Hold My Beer: A Case Study of how Ransomware Affected an Australian Beverage Company

Samir Jarjoui
Gupta College of Business
University of Dallas
Dallas, USA
sjarjoui@udallas.edu

Robert Murimi
Gupta College of Business
University of Dallas
Dallas, USA
rkmurimi@udallas.edu

Renita Murimi
Gupta College of Business
University of Dallas
Dallas, USA
rmurimi@udallas.edu

***Abstract*—This case study follows the cybersecurity attack that impacted Lion, a large Australian beverage company with a portfolio of brands in beer, milk, wine, and other products. The ransomware attack, which impacted Lion in different phases, took place during a time of strained resources and increased restrictions due to the COVID-19 pandemic. This paper provides an overview of the warnings, events, and incidents leading up to the cyberattacks, and describes the impact to the company's operations. This case shows the parallel and connected challenges that the company faced in dealing with the ransomware and the pandemic's impact. While the cyber incidents had a significant impact on Lion's operations, the organization appeared to recover from it and resume operations. The case is suitable for students and practitioners interested in cybersecurity or information systems topics and presents the compounded impacts of cyberattacks and the COVID-19 pandemic on firms.**

Keywords—cybersecurity, ransomware, Lion Australia, case-study, REvil exploits, COVID-19

I. Introduction

The Australian food and beverage industry is Australia's largest manufacturing sector with an annual turnover of $50 billion [1]. Of these, the beverage industry supports more than 45,000 full-time jobs around Australia and contributes more than $7 billion to the economy [2]. Recent statistics on beverage consumption show that the average Australian drinks 96 liters of milk per year, which is high compared to other developed countries [1]. Another compelling statistic is that of alcohol consumption. Alcohol consumption statistics reveal that the average Australian, aged 15 years or over, drinks around 9 liters of alcohol every year [2].

Commanding a lion's share of the market in the Australian alcohol and dairy industry is Lion Dairy and Drinks, which accounts for approximately 20% of the fresh white milk market through its Pura brand and holds the distinction of being the largest brewer in Australia [3]. The former parent company of Lion Dairy and Drinks, Kirin Brewery, is a Japanese beverage giant that has established strategic alliances and operations in Asia, Europe, Australia and the United States.

Employing around 7000 people across Australia, Lion Dairy and Drinks has a range of products in the beverages market, including iced coffee, beer, plant milk, and cider [4]. What does ransomware have to do with milk and beer? A lot, especially if the key production and supply chain processes are frozen, data is breached, and the hackers demand $800,000 in exchange for releasing the company's files.

The rest of this paper is structured as follows. Section II offers the context of the COVID-19 pandemic that frames the timeline of the attack on Lion. Section III presents a timeline of events that comprised the cyberattack on Lion, and its immediate responses. In Section IV, we present details of the economic impact of the cyberattack on Lion. Section V discusses the broader implications of the attack on Lion. Finally, Section VI concludes the paper and presents reflections for cybersecurity practitioners.

II. Context

The first cases of COVID-19 were confirmed in Australia in January 2020. In March 2020, the coronavirus pandemic had entered the mainstream discourse in Australia and around the world. Lion was proactive, and on March 30, its official company website was updated to include a page on "How we're responding to Covid-19" [5]. This webpage outlined three objectives of their COVID-19 strategy centered around "supporting government strategies to limit the spread, support our people's health and well-being, and maintaining supply to our customers and the broader community".

On April 5, 2020, the Australian Government's Department of Health issued its first COVID-19 statistics report documenting 5,687 total confirmed cases at the time [6]. A timeline of the first fifty days of the spread of the virus and its impact on Australia reveals a period of broadening social restrictions on gathering, increase in quarantining measures and attempts to limit outbreaks [7]. Similar to what transpired in most of the world, markets took a direct hit as people and businesses struggled to decipher and live a new normal. Lion Dairy and Drinks was no exception. Along with other businesses, Lion Dairy and Drinks along with other businesses would have to be ready for the lost revenue due to the virus's impact. The Australian government enacted a broad range of lockdown measures in March. Australia's national economy shrank 7% in the three months leading up to June, and unemployment hit a 22-year high [9].

