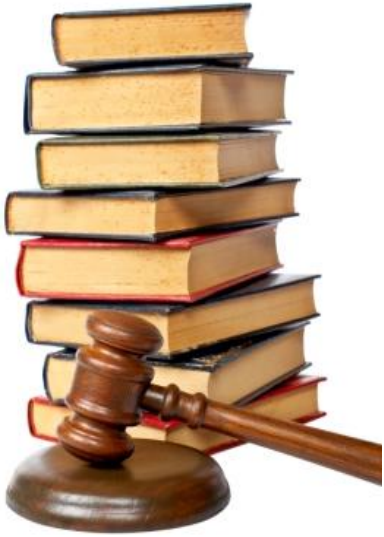
Legal, confidentiality & copyright agreement



- This presentation should be strictly treated as a reference only guide. The content of the presentation do not take into account specific situation and individuals. This information may create an unreasonable risk for readers who choose to apply or use the information in their own activities or to promote the information for use by third parties.

- Stickman consulting and none of the authors, contributors, sponsors, administrators or anyone else connected with Stickman Consulting, in any way whatsoever, can be held responsible for the use of information contained in this document.

- The information contained in this document is confidential and copyright of Stickman Consulting Pvt. Ltd. and STICKMAN Consulting Pty. Ltd. (ABN 49 124 123 548) ("Stickman"). By exposing yourself to the content of this document you agree to the terms of the document which forbids sharing of any content or any part of the discussion during the presentation of this document with anyone without the written permission from Stickman .

- This document is distributed on a Commercial-In-Confidence basis and is restricted to those individuals who have a direct role in assessing its contents. Copies of this document are permitted to be made by the recipient for internal use only; no other copies are to be made without the express written consent of Stickman

- All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

Is it worth carrying the risk of non-compliance to PCI DSS?

Presented By: Ajay Unni
Qualified Security Assessor
Stickman Consulting

STICKMAN® CONSULTING
Keeping your payment card world secure and compliant

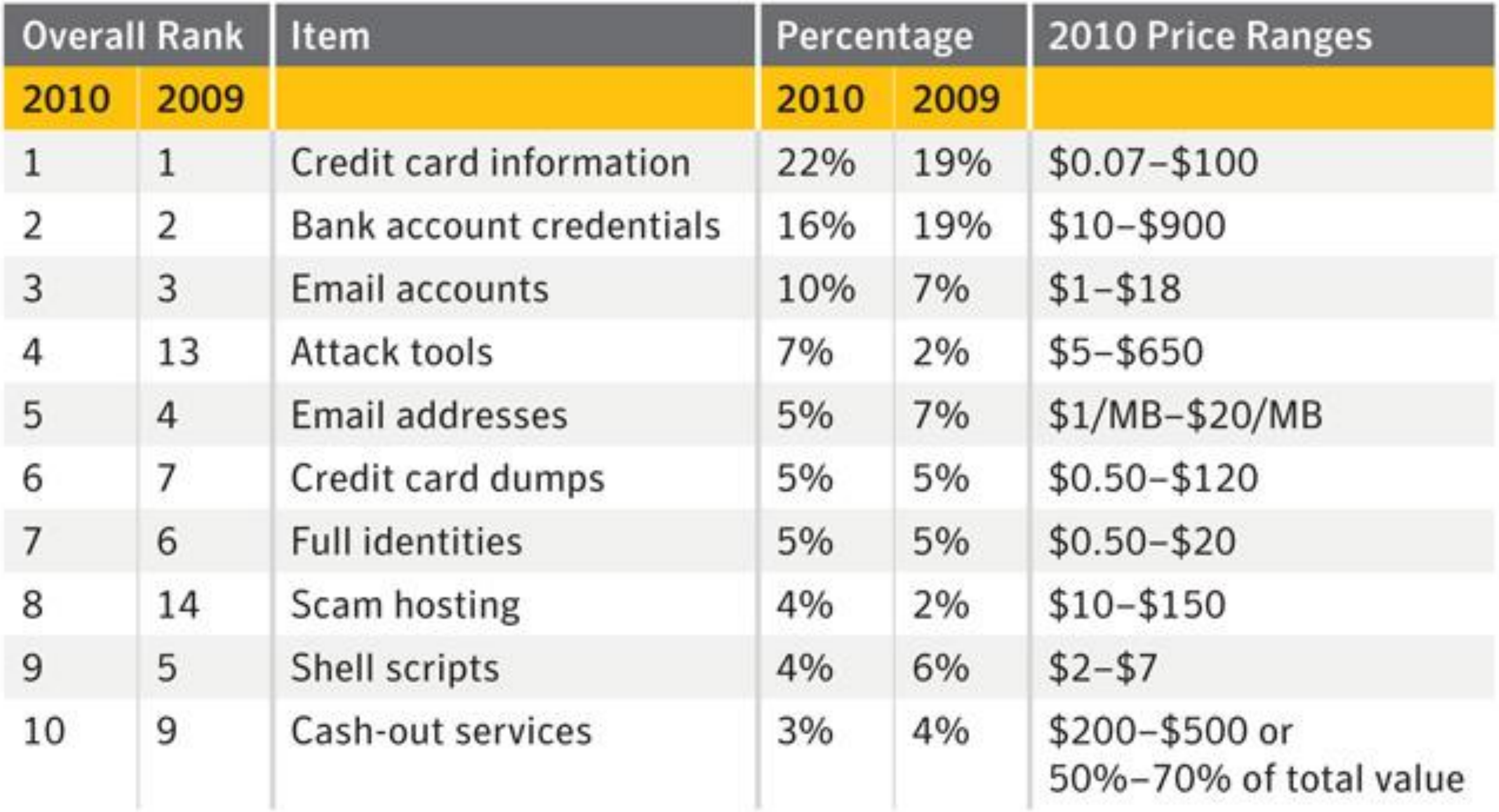
PCI Security Standards Council™ QUALIFIED SECURITY ASSESSOR

what customer data is most valuable for hackers?

