nagarro

# Cyber Security in the BFSI Industry

A deep dive into the evolving state of cyber security in Australia's BFSI industry, trends seen in types of cyberattacks, AI-driven threats that have surfaced in recent years, and how Nagarro can help you build a powerful cyber security strategy.

# Executive Summary

## 35 years of cyberattack: Are we ready for the next generation?

Almost 35 years ago, a Cornell University student in the US created a harmless worm with no intention of causing any monetary theft or data loss. But it crashed thousands of computers, rendering them useless.

That was the first time a cyberattack was ever reported in the world. And the world was never the same again!

Cyberattack since then have come a long way in terms of the nature and the range of attacks, along with the wide ambit of loss they cause. Even after these 35 years, we are still not prepared to counter the cyberattack coming our way.

Cyberattacks are only becoming more sophisticated with rapid AI advancements making cyber incident detection harder.

In this white paper we will explore cyberattacks from all possible angles. We will dive into

1. The extent of damage caused by them in terms of revenue, other collateral damage.
2. The current state of cyber security in place.
3. The actions being taken to be better prepared as we move towards an all-digital world.
4. How Nagarro can help meet cyber security needs of a banking institution.

Also, for the sake of this white paper we have restricted the cyberattacks research only to the Australian subcontinent and specifically to the BFSI industry in Australia.

Cyberattacks in Australia have seen a constant upward trend in recent times. Just to touch the tip of the iceberg, the Australian Cyber Security Centre (ACSC) received over 76,000 cybercrime reports in the financial year 2022, an increase of 13 per cent on the prior year, according to its annual threat report, published in November 2022. That's one attack reported every seven minutes, on average!

# Table of Contents


**Cyber security incidents and their classification** 01

**Understanding the landscape of cyberattacks in the BFSI industry in Australia** 03

1. Types of cyberattacks in the past decade 03
2. Trends seen in various types of cyberattacks 04
3. Number of attacks in BFSI out of total attacks 06
4. The biggest attacks in BFSI in Australia so far 06
5. Kind of losses/damages owing to cyberattacks/crimes in BFSI Businesses 07
6. Regulatory bodies involved 07
7. Remedial actions taken to counter the attacks 08

**Upcoming threats from AI** 09

1. Captcha attacks 09
2. Bypassing KYC/CDD using AI 09

**Nagarro's offerings around cyber security** 10

1. Addressing threats 10
2. Assets Discovery 10
3. Security threat modelling 11
4. Proactive security threat management 12
5. Automated Attack Surface Management 13
6. Granular Remediation Solutions 14

**End Note** 15

# 1. Cyber security incidents and their classification

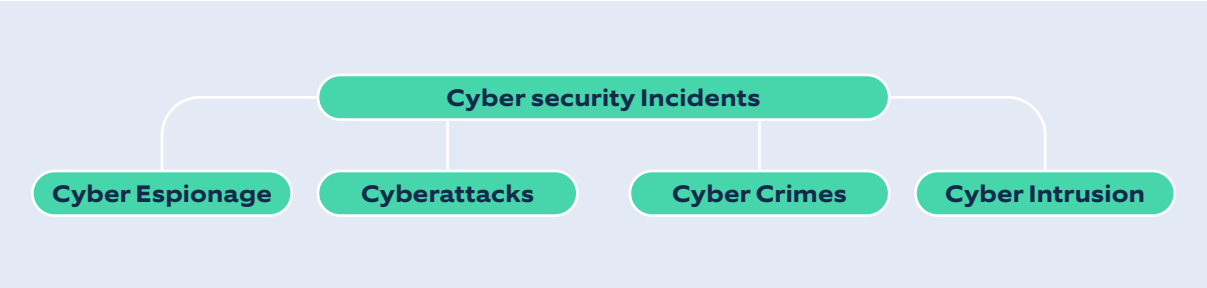



Figure 1 : *Broader classification of cyberattacks*

Before we take a deep dive into this white paper and understand what kind of cyber incidents have afflicted Australia, it's imperative that we first understand what the various kinds are of cyber incidents. (Please see appendix for reports referred)

1. **Cyber security Incidents:** A cyber security incident is a broader umbrella term used to denote any kind of unwanted malicious activity on a computer or a network of computers with an intention to cause damage to the confidentiality, integrity, or availability of a system.

2. **Cybercrime:** Cybercrime refers to any illegal activity carried out using cyber space. These incidents are primarily financial in nature and seek to extract monetary benefits either directly from the victim or indirectly in terms of information which can later be used to extract monetary benefits out of the victim.

   We can further classify cybercrime into following two categories:

   a. Pure cybercrime – Crimes directed at computers.
   b. Technology-enabled crime – Crimes where computers are an integral part of the crime.

3. **Cyberattack:** A deliberate act through cyber space to manipulate, destruct, deny, degrade, or destroy computers or networks, or the information resident in them, with the effect, in cyber space or the physical world, of seriously compromising national security, stability or prosperity.

4. **Cyber-espionage:** Offensive activity designed to covertly collect information from a user's computer network for intelligence purposes.

5. **Cyber intrusion:** Occurs when someone gains access to a computer or device without the owner's permission. Also referred to as unauthorized access or hacking.