Australia was also and continues to be in the crosshairs of another global affront- cyberattacks. Australia is one of the most targeted countries in the world for cyberattacks, ranking sixth in the list of *significant* cyber-attacks over a fifteen-year period from 2006 – 2020 [10]. Significant cyberattacks are defined as attacks on a country's government agencies, defense and high-tech companies or economic crimes equating to a loss of more than a million dollars [11]. Major cyberattacks in Australia over the past five years include attacks by foreign spies on the Australian Bureau of Meteorology in 2015 [12], attacks on the Australian parliament's computer network and national security defense contractors [13], and attacks on the Australian National University exposing details of staff and students [14].

Ransomware represents an emerging class of cyberattacks where hackers attack a network with the intent of denying access to the computer, network or data until the ransom has been paid [15]. Most ransomware-affected systems result in encrypted files, with more than 151.9 million ransomware attacks reported in 2019 [16]. Commonly spread by clicking on phishing emails with malicious links and attachments, ransomware attacks have been deployed against individuals, universities, city and state governments, infrastructure, businesses and hospitals. Bitcoin is the most popular currency for ransom demands, with 98% of ransomware attacks demanding Bitcoin [17]. Ransom payments have steadily increased over the years. Counterintuitively, paying the ransom has been shown to increase the cost of dealing with the attack. This is because even if an organization pays the ransom, it still must deal with the effects of down time and rebuilding the network. Further, paying the ransom is not a sure guarantee that access will be restored. Also, the choice to pay ransom or not does not predict how the ransomed data will be misused. Data from ransomware attacks appear in chunks or as a whole on the dark web, increasing its exposure to malicious actors for future attacks. The ease of deploying ransomware, the versatile nature of files and assets that can be recovered, and the potential for collecting ransom in the format of both cryptocurrencies and fiat currencies makes ransomware a formidable tool in the hacker's toolbox of cyberattacks.

According to the Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report for the period ranging from July 2019 to June 2020, ACSC responded to 2,266 cyber security incidents for this reporting period [18]. As an example, ACSC issued a high-status alert in February 2020 about the Mailto ransomware, also known as Kazakavkovkiz ransomware [19]. Another alert issued on May 22, 2020 was related to COVID-19 malicious cyberactivity. With a status of "high", this alert warned individuals and organizations about COVID-19 scams and phishing emails that lured users desiring information about the pandemic into installing malicious software or stealing personal information.

The country was about to add another statistic to their list. Lion Dairy and Drinks would soon be hit.

III. The Attack Timeline

On June 10, 2020, Lion reported on their company website that their network had been a victim of a cyberattack resulting in an IT system outage [20, 21]. While details of the attack were scarce, the report on Lion's website made references to disruption in their ability to take, process and ship orders.

As an immediate precaution, Lion shut down all systems, and engaged with cyber experts to assess the consequences and impact of the attack. They found no evidence of any data breaches as of June 10, but they continued to monitor the fallout. A broader picture of the fallout slowly began to unfold. Two days later, their website was updated to include the impact of the double whammy delivered first by COVID-19, and then by the cyberattack. Lion reported how they were able to continue brewing operations safely throughout the COVID-19 shutdown and were in fact, gearing up to increase brewing. But the cyberattack limited their visibility of their products, took their breweries offline, and could potentially impact the inventory resulting in shortages. The perishable nature of dairy, juices and other similar beverages caused a greater impact. They reported experiencing "service misses in several customer channels", negative impact to their customer service and some manufacturing sites. Ongoing updates revealed that they had begun working with government authorities, law enforcement agencies and regulatory bodies to deal with the cyberattack.

The upcoming weekend after the first attack saw continued efforts to contain the fallout. Three days later, on June 15, Lion's update indicated that they were beginning to restore a sense of normalcy [22]. Their IT teams and cyber expert advisors were beginning to install new processes and controls to bring systems back online safely. However, supply chain disruptions continued, with several temporary shortages or out-of-stocks across both packaged (bottle/can) and keg brands. Their customer call center and ordering systems were now operational, and one brewery had restored operations. A number of their systems were still offline, and they continued to leverage manual processes as an interim effort to deal with the offline systems.

