PCI-DSS-WTF

Who am I?

- Peter Jakowetz
- Security Architect
- Ex-PCI QSA
- CISSP, CISA, CISM, OSCP etc
- Wellingtonian
- Like cars, cats and camping

What’s this talk about?

- What is PCI-DSS
- Why is this important?
- Does this affect us in NZ?
- What are the basics?
- What else should I know?
- How does OWASP fit into this?
- Resources?

What is PCI-DSS?

- Payment Card Industry Data Security Standard
- A set of minimum requirements for those processing credit card payments
- There are other standards for those creating credit card processing hardware etc
- If you’re dealing with credit card details, you’re obligated to meet the standard by the card brands
- We’re up to version 3.2.1 of the standard

PCI-DSS *is a standard of data security for the credit card industry, and applies only to companies that process, store, or transmit credit card data. For these companies, compliance with the standard is obligatory, though depending on the volume of cards processed, different requirements or obligations may apply.*

Why is this important?

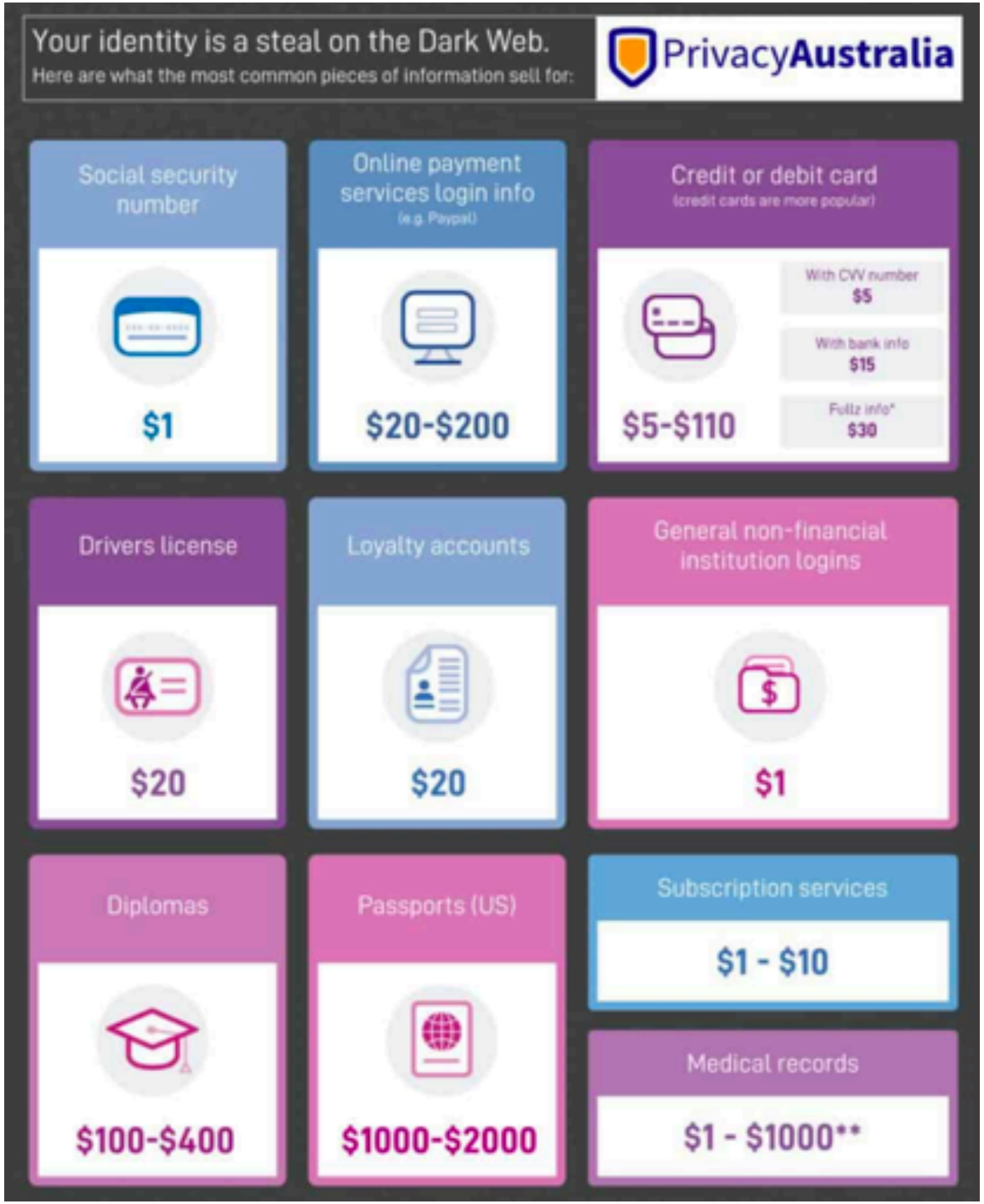
- Keeps you off the front page of the news
- Stops you from being fined by the banks
- Keeps you able to process credit card transactions
- Allows your business to function, so you can stay working!
- Socially responsible thing to do ☺

How is this weaponized?

