Australia's Cyber Security Strategy Call for Views

4th of October 2019

Table of Contents

Overview

In 2016 the Australian government launched a National Cyber Security Strategy covering five themes of action for a time period up to the year 2020. The five themes included:

- national cyber partnership
- stronger cyber defences
- global responsibility and influence
- growth and innovation
- a cyber smart nation

With the ever-changing threat landscape, the federal government has now begun consulting on the development of the next iteration of the Cyber Security Strategy in an effort, to quote the Hon Peter Dutton MP, “to adapt our approach to improve the security of business and the community”.

SecureTrust welcomes the opportunity to partner with the Australian government in that endeavour, through a contribution to “A call for views” as a lead up to Australia’s 2020 Cyber Security Strategy.

In this submission we intend to demonstrate that PCI (Payment Card Industry) compliance improves the overall cyber security posture of both Australian businesses and government with the processes and controls prescribed in the standard. To quote the PCI Data Security Standard it “was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data.” It’s our belief that promoting compliance to PCI standards will help tackle one of the biggest drivers for cyber-crime, obtaining cardholder data.

We will also demonstrate how other governments around the world are also taking interest in, and supporting, PCI compliance through initiatives such as to taking legal avenues to enforce compliance. In light of the premise for this document we believe our submission touches on several questions associated with “A call for views” including:

- **Question 1:** What is your view of the cyber threat environment? What threats should Government be focusing on?
- **Question 2:** Do you agree with our understanding of who is responsible for managing cyber risks in the economy?
- **Question 3:** Do you think the way these responsibilities are currently allocated is right? What changes should we consider?
- **Question 6:** What customer protections should apply to the security of cyber goods and services?
- **Question 7:** What role can Government and industry play in supporting the cyber security of consumers?
- **Question 8:** How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?

- **Question 10:** Is the regulatory environment for cyber security appropriate? Why or why not?
- **Question 11:** What specific market incentives or regulatory changes should Government consider?
- **Question 12:** What needs to be done so that cyber security is 'built in' to digital goods and services?
- **Question 13:** How could we approach instilling better trust in ICT supply chains?
- **Question 16:** How can high-volume, low-sophistication malicious activity targeting Australia be reduced?
- **Question 23:** How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?
- **Question 25:** Would you like to see cyber security features prioritised in products and services?

In August 2010 the Australian Government Law Reform Commission (ALRC) stated under "Mandating Standards" that "Local and international bodies are continuing to develop standards on privacy and security issues such as identification, authentication and encryption. There may not be adequate incentive for agencies and organisations to comply with standards, however, because of a **lack of adequate enforcement mechanisms**. For example, it was noted recently that 83% of large merchants using Visa are not in compliance with the Payment Card Industry (PCI) Data Security Standard."

The reference also stated, "In DP 72, the ALRC proposed that the Privacy Act be amended to empower the minister responsible for the Privacy Act, in consultation with the OPC, to determine which privacy and security standards for relevant technologies **should be mandated by legislative instrument**." Many participating as stakeholders "expressed concern that technical standards could quickly become outdated". However, the intent of standards like PCI DSS, ISO27002 or even CPS 234 (Prudential Standard) are not to call out the specific technology required to meet compliance but rather to ensure the intent of the standards are met. Not to mention those standards are frequently updated. PCI DSS itself has been updated 4 times since the ALRC review and it's about to undergo a fourth update in the way of PCI DSS version 4.0 in 2020.

The **Notifiable Data Breaches Statistics Report: 1 April to 30 June 2019** highlighted that 42% of the notified breaches involved financial details and 62% of the attacks were malicious or criminal. Add to that 34% being related to human error and you make the case for compliance mandates by legislative instrument.

References include:

- Australian Law Reform Commission - Mandating Standards?
- OAIC Notifiable Data Breaches Statistics Report 1 April to 30 June 2019

ABOUT US

SecureTrust (a division of Trustwave) leads the industry in innovation and processes for achieving and maintaining compliance and security. SecureTrust delivers world-class consulting, compliance and risk assessment services and solutions for the enterprise market as well as tailored merchant risk management programs and solutions for merchant program sponsors around the globe.