STICKMAN® CONSULTING
Keeping your payment card world secure and compliant

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

data for sale at underground market



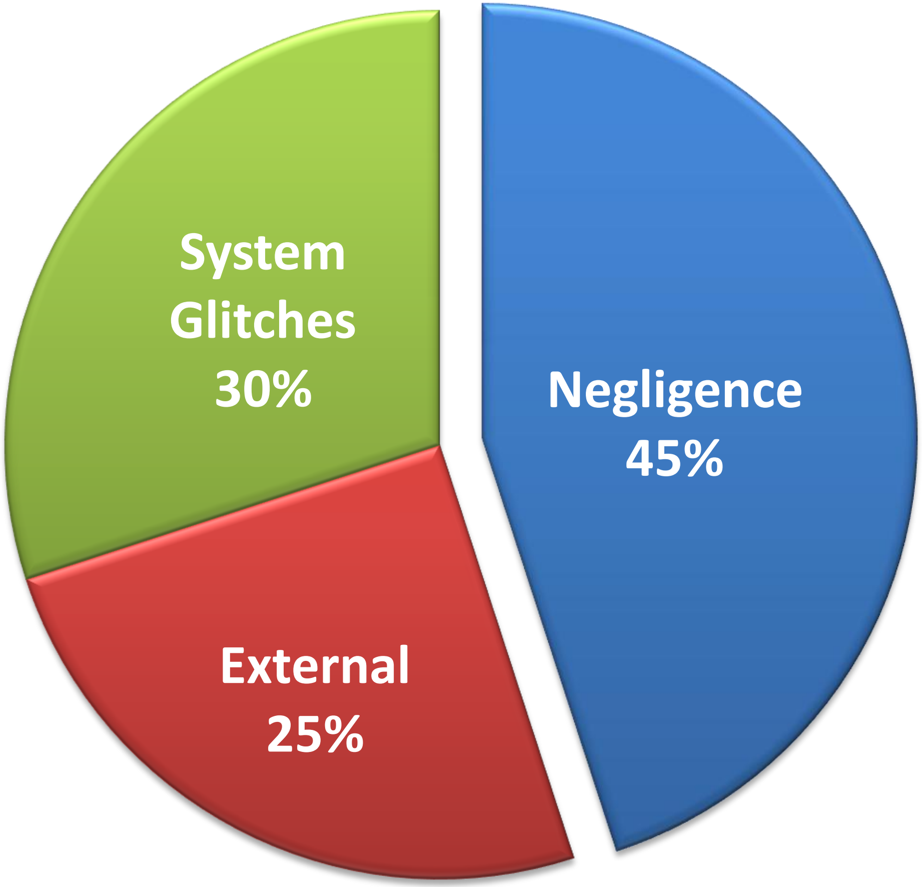
Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	$0.07–$100
2	2	Bank account credentials	16%	19%	$10–$900
3	3	Email accounts	10%	7%	$1–$18
4	13	Attack tools	7%	2%	$5–$650
5	4	Email addresses	5%	7%	$1/MB–$20/MB
6	7	Credit card dumps	5%	5%	$0.50–$120
7	6	Full identities	5%	5%	$0.50–$20
8	14	Scam hosting	4%	2%	$10–$150
9	5	Shell scripts	4%	6%	$2–$7
10	9	Cash-out services	3%	4%	$200–$500 or 50%–70% of total value

Table 11. Goods and services available for sale on underground economy servers, 2009–2010

Source: Symantec Corporation

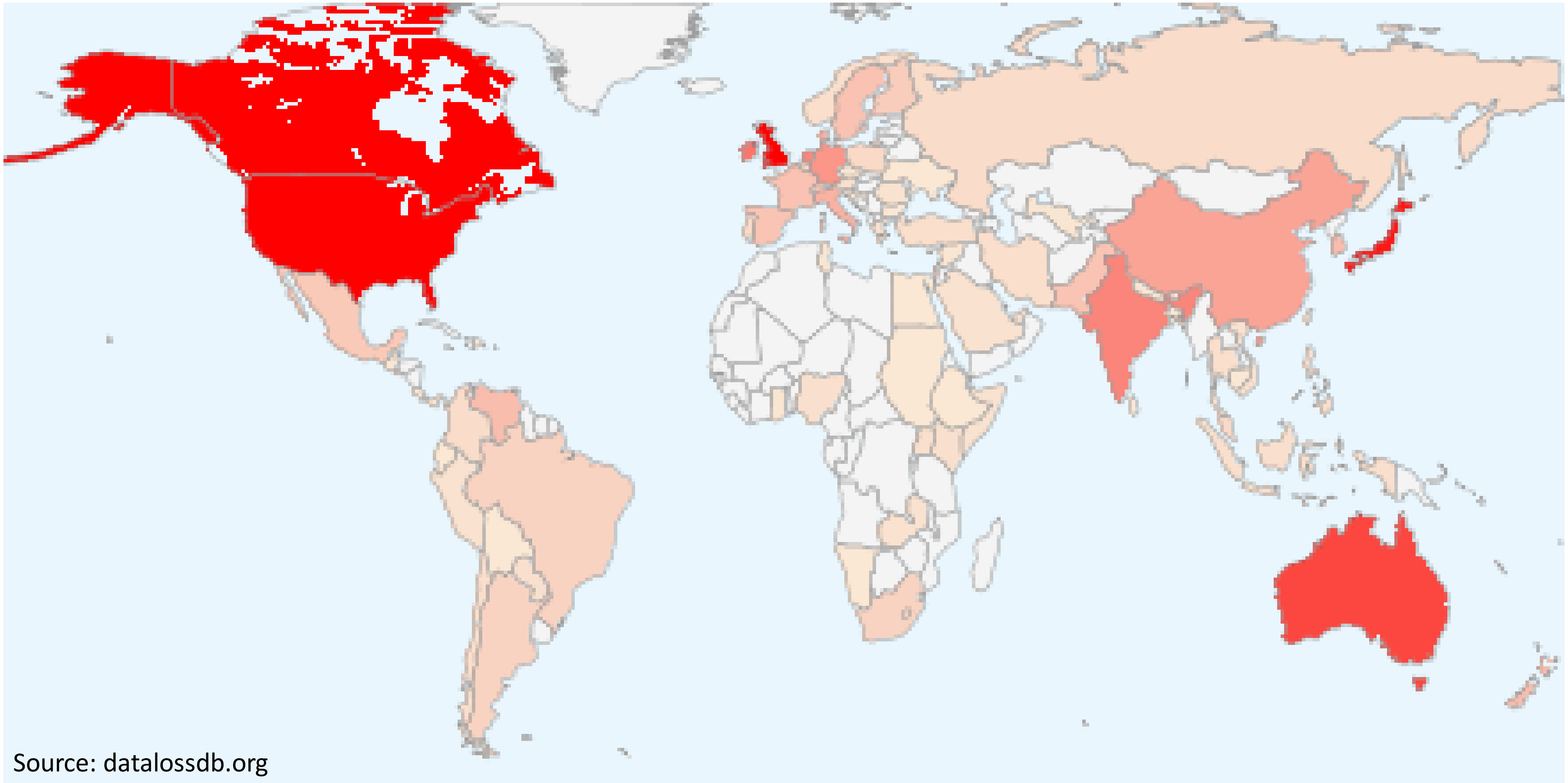
main causes for data breaches?

global causes for data breaches



Source: Data Breach Report March 2012 Ponemon Institute

countries targeted by cyber criminals?