- Steal data off credit card processing websites
- Sell it off at lower prices
  - ~$45 a card – depends on quality of data
  - Price depends on credit available, age, location etc

In 2018 – 444,602 cases of identity theft in US, 160’000 of those were credit card fraud.

Tripled in size between 2014 and 2018



Your identity is a steal on the Dark Web.

Here are what the most common pieces of information sell for:

PrivacyAustralia

Social security number

$1

Online payment services login info
(e.g. Paypal)

$20-$200

Credit or debit card
(credit cards are more popular)

$5-$110

With CVV number
$5

With bank info
$15

Fullz info*
$30

Drivers license

$20

Loyalty accounts

$20

General non-financial institution logins

$1

Diplomas

$100-$400

Passports (US)

$1000-$2000

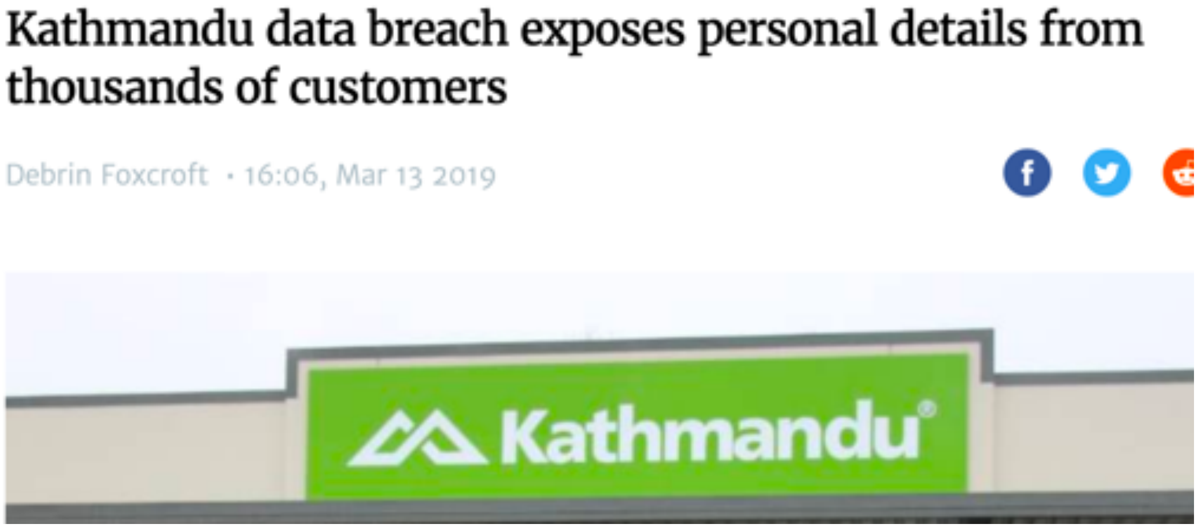
Subscription services

$1 - $10

Medical records

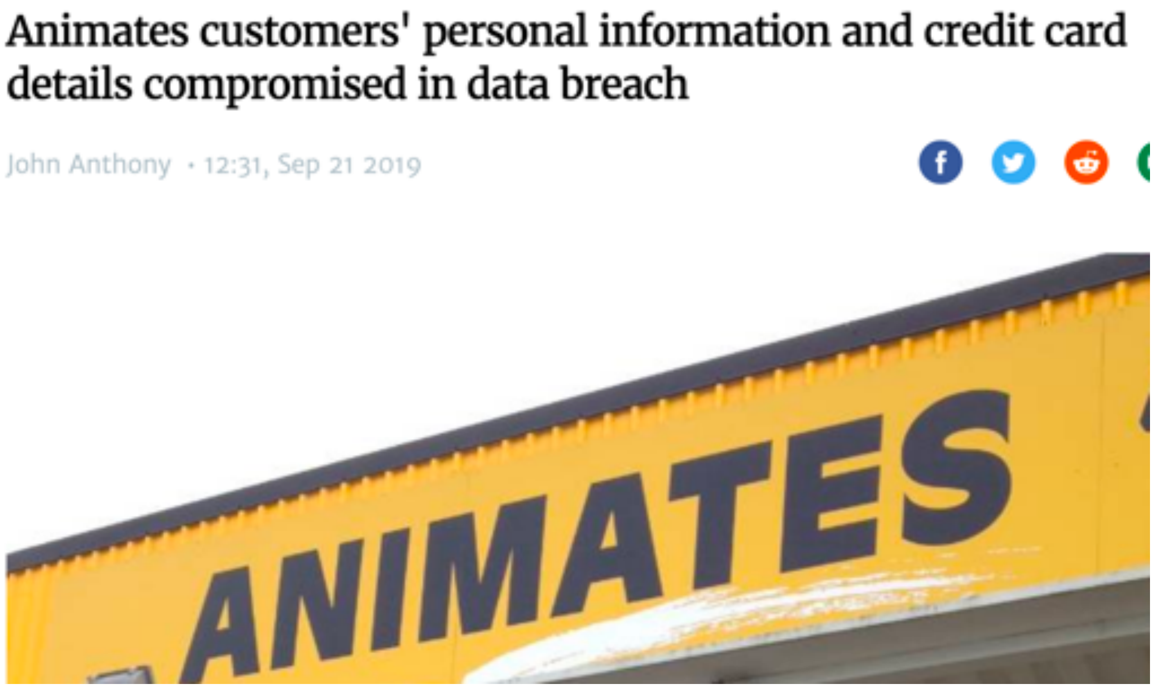
$1 - $1000**

Does this actually happen in NZ?



Kathmandu data breach exposes personal details from thousands of customers

Debrin Foxcroft · 16:06, Mar 13 2019



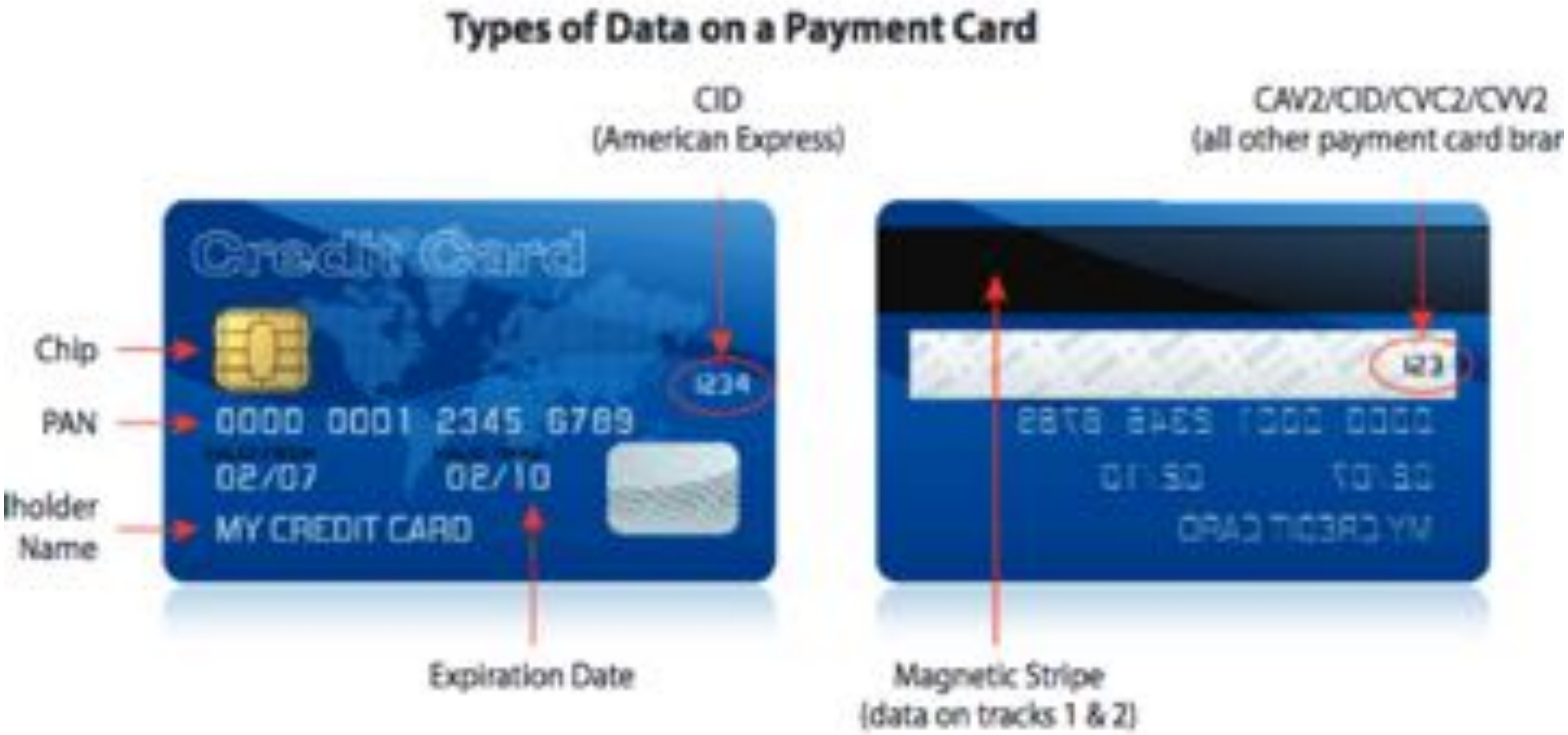
Animates customers' personal information and credit card details compromised in data breach

John Anthony · 12:31, Sep 21 2019

But the Acronyms!?

