Founding Partner
OPTUS

MACQUARIE University

Leadership in Cybersecurity

DR PIERS BAYL-SMITH, DR SIVA SIVASUBRAMANIAN, AND DR MARK WIGGINS

CONTENTS

CONTEMPORARY CYBERSECURITY:

THE CHANGING LANDSCAPE

Contemporary cybersecurity is a high stakes battle. For aggressors, there is the opportunity to gain both power and wealth, while victims face the very real prospect of losing everything.

Cyberattacks have steadily evolved from being a nuisance triggered by so-called 'script kiddies', doing it for the thrill and right to brag, to an economy of thriving mercenaries that are employed by criminals, unscrupulous businesses, nation states and hacktivists. Hackers of the 80's and 90's were not necessarily viewed as disreputable individuals, but rather as tinkerers and enthusiasts intrigued by the challenge of breaking into, and disrupting, computer networks [1]. However, as the world has become more digitised, the opportunity for exploitation and disruption has significantly broadened, leading to the development of increasingly sophisticated techniques to infiltrate and extract information. The *modus operandi* of attackers has changed from publicly showing their might to becoming undetectable in siphoning data in pursuit of economic gain. Cyberattacks have metamorphosed from being a show of technical capabilities to a lethal cocktail of technology, social engineering and manipulative psychology.

Contemporary cybersecurity can therefore be likened to guerrilla warfare. Rather than confront defences 'front-on', attackers now utilise unconventional strategies, deception and surprise to infiltrate computer systems and networks. In 2008, for example, computers in the US military's Central Command were infected by a computer worm, Agent.btz, capable of scanning computers for data and opening security backdoors. A foreign intelligence agent, in a tactic known as a "candy drop", is suspected of leaving a USB flash drive in a parking lot outside of an army base. Out of curiosity, a soldier picked up the drive and decided to insert it into a computer linked to the Central Command network. On connecting the drive, the virus was automatically uploaded into the system. It then took 14 months to clear the worm from infected devices and networks [2].

I am not sure how Prince Alyusi Islassis found my email, but he had a business proposition. Upon concluding a large number of contracts, the Nigerian National Petroleum Company was wanting to transfer $40,000,000 of funds to another region in order to facilitate further global exploration. However, the Nigerian Government was preventing the movement of these funds. By transferring money into my bank account, they would be able to bypass the regulations of the Central Bank of Nigeria. As payment for this service, they would allow me to retain 10% of the funds. Time was of the essence.

However, Michael Neu, aged 67 from Louisiana, was neither a prince, nor Nigerian. Rather, in December 2017, he was arrested for 269 accounts of wire fraud and money laundering. He was a co-conspirator in what is known as an advance-fee scam, where a victim pays a small-up front fee for a share in large quantities of money. Although "Nigerian prince" emails are now the topic of comedy, many people still fall victim to the scam in the hope of easy money. What such examples highlight is that cyber security transcends the technical domain. Organisations may have the right equipment, the right security settings, the right software. Nevertheless, security breaches will occur. Often, it is not the technology, but the people who bring the system down.

In response to the evolution of cybersecurity threats, the role of the Chief Information Security Officer (CISO) has emerged as a critical leadership position within organisations, marshalling technical expertise and resources in the defence of information assets and infrastructure. Where cyber-criminals may only need one successful hit amongst many thousands of attempts, the CISO is expected to anticipate and counter every possible strike. As attacks can arise from a wide range of sources, utilise different methodologies, and target different systems, the CISO is required to engage a broad range of leadership skills to encourage rapid adaptation to new and challenging environments. The failure to swiftly adjust to new threats can result in significant losses of information, intellectual property, and reputation, as well as sizeable financial costs. To understand the role of leadership in advancing a cybersecure network, it is important to dissect the evolution of cyber-threats, now and into the future.

WHERE DOES THE THREAT COME FROM?

