COMP3320 RESEARCH PROJECT

Blair Andrews - 46977880

TABLE OF CONTENTS

1 LITERATURE REVIEW

1.1 HWL EBSWORTH

Extortion is an attack methodology that is currently on the rise and is more prevalent than ever before [1]. HWL Ebsworth, one of the largest legal partnerships in Australia, suffered a catastrophic data breach which released 4 terabytes worth of confidential government and corporate client information to the public on June 9th [2]. The attack occurred through Russian ransomware group BlackCat when they infiltrated an employee's personal computer [3], where specific details of the attack are unknown. As of September 18th, HWL Ebsworth are 'nearing' the completion of the review of data and assessment of the impact of the breach, and as of present day, have yet to update any completion of this task [4].

The media coverage for the HWL Ebsworth breach is dense, and a complete timeline of attack from conception to present can be established. HWL Ebsworth is under compliance with the Privacy Act 1988 and has a written Privacy Policy which discloses their collection and protection of user and client data [5]. The privacy policy was last amended on the 23rd of August, following the breach, which questions what the previous privacy policy contained, and if it was sufficient. Regarding information risk and security management, and governance, HWL Ebsworth stated that following the breach, they are planning to implement long-term security enhancements [4], but no evidence or follow-up about these enhancements being pursued has been provided.

We can ascertain that prior to the breach, HWL Ebsworth's treatment of information security and risk management was poor, considering the breach occurred due to probable social engineering, and employees were not properly trained to be knowledgeable about these kinds of attacks. Sensitive information from 65 government departments and agencies were released [6], and motivated the Australian government to appoint a cyber security coordinator for the first time ever [7], which should put into perspective how underprepared the Australian government is when it comes to cyber-attacks.

1.2 PORT ARTHUR LIBRARY

The Port Arthur Library suffered a minor data breach in June of 2023, when it was found that records of sensitive employee data were made publicly available through the virtual library. More specifically, in the archives of ghost tour guides, records were found that included resumes, birth dates, addresses, phone numbers, and school records, and the archived records were only viewed a total of 36 times. The public was made aware that it was in fact not a cyber-attack but mishandling of sensitive information [8].

The media coverage of this case is sparse, but prior to the breach Port Arthur Library had brief cyber security measures in place. All employees had received a briefing on cyber security, and one employee took an online course. As well as this, Port Arthur Library has a risk management system called PAHSMA (Port Arthur Historical Site Management Authority), which maintains risk management plans and systems, and they state they have a 'Records Retention and Disposal Schedule' [9]. We can ascertain that this methodology in place was not effective, and the careless data breach occurred.

In the PAHSMA five-year strategic plan, which was proposed three months after the breach occurred, there is little to no mention of focus on information risk, information security, or cyber governance techniques and management [10]. However, it was stated that the organisation is filtering through entire series of archived records to ensure there is no more sensitive information remaining and has stated that they are working with the Tasmanian Archives to ensure there is no repeat, supposedly [8].

1.3 Crown Resorts

Crown Resorts fell victim to a data breach that involved a third-party file transfer service they utilised and outsourced through, being breached [11]. A ransomware group contacted Crown Resorts confirming they had stolen several sensitive Crown Resorts organisational files, and Crown Resorts had confirmed no customer information had been accessed, and business operations ran as normal [12]. Specifically, employee information such as timesheets and attendance records, as well as some membership numbers were released, and Crown Resorts has stated they have notified all individuals affected [13].

Crown Resorts were apt in their response to the breach, they notified all authorities and released a statement as they were informed about the breach [13]. Their operations remained stable, and they showed effective cyber governance during the peak of the breach by communicating with the public and showing their strength with information risk management. This breach, however, highlighted a key weakness in Crown Resorts information security management which was the consequences of overlooking a third-party service provider and their security. As Crown Resorts was using this file transfer service as an important utility in their business operations, it is clear they did not perform the relevant security checks and confirm that the provider is not vulnerable to breaches.

It is important to highlight that Crown Resorts has an in-depth risk management strategy document made in 2021, which highlights a very strong information risk and security management strategy, as well as confirms their strengths in cyber governance [14]. However, this risk management strategy document is very focused on qualitative measures of risk impact, which when measuring realistic outcomes of certain scenarios, can be detrimental to the risk mitigation process. It would be highly important to base more risk measures on hard evidence and scholarly research to gauge a more realistic risk and vulnerability scenario outcome.

1.4 Ambulance Victoria

Ambulance Victoria had sensitive employee information exposed in a breach caused by careless human error. In May of 2023, Ambulance Victoria made a statement where they stated that they were launching an investigation on several documents that were made accessible through the local intranet and contained sensitive information of employees such as alcohol and drug test results. The documents were only viewed a handful of times, before they were removed, and an investigation was launched [15].

