2020 - 2021

Compilation of Data Breaches & Cyber Attacks

Ajay Unni
Founder and CEO
StickmanCyber
sales@stickman.com.au
1800 785 626

stickman
CYBER SECURITY BY DESIGN

Disclaimer

The information contained in this report is sourced from publically available data and news articles in our effort to have a single repository of information on data breaches and cyber attacks. StickmanCyber has not verified the authenticity of the information as these breaches have not be investigated by StickmanCyber and/or any of its partners to the best of our knowledge. All logos and trademarks If any, are the property of their respective companies and entities and StickmanCyber does not own any rights to the logos or trademarks that do not belong to us. The views expressed in the report are general in nature and should not be interpreted as advice for your specific situation. You are encouraged to seek professional advice and guidance with regard to your cybersecurity issues and challenges.

Table of Contents

Cyber Attacks 2020 - 2021

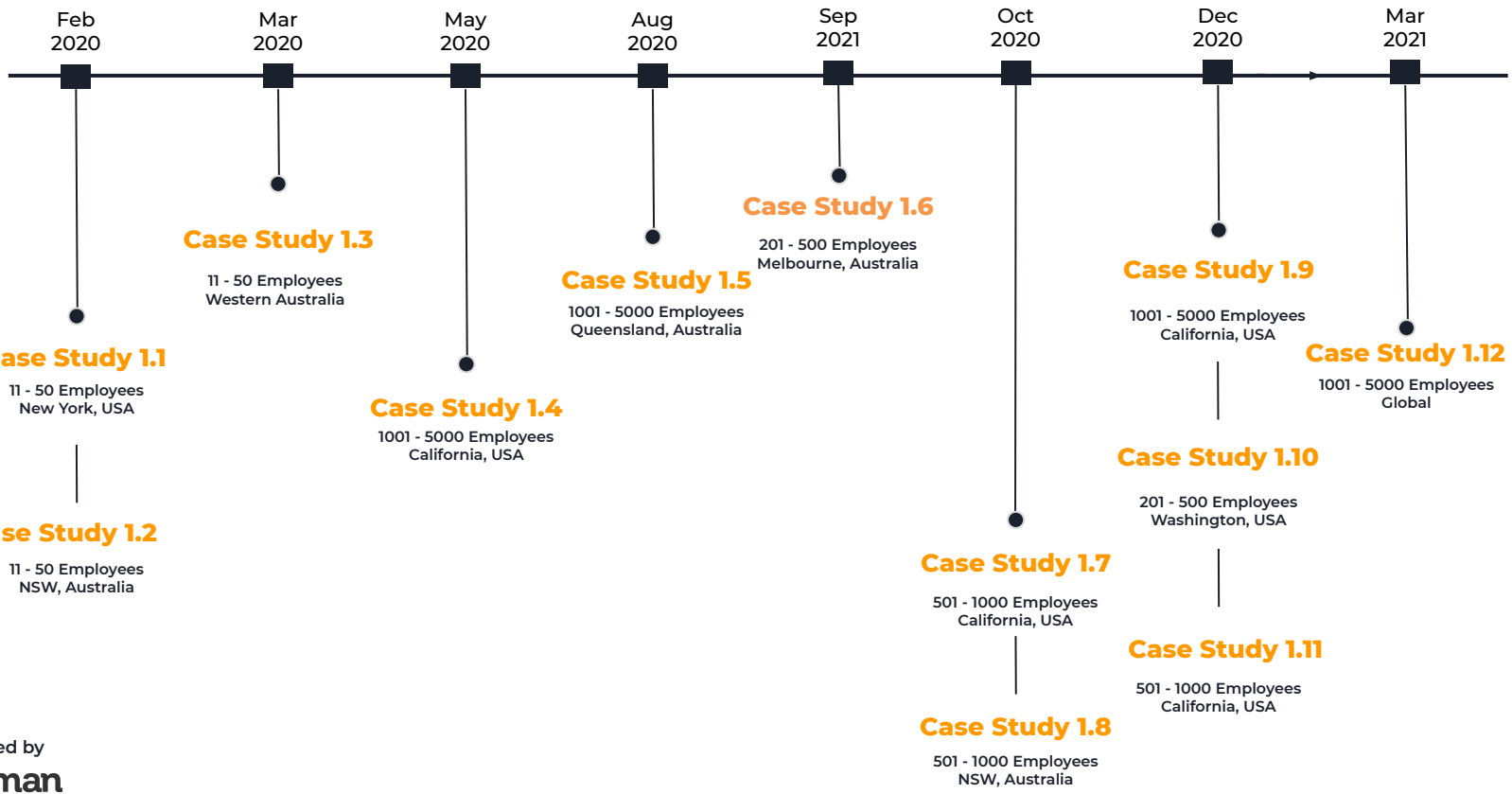
1. Technology

Australia | India
Suite 202 - 60 Pitt Street,
NSW 2000, Sydney

info@stickman.com.au | www.stickman.com.au

Timeline of Cyber Attacks

Technology



Compiled by

stickman

CYBER SECURITY BY DESIGN

Case Study 1.1 - Company A

Software Development

11 - 50 Employees

Feb, 2020

New York USA

How could this attack have been prevented?

What happened

The data stolen included Company A's entire list of customers, the number of searches those customers have made and how many accounts each customer had set up.

The Impact

The breached data primarily affected law enforcement agencies, whose names were exposed publicly. Hackers also released information about the number of user accounts each client had opened and the searches they conducted.

Recovery

Company A claimed that their servers were never accessed and that they were quick to patch up the flaw and would continue to work towards strengthening their security.

Case Study 1.2 - Company B

Information Technology

11 - 50 Employees

Feb, 2020

NSW Australia

How could this attack have been prevented?

What happened

The ransomware attack encrypted production databases, which rendered Company B's systems inoperative

The Impact

The cyber attack stopped preparations for the following days' wool auctions, preventing exporters putting orders together and brokers doing valuations, and the preparation of sale catalogues.

Exporters also could not move wool to dumps for shipment and missed contracted departure dates because of the software issues

Recovery

Company B shifted their systems to new infrastructure rather than reinstating their backup on existing infrastructure. The ransomware infrastructure was persevered to help with the investigation

Case Study 1.3 - Company C

Information Technology

11 - 50 Employees

Mar, 2020

Western Australia

How could this attack have been prevented?

