Managing the escalating threat of cyber attacks in PE portfolios

Cyber attacks cost Australian businesses $323.7 million in 2021[1], yet cyber security remains one of the least understood risks posed to companies operating today. In an increasingly digitised world, it is imperative that companies understand, manage and report on the cyber risk they face as an organisation. Whilst cyber risk is not a new consideration, there are a number of recent factors that have amplified the risk:

- 67% of Australians are now sometimes or always working from home[2] creating a wider "attack surface" outside of controlled office spaces;
- reliance on mobile devices by both customers and employees means that company data is increasingly difficult to monitor and control; and
- rapid adoption of cloud infrastructure (now used by 55% of Australian businesses[3]) creates further opportunity for interception of data.

It is becoming increasingly clear that a cyber breach is potentially a *'not if but when'* event for operating businesses, and this thoughtpiece highlights some of the key considerations and approaches that can be taken to manage cyber risk across a private equity portfolio.

Costs associated with cyber attacks

Cyber security breaches can result in financial, operational and reputational losses.

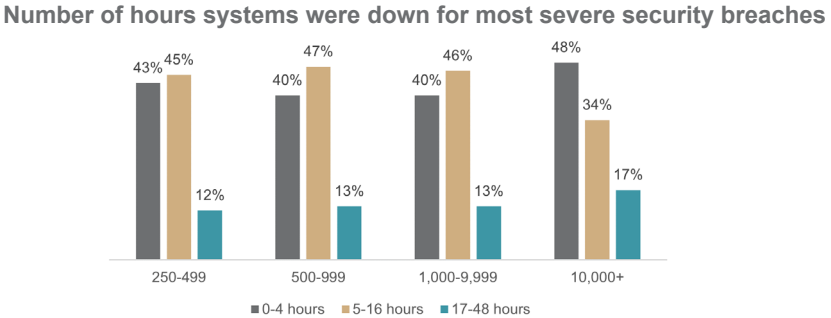
Financial

Financial losses can result from attacks which intercept payment systems or processes (such as a fictitious payment request), ransom payments or regulatory fines. The Australian Cyber Security Centre (ACSC) recorded over 67,500 self-reported incidents of cyber crime in the 2020-2021 financial year, resulting in over A$33 billion of self-reported losses[4]. This number is significantly higher once adjusted for unreported losses, and is increasing over time. In the public markets, the announcement of a data breach typically results in share price underperformance, at least in the short-term (discussed in more detail in the next section).

Source: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics

Operational

Often businesses suffer operational disruption as a result of cyber attacks. More than half of all breaches result in more than four hours of operational downtime[5], costing staff time and resulting in lost productivity.



Source: Cisco 2020 CISO Benchmark Survey, Figure 4

Reputational

Target brand index rating:buzz (consumer perception)

This cost involves destruction of brand value and loss of customer trust following a data breach. In a study carried out by KPMG in the UK, 89% of companies who were impacted by a cyber breach said they saw a long-lasting impact on their reputation evidenced by loss of clients, inability to win new business and brand damage[6]. Varonis (2020)[7] further explains the secondary effects of a cyber attack; 85% of customers tell others about their experience and 33.5% use social media to complain about their experience. The chart[8] opposite demonstrates the five year journey for Target (US) to recover their brand index rating from their 2013 data breach (following significant investment into a customer loyalty program and increased digital security expenditure).

Source: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics

Economic and shareholder value risks posed by cyber attacks

Evidence from the public markets suggests that announcement of a cyber breach results in a negative short-term share price reaction, and longer-term underperformance where the company fails to respond quickly and meaningfully to address the causation and impact.

Share price reaction

Garg[9] found that in the short-term, on average, "firms impacted by a cyber breach experienced a 2.7% decline in their stock price relative to the overall market on the day following the attack". However, history has shown much more severe reactions in certain circumstances, such as Equifax, whose share price plunged 34% in the two weeks following their 2017 data breach, or UK-based Cambridge Analytica whose Facebook-related data breach in 2018 led to their ultimate demise.