SecureTrust is the world leader in PCI compliance with over 20 years’ experience having completed the most assessments and managed the largest programs in the world. We have the world’s largest compliance program for acquirers, processors, payment gateways and independent sales organizations to manage their small merchant programs and help them stay secure.

But PCI compliance isn’t all we do. We have deep compliance and security expertise with General Data Protection Regulation (GDPR) Compliance, ISO27001/27002, Data Privacy, Health Insurance Portability and Accountability Act (HIPAA) and even the more recent APRA Prudential Standard CPS 234 to name a few.

In addition to consulting and management of compliance and sponsor programs, we also have technologies like Web risk monitoring, DLP Discover, an endpoint protection suite and we are a top 10 certificate authority for issuing digital certificates.

https://www.securetrust.com

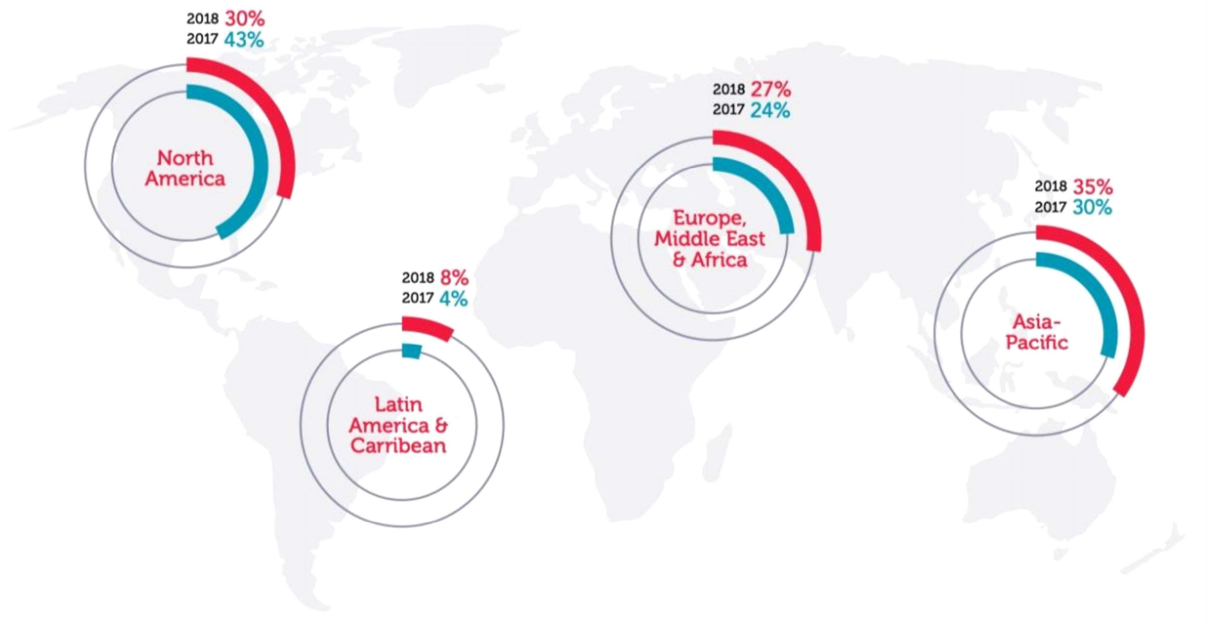
ABOUT THE AUTHOR

Brian Odian is the Director of Asia Pacific Global Compliance & Risk Services Consulting at SecureTrust, based in Sydney. He has over 32 years IT Industry experience including roles as a Security Delivery Manager and Global Security and Transformation Lead for the likes of HP and DXC Technology respectively. He has been published by the Project Management Institute (PMI) and MSSP Alert along with webinars on the General Data Protection Regulation (GDPR) and presentations on PCI Compliance for some of the “big four” banks and the Customer Owned Banking Association (COBA).

You can learn more about Brian via www.linkedin.com/in/brian-odian or contact him at [redacted]

The Cyber Security Landscape

The mission to protect businesses from security risks drives companies like ours to look beyond the statistics and figures to the people and forces behind them. We seek to understand not only what the attacks are, and where they come from, but also who is doing the attacking, why, how, and what they plan to do in the future. The graphic below offers some insight as to the importance of protecting cardholder data, which is a sought-after commodity by the underlying criminal elements behind cyber security attacks (sourced from the 2019 Trustwave Global Security Report).