What happened

In the month of March 2020 Melbourne-based government-accredited IT services provider - Company C - was hit by a REvil Windows Ransomware.

The Impact

Sodinokibi, also known as Sodin and REvil, is part of a new wave of highly sophisticated ransomware designed to cause sizeable damage to IT infrastructure, forcing victims to settle the ransom quickly.

Recovery

There is no confirmation as to whether the ransom was paid or clarity regarding the steps Company C took to recover from the attack.

Case Study 1.4 - Company D

Cloud Software

1001 - 5000 Employees

May, 2020

California USA

How could this attack have been prevented?

What happened

Company D, cloud software provider, has been sued in 23 proposed consumer class action cases in the U.S. and Canada related to the ransomware attack and data breach that the company suffered in May 2020.

The Impact

166 UK Organizations had been affected by the breach, including dozens of universities as well as health-related charities, schools and trusts set up to care for historic buildings. International clients who were affected also included hospitals, human rights organisations, non-profit radio stations and food banks.

Recovery

Company D confirmed they had paid the cyber criminal's demand with confirmation that the copy they removed had been destroyed.

Case Study 1.5 - Company E

Information Technology

1001 - 5000 Employees

Aug, 2020

Queensland Australia

How could this attack have been prevented?

What happened

IT services firm, Company E, disclosed a “cyber incident” that appeared to target a third-party networking service the company used, resulting in 28 of its customers being impacted.

The Impact

Apart from the 28 customers impacted, no material impact was discovered on Company E’s operations

Recovery

The company’s Information Security Incident Response Team was used to remediate and contain the incident. Company E worked with a third party forensic investigator to develop a full analysis of the situation.

Case Study 1.6 - Company F

Software Development

201 -500 Employees

Sep, 2020

Melbourne Australia

How could this attack have been prevented?

What happened

Hackers gained access to a 14GB database containing 77,159,696 records with users' email addresses, full names, bcrypt hashed passwords, titles, company names, IP addresses, and other system-related information

The Impact

Company F has a client base of over 10,000 businesses, so this single breach impacted the businesses using the software. Some of the impacted businesses included Microsoft Google and Apple.

Recovery

Company F's environment was fully secured immediately after the incident was identified. Company F also communicated with customers and implemented a password reset as a precautionary measure

Case Study 1.7 - Company G

Software Development

501 - 1000 Employees

Oct, 2020

California USA

How could this attack have been prevented?

What happened

The DevOps solutions provider discovered a long-lasting data breach affecting the continuous integration and deployment (CI/CD) system. The data breach was discovered by open source code repository Github.

The Impact

CodeShip Basic account holders may have had all information stored in their pipelines exposed, including scripts, environment variables, access tokens and similar data.

Recovery

Company G revoked all Github related tokens and secure shell (SSH) keys upon learning of the suspicious activity, users were also instructed to reauthenticate CodeShip with the code repository provider immediately to avoid service outage.

Case Study 1.8 - Company H

Media Intelligence

501 - 1000 Employees

Oct, 2020

NSW Australia

How could this attack have been prevented?

What happened

Media monitoring provider Company H suffered a “cyber security incident” that affected its flagship intelligence and insights service.

The Impact

The attack shut down it’s SaaS platform, Company H’s net profit before tax from the cyber security incident is expected to be a significant decline in the range of $7m to $8.5m in FY 2021

Recovery

The incident was contained and systems secured with the assistance of external cyber security specialists.

Case Study 1.9 - Company I

Cybersecurity

1001 - 5000 Employees

Dec, 2020

California USA

How could this attack have been prevented?

What happened

Cybersecurity firm Company I, announced that hackers, allegedly Russia's Cozy Bear group, broke into its network and stole tools the company's experts developed to simulate real attackers and test the security of its customers.

The Impact

Public leaks of cyber attack tools in the past, like the 2017 dump of NSA tools or the 2015 leak of tools from surveillance software company Hacking Team, resulted in adoption of those offensive capabilities by many attacker groups.

Recovery

Company I is monitoring the situation and doing everything it can to prevent a scenario where attackers utilise the tools they stole.

Case Study 1.10 - Company J

Smart Home Cameras

51 - 200 Employees

Dec, 2020

Washington USA

How could this attack have been prevented?

What happened

Company J, a company that makes budget home-security cameras, acknowledged a security breach in its system that exposed the information of 2.4 million customers.

The Impact

Camera information, Wi-Fi network details and email addresses of customers were exposed when an employee created a flexible database to quickly pull user analytics. During this the employee removed the security protocols on the new database, exposing customers' personal information.

Recovery

At the time of the breach Company J's executives said that the employee who made the mistake is still employed at the company. Company J released a statement to customers detailing the first breach and the actions the company is taking to further protect their information.

Case Study 1.11 - Company K

Information Technology

501 - 1000 Employees

Dec, 2020

California USA

How could this attack have been prevented?

What happened

Hackers gained administrative-level permissions to Company K's databases hosted on Amazon Web Services (AWS).The attacker had root privilege over all Company K's AWS accounts. The hackers also proved that they had exfiltrated source code from Company K's systems

The Impact

The level of access gained by the hackers allows authentication to cloud-based devices, such as Company K's line of wired/wireless products dispersed across the world.

Recovery

After this attack, the company started to change all employee credentials to make sure that the hacker was locked out of its infrastructure. Next came the alert to customers.

Case Study 1.12 - Company L

Travel & IT

1001 - 5000 Employees

Global

Mar, 2021

How could this attack have been prevented?

What happened

Hackers were able to gain access to Company L's servers which contains passenger data from multiple airlines around the world.

The Impact

Close to dozen airlines had passenger data accessed after the hacker breached Company L's Passenger Service System (PSS)

Over 2.1 million passengers have been impacted with the majority a part of the largest traveler loyalty program in Europe.

Recovery

Company L acted swiftly and initiated targeted containment measures. The matter remains under continued investigation by SITA's Security Incident Response Team with the support of leading external experts in cyber-security."

