Founding Partner
OPTUS

MACQUARIE University

How Can Company Boards Build Trust When Faced By Cybersecurity Risks?

DR JOHN SELBY

CONTENTS

INTRODUCTION

Over the last few years, cybersecurity risks have become a major challenge for companies. This short whitepaper explores the cybersecurity risks facing companies, examines the reasons why those cybersecurity risks are undermining the trust that many stakeholders have traditionally had in companies, and gives recommendations for actions company boards can take to restore trust in their businesses in the face of those cybersecurity risks. Future work will explore aspects of these issues in greater detail.

ROLE OF TRUST IN BUSINESS: HOW TO BUILD IT AND HOW TO LOSE IT

Trust lies at the heart of all successful businesses. [24] Without it, competitive advantages are lost, doing deals becomes much more difficult, quality-control suffers and the benefits achievable from economies of scale are lost. Trust comes in many forms. At its most basic, it is the expectation that one party has that the other will behave in a mutually acceptable manner, and that both parties will not exploit the other's vulnerabilities. [39] Trust creates predictability in business behaviour and allowing a long-term web of relationships to thrive between stakeholders, such as investors, lenders, regulators, the board of directors, managers, employees, suppliers and customers.

A company can build trust in its business through carrying out contractual agreements over time, doing what it says it will do, and/or taking initiatives that are mutually beneficial to the parties in the trusting relationship. [13]

Trust is situated within an overall political, legal, economic, social and technological environment. It builds over time as a consequence of repeated successful interactions between a company and its stakeholders. [13] The company and its stakeholders build up a level of expectations based upon assumptions about the likelihood of further successful interactions in a relatively stable overall environment.

Trusted business relationships can be weakened or lost by a company failing to satisfy its contractual obligations, failing to satisfy the other party's expectations, or taking unfair advantage of the other party. [39] Those failures may be a consequence of changes in the company's behaviour (for example, the growth of a toxic corporate culture focused upon short-term exploitation of stakeholders) or the failure of the company to adapt sufficiently to changes in the overall environment in which the company operates.

Arguably, much of the decline in stakeholder trust that companies currently face from the increase in cybersecurity risks is caused by the latter, rather than the former.

WHAT CYBERSECURITY RISKS DO COMPANIES FACE?

Almost all Australian companies today are connected to the Internet. [3] At the lowest end, this includes email accounts, using electronic banking and hosting a simple website. At the higher end, many Australian companies have integrated the Internet into the core of their business models. Some are utterly dependent upon it to achieve success in their industry.

Many Australian companies have experienced cyber-attacks. [3] It can be difficult to categorise these cyber-attacks by their level of seriousness, as different business models will have different levels of vulnerability to different types of cyber-attacks. For example, a massive distributed denial of service attack on a suburban bakery with a simple website is unlikely to cause significant disruption to its business model whereas the same attack on an online gambling business in the lead-up to Melbourne Cup day might be catastrophic for its business model. Due to the competition between cyber-attackers and defenders, attacks are constantly evolving, leading to new forms and variants of these attacks.

Therefore, it is more useful to categorise cybersecurity attacks by the type of harm caused to a business. This enables each company to conduct its own risk assessment to determine the extent to which each attack poses a risk to its particular business model(s). [2], [49], [19] The five main types of harm are:

a) attacks designed to interrupt a business' communications with its customers and suppliers: denial of service attacks, distributed denial of service attacks, defacement of webpages, etc;
b) attacks designed to interfere with a business' financial systems: hacks of point-of-sale devices, theft of customer credit-card data, theft of payroll data, insertion of false employees into payroll, theft of online advertising budget, theft of online bank deposits, insertion of false invoices, re-routing of legitimate payments, money-laundering, extortion, etc;
c) attacks designed to interfere with a business' operational systems: data ransoming, data corruption, insertion of false data or data deletion, destruction of SCADA-controlled machinery, theft of computer processing, advanced persistent threats, etc;

d) attacks designed to exfiltrate the business' valuable information: spear-phishing, economic espionage (such as theft of trade secrets), theft of customer or employee data, theft of information that enables insider trading (such as the board papers, targets and timing of product launches, proposed mergers/acquisitions or bankruptcy filings), etc;
e) attacks designed to damage the business' reputation: doxxing of senior executives, leaks of sensitive internal reports to the press, Wikileaks or regulators, issuance of false press releases, posting of embarrassing materials to the company's website, etc.