Meanwhile, analysis of the attack on Lion revealed more details. According to the Kaspersky ICS CERT report, the first attack on June 9th was reported to be a variant of ransomware [23]. The attack came at a time of not only pandemic-induced setbacks, but also at a time of strategic uncertainty. Lion Dairy and Drinks was amid a $600 million takeover bid from Chinese dairy giant Mengniu, part-owned by Chinese state-owned food processor COFCO [24]. Rumors swirled about possible involvement of hackers to disrupt the takeover by Mengniu. Making matters worse, the disruption of business followed a major IT upgrade project that spanned across a two-year period. This IT upgrade was reportedly focused on centralizing the company's applications into a cloud-based platform [25]. A timeline of events and activities, leading to the cyberattacks on Lion in 2020, is depicted in Fig. 1.

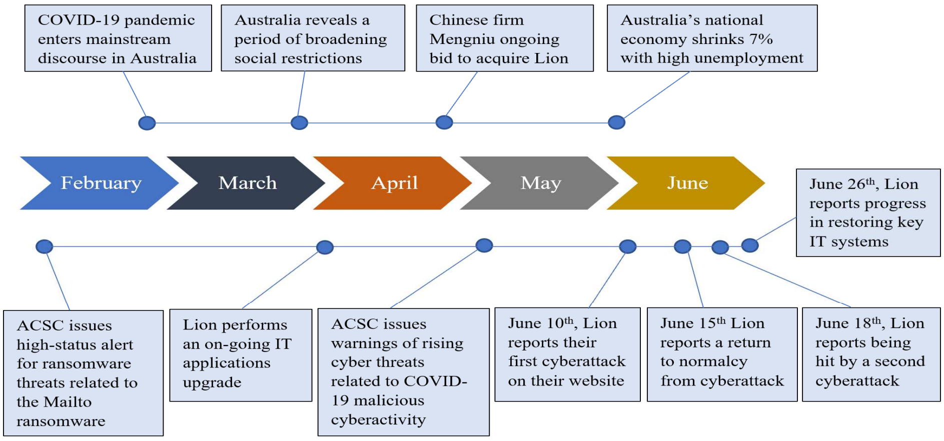
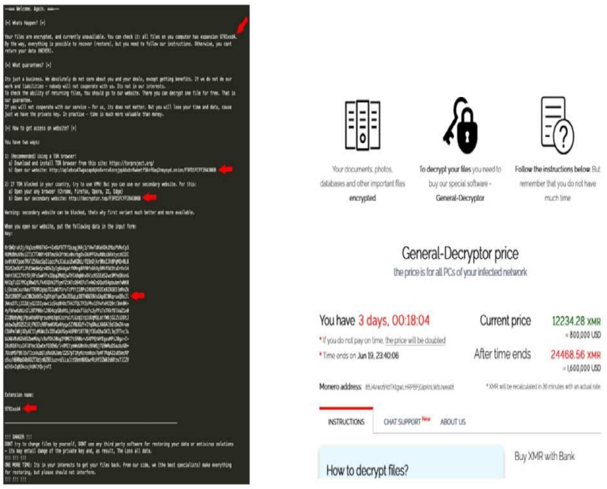

COVID-19 pandemic enters mainstream discourse in Australia
Australia reveals a period of broadening social restrictions
Chinese firm Mengniu ongoing bid to acquire Lion
Australia's national economy shrinks 7% with high unemployment
February
March
April
May
June
June 26th, Lion reports progress in restoring key IT systems
ACSC issues high-status alert for ransomware threats related to the Mailto ransomware
Lion performs an on-going IT applications upgrade
ACSC issues warnings of rising cyber threats related to COVID-19 malicious cyberactivity
June 10th, Lion reports their first cyberattack on their website
June 15th Lion reports a return to normalcy from cyberattack
June 18th, Lion reports being hit by a second cyberattack

Fig. 1. A timeline of events and activities leading to the cyberattacks

A week later, on June 18, Lion Australia got hit by a second attack [26]. This time, the attack was a ransomware attack which further disrupted its IT systems. Still reeling from the fallout of the first attack a week ago, Lion convened an all-staff meeting at 3 pm that day to share the news. Chief Executive Officer, Stuart Irvine, called it a “cyber-crisis” for the company posing “gigantic challenges”. The update on their company website was different from the update following the first attack. This update included the Australian Prime Minister’s comments on a range of cyber-attacks across the nation and provided three helplines for dedicated cyber help. Additional resources for cybersecurity were provided in the update, including best practices for password hygiene, phishing scams, suspicious links, and malicious attachments.