- PCI – Payment card industry
- DSS – Data Security Standard
- QSA – Qualified Security Assessor
- ASV – Approved Scanning Vendor
- SAQ – Self Assessment Questionnaire
- AOC – Attestation of Compliance
- ROC – Report on Compliance
- CHD – Card holder data
- CDE – Card holder Data Environment

What’s in a credit card?



Terminology

- Acquiring bank (merchant bank) – maintains the merchants bank account
- Issuing bank – issues credit card to consumer on behalf of the card brands
- Card brands – Visa, Mastercard, AMEX etc
- Payment Gateway – card not present version of a POS terminal

PCI DSS Requirements	Testing Procedures	Guidance
	3.1.c For a sample of system components that store cardholder data: • Examine files and system records to verify that the data stored does not exceed the requirements defined in the data retention policy • Observe the deletion mechanism to verify data is deleted securely.	Identifying and deleting stored data that has exceeded its specified retention period prevents unnecessary retention of data that is no longer needed. This process may be automated or manual or a combination of both. For example, a programmatic procedure (automatic or manual) to locate and remove data and/or a manual review of data storage areas could be performed. Implementing secure deletion methods ensure that the data cannot be retrieved when it is no longer needed. ***Remember, if you don't need it, don't store it!***
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:* • *There is a business justification and* • *The data is stored securely.* Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	**3.2.a** For issuers and/or companies that support issuing services and store sensitive authentication data, review policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data.	Sensitive authentication data consists of full track data, card validation code or value, and PIN data. Storage of sensitive authentication data after authorization is prohibited! This data is very valuable to malicious individuals as it allows them to generate counterfeit payment cards and create fraudulent transactions. Entities that issue payment cards or that perform or support issuing services will often create and control sensitive authentication data as part of the issuing function. It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data ONLY IF they have a legitimate business need to store such data. It should be noted that all PCI DSS requirements apply to issuers, and the only exception for issuers and issuer processors is that sensitive authentication data may be retained if there is a legitimate reason to do so. A legitimate reason is one that is necessary for the performance of the function being provided for the issuer and not one of convenience. Any such data must be stored securely and in accordance with all PCI DSS and specific payment brand requirements. *(Continued on next page)*
	3.2.b For issuers and/or companies that support issuing services and store sensitive authentication data, examine data stores and system configurations to verify that the sensitive authentication data is secured.	
	3.2.c For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization.	

12 Requirements

Goal: 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.

Goal: Protect Cardholder Data

3. Protect stored cardholder data.

4. Encrypt transmission of cardholder data across open, public networks.

Goal: 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.

12 Requirements

Goal: Implement Strong Access Control Measures

7. Restrict access to cardholder data by business justification (i.e., "need to know").

8. Identify and authenticate access to system components.

9. Restrict physical access to cardholder data.

Goal: Regularly Monitor and Test Networks

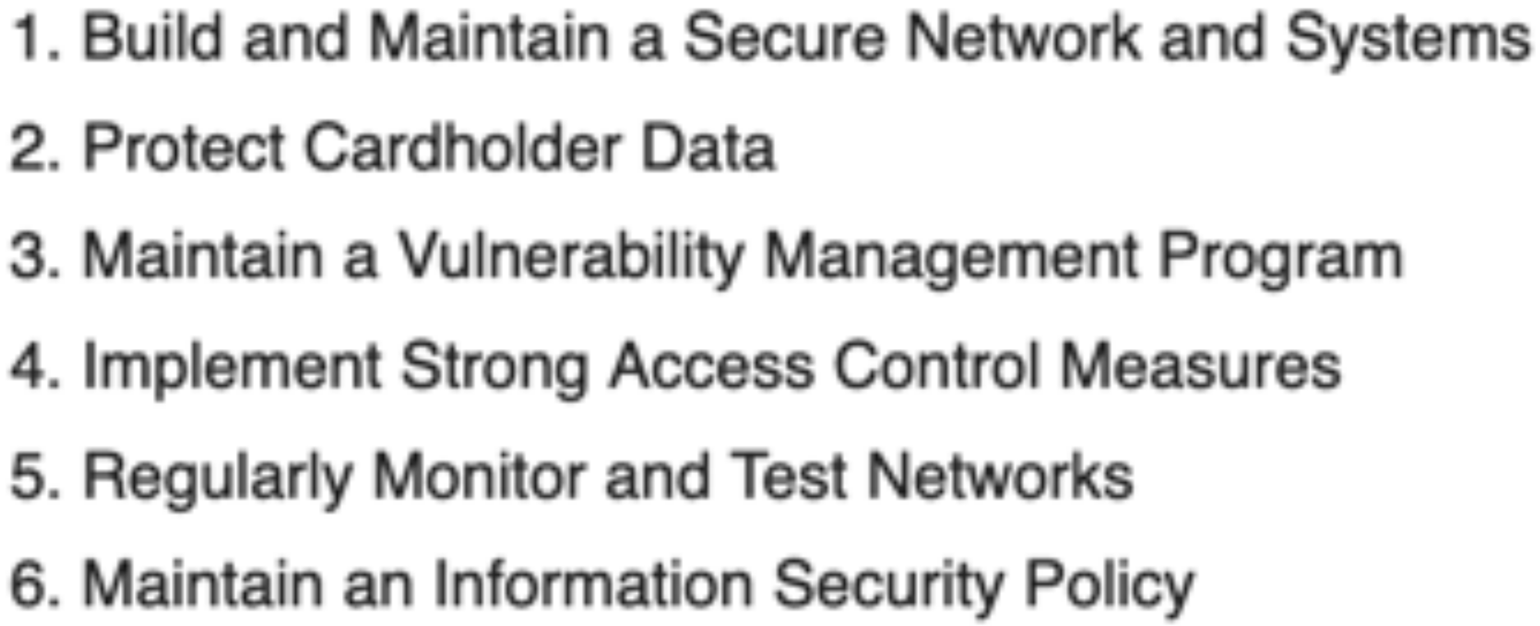
10. Track and monitor all access to network resources and cardholder data.