Ambulance Victoria responded aptly yet waited just over a week to release a public statement [16]. They have confirmed they contacted every individual affected by the breach as soon as they were notified, yet their reluctance to release a public statement is noted. Being a government body, one would hope their timeliness on informing the public about a privacy breach would be swift. This breach highlighted a weakness in the organisation's overall care for individuals' data. To have sensitive employee data accessible and vulnerable is negligent and shows a real lack of information security management at Ambulance Victoria.

This point is further driven by the lack of information security and risk management processes, and cyber governance techniques implemented publicly by Ambulance Victoria. Within their strategic plan for January to June 2022, it is noted that the organisation has implemented cyber security controls, specifically network access controls and network segmentation, as well as focus being shifted on risk mitigation [17]. However, this seems to have yet to be completed and there is clearly no driven focus in the cyber security sphere. While these processes have said to be implemented, clear human error has been established as the cause of this breach, and more focus should be put on training employees as well as maintaining information security management.

1.5 MSI

MSI suffered a cyber-attack where ransomware gangs infiltrated their systems and stole source files for MSI BIOS systems. In April of 2023, MSI's intrusion detection systems detected attackers on their systems, and consequently MSI activated defence mechanisms and recovery measures. MSI suffered little to no impact on their business, and operations remained stable [18].

During the peak of the breach, MSI had little communication with the public, especially its' consumers. As MSI had BIOS firmware documents stolen, it is very possible consumers could be targeted for malware disguised as MSI BIOS firmware [19]. MSI barely communicated this, and only released a press statement. MSI also were not specific in the how and why of the data breach and remained silent as they dealt with the breach behind the scenes. This is a poor response, and an indication of poor cyber governance, and has had an impact on their reputation in how they deal with cyber breaches.

However, it is to be noted that MSI has extensive cyber risk management procedures and processes, as identified in their 2020 annual report. They are ISO27001 certified and have clear focus on information security and risk management, especially in that they use backed evidence and research for their risk identification and have evidence of implementation of security management techniques [20]. Despite this, there have not been any further annual reports made public for MSI and have no conclusive evidence of further security implementations following the breach, indicating a clear gap in essential public communications and potential indifference to information security prior to the breach.

1.6 SERVICE NSW

Service NSW, a government ran application, experienced a privacy breach when user's sensitive data was revealed shortly to other users in a system glitch. Human error consequently led to this glitch occurring for approximately 90 minutes, where users who logged into the Service NSW app saw currently logged in users' sensitive data on the app dashboard [21]. This breach occurred in late March, and Service NSW did not release a statement to the public informing of the software bug until early April [22].

Service NSW suffered a large blow to their reputation, considering it is a government body these 'software glitches' should not occur in the first place if the body truly respected information security management. Service NSW responded within two weeks from the initial breach, informing the public that user data is safe, and they are taking necessary precautions to prevent this from happening again [23]. Although it begs the question, if something as simple as this 'software glitch' happens, how truly focused are Service NSW, and the government in general, on information security and risk management, and sensitive user data and privacy in general? This privacy breach only highlights the weaknesses in how Service NSW handles user data, and highlights their weaknesses in software quality control; how did this pass initial tests?

However, it is important to note that Service NSW released a cyber security policy for their organisation in 2021, and it highlights their strengths in information security and risk management, showing their research and clear implementation strategies, as well as their cyber governance. There is clear identification of accountability frameworks, as well as also predetermined criteria for any information system security levels and priority [24]. However, it once again begs the question if these policies are being properly implemented, given this preventable privacy breach.

1.7 TASMANIAN GOVERNMENT

The Tasmanian Government, specifically the education department, suffered a severe data breach due to a third-party file transfer service having been infiltrated in March 2023. This resulted in near 16,000 documents from children's personal information to financial information from university applicants [25].

Their response was lacklustre, with the minister intentionally waiting approximately a *week* to inform the public of the breach, due to concerns of legitimacy. Along with that, they also were extremely vague with what data had been released [26]. This shows a high level of incompetency within the realm of cyber governance, as well as information security management, given that potentially all children, and adults, that had given their information to the education department [27] could have had their sensitive data leaked. As well as that, not performing the necessary security checks for vulnerabilities when using a third-party service for data transfer shows a strong weakness in the Tasmanian Government's information risk and security management. The Minister of Science and Technology was highly criticised for her response to the breach and was called to step down from her position due to the handling of this breach [26]. It is also important to note that the Tasmanian Government never stated that they would be improving security implementations, only that the public remain 'vigilant' [27]; which shows a colossal lack of accountability and responsibility.