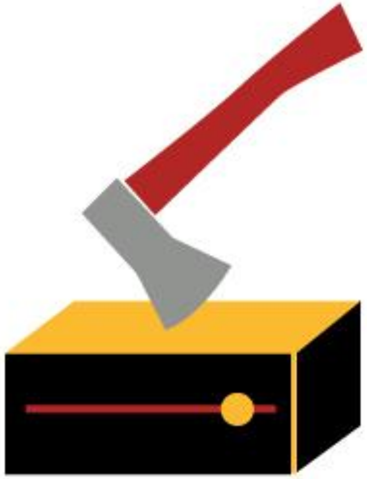


Source: datalossdb.org

data breach report summary

Opportunistic

Dummies



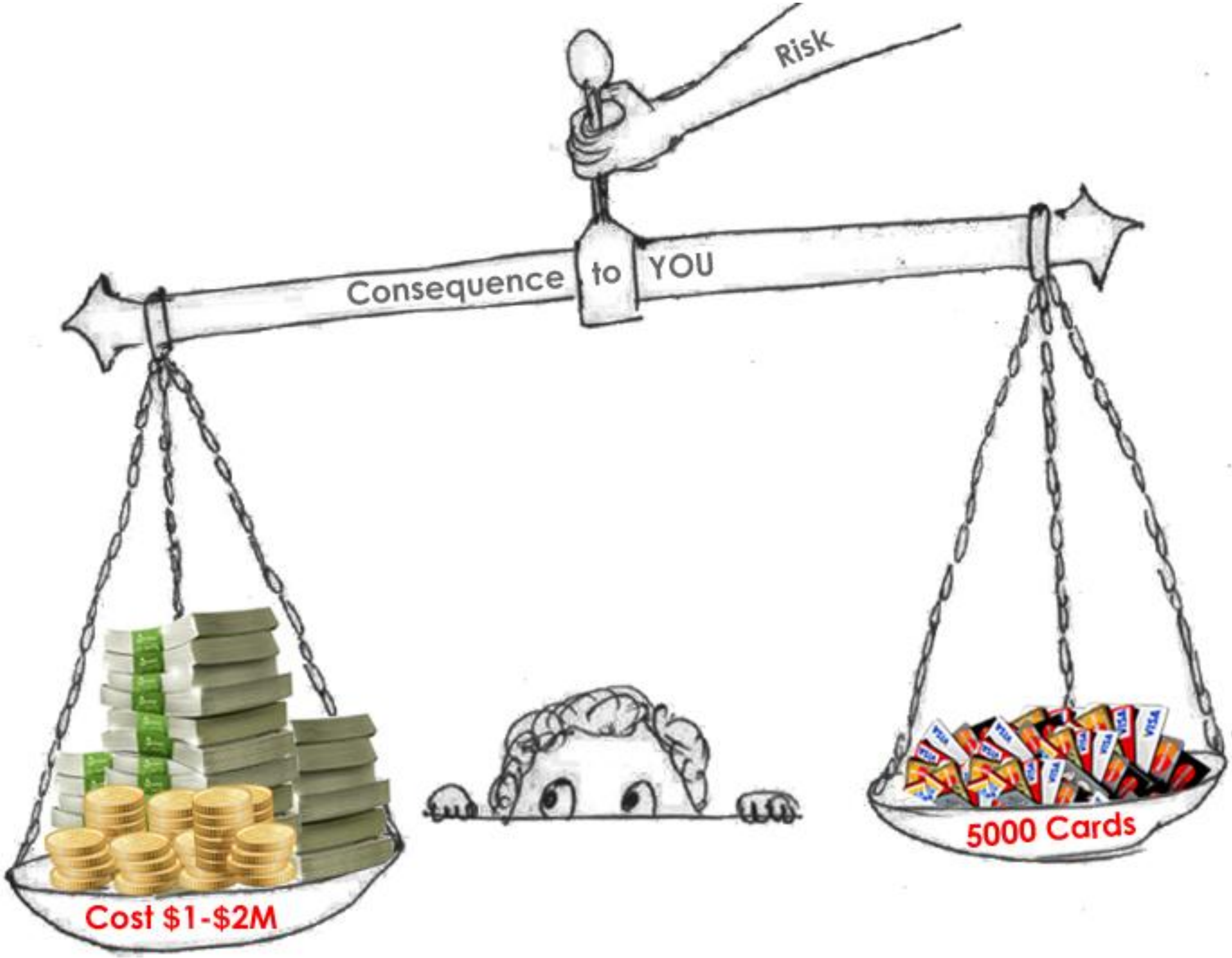
Server Data

data breach report summary

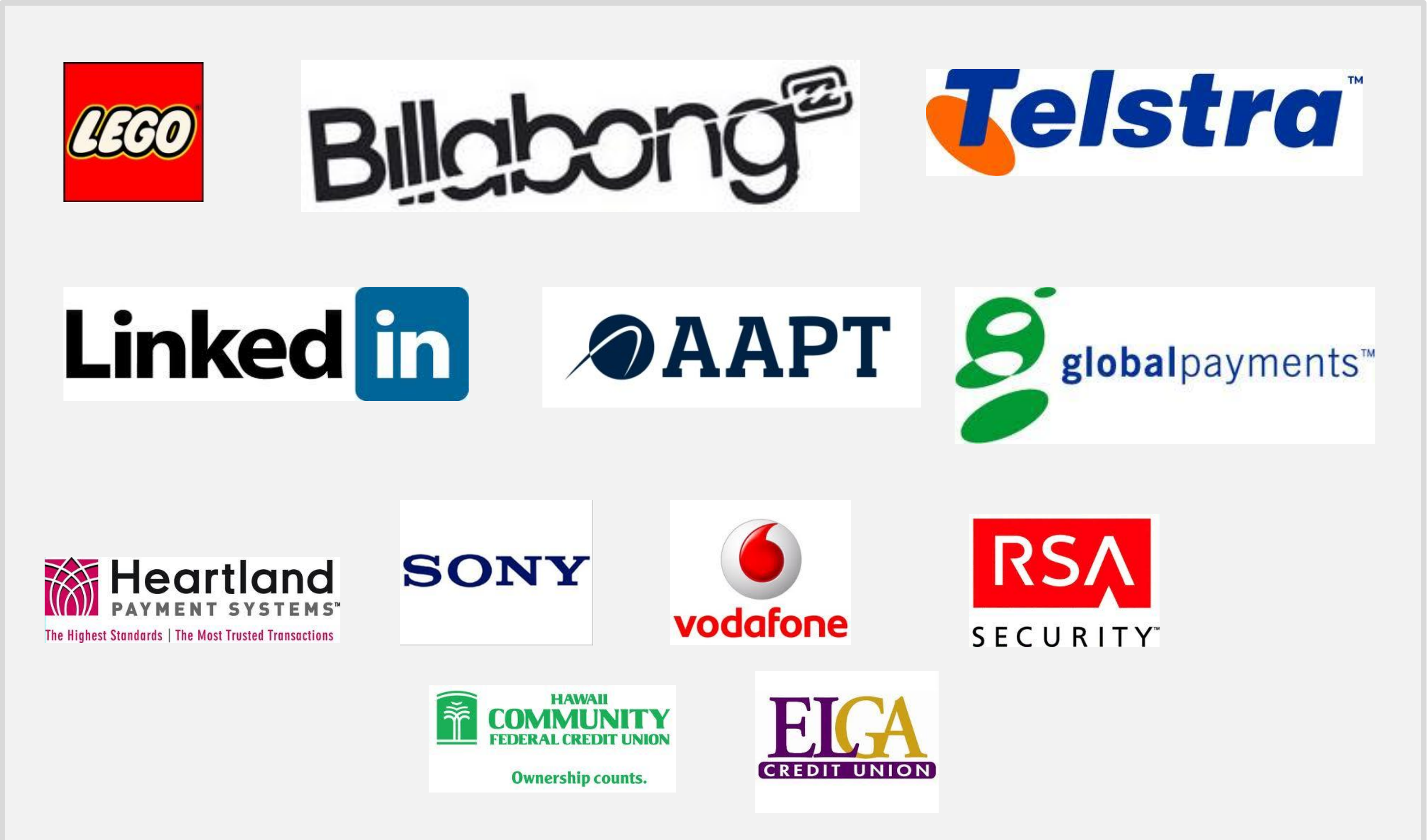
Discovered By

Non Compliant

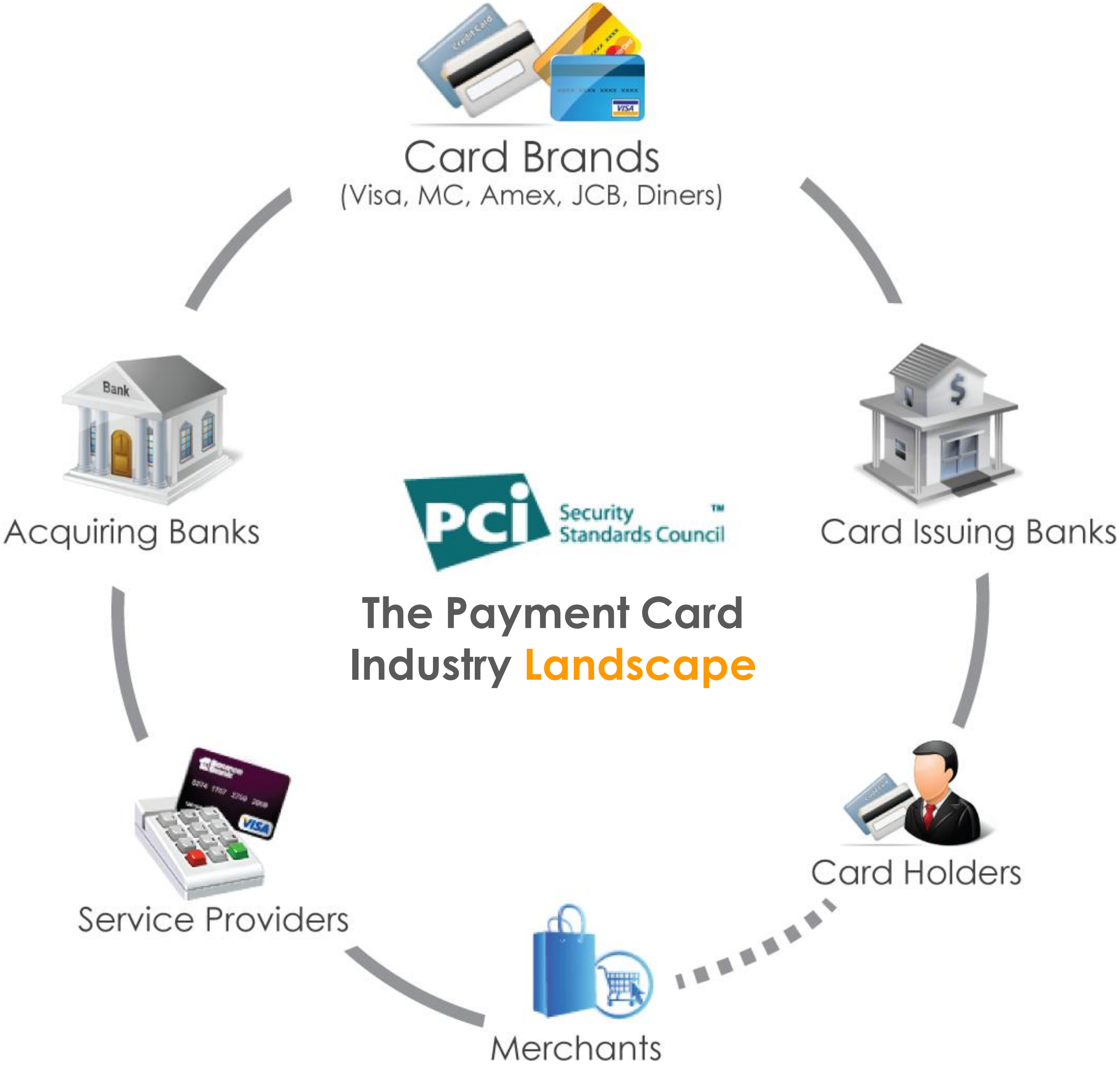
data breach consequences


Risk
Consequence
to
YOU
Cost $1-$2M
5000 Cards

companies recently affected by data breach


LEGO
Billabong
Telstra™
LinkedIn
AAPT
globalpayments™
Heartland PAYMENT SYSTEMS™
The Highest Standards | The Most Trusted Transactions
SONY
vodafone
RSA SECURITY™
HAWAII COMMUNITY FEDERAL CREDIT UNION
Ownership counts.
ELGA CREDIT UNION

The Payment Card Industry Landscape



Card Brands
(Visa, MC, Amex, JCB, Diners)