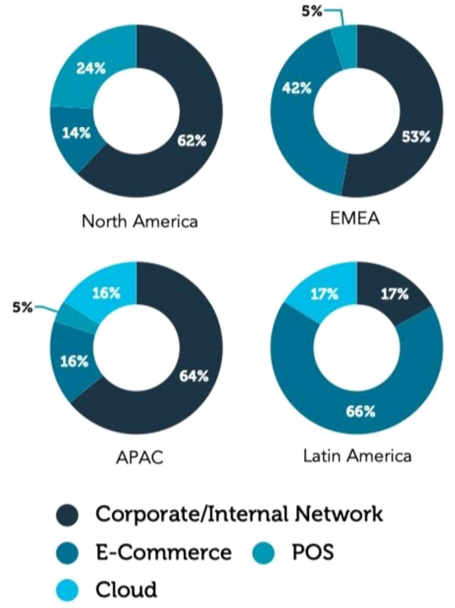


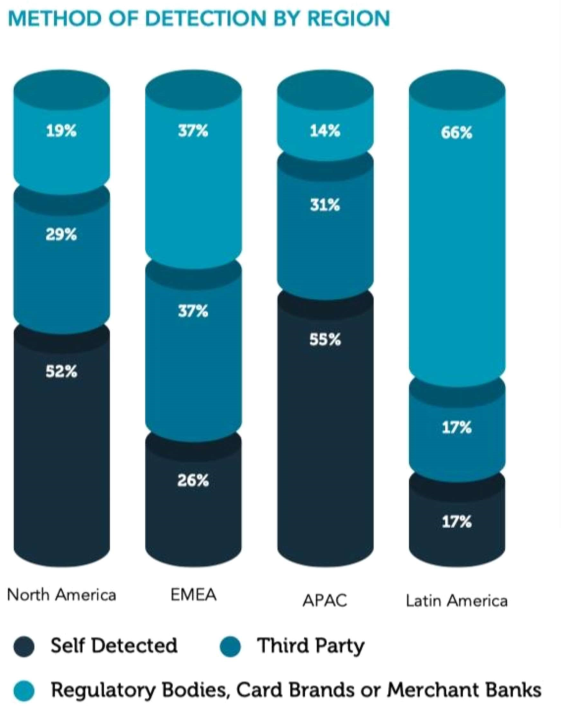
In 2018 attackers appeared to shift their focus from the Americas to Asia-Pacific (APAC), mainly Australia, Singapore and Hong Kong. In Asia-Pacific incidents we investigated involved attacks on POS (Point of Sale) vendors not on merchant endpoints and were considerably more advanced than the attacks we see in most merchant breaches.

To understand how long it takes businesses to detect a breach and how long affected data records remain exposed, investigators recorded the dates of three milestones in a compromise's duration:

- Intrusion: The date of initial intrusion is the day the attacker gained unauthorized access to the victim's systems, as determined by Trustwave investigators.
- Detection: The date of detection when the victim or another party identifies a breach transpired.
- Containment: The date of containment when the attacker can no longer access the environment and records are no longer exposed.

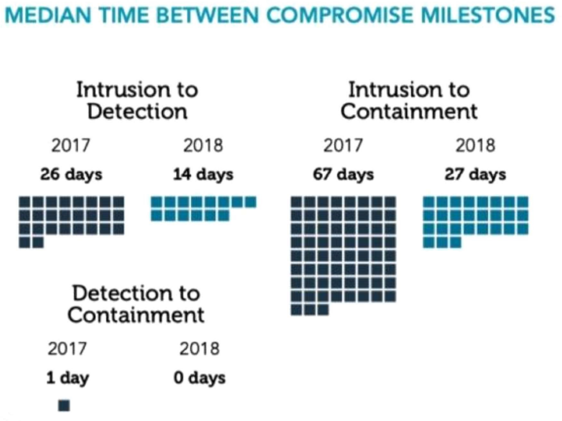
In some cases, the date of containment can occur before the date of detection, as when a software upgrade halts an attack before its discovery or when investigators determine the attacker left the network before they detected the breach.