Cyberattacks and cybercrimes can be further divided into below categories:

a. **Backdoor Trojan:** Creates a backdoor vulnerability in the victim's system, allowing the attacker to gain control remotely.

b. **Denial-of-service (DoS):** DoS and Distributed denial-of-service (DDoS) attacks flood a system's resources, overwhelming them and preventing responses to service requests, which reduces the system's ability to perform. Often, this attack is a setup for another attack.

c. **Domain Name Server tunnelling:** Cybercriminals use DNS tunnelling, a transactional protocol, to exchange application data, like extract data silently or establish a communication channel with an unknown server, such as a command and control (C&C) exchange.

d. **Malware:** Most malware variants destroy data by deleting or wiping files critical to the operating system's ability to run.

e. **Phishing:** These scams attempt to steal users' credentials or sensitive data like credit card numbers. In this case, scammers send users emails or text messages designed to look as though they're coming from a legitimate source, using fake hyperlinks.

f. **Ransomware:** It is a sophisticated malware that takes advantage of system weaknesses, using strong encryption to hold data or system functionality hostage. Cybercriminals use ransomware to demand payment in exchange for releasing the system. A recent development with ransomware is the add-on of extortion tactics.

g. **SQL injection:** Structured Query Language (SQL) injection attacks embedded code in applications, yielding backend database query results and performing commands that user didn't request.

h. **Zero-day exploit:** This attack takes advantage of unknown weaknesses. These vulnerabilities can exist for days, months or years.

However, there are issues and incidents that are unique to Australia, starting from the recent years. (Please see appendix for reports referred)

# 2. Understanding the landscape of cyber-attacks in the BFSI industry in Australia

## 2.1 Types of cyberattacks in the past decade

**Jul'21-Jun'22**

- **Ransomware:** One of the biggest cybercrime threats.
- **Business email compromise:** Similar to spear phishing, criminals target organizations and employees by trying to trick them into revealing important business information.

**Jul'20-Jun'21**

- **Ransomware:** continues to be one of the biggest cybercrime threats.
- **Business email compromise:** Spear phishing where criminals target organizations and target employees to trick them into revealing important business information.

**Jul'19-Jun'20**

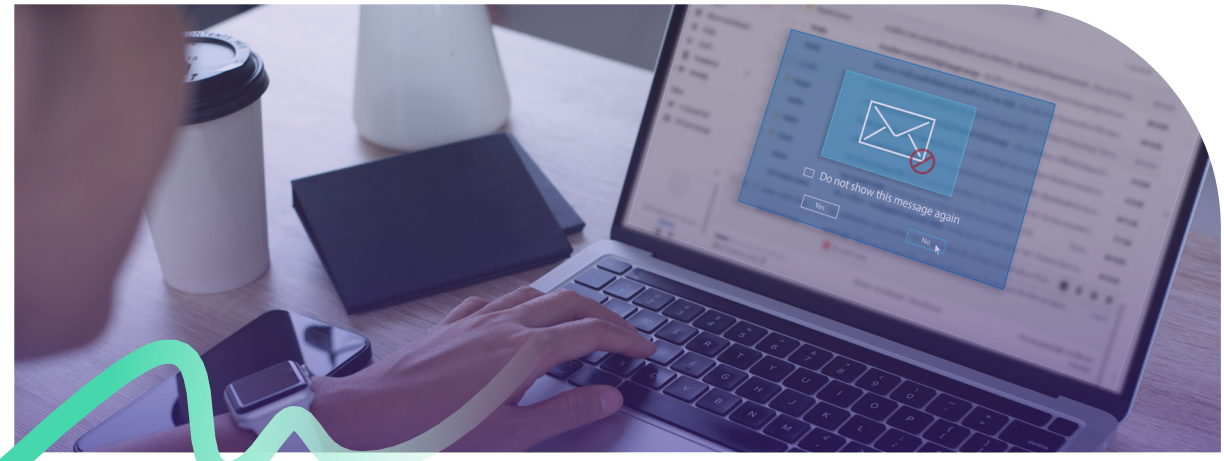
- **Ransomware:** In the mentioned period ransomware continued to be one of the biggest cybercrime threats.
- **Phishing and spear phishing campaigns:** Along with ransomware spear phishing campaigns also continued to plague the banking industry.
- **Business email compromise:** This kind of crime also saw an increase in the said period with a consulting firm being tricked into paying AUD$240,000 to a fraudster in Malaysia.

**2017**

- **Ransomware:** In the mentioned period ransomware continued to be one of the biggest cybercrime threats.
- **Credential harvesting malware:** Stealing credentials, such as login details, from the targeted network's systems in financial sector.
- **Social engineering:** Cybercriminals use these techniques to manipulate human trust and elicit information in support of network exploitation efforts.
- **Personally identifiable information:** Acquiring PII to commit financial crimes and identity theft and steal identity data like name, birth date and address.
- **Distributed Denial of Service threats:** DoS and Distributed denial-of-service (DDoS) attacks flood a system's resources, overwhelming them and preventing responses to service requests, which reduces the system's ability to perform. Often, this attack is a setup for another attack.
- **Business email compromise:** Spear phishing where criminals target organizations and target employees to trick them into revealing important business information.

