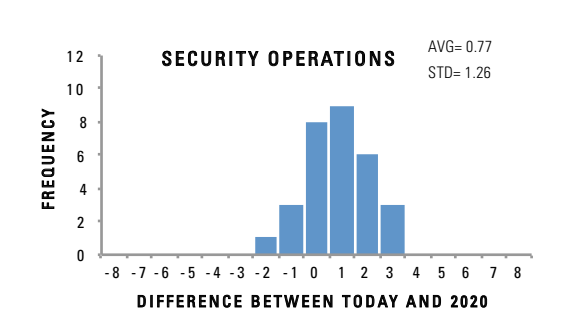
STATISTICAL ANALYSIS

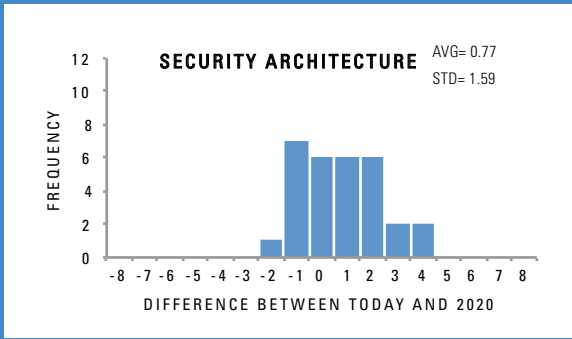
These graphs illustrate analysis conducted of the roles section of the survey. For each role, the numerical difference between the "today" score and the "2020" score was calculated. This numbers below are the 'gap' between today's role position and what is required by 2020. These graphs illustrate the frequency of respondent gaps. (AVG = Average, STD = Standard Deviation)

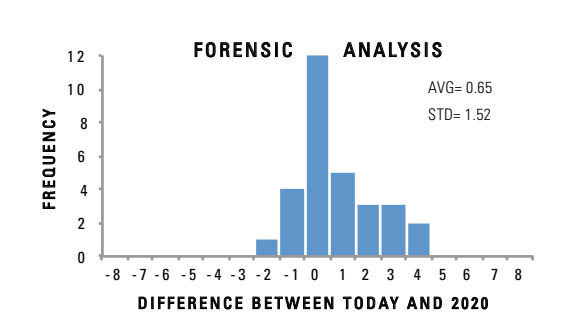


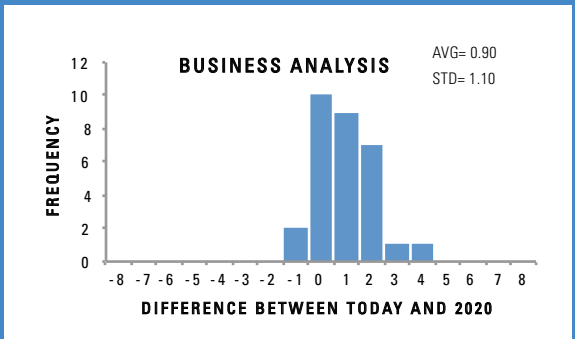












SURVEY RESULTS ROLES

Following the discussion on skills required by 2020, the leadership survey then collected views on "roles" required to meet the rapidly emerging information security trends and challenges of the coming five years. We looked at seven (7) key roles and asked the questions "where is it today?" and "how important will it be in 2020".

The seven (7) key roles were the following:

01. **Privacy** – A role to oversee that the handling of personal information held by an organisation to ensure that the handling practices are in-line with the appropriate laws, regulations and commitments.

02. **Risk Management** – A role that involves identifying, assessing and prioritising risks, often followed by the coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of a risk.

03. **Security Architecture** – A role that involves applying a comprehensive and rigorous method for describing a current and/or future structure and behaviour for an organisation's security processes, information security systems, personnel and organisational sub-units, so that they align with the organisation's core goals and strategic direction.

04. **Business Analysis** – A role to identify business needs and determine solutions to business problems.

05. **Project Management** – A role associated with planning, organising, motivating, and controlling resources, procedures and protocols to achieve specific goals in business or daily problems.