The Tasmanian Government has an existing cyber security policy, but it is, alike to their response to this breach, lacklustre and vague. Within their policy, they name general statements on their promise for handling sensitive user data, as well as vaguely describing an accountability framework and responsibilities [28]. They do, however, identify that they are compliant with standards such as ISO27001, ISO31000, and IS027005, which is positive considering their vagueness when dealing with such a monumental information breach.

1.8 MERITON

Meriton had a severe data breach which compromised over 35 gigabytes of sensitive customer and employee data in January 2023. Information like birth certificates, tax file numbers and bank statements of employees were released, which is severe in nature [29]. To preface Meriton's response, it is important to note that their initial statement of the cyber attack has now been made unavailable on their website [30] as of October 17th, 2023.

Meriton did not inform the public for three months after the initial breach, as the breach occurred in January and a statement was not released until March. Sensitive data of this magnitude being released, and the organisation waits this long to inform the public? As well as that, the breach originated from Meriton's poor security infrastructure, in that, Meriton's data was kept in *one* place, as well as duplicates of that data being sent to suppliers and third parties, not anonymised [31]. This is extremely poor information risk and security management, and clearly there was no consideration of the risks of this methodology of information storage. This breach only highlights Meriton's backwards approach to information security and risk management, and there was no thought or consideration being put into information standards or methodologies.

Meriton also does not have a publicly available cyber security policy, information risk strategy, or any form of documentation proving their implementation of cyber security techniques. Meriton only promised that "it was implementing enhanced cybersecurity measures to protect the company's IT networks" [29]. There has been no proof of implementation, and it speaks volumes that Meriton has removed the initial statement regarding the data breach from their official website. There are clear weaknesses when it comes to all aspects of cyber security management within Meriton's business procedures, and a clear gap in documentation regarding it, which evidently ransomware groups have successfully targeted.

1.9 ID TECH

iD Tech suffered a data breach in January and have lost close to one million records containing sensitive user data. The attacker confirmed that they stole names, dates of birth, 415,000 email addresses and plaintext passwords [32], which would include parent's and children's sensitive information. iD Tech has yet to provide a response, or any public disclosure of the data breach.

iD Tech has declined to confirm the data breach, as well as declined to inform any users of the potential data breach, along with that, have also declined to confirm if they have lodged the data breach to the correct data protection officials [32]. All these facts combined prove that iD Tech have a severe lack of accountability measures, as well as any incident response measures whatsoever. A company withholding information and intentionally being vague about data breach specifics, is extremely concerning from an information risk and security management perspective. Confirming the legitimacy of the attack was also concerningly easy, considering the data breach files are accessible through Google [33].

iD Tech does not have a cyber security policy that is accessible, although it would seem they are not following such a policy considering their response to this attack. Parents that were a victim to this data breach, found that their emails were compromised through an online breach notification service called 'Have I Been Pwned' [32] [34]. The documentation and coverage regarding this data breach indicates a clear gap in information, especially considering the impact this breach potentially had, with the volume of information that was released.

1.10 Latitude Financial

Latitude Financial was subject to a cyber attack in March, which resulted in extremely sensitive user data being stolen and potentially used for criminal purposes. The cyber attack had the attackers steal up to 8 million drivers license numbers, 103,000 copies of passports and licenses, 53,000 passport numbers, and other extremely sensitive financial information [35]. The impact that this breach had over several associated businesses such as Coles, Myer, Harvey Norman, and The Good Guys [36], was severe in nature.

Latitude's response was efficient, and sufficient. Once Latitude had learned of the breach, they notified all users affected, and released a public statement with advice for customers that may have been affected [35]. However, we can view a weakness in Latitude's cyber governance. Latitude's business operations came to a complete halt during the breach, and the business essentially shut down. Not only is this a weakness shown in Latitude's cyber governance, but also information security management. Evidently, Latitude's systems were all interconnected without levels of security. If Latitude's systems were, for example, segregated, the attack could have been further isolated, and risks could have been mitigated. Although, it is noted that the attack occurred through obtaining login information of an employee through a vulnerability in a third-party backend infrastructure [37]. This, once again, highlights a key weakness in Latitude's information security, as they evidently did not guarantee their information security with this third-party provider.

Within Latitude's policies lies several risk management reports, annual reports containing cyber risk summaries, along with a follow up policy update following the data breach [38]. Within their risk management report, they outline several policies and regulations they follow, as well as several in-depth information security management techniques [39]. With evidence-backed research and relevant qualitative research, it seemed Latitude had their information security in check. Latitude also has several documents highlighting cyber governance, and accountability frameworks and decision-making hierarchies involving information risk [40]. While there are high strengths within Latitude, there are also noted weaknesses as presented in the data breach.