Card Issuing Banks

Card Holders

Merchants

Service Providers

Acquiring Banks

PCI Security Standards Council™

STICKMAN® CONSULTING
Keeping your payment card world secure and compliant

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

service providers

Call Centres

Data Storage Entities

Software Vendors

Back Office Services

Data Centres

Third Party Processors

Payment Processing

Hosting Providers

Software Vendors

Issuer Processing

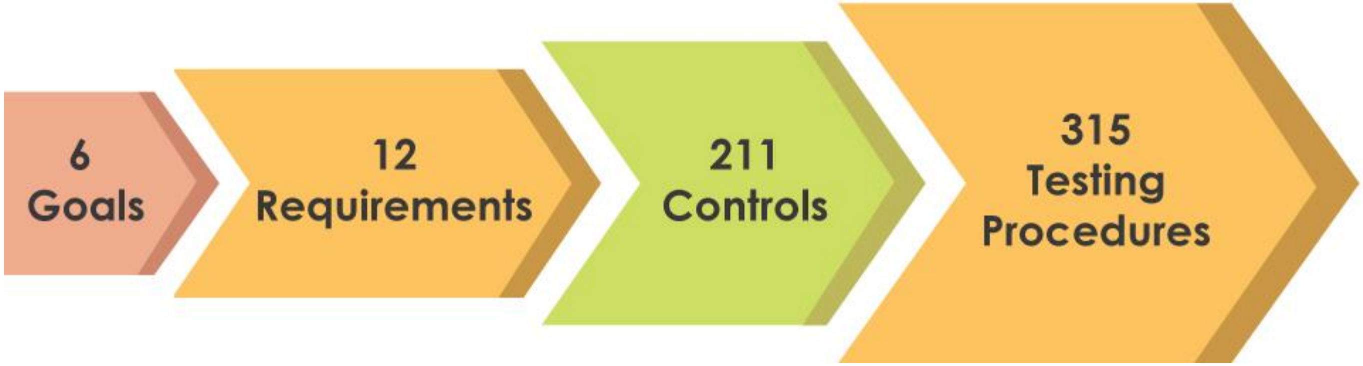
Fraud and Chargeback Services

Loyalty Programs