The ransomware attack was reported to be related to the REvil ransomware. It encrypted Lion’s files and came with a ransom demand of $800,000 USD to be delivered to a Monero address [27]. Monero is an open-source cryptocurrency that offers greater anonymity than Bitcoin [28, 29]. The hackers gave Lion a deadline of June 19, after which the ransom would be doubled. REvil ransomware, also known as Sodinokibi, has been attributed to the Gold Garden Threat group, and attacks computers running the Windows operating system [30]. REvil, which stands for Ransomware Evil, and inspired by the Resident Evil series, first appeared in 2019 and has been deployed around the world, including against a Canadian agricultural production company, and a Swedish security firm [31, 32]. A highly sophisticated piece of ransomware, REvil exploits systems using remote access vulnerabilities, turns off blacklisted processes, encrypts files, and exfiltrates information. REvil’s ransom note is shown below in Fig. 2.



```
---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expansion 9781xxd4.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant
return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our
work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is
our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause
just we have the private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://[illegible].onion/F3FD1FCFF2843B6B

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decryptor.top/F3FD1FCFF2843B6B

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:

[illegible]



Extension name:

9781xxd4

-----------------------------------------------------------------------------------------

!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions
- its may entail damge of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything
for restoring, but please should not interfere.
!!! !!! !!!
```

Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **General-Decryptor**

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

You have 3 days, 00:18:04

* If you do not pay on time, the price will be doubled

* Time ends on Jun 19, 23:40:06

Current price 12234.28 XMR
≈ 800,000 USD

After time ends 24468.56 XMR
≈ 1,600,000 USD

Monero address: [illegible]

* XMR will be recalculated in 36 minutes with an actual rate

Fig. 2. REvil’s Ransomware note [27]

Information about another significant development was provided in the update. It mentioned reports of Lion document lists posted online in recent days [33]. Now, their expert teams had an additional task on investigating these leaks and determining the kind of data that was available publicly. The misuse of this leaked data was an imminent threat that they anticipated. Lion started contacting stakeholders on a precautionary basis.

This incident would have one final update on Lion’s website. A week later on June 26, Lion reported progress in restoring many of their key systems [34]. All their nine breweries were up and running, and they were now brewing, kegging, packaging, and distributing beer across Australia and New Zealand. Further, all of their dairy and juice sites were reported as operational too. Customer ordering and invoice platforms were starting to come online. The update also mentioned continued engagement with cyber experts to safely restore all their systems. At that time, they did not find evidence of data being leaked, but were fully expecting it as a possibility in the near future. The update continued to urge cyber security measures and best practices.

Shortly after the two attacks on Lion, the Australian Government announced a $1.35 billion Cyber Enhanced Situational Awareness and Response (CESAR) package to boost protection and cyber resilience for all Australians. Lion’s parent company at the time, Kirin, was forced in August to scrap an earlier attempt to sell the business to Chinese food conglomerate China Mengniu Dairy Co Ltd for $600 million after the Australian government blocked the sale amid broader geopolitical tension.

IV. ECONOMIC IMPACT OF THE CYBERATTACKS ON LION

Lion suffered an economic impact due to the cyberattacks after being strained by the COVID-19 pandemic. The first cyberattack, which was reported on June 10, resulted in the shutdown of key systems. The company admitted that the cyberattack could not have come at a worse time, given the fluctuating and volatile product demand during the pandemic [35]. While Lion was able to resume operations during the COVID-19 lockdown, the cyberattack resulted in an interruption to critical IT components for the brewing process and related operations. As a result, Lion had reverted to a manual system to process customers’ transactions, however, this workaround had its limitations and could not resolve multiple supply issues [26, 31, 35]. The second cyberattack, reported on June 18, was characterized as a "cyber crisis" for the company, as it presented gigantic challenges and compounded the business interruptions experienced in the first attack [26]. It resulted in shortages and out-of-stock items for several of the company’s brands, as they resorted to limiting products available to customers.