2 INFORMATION SECURITY MANAGEMENT PRACTICES ANALYSIS

The role of information security management practices is crucial to protecting user data and privacy in an evolving cyber-sphere. In 2021-2022, cybercrime reports saw an increase of 13 percent, with a notable 76,000 total reports by the end of 2022 financial year [41]. Through the use of literature reviews, we can analyse and identify gaps in modern organisation incident response and management techniques. Through identifying these gaps and weaknesses, we can further analyse and provide interpretation on the role of information security management within the organisations studied. Analysing how organisations disregard information security techniques until a breach occurs is a common and concerning practice in modern organisations, as well as the issue of vague communication and negligent incident response following a cyber incident. An analysis into the frequency of third-party vendor data breaches leading to chain reaction breaches is a staple of cyber threats that deserves its own paragraph. Through analysing these aspects deeply, we can explore solutions, challenges, and venture deeper into the existing strategies and policies that noted businesses have put in place, as well as identify the need and current trends within Australian cyber threat intelligence on businesses.

Proper information security and risk management techniques are overlooked until an incident occurs that forces response and action. With over 300,000 cyber crimes occurring in Australia every year [41], one would believe that major organisations, such as government bodies, and large business corporations, would have proper implementations of information security in place. More often than not, organisations have a lack of cyber policy until it's too late. Within cases such as HWL Ebsworth, Port Arthur Library, Ambulance Victoria, and Meriton, cyber security policies may have been 'implemented', however, they were clearly not properly followed and only treated as a pleaser for the board, considering the breaches that followed showed their incompetency for information security. In a larger organisation, challenges such as, employee awareness and compliance, board satisfaction, implementation delays can all impact how *and* if an organisation implements a cyber security policy [42]. This challenge is exemplified within Ambulance Victoria's existence of cyber governance techniques, but a clear lack of understanding from employees, given the nature of their breach being simply human error. By ensuring compliance and support from not only employees, but the board also, it would drive the effectiveness of cyber policies highly. To achieve compliance and enthusiasm, it is imperative that top management drives cyber policies, and establishing a solid governance framework [42]. By establishing a governance framework such as this, many low-level breaches that occur would be minimised due to the top-down effect that a cyber-managed governance framework would offer. In a survey conducted, it was noted that only 12.6% of Australian business owners/employees participated in training that enforced knowledge of cyber threats [43]. A critical practice businesses must employ is mandatory cyber hygiene training, to maintain information security. The relationship between this governance framework in question, and information security management, is the compliance necessary to obtain information security and risk management. With proper compliance from employees due to a strong governance framework, a business can achieve business-wide knowledge of cyber threats, as well as handling incident response, and preventing and mitigating risks and threats prior to attack. To have compliance of cyber policies within an organisation is the beginning of a strong information security and risk management policy. In a breach such as Service NSW where it was attributed to human error, a privacy breach such as this would not have happened with sufficient quality assurance within development. If information security practices were

properly followed, the breach would not have occurred in the first place. In a government-based organisation such as Service NSW, there is a clear trust from all citizens using a government application, that their data and information they give to that organisation, is protected thoroughly. In a breach such as this, it proves that Service NSW are not employing information security techniques when handling user data. These would include anonymisation and data encryption, as the information that was temporarily shown was easily linkable to any user using the site at that time. Following the breach, Service NSW stated that they will be further implementing and improving their cyber security operations and handling of user data [21]. This once again begs the question, why are information security and risk management techniques overlooked until an incident occurs that could have been prevented by following cyber policies in the first place?