11. Regularly test security systems and processes.

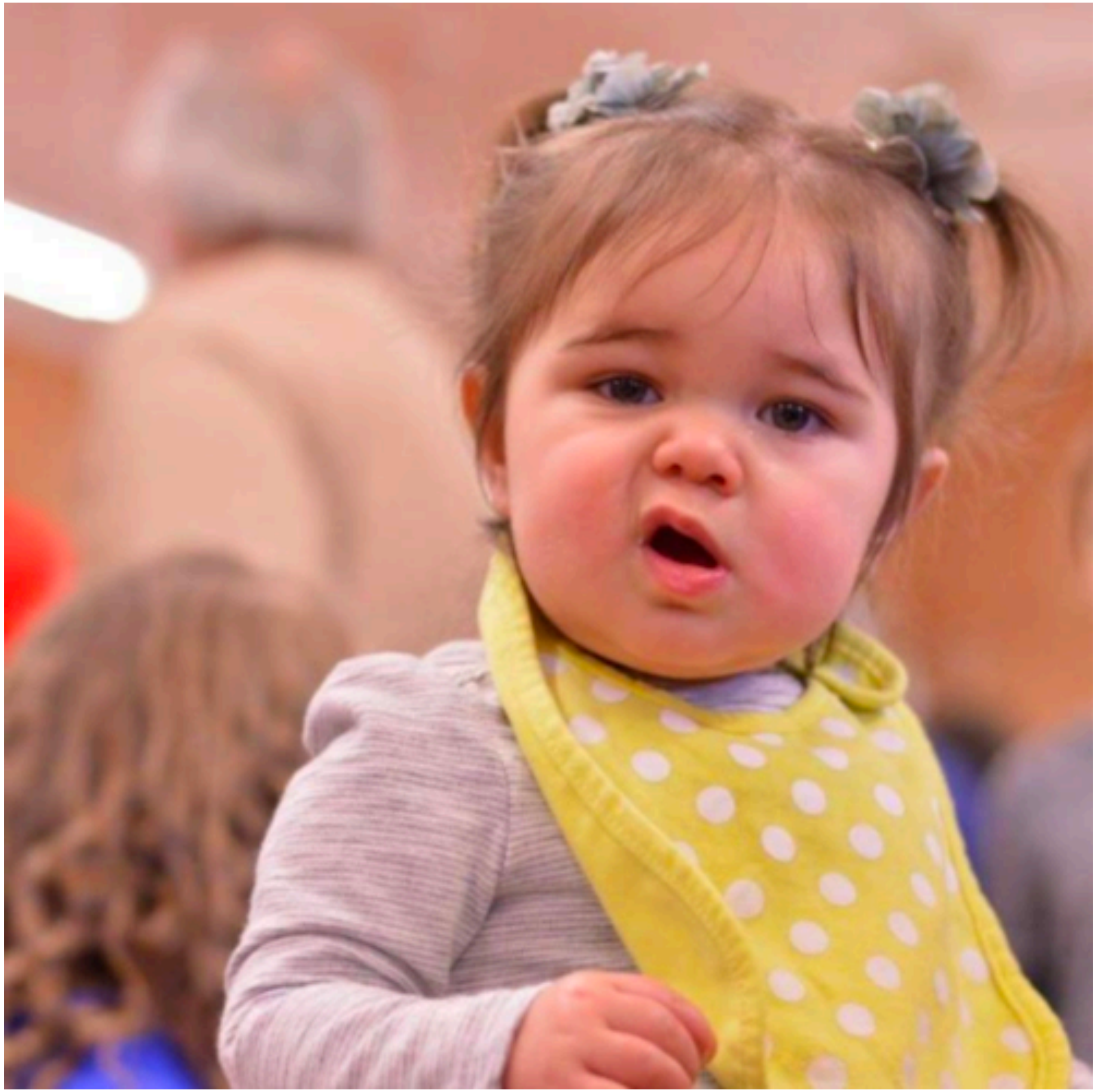
Goal: Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel.