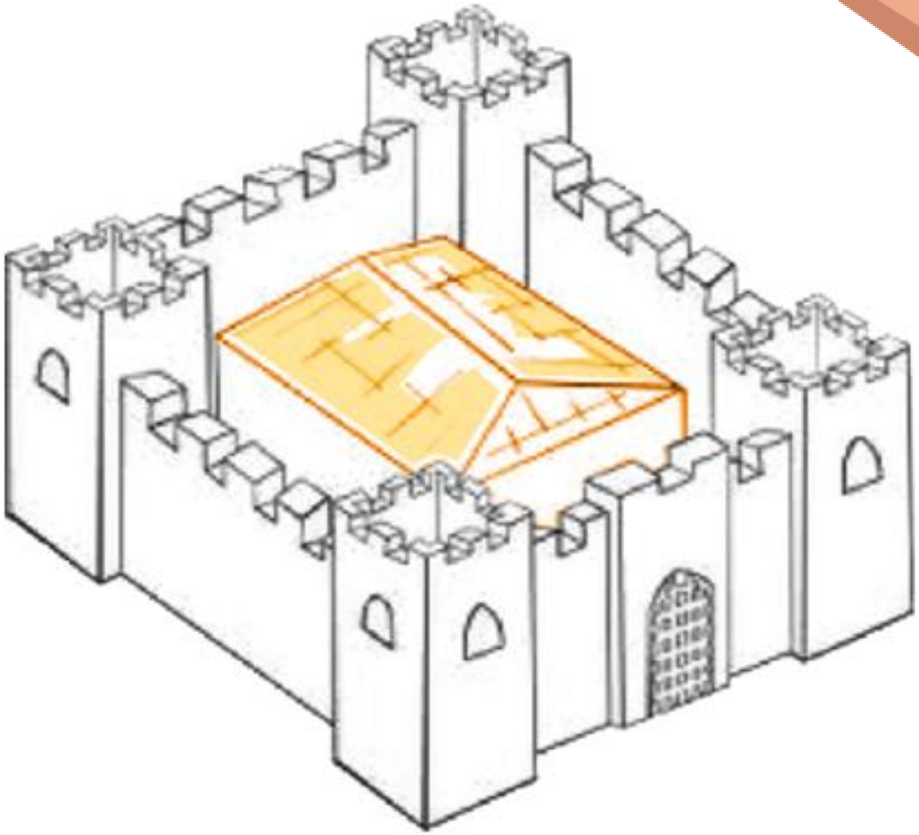
Records Managemen

risk mitigation

Payment Card Industry Data Security Standards (PCI DSS) Compliance

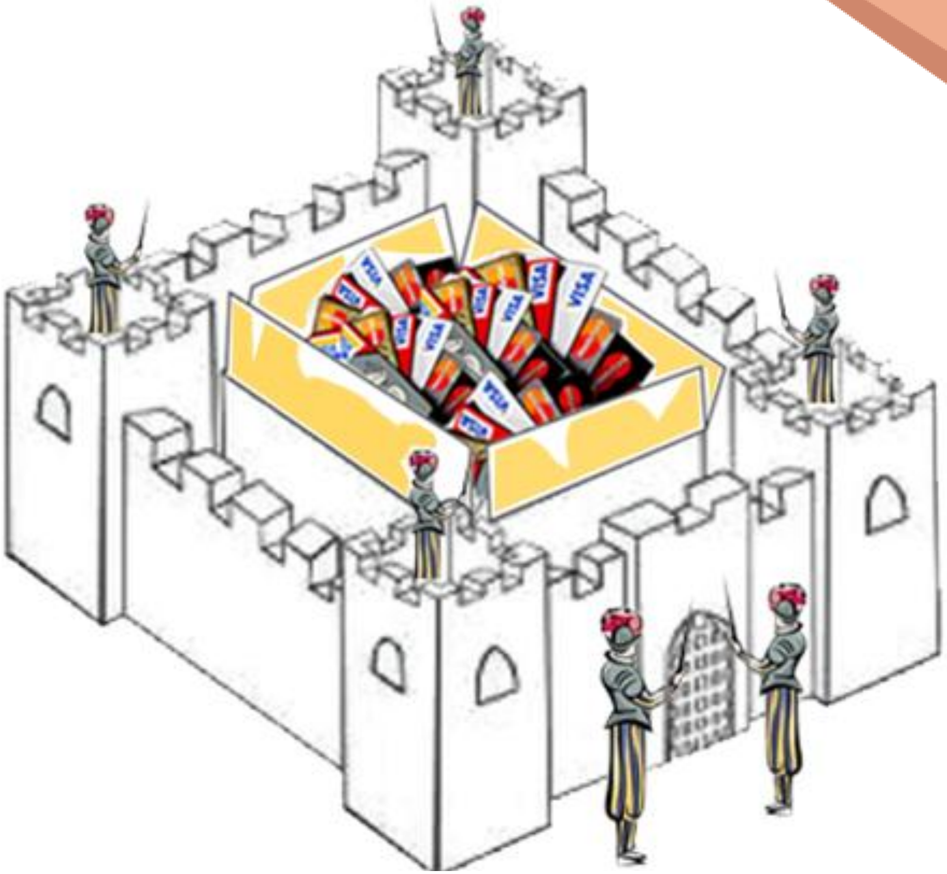


PCI
6
Goals



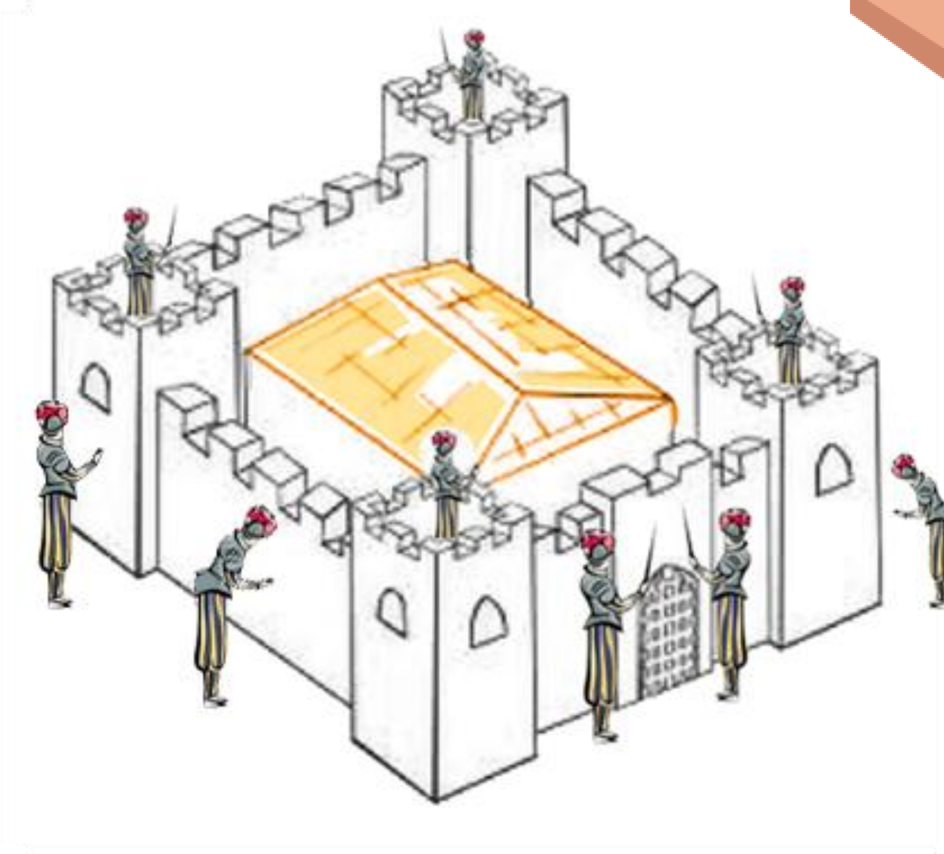
1. Build and Maintain a Secure Network

PCI
6
Goals



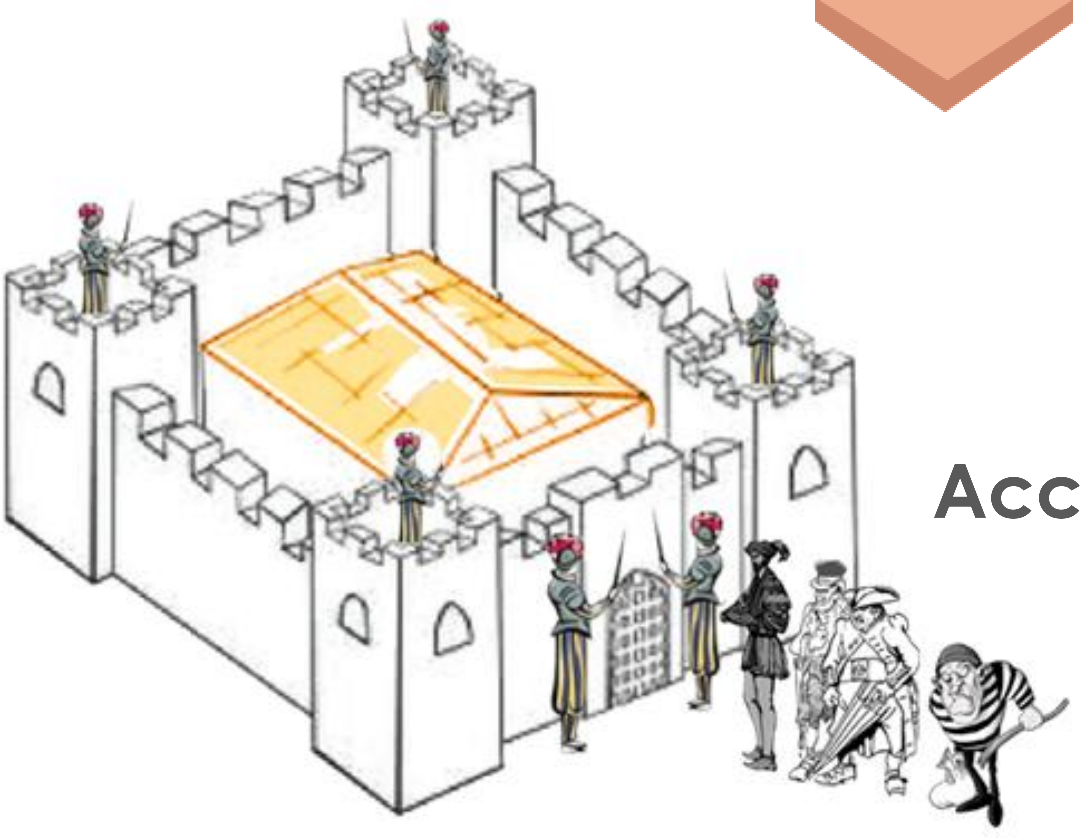
2. Protect Cardholder Data

PCI
6
Goals



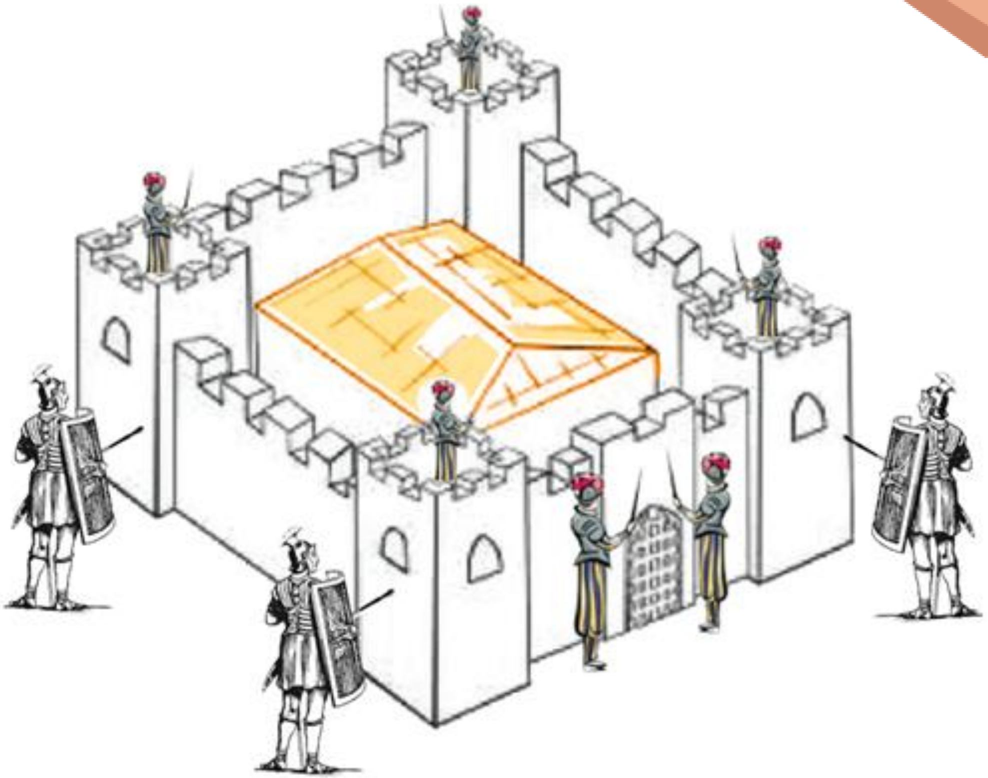
3. Maintain a Vulnerability Management Program

PCI
6
Goals



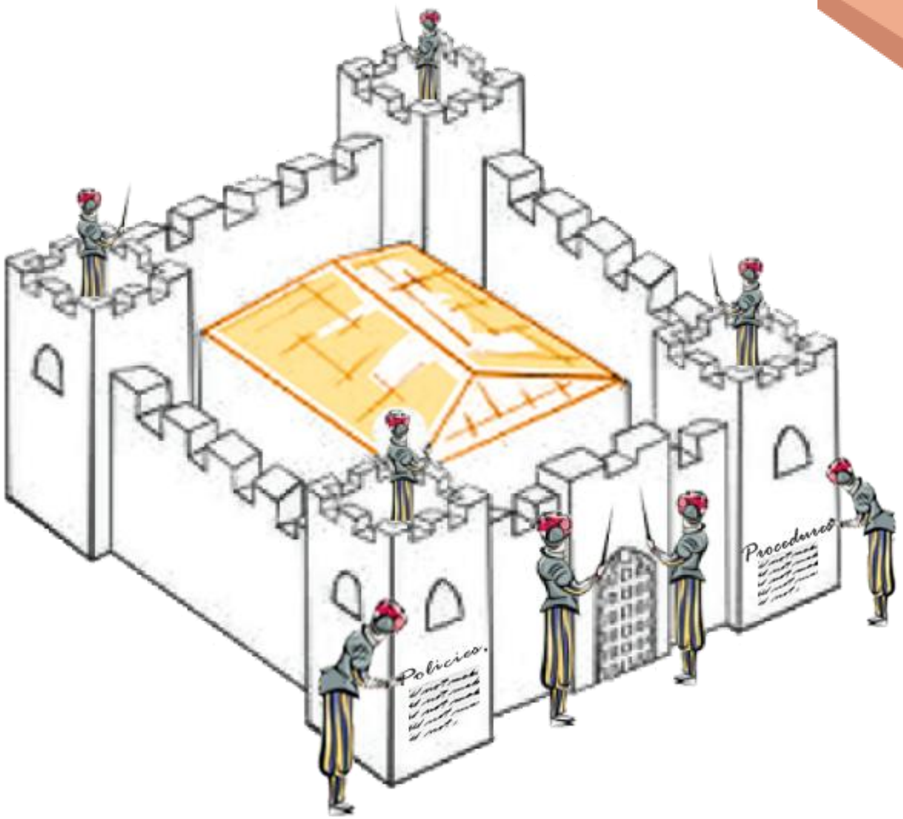
