Current Cyber Threat Landscape

A look at current trends to inform payment security professionals

Dr. Berny Goodheart, Lab Program Manager
PCI Security Standards Council

PCI Security Standards Council®

The True Facts Of What We Are Up Against

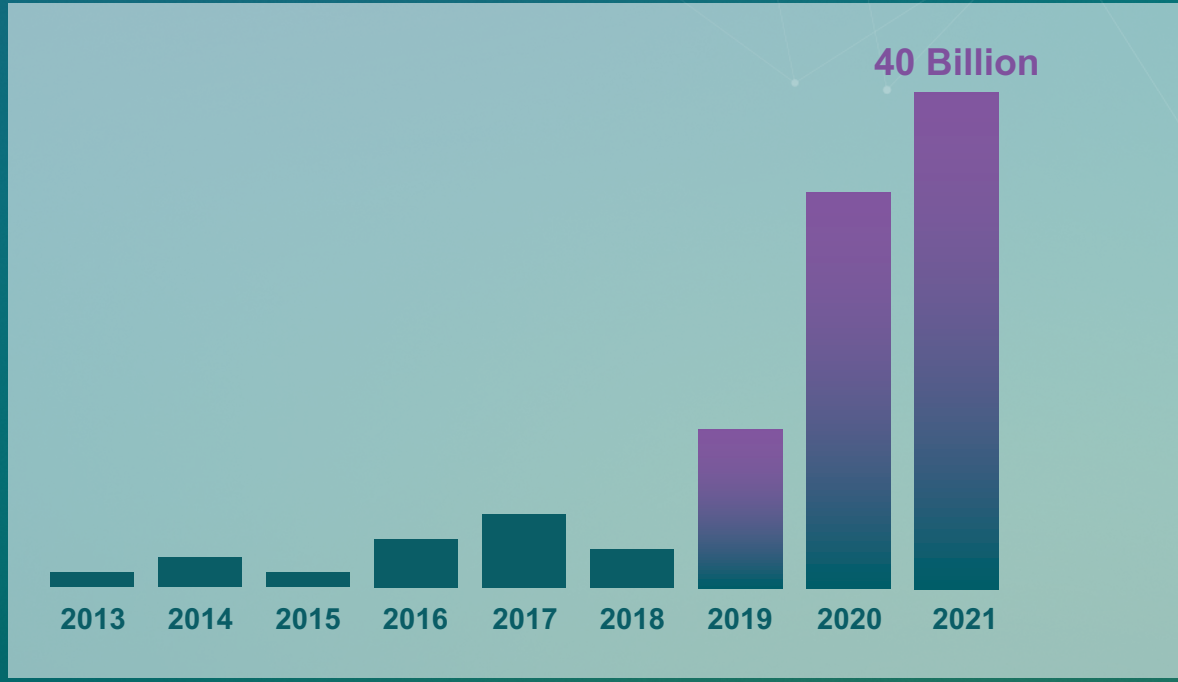
A record 40 Billion records were compromised by data breaches last year

In 2021, millions had their personal data & online accounts exposed due to attacks on healthcare, government, finance and retail databases. Data breaches are getting bigger…

– *…and hackers are getting smarter*

Any time a technology becomes adopted and popular, that technology will be targeted by the bad guys.

– *Jay Abbot, PrticewaterhouseCoopers LLP*



SOURCE: 2020 Year End Data Breach QuickView Report, Risk-Based Security Analytics

PCI Security Standards Council

What Do The Hackers Want?

Cyber attacks and data breaches happen hourly, if not every second!

Cyber criminals are attacking every kind of organisation small or large.

But what are the adversaries targeting?

To understand this, we need to understand what motivates them.

ID theft

Infrastructure theft

DDOS

Ransomware

Data loss

PCI Security Standards Council

Motivation

- PCI PTS POI standards have made it very difficult to hack POI devices directly. The effort is too great.
  - Whilst we must stay vigilant, the profits are not big enough for the hacking effort on these platforms anymore.
- **Ransomware** is high stakes, easier and much more profitable for the hackers.