Cyber Attacks 2020 - 2021

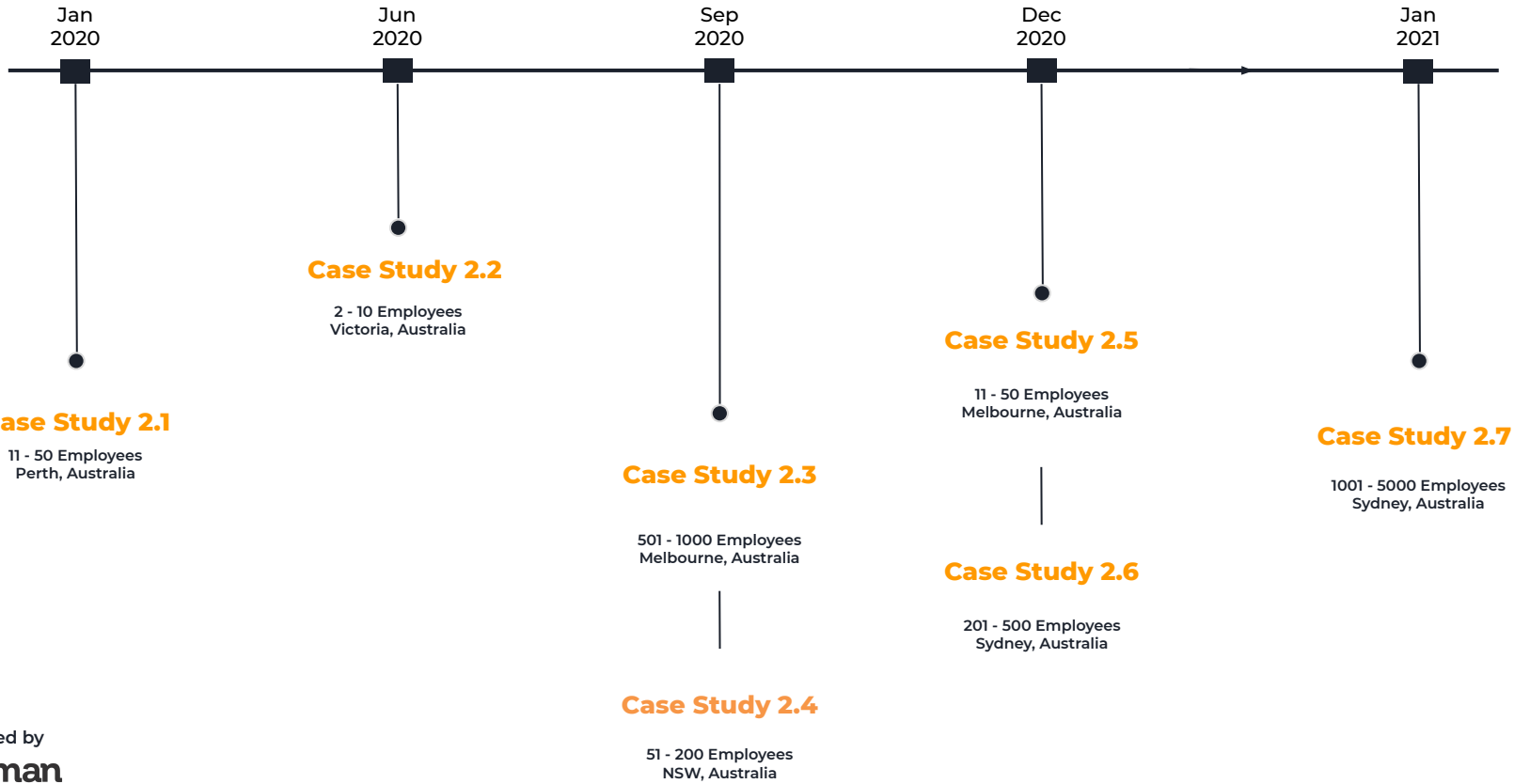
2. Financial/Professional Services

Australia | India
Suite 202 - 60 Pitt Street,
NSW 2000, Sydney

info@stickman.com.au | www.stickman.com.au

Timeline of Cyber Attacks

Financial & Professional Services



Compiled by

stickman

CYBER SECURITY BY DESIGN

Case Study 2.1 - Company A

11 - 50 Employees

Market Insights

Perth Australia

Jan, 2020

How could this attack have been prevented?

What happened

In January 2020, an employee of Company A fell prey to a phishing email scam which infiltrated the company's IT system, this compromised the details of more than 1000 visitors to an Australian Mint.

The Impact

The stolen information included contact details of 1480 people who filled out feedback surveys at the mint's depository and included visitor names, email addresses, home addresses and telephone numbers.

Recovery

Apart from notifying the visitors whose information had been exposed, Company A utilised an independent forensic investigation to pinpoint the source of the phishing link. Results from this investigation have not been divulged to the public.

Case Study 2.2 - Company B

Accounting

11 - 50 Employees

Jun, 2020

Victoria Australia

How could this attack have been prevented?

What happened

Accounting firm Company B was hit by Mespinoza Pysa ransomware in the month of June 2020, data was listed on the dark web but has since been removed.

The Impact

Mespinoza/Pysa is one among a growing number of Windows ransomware that first exfilitrates victims' files to a server specified by the attackers.

Recovery

There is no confirmation as to whether the ransom was paid or clarity regarding the steps Company B took to recover from the attack.

Case Study 2.3 - Company C

HR Consulting

501 - 1000 Employees

Sep, 2020

Melbourne Australia

How could this attack have been prevented?

What happened

Australian workforce design and delivery firm Company C was the victim of a cyber attack in September 2020, with one of its Melbourne offices coming under attack by the Windows NetWalker ransomware.

The Impact

The company's financial data, personal information and passport details posted on the Darkweb

Recovery

Post the incident Company C worked with external data security providers and notified those who may have been impacted as well as the Office of the Australian Information Commissioner.

Case Study 2.4 - Company D

51 - 200 Employees

Building Management

NSW Australia

Sep, 2020

How could this attack have been prevented?

What happened

In the month of July 2020, the Australian strata management company, Company D was hit by a gang using the Maze ransomware that can wreak havoc on Windows systems.