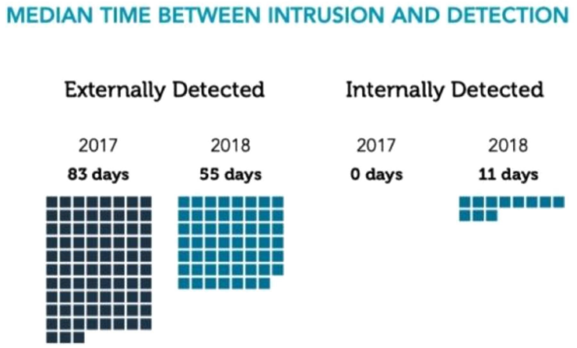



METHOD OF DETECTION BY REGION

To respond to a breach, one must first be able to detect it. Tools, such as endpoint detection and response (EDR) and improved organisational maturity – in terms of processes, training and awareness – led to dramatic decreases in the median times among all three milestones between 2017 and 2018. Median intrusion-to-containment durations fell to just 27 days in 2018 from 67 days in 2017.

Nevertheless, evidence was still found of attackers having access to compromised environments for extended periods, exceeding a year in some cases. This provides them with ample opportunities to obtain sensitive data and even set up mechanisms to collect and exfiltrate new data as it is added. It also means they can install multiple backdoors, significantly increasing the complexity of removing them from the network. Note, too, that operating system and application event logs, which often provide critical information regarding attacker activity, are typically retained only for seven days or less, making them largely useless when investigating an intrusion event that happened months ago.

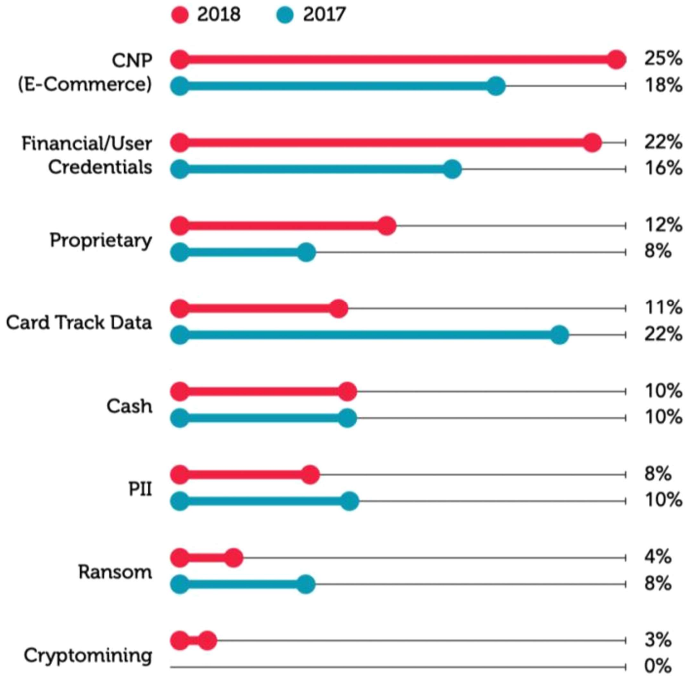

MEDIAN TIME BETWEEN COMPROMISE MILESTONES


MEDIAN TIME BETWEEN INTRUSION AND DETECTION

Internally detected compromises also continued to be contained more quickly than externally detected ones. In cases where containment occurred after detection, the mean duration between the two milestones was just three days for internally detected breaches, compared to 45 days for externally detected breaches. The same tools and techniques that enable businesses to detect breaches on their own or in partnership with a managed security services provider often make it possible to respond to them within days or even minutes. By contrast, a business that needs an outside party to inform it of a breach often is not able to quickly contain the breach. Consequently, the compromise continues, sometimes for many crucial days.

When it comes to data compromises Retail at 18% and Financial at 11% are the industries most affected, with card-not-present data (mostly from payment cards used in e-commerce transactions) accounting for 25% of data breaches targeted and financial/user credentials accounting for 22%.