IMPORTANT: even though large-scale hackers have moved to other opportunities, you should still maintain a security posture that is working…don't let your guard down.

$40,000,000

$570,000

Ransomware attack every 11 seconds

21 DAYS

On average 21 days to recover

https://www.infosecurity-magazine.com/news/ransomware-demands-surge-2021/

Ransomware Hidden Costs

- Downtime
- Customer support
- Replacement equipment
- Higher insurance
- Lost business
- Penalties and fines
- Loss of IP
- Repeat attacks

PCI Security Standards Council

IBM Security

Cost of a Data Breach Report 2021

IBM

Global Average cost of a data breach

$4.24M

Global Average cost per lost record

$161

Average cost of a data breach in the UK

$4.64M

Average time to contain a data breach

287 days

Average cost of a Mega-Breach

(1+ M records lost)

$52M

Mitigating The Attack Surface

Linux

- Boot security
- Patching Linux kernel
- Removal of unnecessary software
- Strong password policy
- Secure root login
- Process security
- Encrypted file system
- Secure APIs
- SE Linux

PCI Security Standards Council

Mitigating The Attack Surface

Android

- Apps run in their own JVM
- Apps are constricted by the underlying Linux OS
- Apps are restricted from interacting with other apps
- Apps present a significantly reduced attack surface to the OS
- Android allows for a security policy, which defines each App security intent
- Apps are developed using Java and Java has its own security features