**2016**

- **Spear phishing:** Emails containing a malicious link or file attachment.
- **Ransomware:** In the mentioned period ransomware continued to be one of the biggest cybercrime threats.
- **Malicious advertising:** Malware ads where hackers use a website a user knows and trusts to inject and execute a dangerous code that can put a user's cyber security at risk.
- **DDoS extortion:** DoS and Distributed denial-of-service (DDoS) attacks flood a system's resources, overwhelming them and preventing responses to service requests, which reduces the system's ability to perform. Often, this attack is a setup for another attack.




## 2.2 Trends seen in various types of cyberattacks

Let's look at various reports published by Australian Cyber Security Centre and determine the trends cyberattacks we have seen in the recent years in terms of types of cyberattacks.
Let's try and identify specific patterns and trends in any specific type of attack seeing prominence over the course of years. (Please see appendix for reports referred)

- **Spear phishing:** Spear phishing will continue to be popular with adversaries, and the use of watering-hole techniques will increase has seen a constant upward trend and is being predicted to continue.
- **Ransomware:** Ransomware attacks have been predicted to be prominent.
- **Business email compromise:** This kind of attack has also seen a rise in the past 3 years.

Figure 2 shows a breakup of various kinds of cyberattacks in the past 3 years:

| | |
|---|---|
| Other | 0.37 % |
| Ransomware | 0.59 % |
| Stalking | 1.75 % |
| ID Theft | 1.79 % |
| Image Shared | 1.94 % |
| Malware | 2.22 % |
| Bullying | 2.58 % |
| Harassment | 2.60 % |
| Threat | 2.64 % |
| Romance | 3.01 % |
| Bulk Extortion | 3.93 % |
| Selling | 4.36 % |
| BEC | 6.12 % |
| Investment | 12.20 % |
| Online Banking | 12.60 % |
| Shopping | 14.40 % |
| Fraud | 26.90 % |

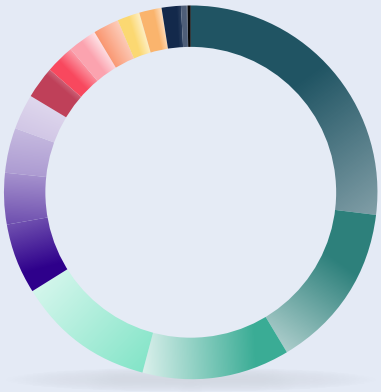


Figure 2.1 : *Jul'21 - Jun'22*

| | |
|---|---|
| Donation | 1 % |
| Image Shared | 2 % |
| Stalking | 2 % |
| Malware | 2 % |
| Threat | 2 % |
| Harassment | 3 % |
| Bullying | 3 % |
| Romance Scams | 4 % |
| Bulk Extortion | 4 % |
| Selling | 5 % |
| Investment | 6 % |
| BEC | 7 % |
| Identity Theft | 7 % |
| Online Banking | 12 % |
| Shopping | 17 % |
| Fraud | 23 % |

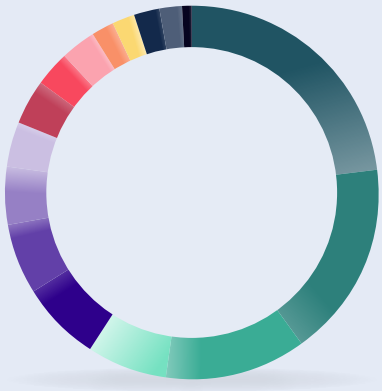


Figure 2.2 : *Jul'20 - Jun'21*

| | |
|---|---|
| Devices | 2.25 % |
| Online Image Abuse | 3.52 % |
| Cyber Abuse | 22.15 % |
| Identity Crime | 32.40 % |
| Fraud | 39.66 % |

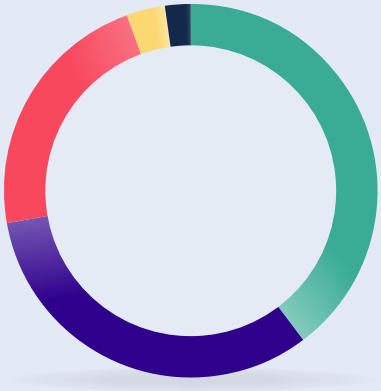


Figure 2.3 : *Jul'19 - Jun'20*

## 2.3 Number of attacks in BFSI out of total attacks

To show the breakup of attacks please see the chart below which clearly elucidates how BFSI has fared against other industries in terms of attacks on it. (Please see appendix for reports referred)