In addition, the cyberattacks on Lion appear to have negatively impacted the stock performance of its parent company, Japan-based Kirin Holdings. A review of Kirin’s stock (KNBWY), which is listed on the Nikkei 225 Index, show the negative impact of the cyberattack. Kirin’s stock fell almost 6% in comparison to the Nikkei-225 drop of about 2%, few days after the first cyber-attack was reported. While the stock market was experiencing volatility due to the pandemic, Kirin’s stock underperformed the market (Nikkei-225) in the days and months after it had experienced the cyberattacks [36]. A stock comparison chart between February 2020 and February 2021, shows that the Nikkei 225 index had risen around 29% during that period, while on the other hand, Kirin’s stock reported fell more than 4%. A plot of the stocks comparison and the cyberattack impact on Kirin’s stock is outlined in Fig. 3.

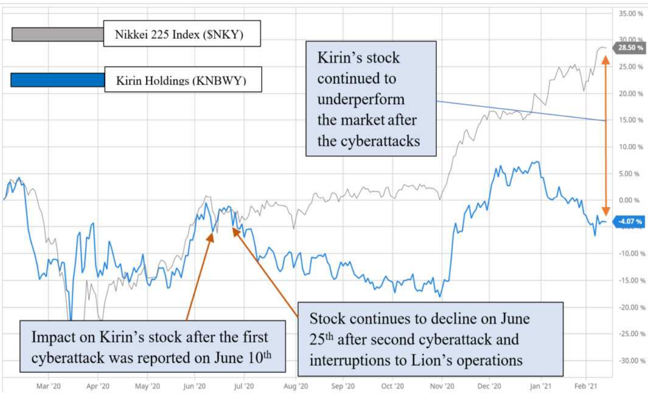


Fig. 3. Cyberattack impact on Kirin stock (Lion's parent company)

V. Discussion

It is unclear how the attackers were able to infiltrate Lion's networks using REvil ransomware and Lion did not disclose any details on how the attacks were initiated. While ransomware attacks are not new, this incident came at a time of strained resources due to the COVID-19 pandemic and an ongoing acquisition bid from a foreign company. As a result, Lion was pushed into a crisis mode [26] and was forced to scramble to investigate the root-cause of the breach and recover operational capabilities at a time of volatile market conditions. In anticipation of a second cyberattack, after the initial one was reported, the company contracted with Accenture, a multinational professional services company to assist with the cyber incident and investigation [37]. It did not appear that Lion had paid the ransomware, and instead, the company chose to rely on manual processes as an interim workaround for the offline systems impacted by the cyberattacks. While Lion was able to resume operations in a limited manner, the attacks significantly disrupted operations as the company was forced to shut down key systems.

There have been a few developments since the attacks on Lion. First, on June 30th, shortly after the cyberattacks on Lion, the Australian Federal Government announced the nation's largest investment in cyber security, with around $1.35 billion, to be invested over the next 10 years. This major investment is intended to improve the current cyber-capabilities to identify more cyber threats, disrupt more foreign cybercriminals, and build better partnerships with the industry [38]. Through this initiative, the Australian government hoped for new capabilities to minimize cyber-attacks, with over $31 million to enhance the ability to disrupt foreign cybercrime and foreign criminals that seek to target Australian entities. In addition, over $35 million has been allocated to deliver a new cyber threat-sharing platform, to facilitate intelligence sharing about malicious cyber activity, and block threats in near real-time. Further, around $62 million have been dedicated to a national situational awareness capability to better to understand and respond to cyber threats on a national scale [38]. The second development was related to the pending acquisition from China Mengniu Dairy, which was blocked in July by the Foreign Investment Review Board, due to national concerns [24]. These developments and cybersecurity efforts, which came at the heels of the Lion attack, highlight the challenges that governments and organizations face. Cyber-investments and efforts should be implemented in a systematic and proactive manner to maximize the effectiveness of cybersecurity controls. In addition, end-user cybersecurity training and awareness programs should be implemented within the organizational context to minimize cyber-threat exposures.

Further, cyber-incident communications are critical during such events to ensure that stakeholders are appropriately informed. Lion established a cyber help line and provided few announcements regarding the attacks [34]; however, no details were provided by the company regarding the root-cause of the incident, or for any risk mitigation actions that the company might have taken in response to the cyberattacks. Many victims of cybercrime are reluctant to share the details of such incidents. However, in a time of a heightened cybersecurity threat environment, it is critical to share some relevant information that may be helpful in preventing or minimizing cyber threats in other organizations. It is important that organizations work together to thwart cyber-threats in this shared economy, in a way that is characterized by an interdependence of technology solutions and economic activities.