The Impact

Systems were seized by hackers and information was posted on the dark web

Recovery

There is no confirmation as to whether the ransom was paid or clarity regarding the steps Company D took to recover from the attack.

Case Study 2.5 - Company E

Cryptocurrency Exchange

11 - 50 Employees

Dec, 2020

Melbourne Australia

How could this attack have been prevented?

What happened

Company E, marketed as one of Australia's largest cryptocurrency exchange, exposed the names and email addresses of all customers - albeit in batches of 1000 - in December after a mistake in a blast email send went undetected.

The Impact

Other than massive reputational damage to Company E, the exposure amounted to a list of usernames that could open those with weak account security settings to potential compromise

Recovery

Company E self-reported the incident to the Office of Australian Information Commissioner (OAIC) and agreed to "fully comply with the data breach reporting requirements" in Australia

Case Study 2.6 - Company F

Legal Services

201 -500 Employees

Dec, 2020

Sydney Australia

How could this attack have been prevented?

What happened

In December, 2020, legal services firm Company F was hit by a ransomware attack, with hackers claiming to have stolen data and threatening to publish it if the company fails to pay up within seven days.

The Impact

Even though the firm released a statement insisting that no evidence of data exfiltration nor anything that indicates Company Fs' customers' networks had been compromised. Possible proof of the ransomed data was published online by the attackers.

Recovery

On learning of the attack the legal services firm ensured that counter measures were immediately implemented to prevent networked systems from being compromised, they then continued to work with cyber security experts to remediate the incident.

Case Study 2.7 - Company G

Regulatory Body

1001 - 5000 Employees

Jan, 2021

NSW Australia

How could this attack have been prevented?

What happened

Company G was hit by a data breach which saw attackers gain access files relating to credit license applications.

The incident was related to a vulnerability in vendor Accellion's legacy File Transfer Appliance (FTA) software, which was vulnerable to the common SQL injection attack vector where hackers gain access to hidden parts of a database or file system.

The Impact

Although Company G did not divulge any details they admitted that there was a risk that some limited information may have been viewed by the threat actor

Recovery

According to Accellion, the FTA vulnerability was remedied "within 72 hours" of its discovery with patches rolled out to users

Cyber Attacks 2020 - 2021

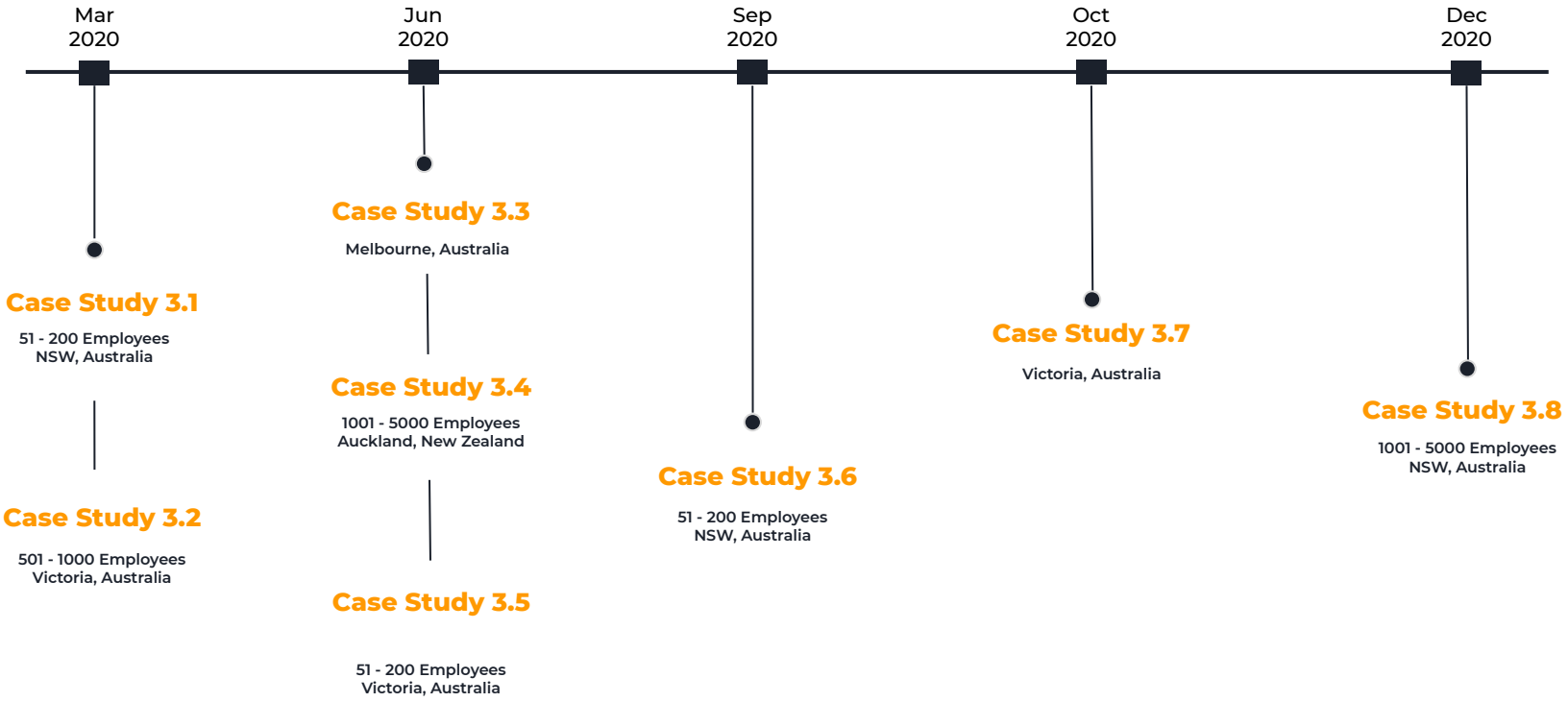
3. Manufacturing & Distribution

Australia | India
Suite 202 - 60 Pitt Street,
NSW 2000, Sydney

info@stickman.com.au | www.stickman.com.au

Timeline of Cyber Attacks

Manufacturing & Distribution



Compiled by

stickman

CYBER SECURITY BY DESIGN

Case Study 3.1 - Company A

Logistics & Freight Forwarding

51 - 200 Employees

Mar, 2020

NSW Australia

How could this attack have been prevented?