6 Control Areas



1. Build and Maintain a Secure Network and Systems
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy



Pete’s top 6

- Document the things
- Harden the things
- Avoid holding CHD
- Secure coding
- Restrict access
- Consider your 3rd parties

What are the basics?

- Document all the things
  - Define your CDE
  - Policies
  - Designs
  - Delegations
  - Decisions
  - Processes (and follow them)
  - Strong information security policy & training
- Assign ownership to the above

1

What are the basics?

- Harden all the things
  - Restrict access
  - Firewalls/ Network access control
  - Implement MFA
  - Put on change detection
  - Log on them
  - Alert on them
  - Change default passwords and parameters
  - Run AV
  - Patch

2

What are the basics?

- Avoid holding cardholder data
- When you do
  - Encrypt all the things (at rest and in transit)
  - Store your keys securely
  - Segregate where you’re storing them
  - Encrypt/ hash/ mask or trunk data

3

HTTPS

- Ensure TLS is enabled
- ‘Early TLS’ is considered badj
- Migrate to TLS 1.1 of **1.2**
- Configure TLS securely

What are the basics?

- Code securely and test all the things
  - Internal penetration testing
  - Internal vulnerability scanning
  - Vulnerability Scanning (ASV scans)
  - External penetration testing
  - Code review
  - Separate dev, test and prod environments
  - Scan for card data in your network

4

Coding tips

- Address common coding vulns in software dev processes:
  - Train devs annually in coding techniques
  - Develop apps based on secure coding guidelines [read: OWASP]
- Follow a change control process/ CI CD process & document changes
- Test after major changes
- Don’t leave test accounts in prod
- Peer review code – don’t mark your own homework

What are we trying to avoid

- Injection flaws (SQL etc)
- Buffer overflows
- Insecure crypto storage
- Insecure comms
- Improper error handling
- High risk vulnerabilities from a vulnerability scan
- XSS
- Improper access control
- CSRF
- Broken authentication and session management
- ‘New threats and vulnerabilities’

What are the basics?

- Keep access restricted
  - Limit access to CHD from WiFi
  - Limit access between test and prod
  - Use strong passwords
  - Use MFA
  - Log access
  - Restrict access
  - Use unique IDs

5

What are the basics

- Consider the other bits you touch (& document and record them!)
  - Data center providers
  - Firewall providers
  - Payment processors
  - Physical destruction companies

6

What else should I think about?

- Don’t think of PCI as aspirational… think of it as the basics of what you need to do
- Limit the data you touch
- When you do touch cardholder data, keep it segregated and touching as few components as possible
- Don’t fall for: “AWS is PCI compliant so I’m sweet” – what about the bits you’ve developed that touch credit card data
- Be careful about saying “I’m ISO27001 compliant so I’ll be sweet for PCI” – they’re looking at 2 different things and the scopes aren’t often the same

Regular requirements

Annual Tasks

- Review information security policies
- Conduct internal & external penetration tests
- Conduct employee security awareness training
- Complete the Self-Assessment Questionnaire or the on-site PCI assessment
- Conduct storage media inventory
- Conduct risk assessment
- Review & disseminate incident response plan

Semiannual Tasks

- Review firewall & router configuration
- Conduct web application security assessment
- Review workstation/Server firewall and antivirus configuration

Regular requirements

Quarterly Tasks

- Conduct and pass an ASV vulnerability scan
- Conduct internal vulnerability scan
- Test for rogue wireless access points