Overall, payment-card data comprised 36 percent of incidents, including track (magnetic stripe) data at 11 percent. Incidents seeking payment-card data decreased substantially over the past few years, down from 41 percent in 2017 and 57 percent in 2016. The decline in track data correlates to the decrease in incidents involving POS systems; although, the rise in e-commerce data makes up for much of the track data decline.



Compromise by Motivation or Type of Data Targeted

Unsurprisingly, attacks on corporate and internal networks targeted a range of data types, while attacks on e-commerce environments heavily sought card-not-present data and POS attacks pursued card-track data.

Different industries face different kinds of attacks. Most of the incidents affecting the finance, hospitality and utility industries involved corporate and internal networks, whereas retail incidents were heavily slanted toward e-commerce attacks. POS attacks primarily affected health care and food and beverage industries. These statistics demonstrate the necessity of asking, "Where is my data of value?" when designing and building systems and then planning security accordingly.

Attackers mostly sought card-track data in the hospitality and food and beverage industries, which routinely collect card-swipe data from patrons. Criminals targeted several different industries for user and financial credentials, proprietary information and personally identifiable information (PII).

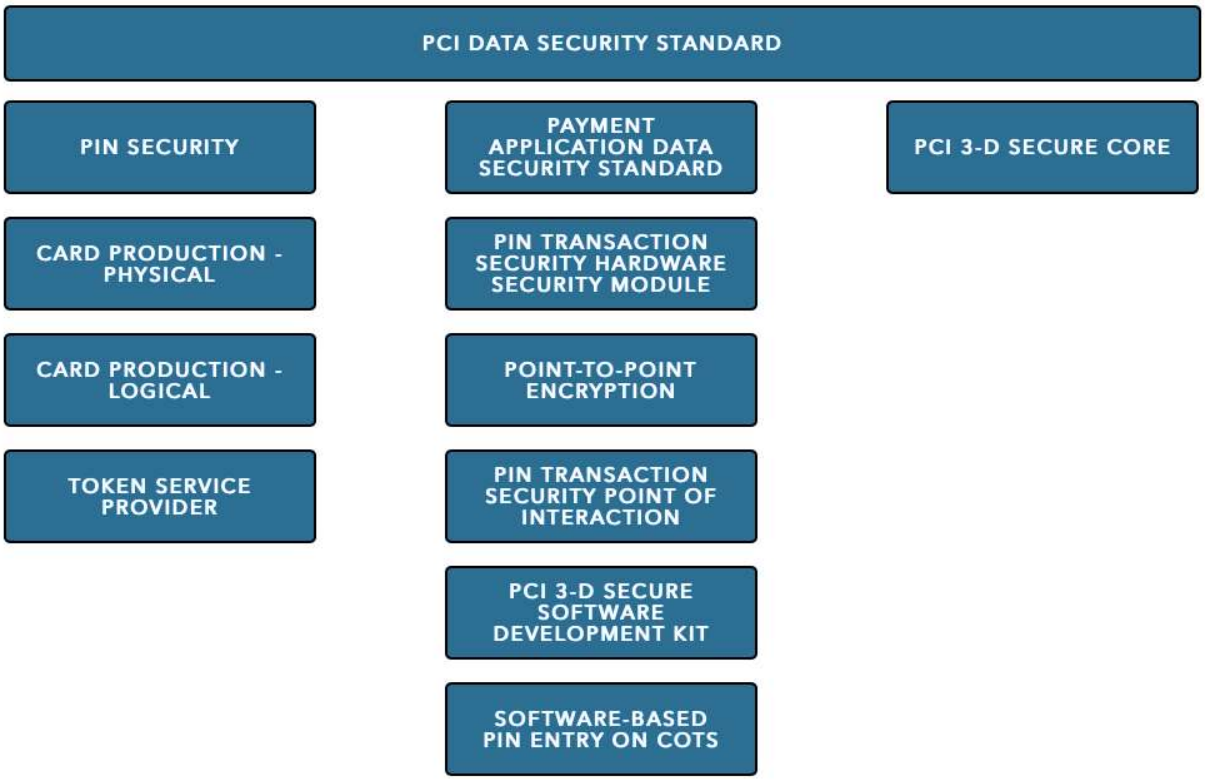
In the case of point-of-sale malware, which typically includes memory scraping/dumping and keystroke-logging functionality to capture as much card data as possible, we are seeing POS malware families like FrameworkPOS, FighterPOS, PoSeidon/FindStr and Carbanak/Anunak being active as ever. Add to that Formjacking (malware that targets e-commerce websites by injecting malicious code into forms on the checkout page to steal payment card data and customer information), remote access trojans (RATs), Magecart (a term assigned for several criminal groups that use similar tools and techniques to compromise e-commerce sites with malicious scripts designed to skim and capture sensitive data like credit card information from unsuspecting shoppers) and database or application vulnerabilities and you start to realise the attack surface for cardholder data can be large if not managed.