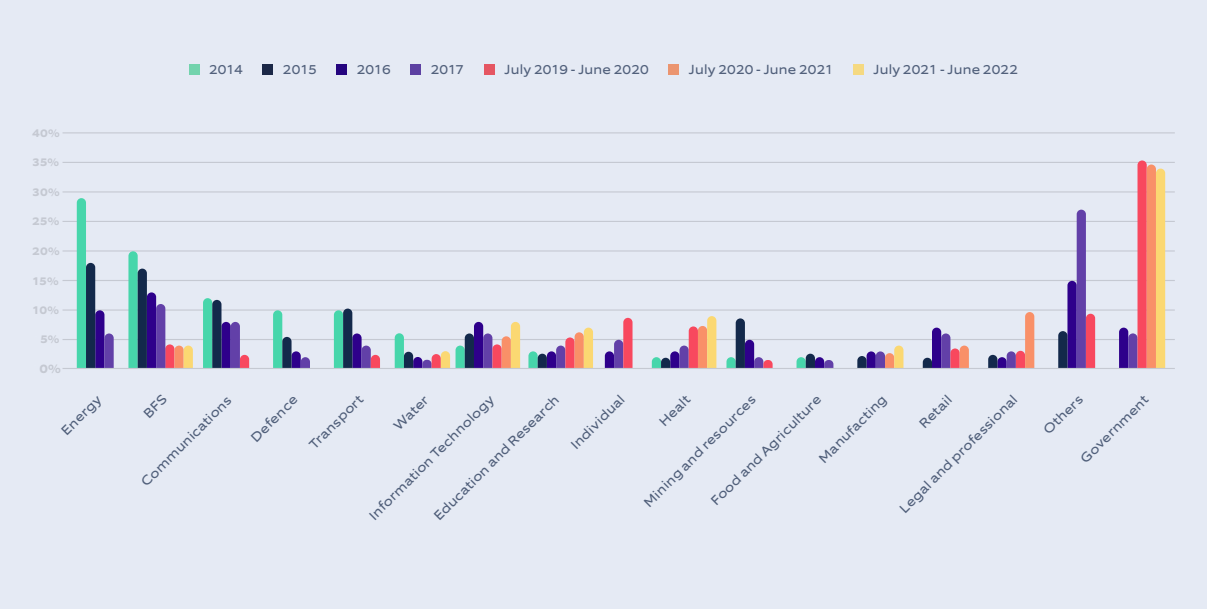



Figure 3 : *Percentage of attacks in BFSI over the years*

## 2.4 The biggest attacks in BFSI in Australia so far

Listed below are some of the biggest attacks in the BFS industry in the recent times:

1. **Medibank data breach (Oct'22):** Though still developing, at the time of writing, it is believed that up to four million current Medibank customers may have had their data stolen, as well as an unknown number of past customers.

2. **Commonwealth Bank of Australia:** The incident involves unauthorized access of a web-based software application used for project management, and the bank's Australian systems were segregated from PTBC systems, CBA said, confirming that the unit's services will operate as usual. Shares of CBA dropped about 0.9% to A$98.04, in line with the broader market (.AXJO) down nearly 1% after the attack.

3. **Other industries:** Similar to Optus and Woolworths, other domains witnessed many high profile cyberattacks in Australia impacting almost 10 million people.

## 2.5 Kind of losses/damages owing to cyberattacks/crimes in BFSI Businesses

There are two types of losses which occur because of cyberattacks/crimes:

**Direct**

- **Revenue loss** – One of the most common direct losses resulting because of cyberattacks, monetary theft. Cyberattacks targets individuals/organizations to extract money, hence resulting in revenue loss.

- **Identity theft** – A kind of crime in which the personal/financial details of an individual are stolen to commit fraud. Fraud in this case would be unauthorized purchases/transactions. Such activities can cause credit, financial and reputational loss to the individual.

**Indirect**

- Reputational damage is an indirect form of loss due to cyberattacks/crimes. Businesses sometimes suffer irrevocable damages in case they have been attacked once. It can make the customer wary of the legitimacy and the strength of cyber security of the business making them switch vendors.

- Loss of business/employment opportunities.

- Impact on emotional/psychological welfare of the victim.

## 2.6 Regulatory bodies involved

The primary body which assists the Australian critical infrastructure owners to understand the risk environment and meet their regulatory requirements is, CISC (Cyber and Infrastructure Security Centre).

But, despite strong regulations in place, sometimes there can be lapses on the organization's behalf in complying with regulations resulting in malicious actors taking advantage and attacking the systems.

One of the primary reasons is the global pandemic COVID-19 that engulfed the entire world.

In the wake of COVID-19 pandemic, there has been a rush in the financial industry to move towards the online platform to compete with the technology companies. The pandemic has dramatically increased the demand for online services where the customer can enjoy the same financial services in the palm of their hands. The tech-savvy Australians have been quick to embrace online services. While some of those services – including online banking – are built with security as a key priority, not all are as diligent.

To fulfil the surge in online services the banks might be leaving few doors unguarded which can lead malicious actors in, and cause cyberattacks.

## 2.7 Remedial actions taken to counter the attacks

Preventing cybercrime is the topmost priority for Australian government to safeguard Australians, businesses, private companies, and government. Australian government will work to sharpen their ability to handle these emerging cyberattacks in the Country. The Australian Government has implemented below measures to address these attacks happening in the country to counter the cyberattacks.

1. **Surveillance Legislation Amendment (Identify and Disrupt) Act 2021(SLAID Act):** This act focuses on to intensify the power of the Australian Criminal Intelligence Commission (ACIC) and AFP to discover, target, investigate and disrupt serious criminal activity occurring online.

2. **Office of the e-Safety Commissioner:** This will facilitate people to safeguard from online harms and to promote positive online experience.

3. **Online Safety Act 2021:** This is to give more power to e-safety commissioner to help protect Australians from serious type of online harm.

4. **Australia's Cyber Security Strategy 2020:** Investing AU$1.67 billion over 10 years to improve Australia's cyber security baseline and capabilities to investigate and disrupt cybercrime.

5. **Report Cyber:** It is an online cyber reporting platform which will allow people to securely report cybercrime.