06. **Security Operations** – A role responsible for developing security engineering solutions to support software development, managing enterprise information security appliances, enforcing information security policy, and engaging in operations directly supporting incident response activities

07. **Forensic Analysis** – A role that typically involves conducting analysis in technology environments to understand what may have transpired, recovering data that has been deleted or encrypted, and uncovering passwords. Depending on the type of evidence that is recovered, the data may also be used as evidence in court.

The following diagram provides a summary snapshot of the average survey responses:

Key observations noted from these results include:

"STRONG PRODUCT SKILLS ARE NEEDED CURRENTLY BUT WE SEE THIS DIMINISHING OVER TIME"

» Four of the seven roles surveyed are predicted to become more important by 2020. The roles are Privacy, Risk Management, Security Architecture and Security Operations. In general, this could be interpreted as an indication that information security is projected to encompass or impact on a broader range of organisational roles and functions over the coming years, some of which are not traditionally regarded as "technical" but more management disciplines (e.g. Privacy and Risk Management). What is also interesting about 'non-traditional' security roles such as these are that, because they require cross-discipline skills, they could be difficult to hire for.

» In terms of gaps of where we are today and to 2020, Business Analysis roles report the largest difference. This is consistent with trends and skills, where business engagement is now growing to be an important skill and trend.

» The increasing importance of the Privacy roles are consistent with the current trend of moving more information to the cloud, increases in third party engagement and increases in outsourcing activities. Such trends are heightening focus on protecting information (vs. technology) and, the privacy of personal data will be of utmost importance.

» The increasing importance in the shift of Security Architecture roles to becoming more important is a reflection of the increasing need for more sophisticated approaches to security – i.e. moving beyond largely increasing security not only within the perimeter based' approaches to protection of information in a range of different contexts (e.g. cloud and BYOD) and using a variety of different methods (e.g. behavioural monitoring and alerting), but also outside, as organisations experience increase usage of cloud software with BYOD being used at work.

» The increasing importance of Security Operations roles is interesting as, in many organisations, traditional tasks such as access management administration over time have been progressively automated. Hence it is likely that security operational roles will not only increase in importance, but also change in their focus away from more administrative activities and towards a more proactive detection and response to security events. With the trends, we saw that in 2020 Internal Visibility is becoming significantly more important, and this is consistent with the Security Operations role becoming more important in 2020.

» Project Management and Forensic skills have a smaller gap from where we are today to 2020. This could be due to project management being part of the Program Office role and Forensic roles being outsourced

"ONCE YOU UNDERSTAND THE INFORMATION OF THE COMPANY, THE ABILITY TO SECURE THE VALUABLE INFORMATION BECOMES MUCH CLEARER AND EASIER"

We found it interesting to note that when we compile the comments from all participants, we noted an age-old debate was still alive and well. Several Leaders enthusiastically believed that it was absolutely imperative that the two 'disciplines' of Risk and Security must be combined for a better outcome. On the other hand, we also had nearly as many respondents who expressed the completely opposite view and believed that if the two should be separated. We think it can work either way depending on the culture of the organisation and personalities in the roles. Regardless, we found the debate is still very much alive and well.

THE ROLE OF THE CISO **SURVEY RESULTS**

"THE CISO CAN DO EVERYTHING RIGHT AND STILL LOSE THEIR JOB"

There is a unanimous view that this role is already changing. At the beginning of the decade, the CISO's role was focussed on securing the perimeter, managing threats and vulnerabilities and developing strategies to defend it. With the advent of BYOD's, cloud computing and other non-company approved cloud applications, the CISO's role has evolved.

The CISO role is now moving to become strongly about marketing – not only upwards to the Executive team and Boards but also to all staff. The challenge of the CISO is to engage the hearts and minds of the organisation so they are empowered to become the protectors of the business customers and sensitive data.

Furthermore, the role is now becoming more of a leadership role. Many organisations are trying creative ways to demystify the role as being all about a "digital protection team". It is moving from a gatekeeper role to an enabler role. Softer skills like communications, negotiation, being business-focused, end-customer-focused are some of the skills that will be more important for the CISO.