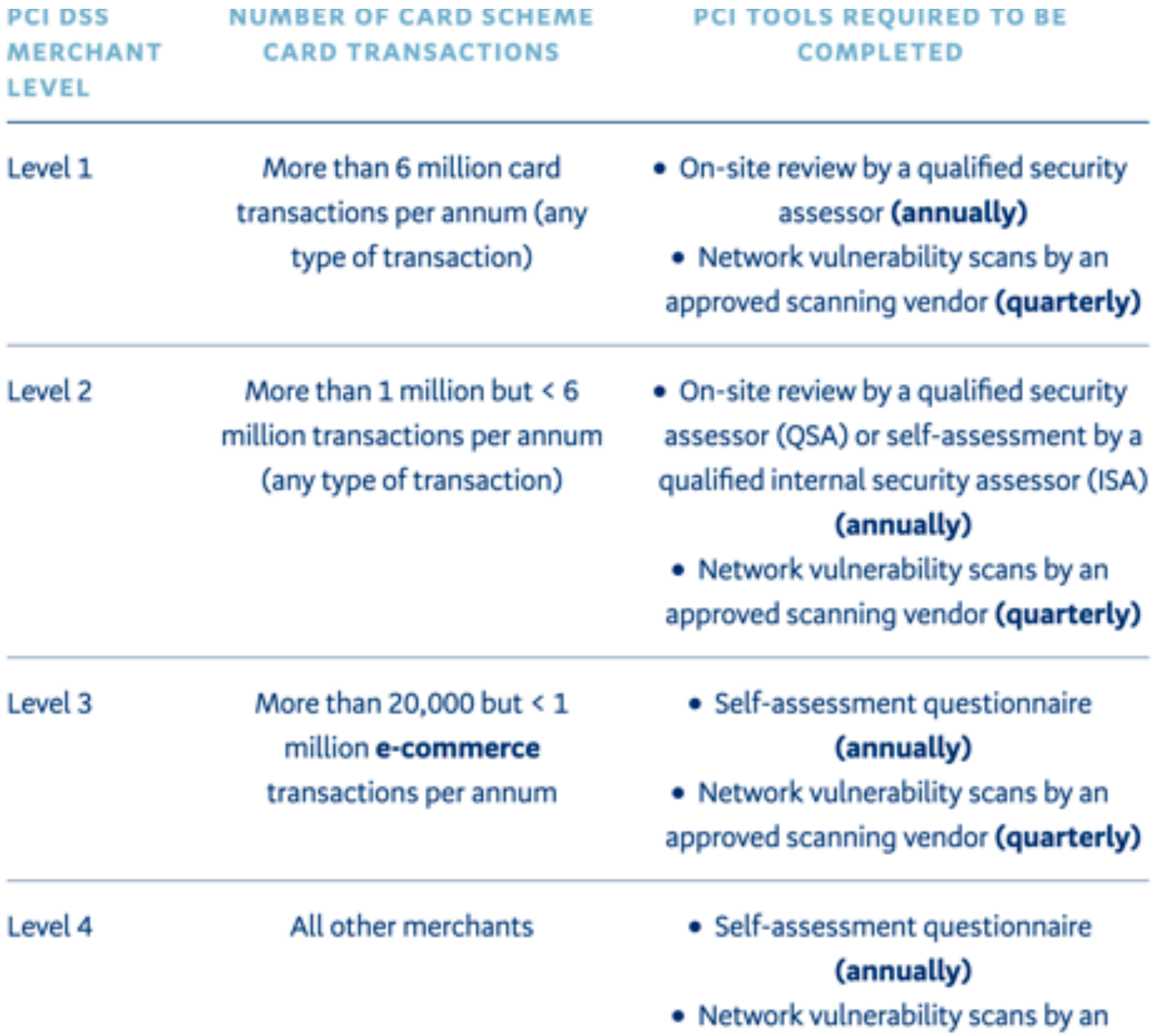
Monthly Tasks

- Update & patch all workstations within the Cardhold Data Enviornment (CDE)

Daily Tasks

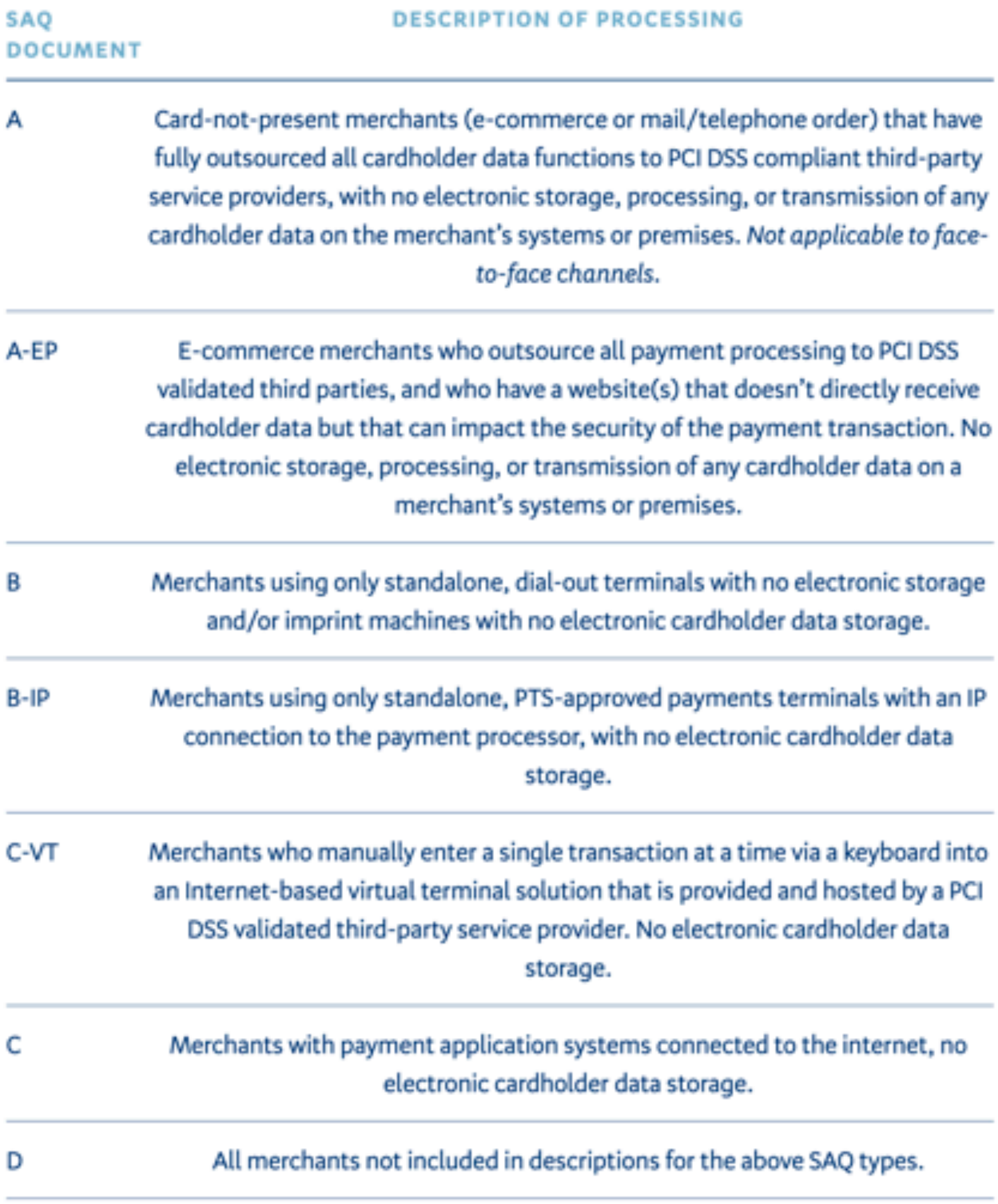
- Review all CDE system logs (network/server/workstation