Long-term impact

The long-term impact on business value is highly dependent on the company's reaction once they fall victim to a cyber attack. Two possible but opposing impacts on shareholder value have been identified in studies:

1. **Value accretion**. A quick reaction to a data breach, including adapting digital strategy and investing to protect against future cyber attacks, can present an opportunity for shareholder value creation. For example, JP Morgan, following a cyber attack in 2014, released extensive information on the breach and expanded its investment in security. This response in part supported share price outperformance vs the S&P500 in the five years following. Similarly, the share price for US home-improvement company, Home Depot, recovered following their data breach in 2014 after the appointment of their first CISO (Chief Information Security Officer) and making significant investments to enhance encryption of customer payment data.
2. **Value destruction**. However, where the company does not change processes and strategies following the breach, business value suffers longer term. Huang etc (2019) note that "the mostly negative impact indicates that those organisations do not effectively turn cyber incidents into opportunities to improve and optimise their business[10]". This has been recently demonstrated by the ride-hailing group Uber, who, following their attempts to conceal a data breach in 2016 by paying a ransom fine, have struggled to regain customer trust and subsequently been subject to over US$148 million in fines to settle legal claims. The stock has underperformed its Russell 1000 benchmark substantially since listing.

Given the risk to company value, businesses need to approach cyber risk as an "economic threat" rather than a "nuisance"[11], reacting proactively to manage cyber risk and have in place robust response plans and reporting frameworks.

What can GPs and investee companies do to protect against cyber threats?

Increasingly our portfolio companies are implementing technology solutions to deliver their products and services. We are seeing cyber security management shift from a focus on maintaining access to these products and services to preventing unauthorised intrusions and cyber attacks which can result in the losses outlined above. Ensuring our portfolio companies protect their customers' data and their own intellectual property, and continue to deliver customer critical services and operate safely, are fundamental to building relationships of trust with key stakeholders and long-term value creation.

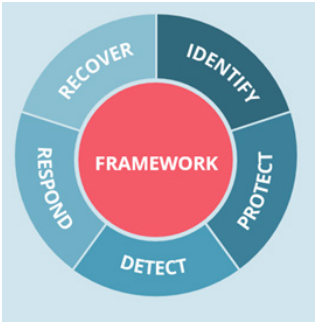
Over the past 12 months we have worked with a cyber security expert to assess the risk profile of our portfolio companies and develop uplift plans to improve their cyber security practices and ability to respond in the event of an incident. Our learnings so far have pointed us to some key areas that need to be addressed to minimise cyber risk exposure:

Strengthen first line of defence

An organisation is best protected against cyber criminals when employees are trained and vigilant in detecting potential security breaches. Role-specific training should be provided at all levels of the organisation to best equip employees with the skills required to detect and report cyber breaches in their daily operations.

Assess against a cyber security framework

There are several frameworks that companies can use to measure and improve their cyber capabilities. Our portfolio review used the Cyber Security Framework (CSF) developed by National Institute of Standards and Technology (NIST), which is responsible for producing standards for the US Government[12]. The Framework is split into five functions, which allows an organisation to measure its cyber security approach across five dimensions – how it identifies, protects, detects, responds and recovers from cyber incidents. To date, there are no specified regulatory standards relevant to cyber security for Australian companies to follow. These may be introduced in the near future, following an open consultation in 2021[13] by the Commonwealth Government on the options for regulatory reforms on cyber security.



Source: National Institute of Standards and Technology, CSF

Develop executive and board experience

Nasdaq recently reported that "91% of board members at the most vulnerable respondent companies were unable to interpret their company's cyber security report[14]". Given the increasing sophistication of cyber criminals, executive teams and board directors must have sufficient experience to be able to interpret risk reports and monitor the effectiveness of the cyber security strategy within the organisation, beyond basic IT skills. Consideration needs to be given to adequately resourcing an in-house function or putting in place appropriate outsourced arrangements to manage this risk within portfolio companies.