6. **IDCARE cyber support services:** Representing Australia's interest in cyberspace by establishing the role of Australia's Ambassador for the cybercrime.

7. **Operation Orcus Taskforce:** This is coordinated by Australian federal police to bring together stakeholders from government agencies to counter rising ransomware attack in Australia.

# 3. Upcoming threats from AI

## 3.1 Captcha attacks

CAPTCHA has developed into the most popular utilized standard security measure for preventing automated computer program attacks. In recent years, many attack methods, developed by hackers or researchers, have effectively cracked all common conventional schemes.

Captcha challenges people to prove they are human by recognizing combinations of letters and numbers that machines would struggle to complete correctly. Researchers developed an algorithm that imitates how the human brain responds to these visual clues.

The neural network could identify letters and numbers from their shapes.

Now, we did not see any attacks on captcha, but in near future we can see such attacks and that can be of many types as listed below:

1. Text
2. Image
3. Audio
4. Cognitive
5. Other CAPTCHAs


## 3.2 Bypassing KYC/CDD using AI

With the advent of ChatGPT text responses using AI has become very sophisticated, but it is not just text which has seen improvement but now using AI voices and images can also be recreated up to a great extent. There are organizations which are now selling Deepfakes-as-a-Service (DFaaS) offering single video for as low as $145. The repercussions of deep fake are massive. As fraudsters are able to access more personal data and generate more believable ID documents using deep fake, the AI models become more accurate and the scam more successful.

# 4. Nagarro's offerings around cyber security

## 4.1 Addressing threats

Now that we have learnt about different types of threats that prevail in the industry, the next best steps are outlined and elaborated further to design and implement security countermeasures for a variety of threats.

- **Enterprise Assets discovery** for information capture about enterprise-wide systems, acts as inputs to the threat modelling tool, this is a prerequisite to threat modelling.
- **Security threat modelling** for depiction of threat and effectively identify countermeasures.
- **Proactive Security threat management**, automated handling of rapidly morphing attack surface.
- **Granular security remediations** for contextual security measures at each level of Enterprise IT.
- **Transaction Fraud Management**
- **Config and awareness (BEC, Phishing)**

## 4.2 Assets Discovery

Enterprise IT Asset discovery, threat agent discovery, risk assessment and vulnerability control discovery are instrumental to envision a 360-degree comprehensive security risk assessment.

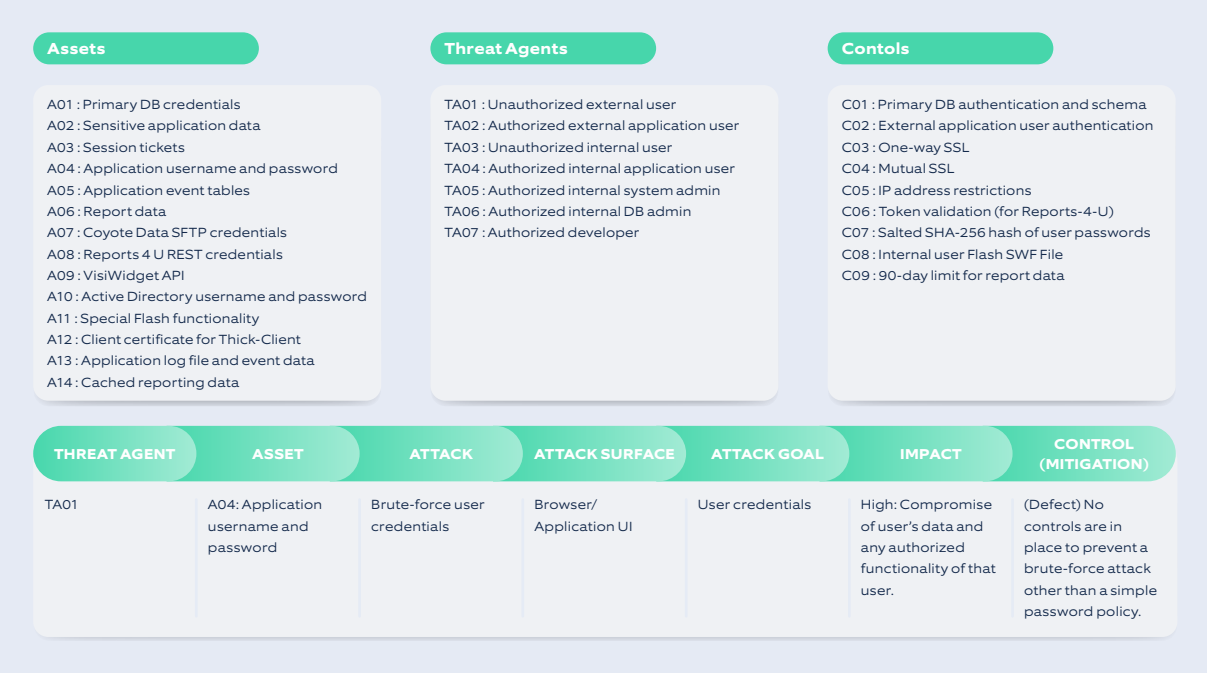



Figure 4 : *IT assets and control discovery example*

## 4.3 Security threat modelling

Ransomware, Spear Phishing, Business Email Compromise primary most prominent in Australian market. Threats are directly proportional to online presence and digital integrations.
Once the assets are discovered to design an effective security model to protect them, we first need to create security a threat model. These models help identify types and location of threats in enterprise IT. The models can be designed for IT systems, devices, network, cloud, IoT etc.