Unlike traditional warfare, there are no clearly delineated 'enemies', nor are adversaries easily identifiable. They can come from varied geolocations, have distinctive purposes and motivations for attack, and are sponsored by a range of organisational and/or state parties. The most successful hackers are those who are able to advertise and monetise their cyber-nuisance. Antagonists forge pseudo-franchise enterprises, known as ransomware-as-a-service (RaaS), where ransomware and hacking tools can be rented or sold to any customer who is willing to pay [3]. Akin to a weapons manufacturer engaging an arms dealer to sell weapons to mercenary soldiers, cybercriminals will develop software and provide technical know-how to other cybercriminals, who then act as vendors and service providers to would-be attackers. Following a successful attack, extorted money is often distributed between the attacker, vendor

and developer. This system has the benefit of allowing developers to widen their distribution channels, whereas those who dispense and utilise these services do not have to write their own malware nor develop the necessary technical expertise to carry out a successful cyber-attack. Therefore, although mercenary soldiers do not have the personal programming capabilities, they have at their disposal the necessary weapons and support through which they can cause significant corporate damage.

Highlighting the financial stakes involved, the direct cost of cybercrime is thought to cost Australians in excess of $1 billion each year, although the actual impact on the Australian economy may be as much as $17 billion [4]. Furthermore, as a demonstration of the threat posed by cyber-attacks against organisations, a survey commissioned by Citrix showed that 42% of UK large companies (250+ employees) are stockpiling cryptocurrency to pay off hackers who may target them with ransomware attacks [5].

As an alternative to obtaining financial gain, some hackers may eschew being characterised as 'bad', but rather see their cyber activities as a form of social activism. The term '*Hacktivism*' describes attempts to promote political or social change, or damage ideological opponents by means of cyber-attack [6]. The damage is often directed towards publicising secret or classified information, causing reputational harm, or disrupting services. Instigators can be individuals, an alliance of parties united by a common cause, or a corporate entity. *Wikileaks* is perhaps the most well-known example of a hacktivist organisation, responsible for publishing a broad suite of secret documents into the public domain. The stated intention is not financial, but rather to ensure that stories are 'heard' that are in the 'public interest'. Organisations that have been perceived to have crossed an ideological line, such as the Recording Industry Association of America's (RIAA) pursuit of copyright infringers or PayPal's withdrawal of services from Wikileaks, have experienced significant disruptions by hacktivist groups, such as *Anonymous*. The danger for many organisations is that ideological lines are ambiguous, and new products, services, customers, partners, and marketing strategies may result in organisations being targeted for undefined moral transgressions. To further complicate matters, many Hacktivist are now seeking to use any insecure website, regardless of the company's standing, to promote their message [7].

Although the threats to organisations are often characterised as arising from outside the system, antagonists may also arise from within an organisation. In*sider threat* is a breach in network security caused by users within the organisation. Even if the network is essentially secure from a technical standpoint, it is the people using the system who can often bring down a network. While some users and past employees may have malicious intent, selling or leaking information for financial gain or perceived retribution, the clear majority of cases involving security breaches are unintentional and are the product of either negligence or human error [8]. By succumbing to phishing scams, inadvertently installing infected software, or inserting a discarded USB memory stick, employees introduce vulnerabilities that are difficult to combat. Networks can be compromised by actors with the best of intentions, resulting in the loss of information, reputation and finances.

CYBERTHREATS: MODUS OPERANDI

Just as there are a variety of actors with differing motivations, the methods of cyberattack can also vary significantly. Perhaps the easiest method of gaining access to a computer system or network is to simply ask for the user's password. Bad actors can contact employees pretending to be from their IT department, explain that there is an issue with their account, and ask whether they could confirm their password as part of a 'systems check'. Unsuspecting users with the best of intentions then give access to the person on the pretence that the problem will be solved. Such scams often end up with malware-ridden computers with users paying unnecessary support costs.

The most common method of cyberattack is via phishing emails [9]. Such attacks have been relatively easy to detect in the past. They contained outlandish stories of lost relatives, tremendous business opportunities or great hardships. They are often simple, text-based messages, with poor spelling and phrasing. However, such phishing emails are quickly giving way to scams of increasing sophistication. More care is taken in their presentation, their message appears more believable, and they utilise psychological principles to bypass critical reasoning. High-resolution company logos, phone numbers linking to active call centres, and appeals to social engineering cues are becoming ever more common [10]. Furthermore, generalised phishing attacks are fast giving way to a more targeted tactic of *spear phishing*. Rather than using a scatter gun approach, where one email is sent to thousands in the hope of catching a single user, time is invested to create targeted campaigns against key individuals. Based on the target's interests and needs, sourced via a varied mix of social media (Google, LinkedIn, Facebook, Twitter, Instagram, WhatsApp etc.) and publicly available information, emails with personalised messages and websites are created to 'trick' the victim into revealing key information. This is a very difficult avenue of attack to track and catches high-value victims.