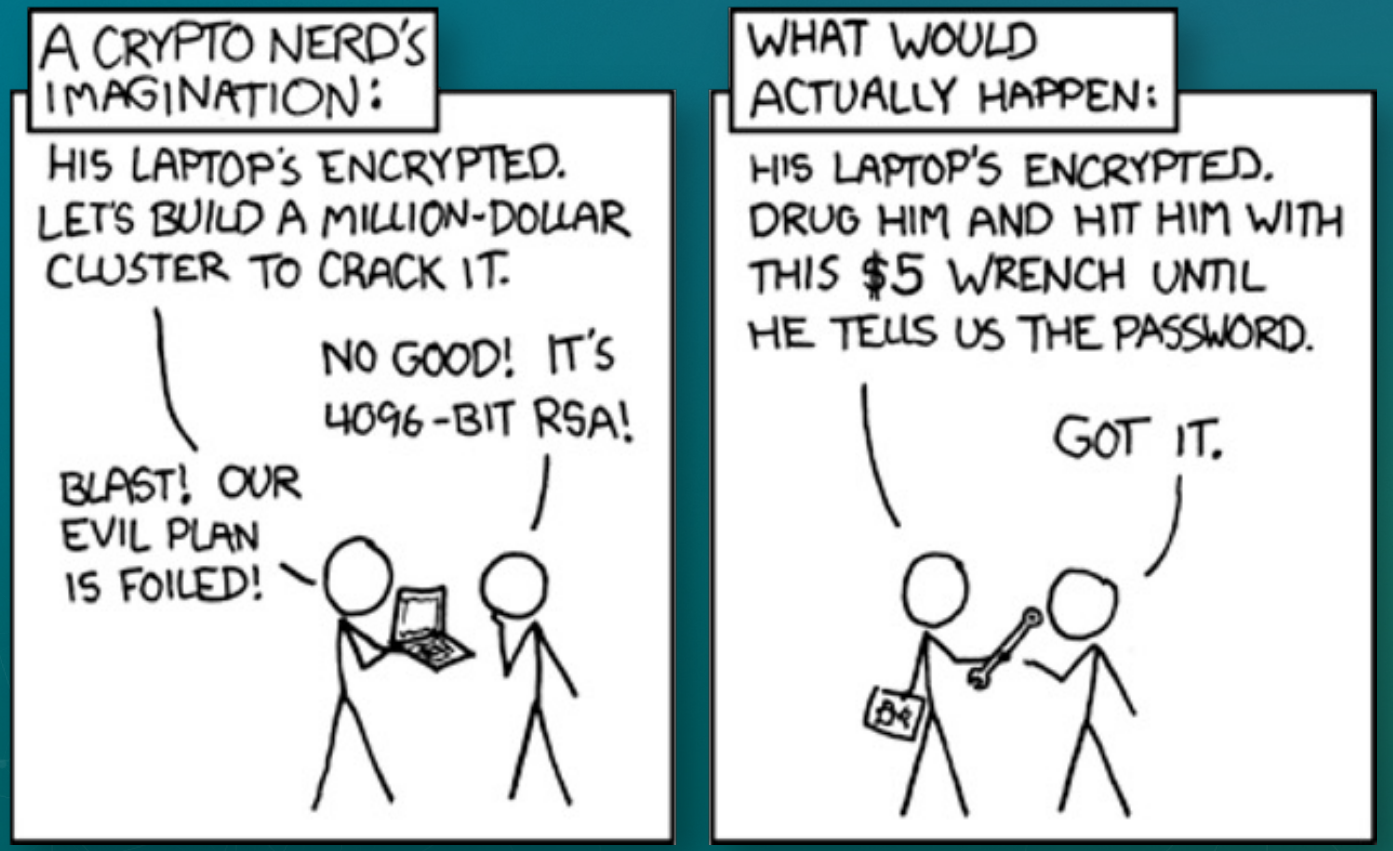
Mitigating The Attack Surface

iOS

- System Security
- Device Controls
- Secure Enclave
- Encryption and Data Protection
  - Support for pointer authentication (PAC)
- Application Security
- Network Security
- Apple Pay
- Privacy Controls
- Proprietary OS, code is closely guarded

PCI Security Standards Council

Mitigating The Attack Surface



xkcd.com/538

PCI Security Standards Council

Mitigating The Attack Surface

Multi-factor Authentication (MFA)

All modern cell phones now provide
for MFA via biometrics

Almost all banks in the UK now implementing MFA

Something
you HAVE

Something
you ARE

Something
you KNOW

PCI Security Standards Council

Mitigating The Attack Surface

PCI PTS POI v6.2

- Purpose built payment terminals hardened over decades
- All devices closely monitored
- All devices tamper protected
- Evaluated by strict conformance to PTS POI standards and approved Lab accreditation

PCI Security Standards Council

GDPR – Largest Fines

Global organization: **$847M**

Large social media company: **$255M**

Global search engine: **$102M**

Very large merchant retailer: **$41M**

Large airline: **$26M**

Large hotel chain: **$23M**

PCI Security Standards Council

State Sponsored Cybercrime

Actions benefit the attacking ‘state’

Focussed on:

Critical national infrastructure

Security and IPR

Very difficult to defend against

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Current Activity > Russian State-Sponsored and Criminal Cyber Threats to Critical Infras

State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

Original release date: April 20, 2022

Print Tweet Send Share

The cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom have released a joint Cybersecurity Advisory (CSA) to warn organizations that Russia’s invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity from Russian state-sponsored cyber actors or Russian-aligned cybercrime groups.

Joint CSA: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, drafted with contributions from industry members of the Joint Cyber Defense Collaborative, provides an overview of Russian state-sponsored advanced persistent threat groups, Russian-aligned cyber threat groups, and Russian-aligned cybercrime groups to help the cybersecurity community protect against possible cyber threats.

U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities urge critical infrastructure network defenders to prepare for and mitigate potential cyber threats by hardening their cyber defenses as recommended in the joint CSA.

For more information on current and historical Russian-state-sponsored cyber activity and recommended mitigations, see the following CISA webpages:

- Russia Cyber Threat Overview and Advisories
- Shields Up
- Shields Up Technical Guidance
- Joint CSA: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