What happened

On March 15th 2020, Australia and New Zealand logistics provider Company A was attacked by a Maze ransomware.

The Impact

The company's cargo tracking system was shutdown and the company confirmed customer commercial data may have been accessed, which would have lead to significant reputational damage.

Recovery

Company A engaged a leading cyber forensics firm to conduct an urgent investigation and commenced a comprehensive internal review of its systems and processes following the attack.

Case Study 3.2 - Company B

Automotive Auctions

501 - 1000 Employees

Mar, 2020

Victoria Australia

How could this attack have been prevented?

What happened

Company B one of Australia's biggest car auction houses were the target of cyber criminals in the month of March. The criminals issued them with a $30 million ransom demand after using malware to lock them out of their computer system.

The Impact

Clients' personal data had not been compromised and the company indicated it would not pay the ransom, therefore had to sacrifice their website.

Recovery

After informing customers the company called on IT experts to restore operations and create a new website.

Case Study 3.3 - Company C

Formulation & Packing

Jun, 2020

?

Employees Unknown

Melbourne Australia

How could this attack have been prevented?

What happened

In the month of June 2020, cyber criminals using the REvil ransomware attacked Company C a Melbourne-based contract formulation and packing company.

The Impact

Attacker posted a screenshot on the dark web of some of the data exfiltrated and advising Company C to make contact. They claimed to have financial information, personal information of clients and other "important private documents".

Recovery

There is no confirmation as to whether the ransom was paid or clarity regarding the steps Company C took to recover from the attack.

Case Study 3.4 - Company D

Appliance Manufacturer

1001 - 5000 Employees

Jun, 2020

Auckland New Zealand

How could this attack have been prevented?

What happened

In the month of June 2020, New Zealand-based whitegoods manufacturer, Company D, was hit by a ransomware attack by the group Nefilim.

The Impact

Nefilim dropped an initial leak of Company D's corporate files on the dark web. Referred to as "Part 1" on the Nefilim 'Corporate Leaks' site, the 424MB folder contains financial data like balance sheets, reviews, and budgets dating back to 2013. Apart from the leak the company's manufacturing and distribution was impacted

Recovery

The firm worked with third party experts to restore their systems and their ability to take and fulfil orders, as well as introducing additional security measures

Case Study 3.5 - Company E

51 - 200 Employees

Industrial Automation

Victoria Australia

Jun, 2020

How could this attack have been prevented?

What happened

Company E an Industrial Automation company was hit by a Mespinoza Pysa ransomware in the month of June 2020

The Impact

Zipped data from Company E has been listed on the Mespinoza/Pysa website

Recovery

There is no confirmation as to whether the ransom was paid or clarity regarding the steps Company E took to recover from the attack.

Case Study 3.6 - Company F

Audio & Lighting

201 -500 Employees

Sep, 2020

NSW Australia

How could this attack have been prevented?

What happened

Cyber criminals in the month of September 2020 appeared to have used the Windows NetWalker ransomware to attack the website of Australian firm Company F.

The Impact

The criminals posted a screenshot of data stolen from Company F on their website. The screenshot included financial data, customer details and other miscellaneous data. This would have lead to significant reputational damage to the company.

Recovery

There is no confirmation as to whether the ransom was paid or clarity regarding the steps Company F took to recover from the attack.

Case Study 3.7 - Company G

Contract Management

Oct, 2020

Employees Unknown

Victoria Australia

How could this attack have been prevented?

What happened

A Melbourne company recruiting horticultural workers, Company G, left an Amazon Web Services Simple Storage Service (S3) instance containing thousands of sensitive personal documents open for anyone to access for over a month.

The Impact

12,709 files in the Company G bucket were leaked, including 532 passport and 422 driver's licence images, agricultural chemical user permits, hundreds of MADEC cards [an employment services provider] and tax forms, and thousands of employment contracts were also available to the public.

Recovery

The Company G CEO secured the data once notified, the breach was also reported to the authorities and the workers affected by Company G

Case Study 3.8 - Company H

Automotive Services

1001 - 5000 Employees

Dec, 2020

NSW Australia

How could this attack have been prevented?

What happened

In the month of December 2020, automotive services provider Company H was compromised by the Windows Ransomexx ransomware, with the cyber criminals who hit the company leaking some data that they stole, on the dark web.

The Impact

IT Systems were impacted that prevented Inchcape from communicating with customers, documents relating to administration, customer fulfilment and client information were also leaked onto the darkweb.

Recovery

There is no confirmation as to whether the ransom was paid or clarity regarding the steps Company H took to recover from the attack.