There is a wide variety of people who may be motivated to commit cybersecurity attacks on a company. These include: employees, consultants, competitors, organised crime, fraudsters, hacktivists, state-sponsored groups and national intelligence agencies. [2], [49], [19] Those attackers may have a variety of motives, including: self-publicity, publicity for a cause, national pride, technical challenge, criminal gain (whether financial or economic espionage), or to achieve strategic national policy goals. [7]

WHY DO THESE CYBERSECURITY RISKS EXIST?

Prior to the development of the Internet as a core component of business, successful companies had built trust with their stakeholders over time by carrying out their contracts, setting their stakeholders' expectations at a level where those expectations could generally be satisfied, and/or by taking initiatives mutually beneficial to those stakeholders in an off-line world. By significantly lowering transaction costs, the Internet has generated both opportunities and creative destruction for companies across the business sector. [47]

As the hardware, networking and software engineers who built the Internet made a critical assumption that users could trust each other to do the right thing, they generally did not build security measures into the core of their original designs. This openness worked well to foster rapid growth in the early days of the Internet. However, once the Internet became ubiquitous, flaws in that assumption have become apparent. The diversity of beliefs, incentives, and wealth of today's Internet users means that a small sub-set of those users will almost certainly act in ways that are harmful to the majority, undermining their trust in both the Internet and each other. Those "bad" Internet users are able to benefit personally by exploiting four other widespread flaws: the relative immaturity of our knowledge about how to design secure computer hardware, networks and software; the economic incentives on Internet companies to release immature products riddled with bugs; the legacy of pre-existing poorly secured systems connected to the Internet; and the difficulty humans face determining who (or what) they should trust. [48]

Companies have seen the myriad potential benefits of the Internet for their business models and incorporated it into their operations, which has unlocked new markets, new customers and significant productivity gains. Unfortunately, whilst boards of directors are usually conscious of the need to balance optimising their companies' for the present versus future, in their haste to capture a share of those gains, many companies have failed to adequately consider the risks posed by the Internet to their business models. It is only in subsequent years that those companies are beginning to experience the crystallisation of many of the risks inherent to the Internet as set out above.

For example, in 2013-14 Yahoo Inc. failed to properly secure its customer data, resulting in 1.5 Billion of its users account data being stolen in two hacks. Whilst the company was aware of those data breaches, it did not disclose their occurrence to its investors (or the victims), the stock exchange or US Securities Exchange Commission. In 2017, due to revelations of these events, Verizon reduced the price it paid to merge with Yahoo by more than $US300 million, numerous state and federal legislators have launched investigations into the cover-up and angry investors (and customers) have filed lawsuits against the company. [37]

HOW CYBERSECURITY RISKS UNDERMINE TRUST

Once companies had established a level of trust with their stakeholders based upon compliance with contractual obligations, meeting expectations and undertaking initiatives to their mutual benefit in the offline world, expectations for that level of trust generally continued whilst those companies undertook the task of adapting their business models to the creative disruption opportunities and challenges presented by the Internet. Unfortunately, many companies have not adequately adjusted their contractual promises or stakeholder expectations to accurately reflect the different risk profiles of an Internet-reliant business environment as compared to an offline business environment. This is not surprising given that many companies are only starting the challenging task of transitioning their corporate governance to be capable of accurately (or even roughly) measuring the cybersecurity risks their businesses face. Companies are often failing to fully appreciate their stakeholders (or their own) vulnerabilities to cybersecurity risks. When those risks crystallise into actual attacks and losses, it is not surprising that trust weakens. [5], [27], [52]

Endless media reports about successful cybersecurity attacks against businesses and studies evidencing the significant consequences of such breaches also undermine this trust. [48] For example, the Ponemon Institute's 2016 report stated the average cost of a data breach in Australia was $US2.59 million, with companies suffering an additional 3.1% customer churn and listed companies a 5% decline in their share price due to those breaches. [33]

WHAT IS THE BUSINESS CASE FOR INVESTING RESOURCES INTO MANAGING CYBERSECURITY RISKS?

Companies that do not yet have a cybersecurity strategy "have either failed to perceive its value proposition or do not yet fear the full force of the consequence of their company suffering a cybersecurity attack." [40] Companies with effective cybersecurity strategies and governance programs are able to conduct their businesses more efficiently, with less risk, and fewer complaints or lawsuits from employees, customers and regulators. Those companies are aware of the cybersecurity risks they face, so they can better mitigate their risks and gain a competitive advantage over their rivals. [36] Cybersecurity governance is part of good corporate governance [40], [51]