That’s where PCI Compliance comes in.

PCI COMPLIANCE

To quote the **Payment Card Industry (PCI) Data Security Standard, v3.2.1** “The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers.”

PCI DSS is the cornerstone that other payment card data security processes are developed upon including the standards below:


PCI DATA SECURITY STANDARD
PIN SECURITY
PAYMENT APPLICATION DATA SECURITY STANDARD
PCI 3-D SECURE CORE
CARD PRODUCTION - PHYSICAL
PIN TRANSACTION SECURITY HARDWARE SECURITY MODULE
CARD PRODUCTION - LOGICAL
POINT-TO-POINT ENCRYPTION
TOKEN SERVICE PROVIDER
PIN TRANSACTION SECURITY POINT OF INTERACTION
PCI 3-D SECURE SOFTWARE DEVELOPMENT KIT
SOFTWARE-BASED PIN ENTRY ON COTS

The Council was founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa Inc. They share equally in governance and execution of the Council's work and the council’s standards continue to evolve based on the current cyber security landscape.

It's worth noting that PCI DSS and the National Institute of Standards and Technology's (NIST) Cybersecurity Framework share a common goal of enhancing data security. To that end a document was created by the PCI SSC which maps PCI DSS to the NIST Framework so that stakeholders can understand how to align security controls to meet both standards, which underlines the reach of PCI DSS compliance when it comes to strengthening a company's overall security posture.

Currently the level of compliance is generally set by the acquirers (i.e. banks) and the number of transactions a business process yearly as per the table below:

Level 1	Level 2	Level 3	Level 4
Visa/MC > 6 Million / Year Amex > 2.5M / Year **Validation Actions** Annual On-site Assessment Quarterly Network Scan **Performed By** PCI QSA or Internal Security Assessor (ISA) Approved Scanning Vendor (ASV)	Visa/MC > 1 Million / Year Amex > 50K – 2.5 Million / Year **Validation Actions** Self-Assessment Questionnaire (SAQ) Quarterly Network Scan **Performed By** PCI QSA or ISA Approved Scanning Vendor	Visa/MC < 1 Million / Year > 20K eCommerce Amex < 50K / Year **Validation Actions** Self-Assessment Questionnaire (SAQ) Quarterly Network Scan **Performed By** Merchant Approved Scanning Vendor	Visa/MC < 1 Million / Year < 20K eCommerce Amex N/A **Validation Actions** Self-Assessment Questionnaire (SAQ) Quarterly Network Scan **Performed By** Merchant Approved Scanning Vendor

A level 1 or 2 merchant require an onsite assessment by a Qualified Security Assessor (QSA) or an Internal Security Assessor, both qualified by the SSC. Level 3 or 4 merchants can self-assess via a Self-Assessment Questionnaire (SAQ) provided by the SSC along with external vulnerability scanning. There are several SAQ types based on how a business handles cardholder data, which can vary the number of assessment questions from 22 all the way through to 250. It's a pragmatic approach based on a risk profile relative to the use of cardholder data, but what is more interesting is that no entity that processes, stores or transmits cardholder data is excluded from focussing on and implementing cyber security solutions. Given the number of business that process payment cards today the standard has a wide reach. Below is a high-level overview of the 12 PCI DSS requirements:

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data

	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

PCI DSS is not just about a point in time assessment. PCI DSS should be implemented into business-as-usual (BAU) activities as part of a business’ overall security strategy, and the standard, including associated guidance from the SSC like **Best Practices for Maintaining PCI DSS Compliance**, promotes that belief. That is significant because if helps change the mindset of Australian businesses away from viewing compliance and cyber security as “tick-in-the-box” activity and towards an ongoing process of keeping data secure.

