RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **RMG-R08**

Securing your M&A Activity with Cyber Security Due Diligence

Murray Goldschmidt

Executive Directory, Cyber Capability
CyberCX.com.au

RSAConference2020 APJ

A Virtual Learning Experience

Buy Side – Cyber Security Due Diligence

Raised Risk Profile

- Type of Deal
- Cross Border
- Profile of Buyer and Seller
- Supply Chain Position
- Regulatory Oversight
- Nation State Interest (Buy/Sell)

Deal Room/Virtual Data Room

- Jurisdiction
- Data Storage
- Data Retention
- Access Controls
- Application Security

Deal Room - Jurisdiction

- Care required!
- Cross border deals
- Local deals with foreign
- Note the requirements

under your Privacy Act

Deal Room – Data Governance

- What data is being collected?
- Data (re)identification
- Breach notification obligations
- Who has access to What data?
  - At the Service Provider
  - Buy Side, Sell Side
  - External Advisors
- Audit, Logging, Monitoring

Deal Room – Data Retention

- Data Persistence
- Access Controls
- Continuous Backup
- Mirroring & BCP
- Crypto Controls
- Key Access & Mgt

CyberCX

Deal Room – Access Control

- MFA, MFA, MFA
- Not on by default!
- Weakness in SMS & Email
  - Esp if your email doesn't have MFA
  - Hard to know when dealing with multiple parties
- Preference for supe ods

https://auth0.com/learn/two-factor-authentication/

CyberCX

Deal Room – Application Security

- Nested Service Provider issues

(esp with Cloud Deployments)

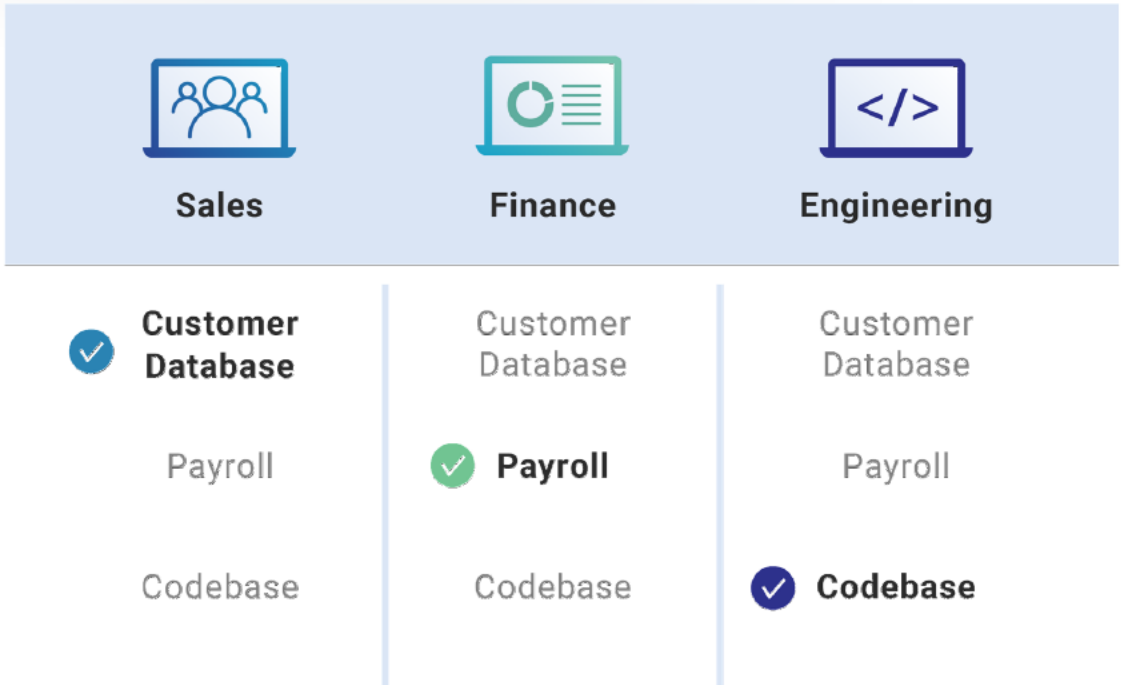
- Multitenancy Security
- Service Provider Compliance
  - Can this be relied on?
  - How thorough?
  - Can you review the security assessment and pen test reports?
- Can conduct your own pen tests?
- Do you have time? And if there are issues then what?

Buy Side - Advisors

- Advisors increase the footprint of Buy/Sell Side – OSINT
- Can be quite extensive
- Each side has
  - Lawyers & Accountants
  - Others
    - Property
    - IP Specialists
    - Tech Specialists
    - Insurance
    - etc

Buy Side – Internal Deal Desk

- Role Based Access Controls
- Business need to know
- Increase in footprint – OSINT
- GRC Levers to Pull?



General Deal Risk – Extension to Cyber

- Tech Debt
- Business Integration
- Supply Chain
- Increased footprint
- Vulnerability Management
- Threat Intelligence

- Does the new business change the business Threat Profile?