### 4.3.1 Classical modeling

Threat modelling tools must be used, that follow standard methodologies like **STRIDE** (**S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, **E**levation of privilege), to create DFD (Data Flow Diagrams) or certain modern PFD (Process Flow Diagrams) based models as visual cues based on information inputs.

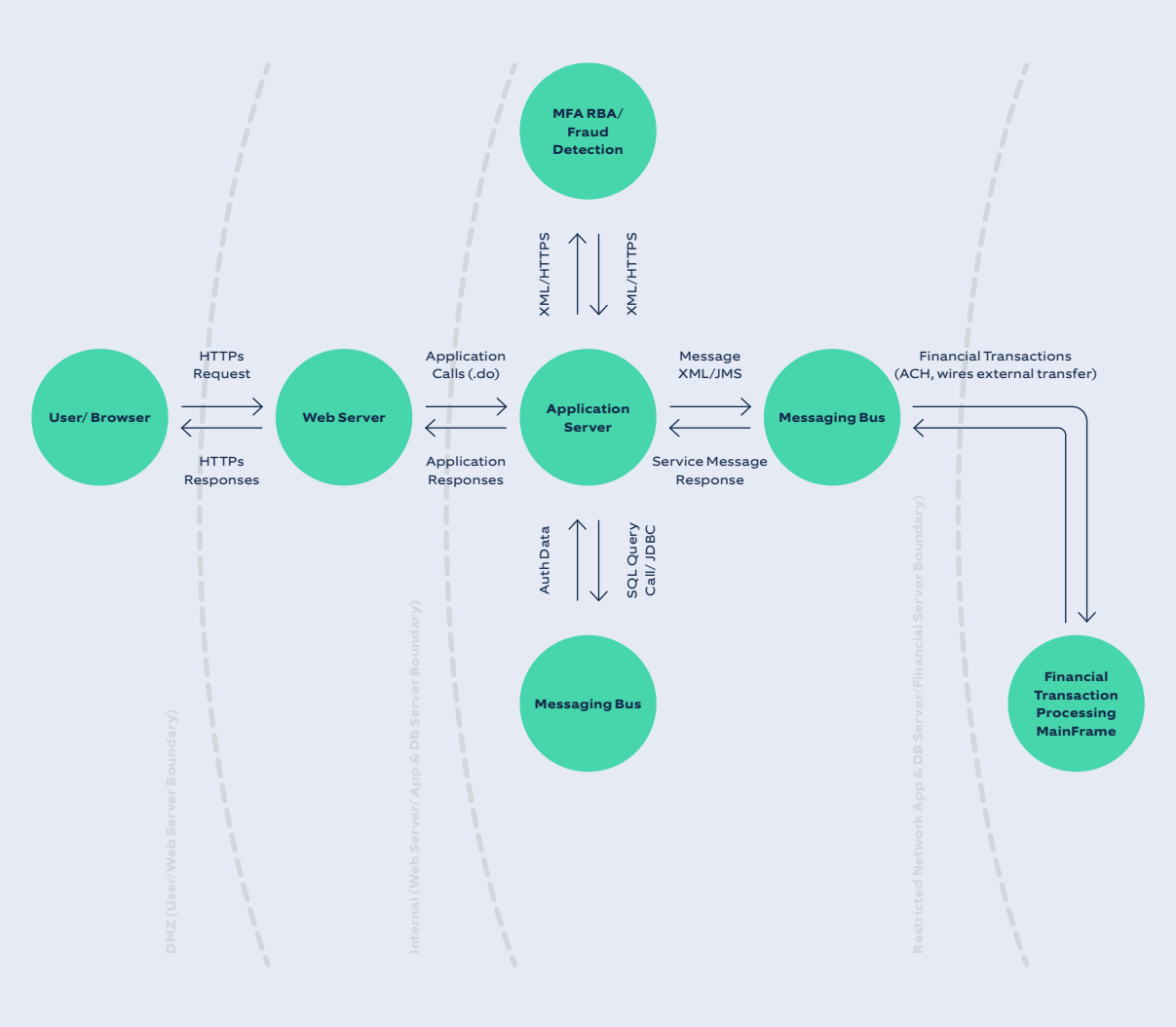



Figure 5 : *Digital Banking Threat Model Data Flow Sample Diagram*

### 4.3.2 Contemporary modeling

Process flow diagramming models that are a step beyond DFDs in depicting the use cases (like login and funds transfer), API integration, dependencies, protocols, infrastructure, code components within enterprise IT. Leading to effective and over communicative modelling suitable to security.