When there is a lack of communication between organisation and individuals, there is a clear negligence for accountability and an indication of a lack of governance. The Meriton data breach showed a lack of accountability and communication. A public statement not being released for two months, and then being removed as of October 17th, as well as not having a publicly accessible cyber policy [30], shows an extreme lack of accountability, and a clear intention to 'forget' about the data breach and inadvertently their poor governance, and in turn, their excessively poor information security and risk management techniques. The importance of information security management is exemplified by the cause of data breaches. In the case of Meriton, having their data infrastructure located in one place, not segregated, as well as sending duplicates of the data to suppliers, unprotected, it was bound that a breach would occur. MSI is also a case that is relevant to communication between organisation and customer. The breach of MSI was met with little communication, simply a statement from MSI [18]. With customers having little information on the breach, information is left vulnerable. Especially when understanding, only due to other organisations investigating the breach's consequences and **not** MSI themselves, that BIOS keys could be duplicated and cause several of MSI's systems to be vulnerable to malware [44]. This lack of communication which would be vital to MSI customers identifying a possible vulnerability within their system, indicates a lack of accountability, and therefore a lack of proper governance techniques. With these cases in mind, it is crucial to understand how important communication and accountability is with information security. In the terms of Meriton, customers *were* contacted, but further information and support was linked to an external source. In terms of MSI, customers would have had **no** idea of the vulnerabilities that would come from the data breach, which MSI explained did not reveal customer information; but the consequences of the BIOS information leaking would, in the future [45]. While MSI is ISO27001 certified, there is no evidence of either companies' compliance with other cyber security regulations, which is a major aspect of information security management and governance. Current trends within cyber security management involve ever-changing and developing regulations and regulatory bodies, such as GDPR, HIPAA, CCPA, PCI DSS, ISO. These regulations, especially GDPR, motivate organisations to adhere to essential cyber security policies, and typically result in fines, or damage to reputation if not followed. These regulations require implementations of information security and risks management techniques, more specifically risk identification, privacy and risk training, policy evaluation methods, vulnerability assessments, risk mitigations, and asset identification [46]. Although these regulations are minimums and essentials, they provide a stepping stone to further influence for cyber policies for organisation boards [47]. These regulations provide stronger solutions to overall information security management, as well as a stronger blueprint for cyber governance frameworks given the influence of the regulations.

Outsourcing third-party vendors can improve business efficiency, but relevant security guarantees must be made to ensure a secure venture. A recent study by Verizon in 2022 found that 62 percent of all data breaches happen due to exposure or vulnerability in third-party vendors [48]. This can be seen in a large-scale breach such as Latitude Financial, where because of a vulnerability in an outsourced third-party backend infrastructure, attackers were able to gain access to employee login credentials, and consequently exfiltrate user data [49]. Another example is Crown Resorts, where a third-party file transfer service was breached and led to files being made vulnerable [12]. Similarly, within the Tasmanian Government data breach where data was once again made vulnerable through a third-party file transfer service [25]. All these cases, and many more, exemplify the common practice of businesses utilising third-party vendors for their data, and evidently not performing the necessary security evaluations, which consequently led to the breach of data. Businesses should align their practices with the data regulation requirements of CPS 234, an information security standard that handles ensuring third-party entities can withstand cyber attacks and have proper security implementation in place [50]. Ensuring a third-party vendor is adhering to information security practices is just as important as ensuring one's own organisation is adhering to information security practices. The importance of information risk and security management, and cyber governance, lies in the pure importance of maintaining and securing user information and privacy. With cybercrime being reported in 47 percent of computer users in Australia [43], it is now more crucial than ever to maintain a strong information risk and security management methodology, as well as have a strong cyber governance framework with relevant compliance procedures. Through the use of techniques such as multi-factor authentication, data encryption, virtual private networks, network segregation, access controls, and so many other mitigation techniques, organisations need to employ a cyber policy, and begin to analyse the role information security would have in their business and begin to develop risk management strategies and accountability frameworks for incident response. A baseline for all organisations to follow are regulations such as ISO27001, PCI DSS, GDPR, COBIT, among others, to develop and implement an adequate information risk and security management framework, which would further improve their cyber governance through the accountability and decision-making frameworks that are included within data regulations [51] [52].

The role of information security management within modern organisations is evidently weaker than one would ascertain such large corporations to maintain. With the majority of cases covered not having a public cyber policy, and those that do more commonly barely mention information security practices any longer than a bullet point, there is a major concern for how organisations, especially government bodies, are handling user data and data privacy as a whole. With the carelessness and negligence of data breaches retaining to human error which exposes thousands of records of sensitive information, to a case such as a government body using an unsecure third-party data transfer service, it is a concern to see the direction modern organisations are taking when it comes to information security management. However, with cybercrime rising, we have seen 62 percent of small business owners reporting a cyber incident in 2022 [53], which indicates the complexity of the cybercrime issue. Not only are large corporations being targeted, but small businesses too. The importance and role of information security management should now be prioritised more than ever, as cybercrime is one of the biggest threats to an organisation and its data, and consumers, and through the analysis of the role in Australian organisations, its damning evidence of a lack of understanding and knowledge of the true threat to privacy is concerning, and change is demanded.

3 SUCCESSFUL IMPLEMENTATIONS OF I.S. FRAMEWORKS

3.1 CASE 1 – MSI

MSI is a business that deals directly with computing systems and has a widespread reach in the cyber-sphere. MSI handles potentially harmful information and has been subject to a data breach which resulted in the potential vulnerability of all MSI motherboards [18]. Although this breach did not result in the release of user data, it resulted in potentially making user data vulnerable, as attackers can disguise BIOS firmware with malware through the release of MSI's internal files and details on the BIOS firmware.