PCI Security Standards Council

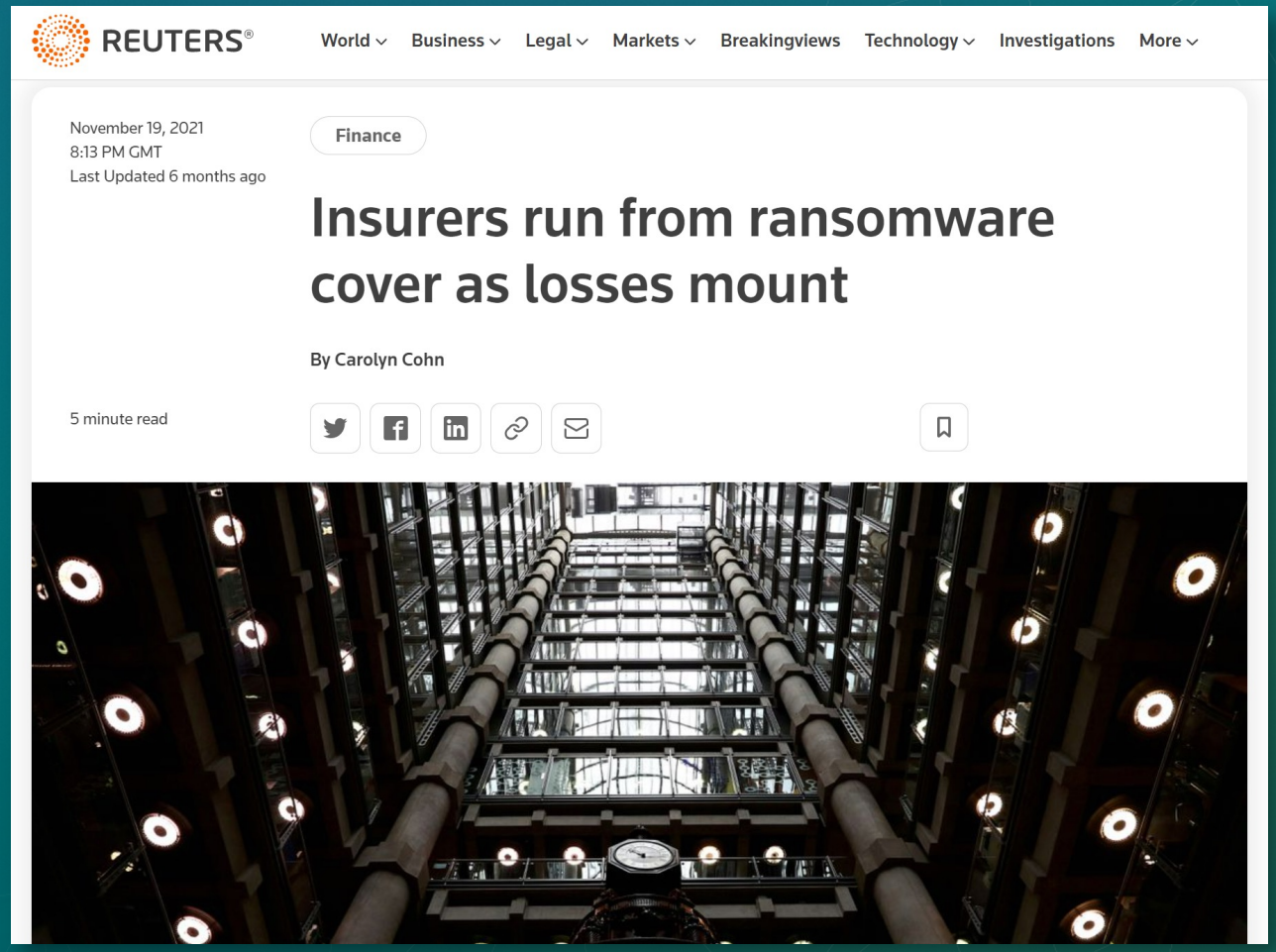
Cyber Insurance

Large number of pay-outs in 2021

Mainly due to ransomware

Resulting in:

- Premiums rising (50% or more)
- Coverage falling (50% or more)



PCI Security Standards Council

Summary

- Continue to follow the PCI security standards
- Develop best practices to mitigate against cyber attacks
- Develop a standard to provide for a global cyber-secure platform
- Work and align with other national security and intelligence agencies
  - FBI
  - NSA
  - UK Cyber Security Council
  - GCHQ
  - Australian Cyber Security Centre
  - Israel National Cyber Directorate
  - …

PCI Security Standards Council