4. Implement Strong Access Control Measures

PCI
6
Goals



5. Regularly Monitor and Test Networks

PCI
6
Goals



6. Maintain an Information Security Policy

the five stages of grief in a PCI project

1. Denial

2. Anger

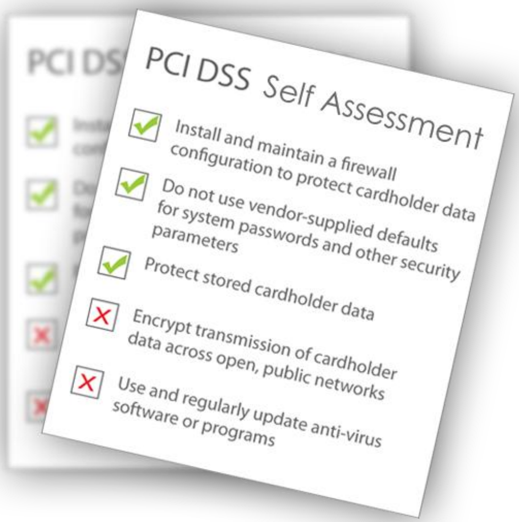
3. Bargaining

the five stages of grief in a PCI project

4. Depression

5. Complacency

PCI DSS myths



PCI DSS Self Assessment

☑ Install and maintain a firewall configuration to protect cardholder data

☑ Do not use vendor-supplied defaults for system passwords and other security parameters