How do I report this?



PCI DSS MERCHANT LEVEL	NUMBER OF CARD SCHEME CARD TRANSACTIONS	PCI TOOLS REQUIRED TO BE COMPLETED
Level 1	More than 6 million card transactions per annum (any type of transaction)	• On-site review by a qualified security assessor **(annually)** • Network vulnerability scans by an approved scanning vendor **(quarterly)**
Level 2	More than 1 million but < 6 million transactions per annum (any type of transaction)	• On-site review by a qualified security assessor (QSA) or self-assessment by a qualified internal security assessor (ISA) **(annually)** • Network vulnerability scans by an approved scanning vendor **(quarterly)**
Level 3	More than 20,000 but < 1 million **e-commerce** transactions per annum	• Self-assessment questionnaire **(annually)** • Network vulnerability scans by an approved scanning vendor **(quarterly)**
Level 4	All other merchants	• Self-assessment questionnaire **(annually)** • Network vulnerability scans by an

What SAQ?



SAQ DOCUMENT	DESCRIPTION OF PROCESSING
A	Card-not-present merchants (e-commerce or mail/telephone order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Not applicable to face-to-face channels.*
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on a merchant's systems or premises.
B	Merchants using only standalone, dial-out terminals with no electronic storage and/or imprint machines with no electronic cardholder data storage.
B-IP	Merchants using only standalone, PTS-approved payments terminals with an IP connection to the payment processor, with no electronic cardholder data storage.
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage.
C	Merchants with payment application systems connected to the internet, no electronic cardholder data storage.
D	All merchants not included in descriptions for the above SAQ types.

How do I benefit by this?

- You’re required to …. But that means your boss is too
    - More training
    - Budget to fix issues
    - Budget to do things rights

Are there any tools that will help me?

- You don’t have to pay a fortune to make this stuff happen
  - Scan your own code using OpenVAS first to make sure it looks clean
  - Check your https headers using sslscan
  - Put ZAP into your CI CD pipeline for automated testing
  - Search databases for cardholder data using regex searches

How can OWASP help me?

- https://www.owasp.org/images/5/5c/Pci-dss.pdf
- https://www.owasp.org/images/3/38/MeucciPciMilan09.pdf
- https://owasp.org/www-pdf-archive/OWASPNightFaspay.pdf
- https://owasp.org/ProjectReviews/review/pci_toolkit/index.html
- https://owasp.org/www-pdf-archive/Dallas_OWASP_9-11-2013.pdf
- https://wiki.owasp.org/index.php/Category:OWASP_PCI_Project

What are some good resources?

- https://www.pcisecuritystandards.org/document_library
- https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf
- https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1_1.pdf
- https://www.pcisecuritystandards.org/documents/PCI_SSC_Overview.pdf
- https://www.pcisecuritystandards.org/documents/PCI%20Data%20Storage%20Dos%20and%20Donts.pdf
- https://www.pcisecuritystandards.org/documents/PCI%20Data%20Storage%20Dos%20and%20Donts.pdf
- https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf
- https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

Cheers

- peter@jakowetz.nz
- @pjakowetz