Cybercriminals can also utilise *drive-by* attacks, installing malicious code on computers after a website is visited, an email is opened, or a pop-up advertisement is selected [11]. This can occur because users are either manipulated into actively downloading software onto their computer, or by exploiting web browser or operating system vulnerabilities. For example, websites may contain a pop-up that indicates that a user's computer is infected by a virus, and suggests a (infected) virus scanner be installed to remove the malicious program. Therefore, to protect the computer, the user engages in behaviour that actually causes the infection. A more concerning form of drive-by attack occurs with the installation of software without the user's knowledge. By exploiting system or browser vulnerabilities (often accentuated with the installation of plug-ins and add-ons), scripts of code can be installed on a computer without the user's knowledge. Simply by visiting a compromised website, a computer can be infected with malicious code.

Cyber-attacks can target physical systems and networks to deny services or obtain information. Distributed Denial-of-Service (DDoS) attacks target the online presence of organisations or their services by flooding their network connections with requests beyond which their hardware or network bandwidth can reasonably manage [12]. The motivation behind such attacks is normally to prevent the normal functioning of online systems (e.g., shopping or banking), or to discredit an organisation (e.g., Anonymous' attack on the Church of Scientology). In Australia, four separate DDoS attacks were held responsible for the problems experienced in completing Australia's first ever online census in 2016, preventing millions of citizens completing the form online.

Another prevalent issue in cyber security relates to poor access control and patching. Like a hotel where one key unlocks access to every room, weak passwords, open information channels, broad access to files, and irregular software patching will result in everyone being burgled. Employee's passwords constitute the keys to their rooms, and it should have a level of sophistication that cannot be simply guessed or bypassed. For example, newly acquired equipment often comes with simple passwords (e.g., password or admin) – that, if not changed, would allow hackers access to that system. However, even if criminals fail to gain access to an employee's 'room', they should not then be able to then gain access to every other 'room' in the hotel. That is, a network should be so configured that only information pertinent to the employee is compromised, rather than the entire organisation. Furthermore, once employees leave the organisation, their key and access rights must be revoked to prevent the possibility that their credentials will be distributed to competitors or to create damage as a means of retribution. This type of poor network configuration, maintenance and patching acts as a beacon for cyber-criminal activity.

In bringing a combination of cyber-attack strategies together, organisations may face the serious challenge posed by Advanced Persistent Threats (APT's) [13]. Often targeted at securing state or corporate secrets, APT's are co-ordinated, covert attacks frequently involving specialised teams. They are advanced, such that they involve significant planning and an array of sophisticated techniques to compromise a system. They also involve a thorough understanding of the organisation, key personnel and infrastructure, together with the information they are seeking and to whom they should target. Such attacks are persistent, in that the threat is ongoing, often taking months of planning and implementation. Once a foothold has been gained, attackers will attempt to increase their network privileges and strengthen their position within the network. Following a successful intrusion, the team will begin to silently siphon information from the organisation to avoid triggering alarms, and then attempt to cover their tracks. APT's are notoriously difficult detect, and then to eradicate once detected.

In examining the methods of cyber-attack, the critical message is that if a network is easy to infiltrate, it will be compromised. Systemic weaknesses within the information security infrastructure, perhaps due to rapid expansion, under investment or increasing complexity, proves tempting for criminals in spirit to become criminals in practice.

IOT: CHANGING LANDSCAPE OF CYBERSECURITY

Further complicating the defence against cyber-attacks, the proliferation of devices and equipment connected to the internet increases opportunities of cyber-criminality and introduces avenues of attack that have not previously been considered. The *Internet of Things* (IoT) describes the wide range of devices connected to the internet, including cars, appliances, machinery, security systems and building automation, and which are thus, open to possible exploitation by hackers. At a Netherlands cybersecurity conference, 2017, attendees were left shocked as an 11 year old boy, armed with his toy teddy bear, was able to hack into the mobile devices of security experts. In 2015, a 'smart' Samsung refrigerator was successfully hacked, with the exploit allowing access to Gmail login details. Evidently, devices as simple as a 'smart' teddy bear or a 'smart' refrigerator can become possible avenues of attack.