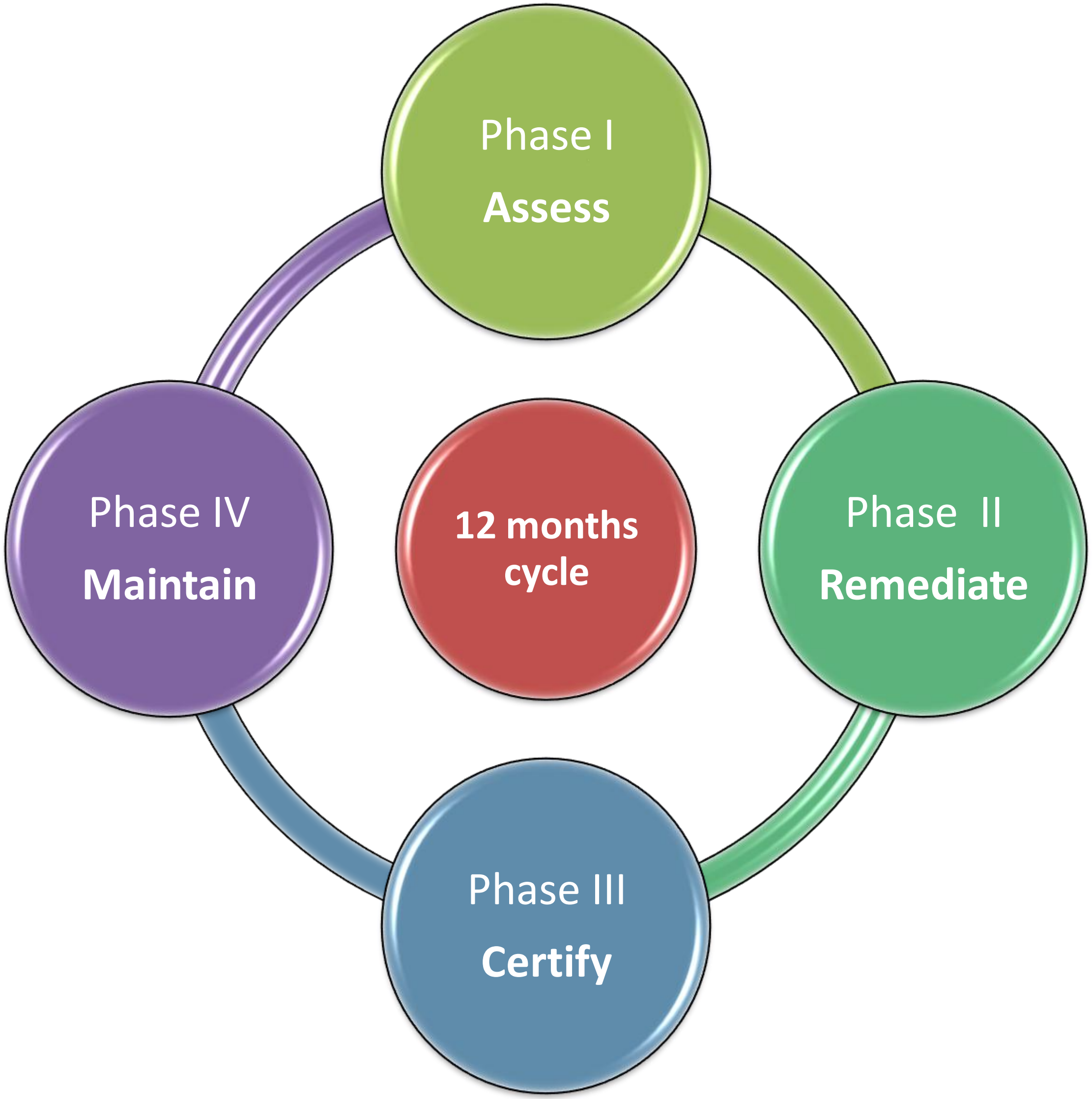
☑ Protect stored cardholder data

☒ Encrypt transmission of cardholder data across open, public networks

☒ Use and regularly update anti-virus software or programs

Outsourced

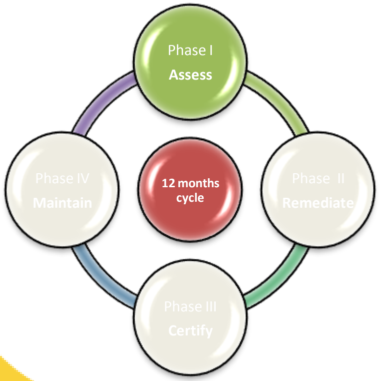
PCI action Plan



scan | data network | assess | gaps | remediation plan

Phase I

Assess



Phase I
Assess

12 months cycle

Phase II
Remediate

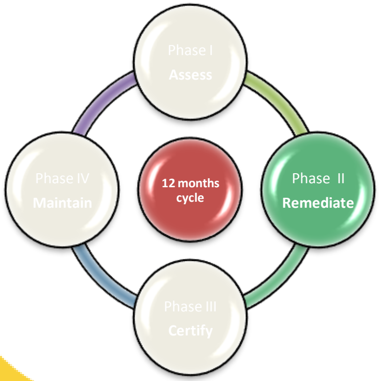
Phase III
Certify

Phase IV
Maintain

remove | reduce | evaluate | implement | scan

Phase II

Remediate



Phase I
Assess

Phase II
Remediate

Phase III
Certify

Phase IV
Maintain

12 months cycle

Phase III

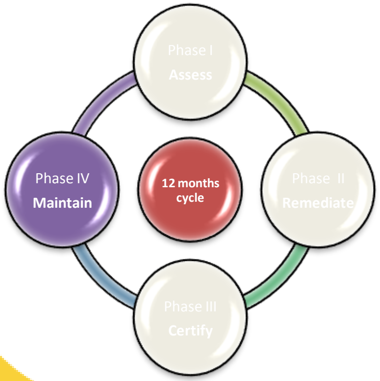
Certify

Phase I
Assess
Phase II
Remediate
Phase III
Certify
Phase IV
Maintain
12 months cycle

logos| file integrity| vulnerability| penetration testing router| firewall | annual assessment

Phase IV

Maintain



inform | investigate | communicate | assess | remediate

Data Breach
Actions

Compliance Management Portal

StickSecure

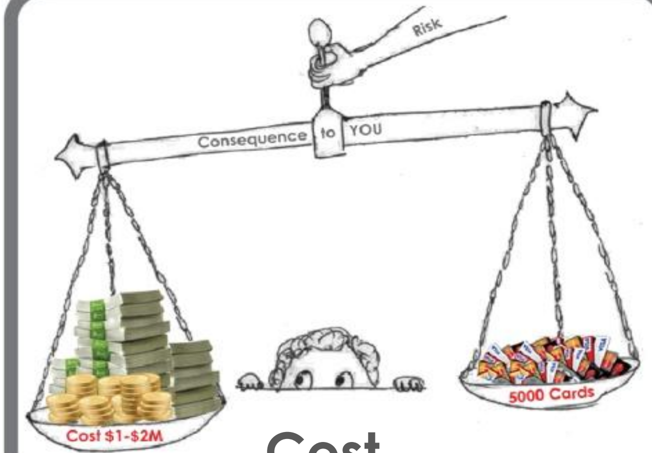
PCI Security and compliance. Simplified.

StickSecure.com

Data Security Risk Summary

Opportunistic

Negligence



Cost

Reputation

STICKMAN® CONSULTING

Keeping your payment card world secure and compliant

PCI Security Standards Council™ QUALIFIED SECURITY ASSESSOR

Thank You

1800 PCI HELP

Ajay Unni
ajay@stickman.com.au

Stickman Consulting

Australia I India I Middle East I Africa

sales@stickman.com.au I pcihelp@stickman.com.au

Call us: 1800 STK MAN | 1800 PCI HELP
1800 785 626 | 1800 724 435

www.stickman.com.au

PCI Security Standards Council™ QUALIFIED SECURITY ASSESSOR