NEGATIVE CONSEQUENCES IF COMPANY BOARDS FAIL TO (RE)BUILD THAT TRUST

Boards that pay insufficient attention to the cybersecurity risks their businesses face are likely to find their company suffer from the resulting loss of stakeholder trust that they have good corporate governance in place. Poorly-managed responses to breaches resulting from cybersecurity attacks are likely to lead to closer scrutiny from regulators, investor and customer lawsuits, rising insurance premiums, declining share prices, loss of customers, declining sales growth, low employee morale, delayed or reduced takeover offers, and potential personal liability for directors for breaches of their directors duties. [12], [14], [30]

WHAT COMPANY BOARDS CAN DO TO (RE)BUILD TRUST WHEN FACED BY CYBERSECURITY RISKS

Given these cybersecurity risks, what practical steps can company boards take to (re)build trust in their businesses? The following recommendations have been synthesised from a survey of the cybersecurity literature:

Recommendation 1: The board should recognise that cybersecurity is not merely a technical issue, but a corporate governance and business issue worthy of attention at the board level. [7] Cybersecurity is another systemic risk to the company alongside financial risks, operational risks, workplace health and safety risks, etc. [5], [19], [30], [32]

Recommendation 2: The board should consider whether the existing makeup of the company's board has the skillset and knowledge to have a sophisticated discussion about cybersecurity risks in a business and legal (not purely technical) context. If not, as part of its renewal strategy, the company should consider up-skilling some of its existing members or recruiting new directors who have those capabilities. The board needs to be able to formulate and ask the right questions before it can develop its response strategies. [1], [17], [44], [45]

Recommendation 3: The board should establish a risk / assurance sub-committee which has meetings dedicated to consideration of systemic risks facing the company, including cybersecurity risks, and the legislative, regulatory and stock exchange obligations facing the company. Given the rate at which new cybersecurity risks emerge, these committee meetings should be held on a relatively regular basis. [1]

Recommendation 4: The board should hire external experts / instruct senior management to undertake a cybersecurity risk assessment for the company. This includes existing business units, supply chains and new businesses/products or services currently under development. It should include the categorisation of the types of data collected and held by the company to determine what is sensitive, confidential, non-sensitive or public based upon the value / risk associated with that data. This facilitates effective investment of resources to protect the most valuable or most at-risk data. [5], [29]

Recommendation 5: Based upon this cybersecurity risk assessment and their own judgement as to the Company's risk tolerance levels, resource-availability, its ability/need to innovate, and the balance of other systemic risks facing the company, the board should prepare a cybersecurity strategy for the company. This will include analysis of which types of data are assets or liabilities for the company, and determine which cybersecurity risks the company chooses to accept, avoid, mitigate or insure against. The Cybersecurity Strategy also needs to align with other strategies and decisions made by the board. [2], [7], [30], [32], [34], [40], [51]

Recommendation 6: The board needs to ensure that senior management have the resources and time necessary to develop and implement a cybersecurity risk response plan that accurately measures, prioritises and addresses the cybersecurity risks relevant to each of its businesses. Executives and senior management should establish and maintain relationships with relevant third parties such as law enforcement, technical consultants, cyber-crisis response experts, regulators, etc before a cybersecurity attack occurs. Such forward-planning will significantly reduce stress when a cybersecurity breach eventually occurs. [5], [34]

Recommendation 7: The board needs to ensure that its cybersecurity strategy and risk response plan cascade down into the key performance indicators and goals of executives, senior management and employees. [44]

Recommendation 8: Once senior management have implemented cybersecurity risk response plans, the board needs to ensure it has the capability to measure the effectiveness of those plans, the extent to which they have been implemented and whether ongoing compliance is occurring in the business. This could be assessed through one of the many different cybersecurity maturity models that have been developed and applied in different industries. [34]

Recommendation 9: The board should ensure that its businesses undertake tests of the effectiveness of their cybersecurity risk response plans. Ideally, these simulations should be as "real-world" as possible, testing not only the technical ability of the company to detect attacks and mitigate breaches, but also the senior management's capability to handle the public relations, press, investor, regulator, employee and customer challenges which flow from such breaches. [40]

Recommendation 10: The board should produce a consolidated risk report which includes assessment of cybersecurity risks that can withstand scrutiny from external auditors. This will assist in the event of potential future litigation, where courts will likely want to see that the board has "used a rational process to make decisions on a well-informed basis through appropriate processes under the circumstances faced by the firm and its board". [27]

Recommendation 11: Based upon its Cybersecurity Strategy and Risk Response Plan, the board should ensure that its businesses accurately communicate with its stakeholders about the ways in which the company has addressed the cybersecurity risks it faces. This will help those stakeholders to more accurately set their expectations about the company and build trust. [2]