As the range of IoT devices expands, an increasing awareness of possible security implications needs to be adopted. Hackers have been able to demonstrate that a modern car's sound systems, air-conditioning, and even accelerator and brakes are all able to be controlled remotely [14]. However, such attacks needn't be so blatant to be equally effective. The functioning of autonomous vehicles requires the vehicle is aware of, and interprets, its situational context. There is the need for a rapid flow of information between different sensors, devices and even external systems to operate safely. Therefore, rather than seek a full denial of service attack, hackers need only delay the flow of information, increase latency between critical systems, to cause untold damage. This is an example of how future attacks may be difficult to decipher, with the hacker hiding in the shadows of hardware, software and network latencies.

The changing cybersecurity landscape has also shifted because of growing connections between organisations, the supply chain, and customers. Many corporations are now inter-connected or networked, having up and downstream suppliers and connected customers, often crossing state or international borders. This raises two major concerns: a reliance upon entities outside organisational control maintaining their own system security; and the identification of jurisdictions of control and the implementation of key resources in the event of a crisis. When a cybersecurity incident occurs, what are the inter-company contractual implications, what state or national laws need to be enacted, and who takes responsibility to resolve the issue? In selecting suppliers, organisations now need to be aware of their cybersecurity standards, stewardship requirements, legal responsibilities and redress in case of a breach. Organisations also need to be able to chart digital trading dependencies and determine their risk profile and domain of responsibility.

THE CHANGING CISO ROLE

Business is changing rapidly as a result of technological innovation and globalisation. Companies are becoming digitised, boundaryless and borderless. Organisations are now expected to be agile, moving from process and control-centric practices to customer comfort-centric. Consequently, the organisational risk profiles and risk appetite (i.e. the level of risk considered acceptable) has shifted significantly, often without any awareness on the part of the company. The CISO is no longer a mere technological-expert protecting the business from technological induced cyber-risk but is an integrated risk professional who must understand the motivation and concerns of the board, business, technologists, customers and cyber-criminals. That is, the CISO role is focussed on risk *management* rather than risk *mitigation*, with a multi-layered approach to cyber-risk for the entire organisation and beyond. Every moment and in every context, the CISO needs to balance the risk against necessity.

CYBERSECURITY IN A CORPORATE WORLD:

EMERGENCE OF THE CISO

In the contemporary corporate environment, targets for cyberattacks range from employees to senior executives, intersecting with all facets of the organisation. In this context, the role of Chief Information Security Officer (CISO) has emerged as a key role in championing cybersecurity from the board through to the end-user.

THE ROLE OF THE CISO

As threats from cyberattacks evolve, organisations have become increasingly reliant on the Chief Information Security Officer (CISO) to build capabilities to defend against possible intrusions, be aware of breaches as they occur or even before they occur, and build organisational resilience to recover and restore capabilities following an attack; all while supporting the strategic goals of the business. Therefore, the contemporary CISO must embody the dual capabilities of *technical specialist* and *business strategist* while performing the role of Risk Manager.

As technicians, CISOs are required to arrange and manage an organisation's cybersecurity plan and operation, including budgeting, procuring new investments that improve security and operational functionality, and building an effective security team. That is, CISOs are now responsible for ensuring that the design, development and implementation of all IT-related systems are secure, that correct procedures are adhered to, and that systems are adequately monitored and reviewed, all in the context of the processes they operate under.

As a strategist, contemporary CISOs need to examine cybersecurity holistically and understand the multiple conflicting priorities of different stakeholder. Each decision needs to be examined from the perspective of serving the mission and goals of the organisation. This requires a comprehensive understanding of the business as a whole. Each piece of hardware, software, and protocol designed to reduce the organisation's risk profile is associated with financial and opportunity costs. For example, at the operational level, requiring customers to use two-factor authentication may increase customer security, but comes at the expense of customer comfort. Likewise, allowing employees Virtual Private Network (VPN) access may provide flexibility to work from home, but increases the footprint through which hackers can gain remote access to the network. Therefore, there is a balance that needs to be drawn between securing the network from possible attack and maintaining operational functionality and comfort.

Given the situation of ever-evolving threats, the price for achieving total security may be unachievable [15]. Absolute protection is no longer an attainable goal. Furthermore, the greater the investment in information security, potentially the lesser the investment in core business practices. Parallels can be drawn here in the balance between government expenditure on defence and law enforcement against the investment in health and education. If spending was exhausted on the former, the nation may be protected, but the government would be less able to fulfil its other duties to citizens. Yet, if investments in defence and law enforcement were neglected, the nation would be at the mercy of rogue nations and would likely descend into a state of crime and anarchy. Therefore, at a strategic level, it is the CISO's role to understand the organisational system, define levels of acceptable risk, determine the necessary costs, and then advocate for, and lead change where necessary.