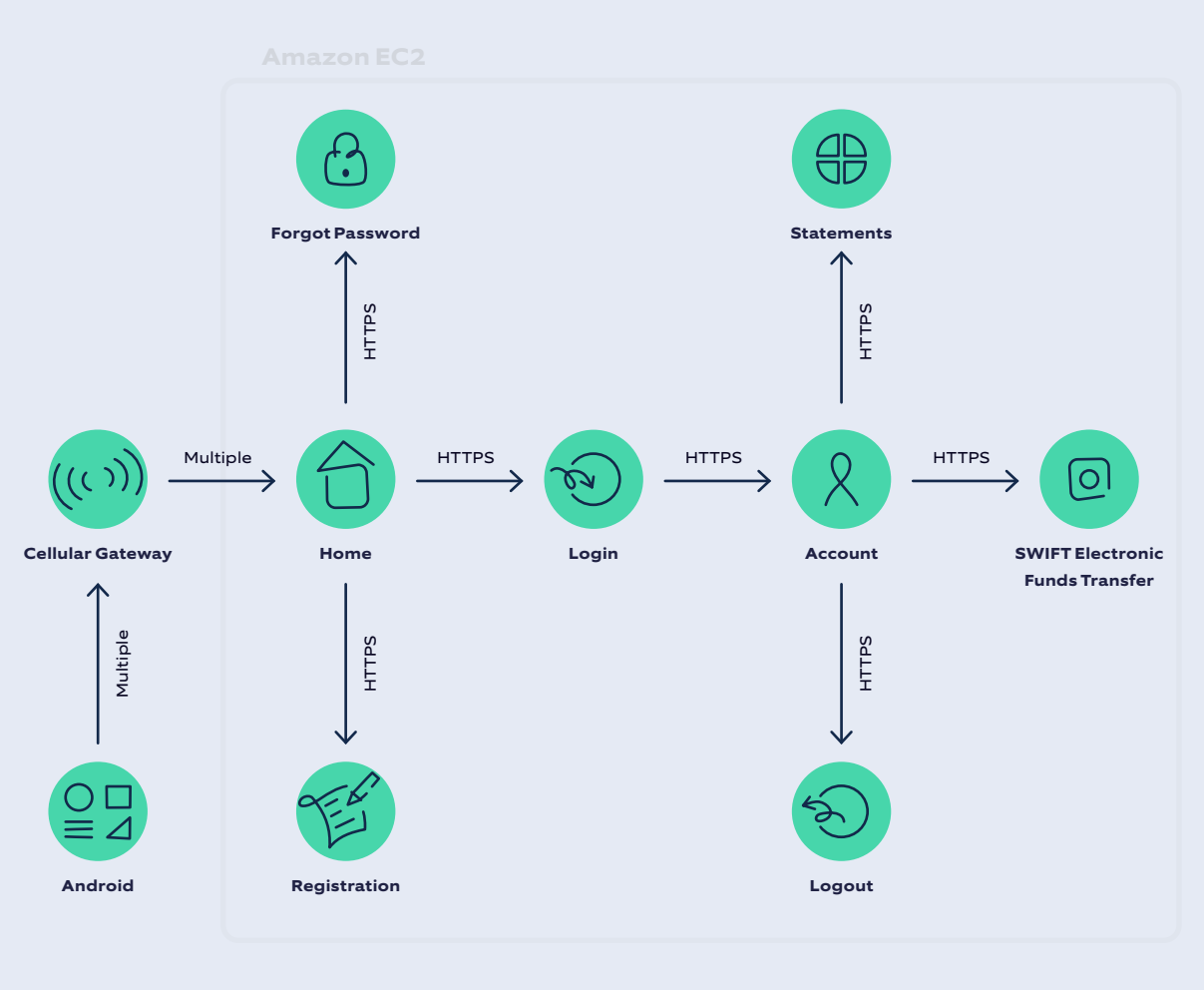



Figure 6 : *Mobile Banking Payments Threat Model Process Sample Flow Diagram*

## 4.4 Proactive security threat management

While some of the above is already practiced by organizations these are linear (defender's perspective), not proactive and evolving measures. It is not a proactive posture (hacker's perspective) for security threat intelligence for a constantly growing and changing attack surface. ASM (Attack Surface Management) solutions provide real-time visibility into vulnerabilities and attack vectors as they emerge.

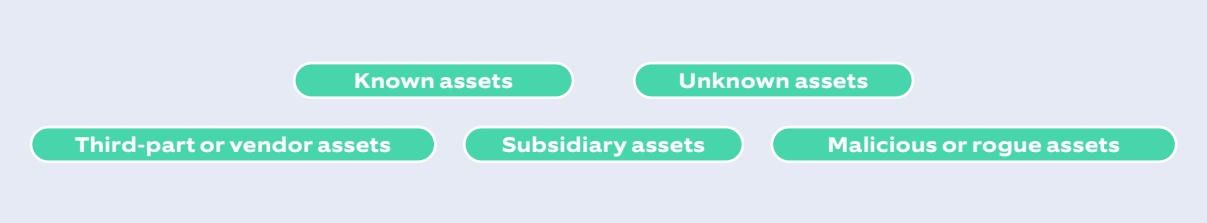
## 4.5 Automated Attack Surface Management

Traditional asset discovery, risk assessment and vulnerability management processes, which were developed when corporate networks were more stable and centralized, can't keep up with the speed at which new vulnerabilities and attack vectors arise.

Penetration testing, for example, can test for suspected vulnerabilities in known assets, but it can't help security teams identify new cyber risks and vulnerabilities that arise daily.