It is noted that MSI has implemented a formally certified information security management system, known as ISO27001. In their annual report of 2020, they describe every aspect of the implementation of ISO27001, such as the creation of an information security policy, the development of a basic information security management structure, asset classification and management, personnel training, access control management, system maintenance, security breach management, auditing, evaluations, and management reviews [20]. All of these aspects cover ISO27001, a formally certified framework, which is considered the international standard for information security management. It allows businesses and organisations to identify assets, identify risks, and manage and mitigate those risks appropriately in order to protect user information.

MSI had obtained the certification for ISO27001 on the 12th of April 2021. This means that they had a formally certified information security framework prior to the breach they suffered in 2023. Although they are formally certified, there is no other documentation that covers the depth of implementation of the ISO27001 framework. We can describe the implementation as successful for MSI considering the certification, however, how can we distinguish if they are truly following the criteria for the ISO27001 framework?

3.2 CASE 2 – TASMANIAN GOVERNMENT

The Tasmanian government and its departments adhere to several different information security frameworks. These frameworks are ISO27001, ISO31000, and ISO27005 [28]. These frameworks cover cyber security and risk management, and the Tasmanian government has stated, although vaguely, that each agency of the Tasmanian government must adhere to these international standards. The Tasmanian government does not go in-depth with the extent of which they are adhering to the standards, but they describe vague practices and responsibilities based on standards for risk management, as well as governance and decision-making hierarchies.

It is also important to note that the Tasmanian government has developed their own cyber security strategies and frameworks for Tasmanian organisations to use and follow as guidelines [54]. Although these are not formal certifications unlike the certifications that every department of the Tasmanian government follows, they still provide brief insight into the extent of development of understanding information security. With not only an information security policy, the Tasmanian government also implements their own Information and Records Management Standard which describes the life cycle of any records in any archive, Information Security Classification Standard, and the Physical Storage Technical Standard which describes the guidelines for physical storage media and how it is maintained and protected [54].

4 REFERENCES

[1] Mandiant, “Cyber Security Forecast 2023,” 2023.

[2] M. P. Sam Buckingham-Jones, “Revealed: Inside HWL Ebsworth’s negotiations with the BlackCat hackers,” 2023. [Online]. Available: https://12ft.io/proxy?q=https%3A%2F%2Fwww.afr.com%2Fcompanies%2Fmedia-and-marketing%2Frevealed-inside-hwl-ebsworth-s-negotiations-with-the-blackcat-hackers-20230614-p5dgf7. [Accessed 15 October 2023].

[3] N. N. Lauren Croft, “Inside HWL Ebsworth’s plan to manage a 4TB data leak,” 2023. [Online]. Available: https://www.lawyersweekly.com.au/biglaw/37537-inside-hwl-ebsworth-s-plan-to-manage-a-4tb-data-leak. [Accessed 15 October 2023].

[4] HWL Ebsworth, “Cyber Incident - HWL Ebsworth Lawyers,” 2023. [Online]. Available: https://hwlebsworth.com.au/cyber-incident/. [Accessed 15 October 2023].

[5] HWL Ebsworth, “HWL Ebsworth Privacy Policy,” 2023. [Online]. Available: https://hwlebsworth.com.au/hwl-ebsworth-privacy-policy/. [Accessed 15 October 2023].

[6] J. Taylor, “HWL Ebsworth hack: 65 Australian government agencies affected by cyber-attack,” The Guardian, 18 September 2023. [Online]. Available: https://www.theguardian.com/australia-news/2023/sep/18/hwl-ebsworth-hack-65-australian-government-agencies-affected-by-cyber-attack. [Accessed 15 October 2023].

[7] N. A.-N. Stephanie Borys, “Nation's first cyber security coordinator appointed, as government reckons with HWL Ebsworth breach,” ABC News, 23 June 2023. [Online]. Available: https://www.abc.net.au/news/2023-06-23/cyber-security-coordinator-appointed-ebsworth-breach/102514454. [Accessed 15 October 2023].

[8] ABC News, “Human error, not data breach, behind Port Arthur staff information appearing 'live' on library website,” ABC News, 20 June 2023. [Online]. Available: https://www.abc.net.au/news/2023-06-20/no-data-hack-in-port-arthur-historic-site-staff-records-release/102497682. [Accessed 15 October 2023].

[9] Port Arthur Historic Site Management Authority, “Annual Report 2021-2022,” Port Arthur, 2022.

[10] Port Arthur Historic Site Management Authority, “PAHSMA Strategic Plan 2023-2028,” 2023.