Cyber Attacks 2020 - 2021

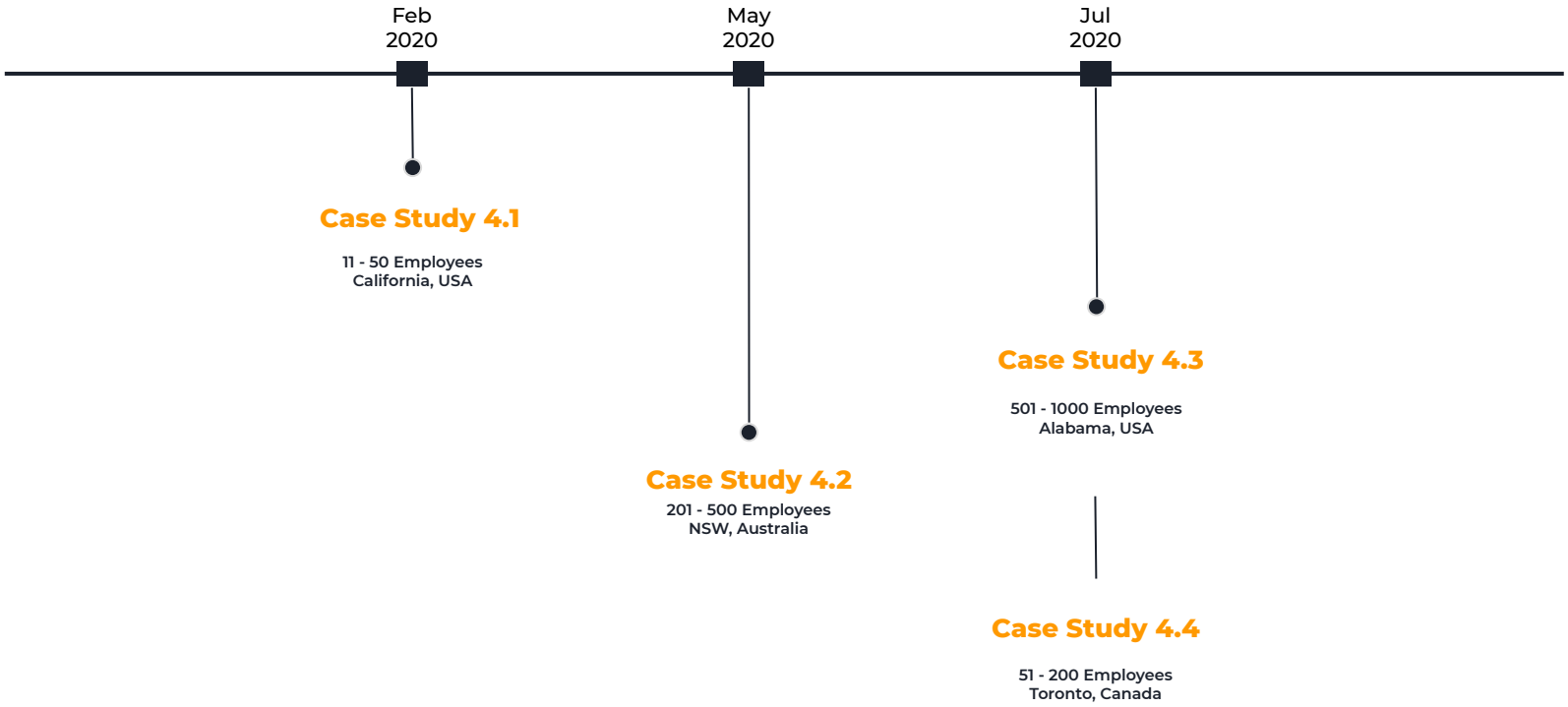
4. eCommerce & Retail

Australia | India
Suite 202 - 60 Pitt Street,
NSW 2000, Sydney

info@stickman.com.au | www.stickman.com.au

Timeline of Cyber Attacks

eCommerce & Retail



Compiled by

stickman

CYBER SECURITY BY DESIGN

Case Study 4.1 - Company A

Phone Accessories

11 - 50 Employees

Feb, 2020

USA

How could this attack have been prevented?

What happened

Company A suffered a data breach after a security researcher accessed their systems and after receiving no response to emails, publicly disclosed how they gained access to the site and the data that was exposed.

The Impact

The resumes of employees, 9GB of personal customer photos, ZenDesk ticketing system, API credentials, and personal customer information such as hashed passwords, addresses, email addresses, phone numbers, and transactions were leaked.

Recovery

In a statement posted to their Twitter account, Company A's CEO apologized for the data breach and promised to do better in the future.

Case Study 4.2 - Company B

Sports Retailer

201 -500 Employees

May, 2020

NSW Australia

How could this attack have been prevented?

What happened

Company B,, a NSW-based retailer, had its head office server and computers ransomwared in the month of May. The attackers used the REvil/Sodinokibi ransomware, which exploits a 2018 elevation of privilege vulnerability in Windows

The Impact

The retailer's online systems were unaffected but they were unsure of what files were accessed by the virus. Attacks like this can have irreversible impacts on brand image and reputation.

Recovery

After realising what had happened the company brought in external IT and security specialists to isolate and rebuild their head office system.

Case Study 4.3 - Company C

Online Service

501 - 1000 Employees

Jul, 2020

Alabama USA

How could this attack have been prevented?

What happened

Company C has confirmed that on July 27, 2020, a user on a web forum offered to share data files containing approximately 444,000 user records.

The Impact

Australian universities using the Company C online exam monitoring tool were included in a data breach affecting 444,000 users of the platform. The data contains usernames, unencrypted passwords, legal names and full residential addresses.

Recovery

Following the breach, Company C disabled the server, terminated access to the environment in the hopes to investigate what occurred.

Case Study 4.4 - Company D

201 -500 Employees

Social Media Website

Toronto Canada

Jul, 2020

How could this attack have been prevented?

What happened

Company D suffered a breach where a database containing personally identifiable information (PII) in addition to the user account credentials was stolen. The breached SQL database contained one large user table, consisting of 270,784,079 email addresses.

The Impact

This recent hack will leave users and businesses exposed to a variety of cyberattacks. User credentials are often leveraged by threat actors in attempts to gain access to other valuable platforms

Recovery

Company D upon learning off the breach started working with external security consultants to investigate. Company D also released an update that reset their users passwords