Interestingly, there were some opposing views on the position of this role. There was a view that the role of security will trend towards being embedded in the business and the respective roles will be merged within the business. Then, there was the view that the role will become more important than it is today and will need to have greater access to Boards and Executive teams and will report more broadly outside of IT. Where this will end up in 2020, will be somewhat like the Risk/Security debate, and the debate will rage for years to come.

Indeed there are world-wide examples where the CISO is employed as the "sacrificial lamb" in the event of a data breach. This was reflected in an insightful comment "where the CISO can do everything right and still lose your job".

NOTABLE INSIGHTS

Our industry leaders provided us with some interesting thoughts with respect to the role of CISO, which took the form of comments, as summarised below.

» I would love to be at the spot where a CISO doesn't exist by 2020 as security is a core part of the business that everyone is operating under.

» The CISO will need to have greater access to leadership team and boards. They must be an excellent communicator, and become the 'cyber whisperer'. It's less about technology, more about people and the ability to articulate complex risk into simple terminology.

» CISO's need to become better 'marketers'.

» They need to be a strong technologist, but now it is a business role.

» Engagement with end clients/customers (outside of the company) is becoming much more important.

» There must be an emphasis towards education and changing culture.

» There must be a greater focus on human behaviour and how people respond / act to things.

» It's not 'OK to be the victim" and simply apologise. Organisations must take responsibility to secure.

» The role is getting harder – 'you can do everything right, and still get fired" – the role has become much more important and about 'protecting trust'.

» We need to look at trends and implications 'in the eyes of the end customer' not just internally – the CISO role should be to protect the end customer.

» If you look at the companies that have had data breaches in the last few years, there aren't many commonalities or consistent things that were done poorly. However, what is clearly apparent to us, is the difference between the company that was adequately prepared to proactively respond in the event of a data breach, versus those that weren't prepared.

THE WAY FORWARD

Today's Digital Age represents an era much more powerful and significant to the face of business from what we've seen in the history of mankind. We live in an exciting time where everything is digitally interconnected, and partners, employees, customers, and even competitors are often collaborators in the process of business innovation. Indeed, information security can mark the difference between success and failure in this Digital Age.

As the Trusted**Impact** survey results have shown, the information security industry faces a period of considerable change. The role of the CISO is changing, and the skills of the security team of 2020 must too evolve to meet these changes.

In addition, the successful security team of 2020 will need to evolve in an era where the 'supply' of qualified security professionals will likely fall woefully short of overall 'demand'. Therefore, what is more important is the mix and composition of skills, not just filling positions.

Organisation looking to succeed in the Digital Age will need a security capability that is responsive to the fast moving industry trends. In addition, significant shifts in skills are needed to align with these trends. However, if an organisation does not respond to these issues TODAY and put actions into play now, waiting until 2020 to respond will be too late.

The adage of 'a stitch in time, saves nine' was always relevant in information security, but with the data gathered and insight gained from a breadth of industry leaders, it's an absolute necessity to plan today if your organisation wants to succeed in 2020. This plan must gain clarity on how to resolve key questions such as:

- ❒ Do I have a clear strategy on how to develop the security capability needed for 2020 – whether that be some or a combination of employees, contractors, partners, or outsourcers?

- ❒ Do I have adequate acquisition plans in place to source skilled security professionals (permanent and contractor) for the roles needed?

- ❒ Do I have appropriate budget assumptions in place to reflect changing industry dynamics?

- ❒ Do I have robust retention plans to keep talented security staff?

- ❒ Do I have development programs in place to develop the skill gaps identified?

- ❒ Do I have meaningful business relationships with external partners who align with the company's strategy to develop capability?

THE SECURITY LEADERSHIP SERIES

THE SECURITY TEAM OF 2020

Level 9, 22 Albert Road,
South Melbourne VIC 3205

+61 (0)3 9023 9710
www.trustedimpact.com
Twitter: @trustedimpact
LinkedIn: https://www.linkedin.com/company/trusted-impact

TrustedImpact
PROTECTING DIGITAL