CHAMPION FOR CHANGE

Technical and strategic abilities are necessary but not sufficient to facilitate success as a CISO. Information security ultimately rests on an organisation's people and its culture. Often, it is easier for a cyber-criminal to compromise a system through an employee's actions or ignorance, than probe code and hardware for potential weaknesses. It is people who will set "123456" as a password, or who will insert an infected USB-drive found in a car-park into their computer, or who will be manipulated to click on a phishing scam that are likely to pose the greatest threat to the security of an organisation. Employees need to be educated in cyber-risks, but importantly, they need to recognise that information security is the core responsibility of every employee and not the exclusive domain of IT specialists. Cybersecurity also needs to be adopted as fundamental component of executive responsibilities [16]. If the *C-suite* is not convinced that there is a genuine threat, nor recognise the potential costs associated with a cyber-attack, investment in cybersecurity projects will be under resourced, defences will not be maintained, and staff will remain

ignorant to the risks posed by cyber-attacks. Therefore, the CISO is accountable for developing a cyber-alert security culture both within the executive and across the company.

In late May 1940, Foreign Secretary Lord Halifax of the British war cabinet argued for a peace settlement between Britain and Germany. Prime Minister Winston Churchill, recognising the tyranny of the Nazi regime and the potential for capitulation, believed that Britain would be better placed remaining steadfast in its armed opposition to the regime. Although Churchill faced significant opposition in the war cabinet, he convinced members of the outer cabinet to continue their war efforts, "I have thought carefully in these last days whether it was part of my duty to consider entering into negotiations with That Man [Hitler]. But it was idle to think that, if we tried to make peace now, we should get better terms than if we fought it out... We should become a slave state... If this long island story of ours is to end at last, let it end only when each one of us lies choking in his own blood upon the ground."

In the same way, a CISO needs to contend with the *C-suite*, often in the face of significant and sustained opposition. It is the responsibility of the CISO to argue for the organisation's security. Hindering this objective, the *C-suite* may underestimate the threat posed by cyberattacks and/may not appreciate the need for investment. Indeed, cybersecurity, like safety, is often intangible. Only when a breach or a system failure has occurred will questions be asked as to why adequate defences were not in place. Therefore, the contemporary role of the CISO is to effectively communicate the importance of information security and how it promotes organisational strategic objectives.

In effect, a CISO is a 'champion of change', building a culture supportive of cyber security initiatives from the entry-level employee through to the CEO. Just as defence and police chiefs must secure 'buy-in' and investment from politicians and the public, it is incumbent upon the CISO to identify the security needs of the organisation, propose well-designed solutions that minimise conflicting priorities, and market the benefits of the process. This will invariably involve building social capital through the creation of alliances, fostering interpersonal relationships, working alongside the executive team and end users to fashion effective solutions to complex issues, and communicating the costs and benefits with non-technical jargon. Therefore, success as a CISO is not necessarily dependent upon technical abilities or a capacity to think strategically, but rather, is deeply rooted in a capacity to understand and respond to the threats imposed by potential attackers, and appreciate both the goals and limitations of potential victims.

In sum, the CISO needs to be an *effective leader*. Static technical solutions will eventually become compromised; therefore the CISO must understand the present and future means and motivations of attack, comprehend the strategic aims of the organisation, balance competing needs of security and comfort, facilitate the generation of innovative solutions, and engender buy-in from all levels of the organisation. Scholars and practitioners have identified a range of CISO competencies emphasising the importance of technical knowledge, strategic thinking and communication [17]. There is a recognition that the CISO needs to exhibit leadership to be successful in driving change at both the executive and employee level. However, leadership is a fraught concept, often coupled with power and control. It is common to conceive the leader as being the expert with the answers, the bringer of certainty, the puppet master. For the CISO, such a leadership approach would only invite disaster.

LEADERSHIP IN CYBERSECURITY:

DESIGN THINKING AS A SERVANT LEADER

At its core, CISO leadership concerns the process of enabling change to cope with new circumstances and environments. Consequently, servant leadership and design thinking align with the essential aims of a CISO in creating a cyber-aware organisation. It is non-hierarchical, follower-centric, and focused on creating meaningful adjustments in an environment that is rapidly evolving.