If PCI DSS was implemented across a business as part of their cyber security programme and not just restricted to a card data environment (CDE) the security posture of many would increase. It provides a good security foundation with ties to NIST and ISO27002 and other standards such as GDPR compliance could partially be addressed if PCI DSS was already in place.

In short promoting PCI DSS compliance amongst Australian business would uplift the overall security posture of the country as a whole by tackling one of the primary reasons behind cyber-crime in the first place. But how do other governments around the world support PCI DSS compliance and what can we learn from them?

Global Government Involvement in Compliance

The Australian Government is currently spreading the right message about PCI compliance through websites like business.gov.au however the message is sparse, and unlike some of the other examples below, there is no real drive to push businesses towards compliance. There are penalties for non-compliance issued by the card brands but often there are factors that may or may not see those fines levied. It leads to some businesses viewing PCI compliance, and subsequently protection of cardholder data, as a "tick in the box" check to get out of the way. There may also be assessors willing to support such a mentality to the detriment of cyber security. So how can governments help drive compliance which will lead businesses to a stronger security posture overall? Let's take a look at the direction two major economies took in recent times, Japan and the United States.

JAPAN - MINISTRY OF ECONOMY, TRADE AND INDUSTRY

In February 2016 the Japanese Ministry of Economy, Trade and Industry (METI) released a "Compilation of an Action Plan for the Strengthening of Measures for Security in Credit Card Transactions". The aim of which was "to develop an environment which ensures security in credit card transactions meets global standards, an action plan in which specific goals to be achieved by 2020 and the responsibilities of each relevant entity were set forth". The outline of the action plan included:

- Protection of card information
- Measures for the prevention of card forgery
- Measures against fraudulent use of credit cards in EC

Background statements made it clear what the main drive of the initiative was and provided further details as to the aim. In part METI stated their intention was "to develop an environment which ensures security in credit transactions meets global standards in preparation for the 2020 Summer Olympic Games and Paralympic Games in Tokyo, the Council on Measures for Security in Credit Transactions was established, composed of credit card companies and a wide range of business operators involved in credit transactions and the Council has formulated an action plan in which set various matters including specific goals and efforts to be made by each relevant entity."

The safety cardholder data associated is at the forefront of Olympic organisers in Japan. The Japan Times reported in July this year "Previous Olympic organizers have faced an enormous number of cyberattacks, with 500 million estimated during the 2016 Rio Games and 250 million during the 2012 London Games. The threat to Tokyo is expected to be on a similar scale. Organizers faced such a threat last September when a group of hackers tried unsuccessfully to steal private information from people in the United States and Japan by emailing fake ticket offers"

The involvement of Japanese government departments in compliance standards surrounding the use of credit cards has since steadily increased. For example, in March 2017 METI released two documents titled Cashless Vision and API Guidelines for Utilization of Credit Card Data. Some of the key points from the documents included:

- Measures for security and protection of users
- Relationship with regulations under the related laws, other guidelines, etc.
- Current situations of cashless settlement in Japan

In both documents METI covered "Future efforts" where they looked to events as far away as 2025 and as such they developed a commission tentatively called "Commission for Promotion of Cashless Settlement," where the industry, academia and government sectors would collaboratively advance efforts under their proposed frameworks for initiatives in Japan.

Right through to this year METI has taken an active role in ensuring the security of cardholder data and the protection of payment systems. For example, in April this year METI announced "that the Payments Japan Association formulated the Guidelines for Measures for Preventing Unauthorized Use of Credit Card Information Wrongly Leaked during QR Payment" after "at the end of 2018, unauthorized use of consumer credit card information, e.g., card number, expiration date and security code, occurred after consumers used QR payment services through their smartphones."

It is clear that the Japanese government is taking a hands-on approach to the protection of card information (or cardholder data) and doing so with fixed dates in mind, like the 2020 Olympic Games. This drive is strengthening the overall cyber security landscape of Japan as compliance to standards takes centre stage. There is always a knock-on effect with compliance to certain standards given the implementation of controls often reaches a wider footprint of systems other than those in scope for an assessment. Hence the Japanese government's initiatives in this one space will ultimately lead to a stronger cyber security baseline.