Recommendation 12: The board should recognise that their businesses are just beginning an ongoing journey towards identifying and responding to cybersecurity risks. Mistakes and breaches are likely to occur, so promoting a culture that rewards openness and best efforts in addressing cybersecurity risks and breaches is healthier than a culture of fear and secrecy. External testing (whether through consultants or public bug-bounties) can provide help identify risks. [5], [17]

Recommendation 13: The board needs to commit to regularly planning, testing and updating their Cybersecurity Strategy, Risk Response Plan and testing protocols in the face of rapidly evolving cybersecurity risks. Knowledge captured from cybersecurity tests, attacks and breaches should be incorporated into subsequent versions of strategies and plans. [17], [31]

BIBLIOGRAPHY

1. Commissioner Luis Aguilar, 'Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus', (2014) *"Cyber Risks and Boardroom" Conference, New York Stock Exchange, New York NY*
2. Commissioner Cathie Armour, 'Cyber resilience health check', (2015) *Governance Directions* 264
3. Australian Government, *Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity* (2016, Canberra)
4. Jeremy Barbanell, 'Needing a New Approach to Address Employee Data Breach in the American Workplace', (2015) *Journal of Law and Cyber Warfare* 43
5. Grant Barker, 'Are boards fulfilling their duty of care on cyber security?', (2015) *Governance Directions: Governance Institute of Australia* 359
6. Nadya Bartol, 'Cyber supply chain security practices DNA – Filing in the puzzle using a diverse set of disciplines', (2014) 34 *Technovation* 354
7. Martin Borrett, Roger Carter and Andreas Wespi, 'How is cyber threat evolving and what do organisations need to consider?', (2013) *7 Journal of Business Continuity & Emergency Planning* 163
8. Sandor Boyson, 'Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems' (2014) 34 *Technovation* 342-353
9. Nazli Choucri, Stuart Madnick, Priscilla Koepke, 'Institutions for Cyber Security: International Responses and Data Sharing initiatives', (2014) 20(2) *Information Technology for Development* 96-121
10. Sharon Christensen, William J. Caelli, William D. Duncan and Eugenia Georgiades, 'An Achilles heel: denial of service attacks on Australian critical information infrastructures', (2010) *19 Information & Communication Technology Law* 61
11. E, Eugene Clark, 'Reflecting Inward and Looking Outward' 'Future Trends Impacting Corporate Governance Research and Practice', (2013) *2 Global Journal of Comparative Law* 115
12. Thad A. Davis, Michael Li-Ming Wong and Nicola M. Paterson, 'The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite, (2016), *2015 Columbia Business Law Review* 613
13. Fernando Flores and Robert Solomon, 'Creating Trust' (1998) 8(2) *Business Ethics* Quarterly 205
14. David Gerber, Partner, Clayton Utz, 'ASIC calls for health check on cyber resilience', (2016) *Governance Directions* 232
15. Parveen R Gupta and Tim Leech, 'The next frontier for boards: Oversight of risk culture', (2015) *Governance Directions* 497
16. Melissa Hathaway, 'Creating the Demand Curve for Cybersecurity', (2010-2011) *11 Georgetown Journal of International Affairs* 163
17. Fredrik Hult and Giri Sivanesan, 'What good cyber resilience looks like', (2013) *7 Journal of Business Continuity & Emergency Planning* 112
18. P.C. Jacobs, Prof. S.H. von Solms, Prof. M.M Grobler, 'Framework for the implementation of business cybersecurity capabilities', *Paper presented to the International Conference on Business and Cyber Security* (12-13 May 2016, London)
19. Kristin N. Johnson, 'Managing Cyber Risks', (2015-2016) *50 Georgia Law Review* 547
20. Kristin N. Johnson, 'Cyber Risks: Emerging Risk Management Concerns For Financial Institutions', (2015-2016) *50 Georgia Law Review* 131
21. Christopher Keegan, 'Cyber security in the supply chain: A perspective from the insurance industry', (2014) 34 *Technovation* 339
22. Clara Kim, 'Granting Standing In Data Breach Cases: The Seventh Circuit Paves the Way Towards a Solution to the Increasingly Pervasive Data Breach Problem', (2016) *2016 Columbia Business Law Review* 544
23. Ki-Chan Kim and Il Im, 'Issues of Cyber Supply Chain security in Korea' , (2014) 34 *Technovation* 387
24. Christel Lane and Reinhard Bachmann (eds.), *Trust Within and Between Organizations: Conceptual Issues and Empirical Applications*, (Oxford University Press, Oxford, 1997)
25. Jonathan Linton, Boyson, S.B. & Aje, J. 'The challenge of cyber supply chain security to research and practice – An introduction', (2014) 34 *Technovation* 339
26. Che-Wei Liu, Peng Huang, Henry C. Lucas, 'IT Governance, Security Outsourcing, and Cybersecurity Breaches: Evidence from the U.S. Higher Education', (2016) https://ssrn.com/abstract=2850178
27. Brad Lunn, 'Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine' (2015) *4 Journal of Law and Cyber Warfare* 109
28. Andrew Maher and Stuart Packham, 'Insuring against cyber risks: A changing landscape', (2015) *Governance Directions* 528