CISO AS LEADER

Although leadership is a construct well-researched, leadership in the context of cybersecurity needs to embrace the adaptive challenges posed by evolving cyber-threats. Leadership has variously been understood and defined throughout history, emphasising either power, the ability to influence, or as a set of behaviours or traits. However, contemporary notions define leadership as, "...a process whereby an individual can influence a group of individuals to achieve a common goal [18]." Leadership, as a *process,* implies a distinction between what one does as a leader from the traits or characteristics that a leader may possess. Therefore, one is not born a leader or is a leader by virtue of beauty, personality, or intelligence, but rather, is a leader by virtue of activities or achievements.

As a process, leadership is concerned with interactions between leaders and followers, rather than a linear edict from above. It also involves the creation of a vision for a *common goal*, which implies an aspiration of mutual beneficence for both leaders and followers. Finally, leaders must be able to impact followers, and be able to *influence* others toward the pursuit of a common goal. The CISO Is engaged in the process of silently Influencing and changing behaviour of the corporation [19]. When changing the online habits of employees, by driving a culture of cyber-awareness, by guiding the *C-Suite* through the new battleground with the purpose of creating a secure networked environment, the CISO is engaged in such a process.

In the contemporary workplace, the CISO is required to exhibit robust servant leadership mainly to those he or she leads and engages In effecting the change. According to Greenleaf, servant-leaders desire to serve others first rather than pursue their own drive for power or acquisition, "The difference manifests itself in the care taken by the servant-first to make sure that other people's highest priority needs are being served [20]." Rather than approach employees and the executive with answers and pre-set plans, a CISO should exhibit humility, seeking to understand end-user needs in the context of their existing organisational culture. If staff repeatedly fall for phishing scams, set insecure passwords, or engage in other cyber-risky behaviour, it is important for the CISO to understand why such activities are taking place, rather than immediately seek to censure and limit access. In a nod to the Design Thinking approach, solutions need to match the needs of the people with what is technically feasible, pursuing strategies that create real value for the organisation [21]. It may be the case that unsafe behaviour exhibited by employees is a result of being time-poor, or by a need that is not met by the current infrastructure. A perspective that starts first with the end-user in mind allows for genuine solutions to be implemented. This can often be challenging in an environment that demands certainty and quick fixes. Hence, a CISO needs to persuade stakeholders for the need of change derived from their expertise and strategic knowledge. The CISO's most important skill is to lead the leaders, operate the levers of influence, not out of a desire for power or prestige, but out of genuine need to serve the members of the organisation. By leading from the front, acting with integrity, seeking the benefit of the other, they can best persuade others to follow, and in turn, also serve the security needs of the organisation.

Given the challenges, cybersecurity leadership needs to be non-hierarchical, follower-focussed, and continuously adaptive, founded upon competence, performance and good character. This contrasts with many common conceptions of leadership that portray leadership as individualistic, hierarchical, and unidirectional [22]. Leaders are often conceived as those individuals who hold the power to make the decisions. While the CISO has a source of legitimate power in this sense, final decisions as to where financial and personal resources are directed is ultimately the domain of the CEO and CFO. The role of the CISO is to influence those individuals who hold power to invest in cybersecurity, and to obtain compliance to policies not by coercion but through education and establishing a common purpose. Therefore, it is as important for the CISO to lead *upwards* as it is to lead sideways and downwards. Recent theories of leadership, such as servant leadership, suggest that the CISO must engage in behaviours and activities that

put people first, equipping and empowering them to overcome obstacles and threats. They must be able to tap into to the needs of both the executive and the end-user by increasing the awareness of issues around cybersecurity, and motivate them to act in the interests of the organisation. A successful cybersecurity environment requires the participation and innovation of all stakeholders.

ABOUT THE AUTHORS

Dr. Piers Bayl-Smith is a research fellow at Macquarie University investigating human factors and cybersecurity within the organisational context. Piers was awarded his PhD in 2017, receiving the Vice-Chancellor commendation for his PhD thesis. Piers has published several peer-reviewed articles in the domains of older workers, selection and cyber-security.

Dr. Siva Sivasubramanian (Siva) has operated as CISO in global telecommunications companies for nearly 20 years, and is currently CISO of Singtel Optus. At Singtel Optus, Siva was responsible for transforming information security from a reactive virus management hub to a vibrant corporate cyber security division that provides security as a business enabler and a channel for enhancing customer experience. In 2012, Siva completed his PhD on leadership practices for innovation at the University of Technology, Sydney, and has been active in encouraging corporate innovation and efficiency through lectures and articles.