Report on progress

With effective reporting, executive teams, board directors and investors are better equipped to control and mitigate cyber risk. We are working across our portfolio to ensure that cyber risk is adequately integrated into risk management frameworks and risk registers, as well as developing a clear set of cyber reporting metrics to be monitored regularly at the board level. Cyber assessment is not a point in time activity, and a regular program of reassessment is key to understanding and managing this risk.

Develop a response plan

A response plan, to be enacted during or after an incident, is key to minimising the long-term impact of that incident on business value. Response Plans should be made up of four key components:

1. Contingency Planning – including a Business Continuity Plan and Disaster Recovery Plan[15]
2. Communication Approach – how appropriate stakeholders will be notified, both internally and externally
3. Analysis – how the business will identify what controls failed and the extent of the breach
4. Mitigation – what steps the business will take to resolve the incident, prevent expansion, mitigate its effects and invest in future protections

The Adamantem approach

We have built on the knowledge we have developed through our cyber security work across the portfolio over the past 12 months and now integrate cybersecurity due diligence into our investment decision making, enabling us to better analyse risk and make better investment decisions. By working with our portfolio companies to develop cybersecurity improvement action plans during our ownership period we are creating more resilient businesses, contributing to long term value creation. These activities are supported by:

- specific investment team training to ensure we are better able to identify and analyse material cyber security risks during pre-investment due diligence; and
- dedicated company director and portfolio company operations and management team training to ensure we are better able to manage cyber security risks during our ownership period.

In relation to cyber security practices within our own operations, Adamantem has a Cyber Security Policy in place, as well as a number of measures to mitigate cyber security risk including: mandated regular staff training, implementing infrastructure and software-based cyber risk mitigation solutions and monthly reporting to management on cyber metrics and managing cyber-related risks within our business in accordance with our Australian Standard ISO 31000-2018-aligned risk management framework.

1 ACSC Annual Cyber Threat Report 2020-21 | Cyber.gov.au
2 The Families in Australia Survey: Towards COVID Normal found that among the employed survey respondents, 67% were sometimes or always working from home, compared to 42% pre-COVID. Two thirds of Australians are working from home. | Australian Institute of Family Studies (aifs.gov.au)
3 55% all businesses reported use of paid cloud computing in 2019-2020 (42% in 2017-2018) Characteristics of Australian Business, 2019-20 financial year | Australian Bureau of Statistics (abs.gov.au)
4 ACSC Annual Cyber Threat Report 2020-21 | Cyber.gov.au
5 Cisco 2020 CISO Benchmark Survey, Figure 4
6 Small Business Reputation & The Cyber Risk (assets.kpmg) p2
7 Analyzing Company Reputation After a Data Breach (varonis.com)
8 Provided by Analyzing Company Reputation After a Data Breach (varonis.com)
9 [1] Garg, A., Curtis, J. and Halper, H. (2003). "Quantifying the Financial Impact of IT Security Breaches: What Do Investors Think?". Information Management & Computer Security 11(2): pp. 74-83
10 Keman Huang, Rebecca Ye, Stuart Madnick (2019)," Both Sides of the Coin: The Impact of Cyber Attacks on Business Value", Massachusetts Institute of Technology: p4
11 Gordon, L. A., Loeb, M. P. and Zhou, L. (2011). "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?". Journal of Computer Security 19(1): pp. 33-56.
12 An Introduction to the Components of the Framework | NIST13 https://www.boardreport.org/the-sustainability-board-report-2021
13 Australia's Cyber Security Strategy 2020, Strengthening Australia's cyber security regulations and incentives (homeaffairs.gov.au)
14 Nasdaq accountability Gap report, 2016 Bridging the Accountability Gap: Why We Need to Adopt a Culture of Responsibility | Nasdaq
15 Respond | NIST

W: adamantem.com.au
T: +61 2 9004 6060
E: info@adamantem.com.au

ADAMANTEM CAPITAL