VI. Conclusion

While the cyberattack discussed in this paper was focused on Lion, it is imperative to note that cyber-incidents are becoming more pervasive and sophisticated over time. Thus, we believe that the lessons that can be learned from this case, through an examination of the events and activities, can shed useful insights regarding the anatomy of cyber threats. For instance, the heightened cyber-threat environment and the multiple warnings and alerts from the ACSC, should have served at a wake-up call for many organizations to bolster their cyber-defenses. In addition, while facing multiple major disruptive events has not been a routine concern in the past, considering the compounded impact that Lion faced from the cyberattacks and COVID-19, it is important to prepare for major environmental disruptors such as the COVID-19 pandemic. Best practices should be established and implemented by organizations as they prepare for the inevitable. In conclusion, this case study provides an objective perspective on the cyberattacks, and outlines both the events and activities before and after the incidents, along with an overview of the actions taken by Lion. The goal of this paper is to promote knowledge on how organizations are impacted by such cyberattacks, while having to deal with a pandemic. This teaching case study adds value to cybersecurity professionals in industry and academia by providing a real-life example of a cybersecurity incident in detail.

Acknowledgment

The authors thank Aunshul Rege at Temple University for sharing the Critical Infrastructure Ransomware Incident Dataset, Version 10.6 [39]. This dataset contained the listing of the Lion ransomware incident, among others. That listing led the authors on an interesting pursuit of the events and activities surrounding the attack, which ultimately resulted in this paper.

References

[1] Parliament of Australia, "Food and beverage industry," *Country of origin guidelines to the Trade Practices Act*, *aph.gov.au.* [Online]. [Accessed: Feb. 1, 2021]

[2] Australian beverages council, “Beverages,” *australianbeverages.org.* [Online]. Available: https://australianbeverages.org/beverages [Accessed: Feb. 1, 2021]

[3] C. Jasper and J. Becker, “Bega Cheese confirms purchase of Lion Dairy and Drinks, owner of Pura Milk, Dare and Yoplait,” *ABC News*, Nov. 20, 2020. [Online]. Available: https://www.abc.net.au/news/rural/2020-11-26/bega-cheese-to-buy-lion-dairy-from-japanese-kirin/12910480 [Accessed: Feb. 4, 2021]

[4] “Leadership, diversity and the importance of great people,” *AFR Business Case Studies*. [Online]. Available: http://www.afrbiz.com.au/case-studies/lion-leadership-diversity-and-the-importance-of-great-people.html?print=1&tmpl=component [Accessed: Feb. 4, 2021]

[5] Lion Pty, “How we’re responding to COVID-19,” *Lionco.com*, Mar. 30, 2020. [Online]. Available: https://lionco.com/2020/03/30/how-were-responding-to-covid-19 [Accessed: Feb. 4, 2021]

[6] Australian Department of Health, “Coronavirus (COVID-19) at a glance”, *Health.gov.au*, Apr. 5, 2020. [Online]. Available: https://www.health.gov.au/resources/publications/coronavirus-covid-19-at-a-glance-5-april-2020 [Accessed: Feb. 5, 2021]

[7] “Australia Says Coronavirus Restrictions to Continue at Least Four More Weeks,” *USNews.com*, Apr. 16, 2020. [Online]. Available: https://www.usnews.com/news/world/articles/2020-04-16/australia-says-coronavirus-restrictions-to-continue-at-least-four-more-weeks [Accessed: Feb. 4, 2021]

[8] “Australia Says Coronavirus Restrictions to Continue at Least Four More Weeks,” *USNews.com*, Apr. 16, 2020. [Online]. Available: https://www.usnews.com/news/world/articles/2020-04-16/australia-says-coronavirus-restrictions-to-continue-at-least-four-more-weeks [Accessed: Feb. 4, 2021]

[9] S. Pandey, “Australia records worst economic slump as pandemic ends golden run,” *Reuters*, Sep. 1, 2020. [Online]. Available: https://www.reuters.com/article/us-australia-economy-gdp/australia-records-worst-economic-slump-as-pandemic-ends-golden-run-idUSKBN25T0I8 [Accessed: Feb. 4, 2021]

[10] T. Livingstone, “Cyber attacks: Australia the sixth most targeted country in world,” *9News.com.au*, Jul. 14, 2020. [Online]. Available: https://www.9news.com.au/national [Accessed: Feb. 4, 2021]