29. Jason Mallinder and Peter Drabwell, 'Cyber security: A critical examination of information sharing versus data sensitivity issues for organisations at risk of cyber attack', (2013) *7 Journal of Business Continuity & Emergency Planning* 103
30. James North and Richard Pascoe, 'Cyber security and resilience — it's all about governance', (2016) *Governance Directions* 146
31. Stefan Peintinger, 'Cybersecurity - (K)eine Chance gegen Internetspione? - Is There (No) Chance Against Internet Espionage?', (2014) *39 ZDAR* 173
32. John Price, 'Good practices in cyber-risk governance', (2016) *Governance Directions* 200
33. Ponemon Institute, 2016 Cost of a Data Breach Study https://securityintelligence.com/cost-of-a-data-breach-2016/
34. PriceWaterhouseCooper, ' PwC's Board Cybersecurity Governance Framework' (2016) PwC Publication, http://www.pwc.com/ca/en/consulting/publications/20160310-pwc-reinforcing-your-organizations-cybersecurity-governance.pdf
35. Dan Reddy, (2014), 'Criticality analysis and the supply chain: Leveraging representational assurance' (2014) 34 *Technovation* 362-379
36. Charles R. Ragan, 'Information Governance: It's Duty and It's Smart Business', (2012-13) 19(4) *Richmond Journal of Law & Technology* 1
37. Jeff Roberts, 'How the Yahoo Probe Points to Possible Cover-Up' *Fortune* (23 January 2017)
38. Mu Rongpin and Fan Yonggang, 'Security in the Cyber Supply Chain: A Chinese Perspective', (2014) 34 *Technovation* 385
39. Mari Sako, 'Does Trust Improve Business Performance?' in Christel Lane and Reinhard Bachmann (eds.), *Trust Within and Between Organizations: Conceptual Issues and Empirical Applications*, (Oxford University Press, Oxford, 1997)
40. Tim Scully, 'The cyber security threat stops in the boardroom', (2013) 7 *Journal of Business Continuity & Emergency Planning* 138
41. Scott J. Shackelford and Scott Russell, 'Risky Business: Lessons for Mitigating Cyber Attacks From the International Insurance Law on Piracy', (2015*)* 24 *Minnesota Journal of International Law* 1
42. Alexander Sokolov, Mesropyan, V. & Chulok, A. 'Supply Chain Cyber Security: A Russian Outlook', (2014) 34 *Technovation* 389
43. Adam J. Sulkowski, 'Cyber-Extortion: Duties and Liabilities Related to The Elephant in the Server Room', (2007) *Journal of Law, Technology & Policy* 21
44. Lawrence J. Trautman, Kara Altenbaumer-Price, 'The Board's Responsibility for Information Technology Governance', (2010-2011) 28 *Journal of Computer and Information Law* 313
45. Lawrence J. Trautman, 'The Matrix: The Board's Responsibility for Director Selection and Recruitment', (2012) 11 *FSU Business Review* 75
46. Lawrence Trautman, Triche, J. and Wetherbe, J., 'Corporate Information Technology Governance Under Fire' (2013) 8(3) *Journal of Strategic and International Studies* 105
47. Roland L. Trope and Stephen J. Humes, 'Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks that Target and Degrade the Grid', (2013-2014) 40 *William Mitchell Law Review* 647
48. Michael Warner, 'Cybersecurity: A Pre-History' (2012) 27(5) *Intelligence and National Security* 781
49. Alexandra Wedutenko, 'Cyber attacks: Get your governance in order', (2015) *Governance Directions* 598
50. Colin Williams, 'Security in the cyber supply chain: Is it achievable in a complex, interconnected world?', (2014) *34 Technovation* 382
51. Victoria C. Wong, 'Cybersecurity, Risk Management and How Boards can Effectively Fulfill their Monitoring Role', (2014-2015) 15 *UC Davis Business Law Journal* 201
52. James Young, 'IT security as a boardroom issue', (2014) *Governance Directions* 681

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**