References include:

- METI Compilation of an Action Plan for the Strengthening of Measures for Security in Credit Card Transactions
- The Japan Times Article on Cyberthreats
- METI Cashless Vision and API Guidelines for Utilisation of Credit Card Data
- METI Guidelines for Measures for Preventing Unauthorized Use of Credit Card Information Wrongly Leaked during QR Payment

USA – FEDERAL TRADE COMMISSION

In the United States of America, the Federal Trade Commission (FTC) protects consumers by stopping unfair, deceptive or fraudulent practices in the marketplace. In August 2015 the FTC sued Wyndham Worldwide Corporation for data security failures led to three data breaches at Wyndham hotels in less than two years. According to the complaint "those failures resulted in millions of dollars of fraudulent charges on consumers' credit and debit cards – and the transfer of hundreds of thousands of consumers' account information to a website registered in Russia."

The FTC went onto state "If your clients are concerned about data security – and they should be – you'll want to read the entire opinion. But the long and the short of it is that the Third Circuit upheld the District Court's ruling that the FTC could use the prohibition on unfair practices in section 5 of the FTC Act to challenge the alleged data security lapses outlined in the complaint." Basically, the FTC has determined that inadequate data security can be an "unfair practice".

The ruling by the District Court of New Jersey included an order for 20 years that Wyndham Worldwide Corporation maintain "a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of Cardholder Data that is collects or received in the United states from or about consumers." The ruling went on to define further requirements including a requirement to annually undergo an assessment against PCI Data Security Standard (DSS) which was attached to the ruling. The Third Circuit upheld the District Court's ruling.

The Federal Trade Commission Chairwoman (at the time) Edith Ramirez stated "Third Circuit Court of Appeals decision reaffirms the FTC's authority to hold companies accountable for failing to safeguard consumer data. It is not only appropriate, but critical, that the FTC has the ability to take action on behalf of consumers when companies fail to take reasonable steps to secure sensitive consumer information."

In 2016 the FTC had followed up and "issued orders to nine companies requiring them to provide the agency with information on how they conduct assessments of companies to measure their compliance with the Payment Card Industry Data Security Standards (PCI DSS)."

What is clear is that the US government is taking a strong interest in the protection of cardholder data utilising the likes of courts to enforce non-compliance with available standards such as PCI DSS.

References include:

- District Court of New Jersey Stipulated Order for Injunction
- Third Circuit rules in FTC v Wyndham case
- Statement from FTC Chairwoman Edith Ramirez on Appellate Ruling in the Wyndham Hotels and Resorts Matter
- FTC To Study Credit Card Industry Data Security Auditing

Conclusion

It is clear from the statistics attacks on Australian businesses and consumers that specifically target financial credentials, including payment card information, are increasing and are one of the primary motives for criminals online. PCI DSS compliance can help reduce the attack surface with the added benefit of increasing awareness and improving a business' security posture overall. Not only does the standard cover the securing of data it also tackles information and physical security as well.

It's our position that PCI DSS compliance should be mandated by legislative instrument, or at the very least gain the focus and attention it gets from countries like the United States and Japan. While stopping short of legislating for compliance they do use the mechanisms available to them to implore businesses and customers to take them seriously. A 20-year court order in the US mandating compliance on a company is proof of that.

As the security of businesses increases, so will consumer confidence, especially if they can differentiate compliant and non-compliant organisations. A consumer may choose to pick a compliant business knowing that a certain level of security is in place which in turn increases their own data security. Note the lack of consumer confidence in a brand once breached, not to mention the recovery of the businesses breached and the financial impacts as a result. Most consumers hear of breaches on two levels, either credential or financial. Given PCI DSS compliance addresses both for payment card data it stands to reason it would have a positive impact on consumers and businesses alike.

SecureTrust would be more than available to work with the government on a PCI DSS compliance approach that would benefit the country as a whole given the focus of cyber-criminals. Australia has an opportunity to lead the world when it comes to protection of payment card data and we would value the opportunity to participate in that initiative.