Cyber Attacks 2020 - 2021

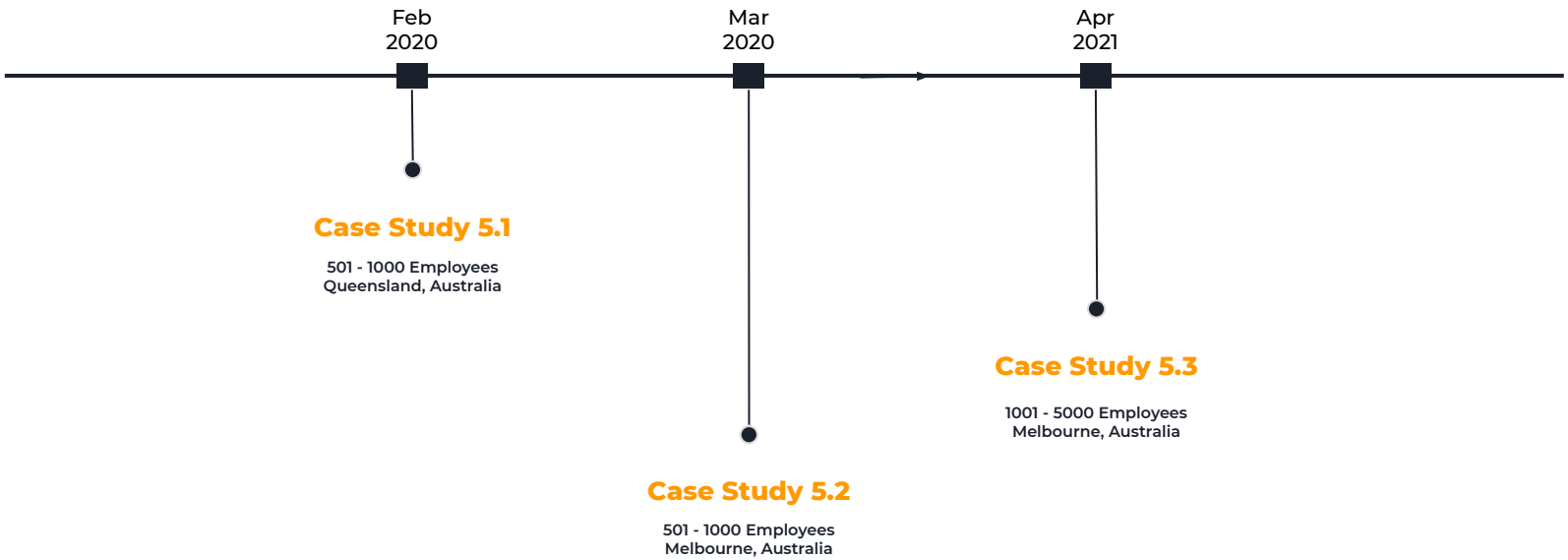
5. Education

Australia | India
Suite 202 - 60 Pitt Street,
NSW 2000, Sydney

info@stickman.com.au | www.stickman.com.au

Timeline of Cyber Attacks

Education



Compiled by

stickman

CYBER SECURITY BY DESIGN

Case Study 5.1 - Company A

Research Institute

501 - 1000 Employees

Feb, 2020

Queensland Australia

How could this attack have been prevented?

What happened

Company A was notified that its data stored on an external file-sharing system hosted by Accellion was breached on by an unknown entity in the month of February..

The Impact

About 620MB of data - including clinical patients' information like their age, sex and ethnic group and potentially staff member CVs - were accessed, CVs of 30 current and former staff may have also been accessed.

Recovery

Company A's director and chief executive apologised for the breach and says the Accellion system has been decommissioned.

Case Study 5.2 - Company B

University

501 - 1000 Employees

Mar, 2020

Melbourne Australia

How could this attack have been prevented?

What happened

In the month of March 2020, it was discovered that a data breach at Company B that had occurred back in 2018 had exposed 55k student and staff files.

The Impact

Personal, health and financial data were accessed and a small number of people may have also had passport, driver's licence, credit or debit card, superannuation account, tax file number and Medicare details accessed.

Recovery

The university conducted an independent review of its cyber security procedures in light of the breach and implemented a range of improvements including software and hardware upgrades to better protect their IT systems

Case Study 5.3 - Company C

University

501 - 1000 Employees

Apr, 2020

Melbourne Australia

How could this attack have been prevented?

What happened

In the month of April 2021, Company C suffered a data breach where the details of more than 5000 staff and students were inadvertently made available on the internet.

The Impact

Huge amounts of data collected for registration for events since the year 2013 was leaked. The data, included names, email addresses and phone numbers.

Recovery

Following the attack Company C removed the information from the internet and conducted an “audit across other similar sites”.

Cyber Attacks 2020 - 2021

6. Healthcare

Australia | India
Suite 202 - 60 Pitt Street,
NSW 2000, Sydney

info@stickman.com.au | www.stickman.com.au

Timeline of Cyber Attacks

Healthcare

Compiled by

stickman

CYBER SECURITY BY DESIGN

Case Study 6.1 - Company A

Aged Care

1001 - 5000 Employees

Aug, 2020

Sydney Australia

How could this attack have been prevented?

What happened

Company A was held to ransom over 17 gigabytes of data stolen from its computer system via ransomware.

The Impact

The cyber attack caused distress amongst the ones in their care who are already vulnerable as reported by staff members

Recovery

Department of Communities and Justice (DCJ) took immediate protective action to ensure the cyber breach did not impact Company A's systems.

Case Study 6.2 Company B

Aged Care

5000 - 10,000 Employees

Aug, 2020

Sydney Australia

How could this attack have been prevented?

What happened

Company B fell prey to Maze Ransomware which lead to cyber criminals copying some data from the company's IT system and releasing certain personal data publicly

The Impact

Documents with details of individual residents' care and accommodation agreements, employee appraisals and passwords relating to one of Company B's facilities were posted to a public website

Recovery

Company B was able to implement its backup business continuity systems and its day-to-day operations were able to continue. The company is contacting parties whose personal data has been publicly released.

Case Study 6.3 - Company C

Ambulance Service

1000 Employees

Jan, 2021

Sydney Australia

How could this attack have been prevented?

What happened

Due to an outdated paging system that had been compromised the private details of every Tasmanian who had called an ambulance since November 2020 had been published online.

The Impact

Information made public also included a patient's HIV status, gender and age, raising concerns it could lead to discrimination or stigmatisation. The attack opened the government of to litigation.

Recovery

The site has been taken down and the Australian Cyber Security Centre has been authorised to remove it should it reappear.

Case Study 6.4 - Company D

Hospital

1001 - 5000 Employees

Mar, 2021

Victoria Australia

How could this attack have been prevented?

What happened

Ransomware shutdown IT systems across all Company D's Hospitals

The Impact

Removed staff access to patient records, booking and management systems and prompted the cancellation of non-urgent surgeries

Recovery

Back-up processes were implemented during recovery efforts, including the use of paper-based documentation.

The support of the state and federal governments alongside IT experts, helped Company D to bounce back.

Case Study 6.5 - Company E

Hospital

5001 - 10,000 Employees

Auckland New Zealand

May, 2021

How could this attack have been prevented?

What happened

A ransomware attack crashed the phone lines and computers across multiple New Zealand hospitals including Company E.

The Impact

All clinical systems and IT services, except email, were disrupted by the attack. Elective surgeries postponed, staff forced to use pen and paper for all patient interactions.