Prof. Mark Wiggins research and teaching interests lie in the assessment and development of expert performance, particularly in the context of cognitive skills such as diagnosis, sensemaking, and situation assessment. He has led a number of national and international research projects in domains including power system control, software engineering, medicine, and aviation. Mark leads the development, evaluation, and implementation of the Expert Intensive Skills Evaluation (EXPERTise 2.0) software package for the assessment of diagnostic skills in practice.

BIBLIOGRAPHY

1. B Middleton, A History of Cyber Security Attacks: 1980 to Present (New York: Auerbach Publications, 2017).
2. P. W. Singer and A. Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know (New York: Oxford University Press, 2014).
3. Australian Cyber Security Centre, ACSC Threat Report 2017, 2017.
4. Commonwealth of Australia, Australia's Cyber Security Strategy, 2016.
5. Chris Mayers, 'Ransomeware in the UK: One Year On', Citrix, 2017 ‹https://www.citrix.com/blogs/2017/06/06/ransomware-in-the-uk-one-year-on/›.
6. Singer and Friedman.
7. Marco Romagna and Niek Jan Van Den Hout, 'Hacktivism and Website Defacement : Motivations, Capabilities and Potential Threats', in 27th Virus Bulletin International Conference (Madrid, 2017).
8. Domenic Antonucci, The Cyber Risk Handbook (Hoboken, NJ: John Wiley & Sons, Inc., 2017).
9. Australian Cyber Security Centre.
10. Michael Workman, 'Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security', Journal of the American Society for Information Science and Technology, 59.4 (2008), 662–74; Emma J. Williams, Joanne Hinds and Adam N. Joinson, 'Exploring Susceptibility to Phishing in the Workplace', International Journal of Human-Computer Studies, 120.June (2018), 1–13.
11. Singer and Friedman.
12. Australian Cyber Security Centre.
13. Singer and Friedman.
14. Andy Greenberg, 'Hackers Remotely Kill a Jeep on the Highway - with Me in It', Wired, 2015 ‹https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/›.
15. M. C. Libicki, L. Ablon and T. Webb, The Defender's Dilemma: Charting a Course toward Cybersecurity (Santa Monica (CA): RAND Corporation, 2015).
16. Bill Sweeny, 'Cybersecurity Is Every Executives Job', Harvard Business Review, 2016 ‹https://hbr.org/2016/09/cybersecurity-is-every-executives-job›.
17. Richard Klimoski, 'Critical Success Factors for Cybersecurity Leaders.', People & Strategy, 39.1 (2016), 14–18; Val Hooper and Jeremy McKissack, 'The Emerging Role of the CISO', Business Horizons, 59.6 (2016), 585–91.
18. Peter G Northouse, Leadership: Theory and Practice, 7th edn (Los Angeles: SAGE Publications, Inc., 2016), p. 6.
19. Northouse.
20. Robert Greenleaf, 'The Servant as Leader', Corporate Ethics and Corporate Governance, 2002, 79–85, p. 83.
21. Tim Brown, 'Design Thinking', Harvard Business Review, 2008, 84–92.
22. D. Scott DeRue, 'Adaptive Leadership Theory: Leading and Following as a Complex Adaptive Process', Research in Organizational Behavior, 31 (2011), 125–50.

Founding Partner
OPTUS

MACQUARIE University

OPTUS MACQUARIE UNIVERSITY

Cyber Security Hub

CRICOS Provider 00002J

This white paper is part of an insight and knowledge-sharing series from the Optus Macquarie University Cyber Security Hub.

The Cyber Security Hub relies on a network of experts across business, government and higher education. It promotes an interdisciplinary understanding of cyber security by bringing together technology, business, legal, policy, security intelligence and psychology perspectives.

The Cyber Security Hub offers a range of services and collaborative opportunities. This includes professional education, hosting events to promote up-to-date knowledge, publishing key insights and updates, and working with partners on their business challenges.

If your organisation would benefit from being a part of a cross-sector network and have a greater understanding of the complex issues surrounding cyber security, please contact us to discuss opportunities for collaboration at **cybersecurityhub@mq.edu.au**

For more information visit **mq.edu.au/cyber-security-hub**