[11] ABC News, “Crown Resorts investigating potential data breach after being contacted by hacking group,” ABC News, 27 March 2023. [Online]. Available: https://www.abc.net.au/news/2023-03-27/crown-resorts-ransomware-threat-by-hackers-data-breach/102151816. [Accessed 16 October 2023].

[12] M. Achenza, “Crown Casinos investigates as ransomware group claims to have breached data,” NCA NewsWire, 28 March 2023. [Online]. Available: https://www.news.com.au/technology/online/hacking/crown-casinos-investigates-as-ransomware-group-claims-to-have-breached-data/news-story/dcb6b0365633dd199e75b93911f6b098. [Accessed 16 October 2023].

[13] K. Taute, “Media Releases - Crown Resorts,” Crown Resorts, 5 April 2023. [Online]. Available: https://www.crownresorts.com.au/media-centre/media-releases. [Accessed 16 October 2023].

[14] Crown Resorts Limited, “Crown Resorts Limited Risk Management Strategy,” 2021.

[15] A. Anderson, “Employee records exposed in Ambulance Victoria data breach,” NCA NewsWire, 12 May 2023. [Online]. Available: https://www.news.com.au/technology/online/security/employee-records-exposed-in-ambulance-victoria-data-breach/news-story/8229ff2991fb1ac77cc4b777438de734. [Accessed 16 October 2023].

[16] Ambulance Victoria, “Notice relating to privacy breach,” Ambulance Victoria, 19 May 2023. [Online]. Available: https://www.ambulance.vic.gov.au/notice-relating-to-privacy-breach/. [Accessed 16 October 2023].

[17] Ambulance Victoria, “Ambulance Victoria Strategic Plan Update January to June 2022,” 2022.

[18] MSI, “MSI Statement,” Micro-Star International, 7 April 2023. [Online]. Available: https://www.msi.com/news/detail/MSI-Statement-141688. [Accessed 16 October 2023].

[19] S. Gatlan, “MSI confirms security breach following ransomware attack claims,” Bleeping Computer, 7 April 2023. [Online]. Available: https://www.bleepingcomputer.com/news/security/msi-confirms-security-breach-following-ransomware-attack-claims/. [Accessed 16 October 2023].

[20] Micro-Star International Company Limited, “2020 Annual Report,” 2020.

[21] S. Lock, “Service NSW breach exposes personal data affecting thousands of customers,” 7 News, 4 April 2023. [Online]. Available: https://7news.com.au/news/nsw/service-nsw-breach-exposes-personal-data-affecting-thousands-of-customers-c-10240008. [Accessed 17 October 2023].

[22] D. Croft, “Service NSW exposes details of thousands after website update,” Cyber Daily, 4 April 2023. [Online]. Available: https://www.cyberdaily.au/critical-infrastructure/8882-service-nsw-exposes-thousands-of-customer-details-after-website-update. [Accessed 17 October 2023].

[23] R. Ciccarelli, “Service NSW 'technical issue' may have exposed data of 3700 customers,” 9 News, 4 April 2023. [Online]. Available: https://www.9news.com.au/national/service-nsw-data-breach-technical-issue-may-have-exposed-customers-data/884325c7-919a-4ae3-b545-9235fc81679e. [Accessed 17 October 2023].

[24] NSW Government, “NSW Cyber Security Policy,” 2021.

[25] M. Ogilvie, “Update on cyber investigation,” Tasmanian Government, 7 April 2023. [Online]. Available: https://www.premier.tas.gov.au/site_resources_2015/additional_releases/update-on-cyber-investigation. [Accessed 17 October 2023].

[26] E. Coulter, “Tasmanians affected by security breach of third-party file transfer service,” ABC News, 31 March 2023. [Online]. Available: https://www.abc.net.au/news/2023-03-31/data-breach-third-party-file-transfer-service-tasmania/102173432. [Accessed 17 October 2023].

[27] M. W. Clancy Balen, “Minister confirms 16,000 documents released online in Tasmanian data breach, helpline set up,” ABC News, 7 April 2023. [Online]. Available: https://www.abc.net.au/news/2023-04-07/tasmania-goanywheremft-file-share-data-breach-16k-documents-out/102197658. [Accessed 17 October 2023].

[28] Tasmanian Government, “Tasmanian Government Cyber Security Policy,” 2022.

[29] D. Tran, “Hotel and property giant Meriton hit by data hack, personal documents may be at risk,” ABC News, 29 March 2023. [Online]. Available: https://www.abc.net.au/news/2023-03-29/australian-hotel-chain-meriton-hit-by-data-breach-hack/102141880. [Accessed 17 October 2023].

[30] Meriton Suites, “Cyber Response (Not Found),” Meriton Suites, [Online]. Available: https://www.meritonsuites.com.au/cyber-response/. [Accessed 17 October 2023].