Recovery

Outside cybersecurity firm and law enforcement supported the hospital's recovery team with the investigation and response.

Cyber Attacks 2020 - 2021

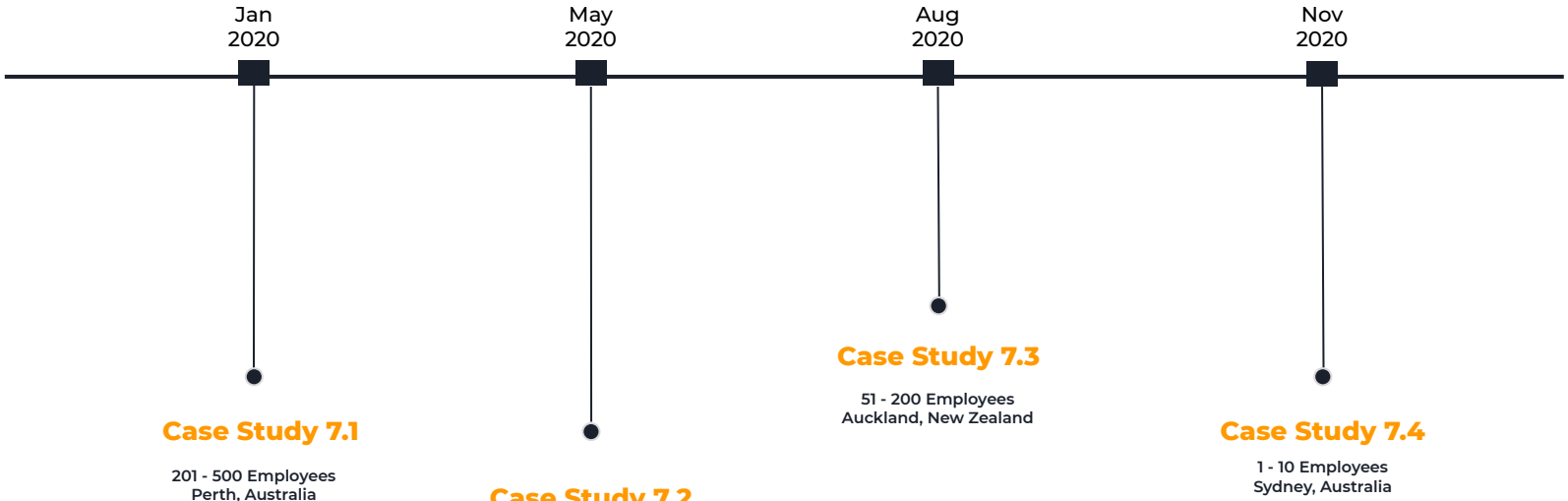
7. Banking & Finance

Australia | India
Suite 202 - 60 Pitt Street,
NSW 2000, Sydney

info@stickman.com.au | www.stickman.com.au

Timeline of Cyber Attacks

Banking & Finance



Compiled by

stickman

CYBER SECURITY BY DESIGN

Case Study 7.1 - Company A

Bank

201 -500 Employees

Jan, 2020

Western Australia

How could this attack have been prevented?

What happened

Data breach via an attack during a server upgrade, on a third party company that Company A engages to provide hosting services.

The Impact

Data was stolen from the customer relationship management system Company A used. Information like customer names and ages, residential addresses, email addresses, phone numbers, customer numbers, account numbers and account balances was stolen.

Recovery

Company A shut down the source of the vulnerability and worked closely with independent expert advisers to investigate and protect customers from any further risk

Case Study 7.2 - Company B

Financial Services

201 -500 Employees

May, 2020

Adelaide Australia

How could this attack have been prevented?

What happened

Company B was hit with a Menispoza/Pyza Ransomware Attack, which first exfiltrate files from a victim's system and then encrypt them on-site. Company B was held for ransom to get their stolen data back.

The Impact

The company's payment services, app, client portal and messaging services were down for days. The criminal hackers threatened to post stolen customer data on the dark web.

Recovery

In the final week of May, Company B was listed on the Menispoza/Pyza website but was eventually removed which may have meant that the company paid the ransom or negotiated its removal as a bargaining tactic.

Case Study 7.3 - Company C

Stock Exchange

51 - 200 Employees

Aug, 2020

Auckland New Zealand

How could this attack have been prevented?

What happened

Company C was hit with a series of volumetric distributed denial-of-service attacks in August 2020 as part of an extortion attempt.

The Impact

The DDoS attacks did not directly affect Company C's trading engines or clearing systems, Company C's main website, including its Market Announcements Platform, were affected. Company C shut down trading after it could not publish those announcements.

Recovery

The website outage was intermittent for four days while Company C worked with its ISP to deflect the attacks.

Case Study 7.4 - Company D

Investment Company

1 - 10 Employees

Nov, 2020

Sydney Australia

How could this attack have been prevented?

What happened

After opening a fake Zoom invitation, one of the hedge fund managers, had his system infected by malware that ceded control of his emails.

The Impact

$800k AUD was lost through fraudulent wire transfer attempts and hackers sent 8.7 million worth of invoices from the fund manager's email account.

Company D also lost their main client when they pulled out of an investment worth $16M

Recovery

These events unfortunately lead to Company D's closure.

How could have these attacks been prevented?

#	Most of these attacks could have been prevented with a comprehensive cybersecurity program including but not limited to:
1	24x7x365 days Monitoring, Detection and Response and Threat Hunting Capabilities to identify threats before they occur
2	3rd Party Service Provider Risk Assessments to help ensure and be aware of the riks of the service providers we use to conduct our business.
3	Dark Web Scanning to identify any lost of stolen credentials of the company
4	Multi factor Authentication to systems so users can't just log in with username and password and need an 2nd and/or 3th from of authentication to log into systems including emails. Identity and Access align with Privileged Access Management.
5	Training and Awareness to enhance staff to detect malicious emails
6	Security Vulnerability Management, Penetration Testing and Timely Patching of systems to prevent systems glitches for cyber attackers to take advantage off.

Book A Free Consultation

Learn More

THANK YOU

Book A Free Consultation

Learn More

Ajay Unni
Founder and CEO | StickmanCyber
sales@stickman.com.au
1800 725 626