[11] K. Brasseur, “Study: U.S. largest target for ‘significant’ cyber-attacks,” *Compliance Week*, Jul. 13, 2020. [Online]. Available: https://www.complianceweek.com/cyber-security/study-us-largest-target-for-significant-cyber-attacks/29180.article [Accessed: Feb. 4, 2021]

[12] A. Greene, “Bureau of Meteorology hacked by foreign spies in massive malware attack, report shows,” *ABC News*, Oct. 11, 2016. [Online]. Available: https://www.abc.net.au/news/2016-10-12/bureau-of-meteorology-bom-cyber-hacked-by-foreign-spies/7923770 [Accessed: Feb. 4, 2021]

[13] I. Kwai, “Australian Parliament Reports Cyberattack on Its Computer Network,” *NY Times*, Feb. 7, 2019. [Online]. Available: https://www.nytimes.com/2019/02/07/world/australia/cyberattack-parliament-hack.html [Accessed: Feb. 4, 2021]

[14] S. Groch, “ANU data breach: How hackers got inside Australia's top university,” *Canberratimes.com.au*, Oct. 2, 2019. [Online]. Available: https://www.canberratimes.com.au/story/6414841/like-a-diamond-heist-how-hackers-got-into-australias-top-uni/ [Accessed: Feb. 4, 2021]

[15] R. Murimi, “Use of Botnets for Mining Cryptocurrencies”, in Botnets: Architectures, Countermeasures, and Challenges CRC Series in Security, Privacy and Trust by Taylor & Francis, 2019.

[16] Security Magazine, “First Three Quarters of 2019: 7.2 Billion Malware Attacks,” *Securitymagazine.com*, Oct. 22,2019. [Online]. Available: https://www.securitymagazine.com/articles/91133-first-three-quarters-of-2019-72-billion-malware-attacks-1519-million-ransomware-attacks [Accessed: Feb. 12, 2021]

[17] Marsh Research and Briefings, “Ransomware: Paying Cyber Extortion Demands in Cryptocurrency,” *marsh.com.* [Online]. Availabe: https://www.marsh.com/us/insights/research/ransomware-paying-cyber-extortion-demands-in-cryptocurrency.html [Accessed: Feb. 12, 2021]

[18] Australian Cyber Security Centre, “ACSC Annual Cyber Threat Report - July 2019 to June 2020”, *Cyber.gov.au*. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf [Accessed: Feb. 5, 2021]

[19] Australian Cyber Security Centre, “2020-003: Mailto ransomware incidents”, *Cyber.gov.au*, Feb. 16, 2020. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/alerts/2020-003-mailto-ransomware-incidents [Accessed: Feb. 5, 2021]

[20] “Cyber attack halts Lion production of milk and beer,” *MSN.com*, Jun. 11, 2020. [Online]. Available: https://www.msn.com/en-au/news/australia/cyber-attack-halts-lion-production-of-milk-and-beer/ar-BB15kiBu [Accessed: Feb. 4, 2021]

[21] Lion Pty, “Lion Cyber incident update,” *Lionco.com*, Jun. 10, 2020. [Online]. Available: https://lionco.com/2020/06/26/lion-update-re-cyber-issue [Accessed: Feb. 4, 2021]

[22] Lion Pty, “Lion Cyber incident update,” *Lionco.com*, Jun. 15, 2020. [Online]. Available: https://lionco.com/2020/06/26/lion-update-re-cyber-issue [Accessed: Feb. 4, 2021]

[23] Kaspersky ICS CERT, “Threat landscape for industrial automation systems,” *Kaspersky.com,* Sep. 24, 2020. [Online]. https://ics-cert.kaspersky.com/reports/2020/09/24/threat-landscape-for-industrial-automation-systems-h1-2020 [Accessed: Feb. 4, 2021]

[24] K. Hamlin, “Breakingviews - Australian milk deal looks a little too local,” *Reuters*, Nov. 24, 2020. [Online]. Available: https://www.reuters.com/article/us-kirin-holdings-m-a-breakingviews/breakingviews-australian-milk-deal-looks-a-little-too-local-idUSKBN2840CB [Accessed: Feb. 4, 2021]