[31] T. Biggs, “Private financial, health information exposed in Meriton data breach,” The Sydney Morning Herald, 29 March 2023. [Online]. Available: https://www.smh.com.au/technology/financial-health-contact-information-exposed-in-meriton-data-breach-20230329-p5cw58.html. [Accessed 17 October 2023].

[32] Z. Whittaker, “Kids tech camp iD Tech still silent weeks after data breach,” Tech Crunch, 24 March 2023. [Online]. Available: https://techcrunch.com/2023/03/23/id-tech-kids-tech-camp-data-breach/. [Accessed 17 October 2023].

[33] Breach Forums, “iD Tech Database - Leaked, Download!,” Breach Forums, 12 June 2023. [Online]. Available: https://breachforums.is/Thread-iD-Tech-Database-Leaked-Download. [Accessed 17 October 2023].

[34] Have I Been Pwned, “Have I Been Pwned? Check if your email address is in a data breach,” [Online]. Available: https://haveibeenpwned.com/. [Accessed 17 October 2023].

[35] Latitude Financial, “Latitude Cyber Response,” Latitude Financial, March 2023. [Online]. Available: https://www.latitudefinancial.com.au/latitude-cyber-incident/. [Accessed 17 October 2023].

[36] A. Kollmorgen, “Latitude Finance breach affecting customers of many current and former businesses,” Choice, 10 May 2023. [Online]. Available: https://www.choice.com.au/consumers-and-data/protecting-your-data/data-privacy-and-safety/articles/latitude-finance-data-breach. [Accessed 17 October 2023].

[37] E. T. Kate Ainsworth, “Latitude Financial hit by cyber attack, more than 300,000 identity documents stolen,” ABC News, 16 March 2023. [Online]. Available: https://www.abc.net.au/news/2023-03-16/latitude-hack-300000-identity-documents-stolen/102104424. [Accessed 17 October 2023].

[38] Latitude Financial, “How We Protect You,” Latitude Financial, 2023. [Online]. Available: https://www.latitudefinancial.com.au/security/how-we-protect-you/. [Accessed 17 October 2023].

[39] Latitude Financial, “Enterprise Risk Management Framework,” 2022.

[40] Latitude Financial, “Latitude Corporate Governance Statement,” 2022.

[41] N. Dekker, “Critical Cyber Crime Statistics in Australia 2023,” Eftsure, 7 February 2023. [Online]. Available: https://eftsure.com/en-au/statistics/cyber-crime-statistics/#source-wrapper. [Accessed 18 October 2023].

[42] S. AlGhamdi, “Information security governance challenges and critical success factors: Systematic review,” *Computers & Security,* vol. 99, 2020.

[43] A. M. Isabella Voce, “Cybercrime in Australia 2023,” 2023.

[44] P. Arntz, “Ransomware attack on MSI led to compromised Intel Boot Guard private keys,” Malwarebytes, 9 May 2023. [Online]. Available: https://www.malwarebytes.com/blog/news/2023/05/ransomware-attack-on-msi-led-to-compromised-intel-boot-guard-private-keys. [Accessed 19 October 2023].

[45] Steven, “Intel Boot Guard Protection is Compromised on MSI Devices Due to MSI Breach,” ID Strong, 17 May 2023. [Online]. Available: https://www.idstrong.com/sentinel/intel-boot-guard-keys-compromised/. [Accessed 19 October 2023].

[46] M. K. Harold F. Tipton, in *Information Security Management Handbook*, 2010, pp. 100-102.

[47] I. B. S. S. Megan Gale, "Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead," *Computers & Security,* vol. 121, 2022.

[48] Verizon, "2023 Data Breach Investigations Report," 2023.

[49] J. Davidson, "Revealed: how hackers used a tech giant to get inside Latitude Financial," Financial Review, 24 March 2023. [Online]. Available: https://www.afr.com/technology/revealed-how-hackers-used-a-tech-giant-to-get-inside-latitude-financial-20230323-p5cukr. [Accessed 20 October 2023].

[50] APRA, "Prudential Standard CPS 234 Information Security," 2019.

[51] ISACA, "COBIT | Control Objectives for Information Technologies | ISACA," ISACA, [Online]. Available: https://www.isaca.org/resources/cobit. [Accessed 20 October 2023].

[52] ISO, "ISO/IEC 27001:2022," 2022.

[53] ACSC, "Cyber Security and Australian Small Businesses," 2022.

[54] Office of the State Archivist, "Tasmanian Government Information Management Framework," Tasmanian Government, July 2022. [Online]. Available: https://www.informationstrategy.tas.gov.au/Government-Information-Strategy. [Accessed 22 October 2022].