### 4.5.1 Automated Asset discovery

Asset discovery automatically and continuously scans for and identifies internet-facing hardware, software, and cloud assets that could act as entry points for a hacker or cybercriminal trying to attack an organization. These assets may include:




### 4.5.2 Inventoried, analyzed and prioritized assets

Classification, vulnerabilities analysis, and prioritization of assets by 'attack affinity' (likelihood of hackers targeting them).

- **Inventoried** by identity, IP address, IT and business ownership, integrations with other upstream or downstream assets.
- **Analyzed** for the exposures (e.g., misconfigurations, coding errors, missing patches), and the types of attacks possible these exposures (e.g., stealing sensitive PII or IP data, spreading ransomware or other malware).
- **Prioritization** of vulnerabilities for remediation is done by security ratings or risk score basis the:

  **1.** Information from classification and analysis.

  **2.** Data from alternative sources like threat intelligence feeds, security rating services etc.

  **3.** Results of the organization's own Red Teaming efforts, penetration testing all potential target assets by in-house or third-party.

### 4.5.3 Remediation

Vulnerabilities are remediated in order of priority. This can involve:

1. Applying software or operating system patches, stronger data encryption.
2. Bringing previously unknown assets under control, integrating subsidiary assets into the organization's cyber security strategy, policies, and workflows.
3. Implementing least-privileged access or multi-factor authentication (MFA) or Adaptive MFA.

### 4.5.4 Monitoring

New assets deployment or ex isting assets modifications can change exposure levels, inventoried assets of the network and the network itself are continuously monitored and scanned for vulnerabilities. Continuous monitoring enables detection and assessment of new vulnerabilities and attack vectors in real time, and alert security teams to any new vulnerabilities that need immediate attention.

## 4.6 Granular Remediation Solutions

| Remediation | Impact | Tech |
|---|---|---|
| Zero Trust/Never Trust architecture | Eliminates implicit trust between systems that are part of same systems boundary | • Identity and Access Management<br>• OAuth 2.0<br>• OIDC |
| Cloud and Multi-Cloud Security | Public cloud assets protection | Natively provisioned security solutions |
| Legacy security | Incompatibility with modern security | Middleware and wrapper integrations |
| Application, Network, Infra, Data, Source Code and AI/ML/Model security | Most important area for granular security | • SDLC integration for SAST and DAST, common OWASP, CWE, PCI DSS vulnerabilities<br>• API security and governance<br>• Consumer behavior-based Transaction Fraud Management System<br>• SIEM and SOAR platforms<br>• IAM, DLP, IPS/IDS, UEBA, XDR<br>• HSM appliance for cryptography<br>• IT Incident Response Playbooks and automated Runbooks to deal with security incidents. |
| Standard frameworks and bodies of COBIT, CISSP, CCSP, NIST, ISO-xxxx | Security best practices coverage | Certified professionals |

Figure 7 : *Granular Remediation Solutions*

# 5. End Note

When it comes to cyber security, the irony is while the number of threats is constantly on the rise, most financial institutions have not formalized their security threats models. In fact, security is often seen as an obstacle by IT functions of such organizations.

With the advent of AI on the cyberattack scene, it is becoming even more difficult for regular security systems to detect an incoming AI attack. We need sophisticated threat models in place which can effectively mitigate these AI attacks.

Most importantly what we need right now is for the industry to be sensitized about the ever-morphing attack surfaces of organization's digital landscape, that requires security as part of IT culture and be ready for an imminent danger looming on the horizon.

We at Nagarro would love to talk to you about your cyber security needs.

Our experts are trained in:


## Glossary

1. ASD - Australian Signals Directorate (within the Ministry of Defense)
2. CERT - Computer Emergency Response Team
3. ACSC - Australia Cyber Security Centre
4. CISC - Cyber and Infrastructure Security Centre (within the Ministry of Home Affairs)

## Appendix

1. 2015 Report
2. 2016 Report
3. 2017 Report
4. 2019-2020 Report
5. 2020-2021 Report
6. 2022 Report

# Meet the Authors

## Sandeep Shukla

Sandeep Shukla is a CTO with BFSI Practice at Nagarro.
He carries over 20 years of global experience implementing large technology programs with a focus on rapidly transforming industry trends. Sandeep has partnered with top industry players in their quest to create IT assets that helped them gain competitive edge and long-term business relevance.

## Hemant Joshi

A seasoned IT professional with 12+ years of experience in the Industry spanning across various domains, BFSI the most expansive. Hemant is a consultant by role, but a product enthusiast at heart. When not dealing with IT problems, you can find him unwinding with a book or playing his guitar.

## Shraddha Sirse

A seasoned Research Analyst with over 5 years of expertise in BFSI research, brings her contribution—a pioneering white paper on cyber attacks in Australia.

## About Nagarro

Nagarro is a global digital engineering leader with a full-service offering, including digital product engineering, digital commerce, customer experience, AI and ML-based solutions, Cloud, immersive technologies, IoT solutions, and consulting on next-generation ERP. We help our clients become innovative, digital-first companies through our entrepreneurial and agile mindset, and we deliver on our promise of thinking breakthroughs.

We have a broad and long-standing international customer base, primarily in Europe and North America. This includes many global blue-chip companies, leading independent software vendors (ISVs), other market and industry leaders, and public sector clients.

Today, we are over 19000 experts across 36 countries, forming a Nation of Nagarrians, ready to help our customers succeed.

For more information, visit www.nagarro.com