[25] R. Crozier, “Drinks maker Lion shuts IT systems after 'cyber incident',” *itNews.com.au,* Jun. 9, 2020. [Online]. Available: https://www.itnews.com.au/news/drinks-maker-lion-shuts-it-systems-after-cyber-incident-549049 [Accessed: Feb. 4, 2021]

[26] B. Grubb, “'Cyber crisis' deepens at Lion as second attack bites beer giant,” *The Sydney Morning Herald,* Jun. 18, 2020. [Online]. Available: https://www.smh.com.au/technology/cyber-crisis-deepens-at-lion-as-second-attack-bites-beer-giant-20200618-p5540c.html [Accessed: Feb. 4, 2021]

[27] F. Erazo, “Australian Beverage Giant Faces Monero Ransom Demand of Nearly $1M,” *Cointelegraph.com,* Jun. 18, 2020. [Online]. Available: https://cointelegraph.com/news/australian-beverage-giant-faces-monero-ransom-demand-of-nearly-1m [Accessed: Feb. 4, 2021]

[28] Tokeneo, “Monero (XMR) - The Most Anonymous Cryptocurrency,” *Tokeneo.com,* Jul. 12, 2020. [Online]. Available: https://tokeneo.com/monero-xmr-the-most-anonymous-cryptocurrency [Accessed: Feb. 4, 2021]

[29] S. Aaron, “The Complete Guide to Monero Cryptocurrency,” *Bitdegree.org,* Jan. 11, 2021. [Online]. Available: https://www.bitdegree.org/crypto/monero [Accessed: Feb. 4, 2021]

[30] Secureworks, “REvil/Sodinokibi Ransomware,” *Secureworks.com,* Sep. 24, 2020. [Online]. Available: https://www.secureworks.com/research/revil-sodinokibi-ransomware [Accessed: Feb. 4, 2021]

[31] H. Solomon, “Canadian firm apparently victim of new ransomware tactic: Auctioning stolen data,” *IT World Canada,* Jun. 3, 2020. [Online]. Available: https://www.itworldcanada.com/article/canadian-firm-apparently-victim-of-new-ransomware-tactic-auctioning-stolen-data/431591 [Accessed: Feb. 4, 2021]

[32] Cloudsek, “REvil targets video games, claims massive revenue, Emotet uses parked domains to deliver malware, and more,” *Cloudsek.com,* Oct. 30, 2020. [Online]. Available: https://cloudsek.com/threatintel/revil-targets-video-games-claims-massive-revenue-emotet-uses-parked-domains-to-deliver-malware-and-more/ [Accessed: Feb. 4, 2021]

[33] A. Barbaschow, “Lion faces further 'setbacks' as it recovers from ransomware attack,” *Zdnet.com*, Jun. 19, 2020. [Online]. Available: https://www.zdnet.com/article/lion-faces-further-setbacks-as-it-recovers-from-ransomware-attack/ [Accessed: Feb. 4, 2021]

[34] Lion Pty, “Lion Cyber incident update,” *Lionco.com*, Jun. 26, 2020. [Online]. https://lionco.com/2020/06/26/lion-update-re-cyber-issue [Accessed: Feb. 4, 2021]

[35] P. French, “Australian brewer lion suffers major cyber attack ,” *The Drinks Business*, Jun. 12, 2020. [Online]. https://www.thedrinksbusiness.com/2020/06/australian-brewer-lion-suffers-major-cyber-attack/ [Accessed: Feb. 4, 2021]

[36] Barchart, *Nikkei 225 Index and KNBWY Stock Comparison*. [Online]. https://barchart.com/stocks/quotes/$NKY/interactive-chart [Accessed: Feb. 12, 2021]

[37] Digitpol, “Lion hit by a second cyber attack,” *Reportcybercrime.com,* Jun. 18, 2020. [Online]. https://reportcybercrime.com/lion-hit-by-a-second-cyber-attack/ [Accessed: Feb. 10, 2021]

[38] Prime Minister of Australia “Nation’s largest ever investment in cyber security, *pm.gov.au,* Jun. 30, 2020. [Online]. Available: https://pm.gov.au/media/nations-largest-ever-investment-cyber-security [Accessed: Feb. 10, 2021]

[39] A. Rege, "Critical Infrastructure Ransomware Incident Dataset". Version 10.6. Temple University, 2020. [Online]. Available: https://sites.temple.edu/care/downloads/