RSAConference2020 APJ

A Virtual Learning Experience

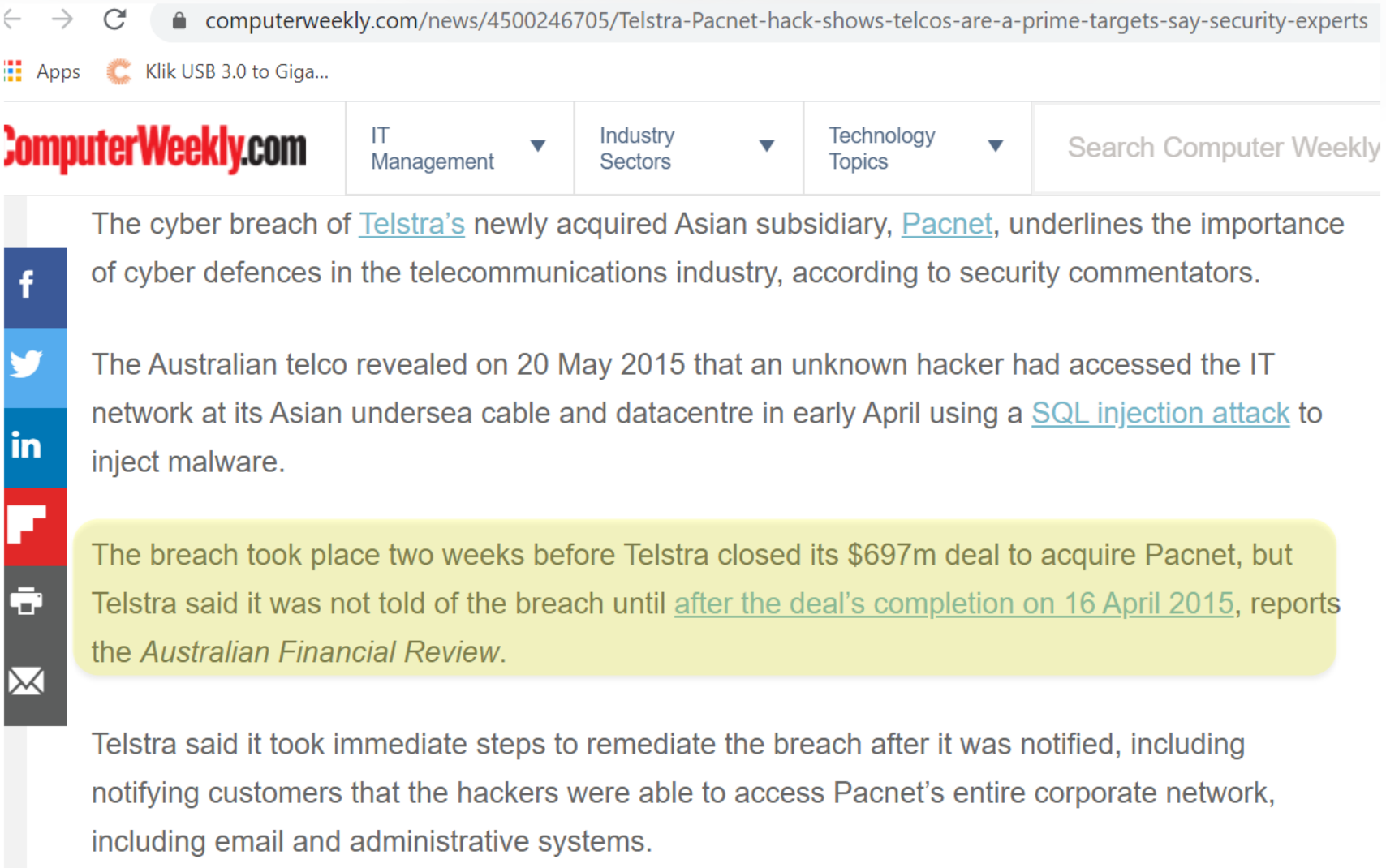
Reference Cases

Marriott – Starwood Data Breach

Cloud misconfigurations can cost you big. Take a look at the example of Marriott. In 2016, there was a huge merger between Marriott and Starwood Hotels. In September 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database. The ensuing investigation revealed that there had been unauthorized access to the Starwood network since 2014. Every company should have in place the people, processes and tools to support day zero evaluation of cloud security during a mergers and acquisitions (M&A) event. Without this you leave yourself open to massive financial, regulatory, and reputational risk.

https://dbac8a2e962120c65098-4d6abce208e5e17c2085b466b98c2083.ssl.cf1.rackcdn.com/cloud-security-during-mergers-acquisitions-pdf-6-w-6010.pdf

Telstra - PacNet



The cyber breach of Telstra's newly acquired Asian subsidiary, Pacnet, underlines the importance of cyber defences in the telecommunications industry, according to security commentators.

The Australian telco revealed on 20 May 2015 that an unknown hacker had accessed the IT network at its Asian undersea cable and datacentre in early April using a SQL injection attack to inject malware.

The breach took place two weeks before Telstra closed its $697m deal to acquire Pacnet, but Telstra said it was not told of the breach until after the deal's completion on 16 April 2015, reports the *Australian Financial Review*.

Telstra said it took immediate steps to remediate the breach after it was notified, including notifying customers that the hackers were able to access Pacnet's entire corporate network, including email and administrative systems.

PayPal - TIO

databreaches.net/update-tio-networks-notifies-consumers-of-breach-going-back-to-2014-or-earlier/

pps Klik USB 3.0 to Giga...

DataBreaches.net
The Office of Inadequate Security

OCTOBER 24, 2018 DISSENT

TIO Networks USA was acquired by PayPal in July, 2017. Months later, they reported, services were suspended after discovery of vulnerabilities. Investigation into those vulnerabilities resulted in TIO having to report that it had been hacked by 2014 and possibly earlier. According to information provided in December, 2017, 1.6 million consumers were affected.

TECH

PayPal shelled out $238 million for company that may have had 1.6 million customers breached

Elizabeth Weise USA TODAY

Published 12:04 p.m. ET Dec. 4, 2017 | **Updated 5:27 p.m. ET Dec. 4, 2017**

SAN FRANCISCO — A payment processing company acquired by PayPal has revealed that as many as 1.6 million of its customers may have had personal information stolen in a data breach.

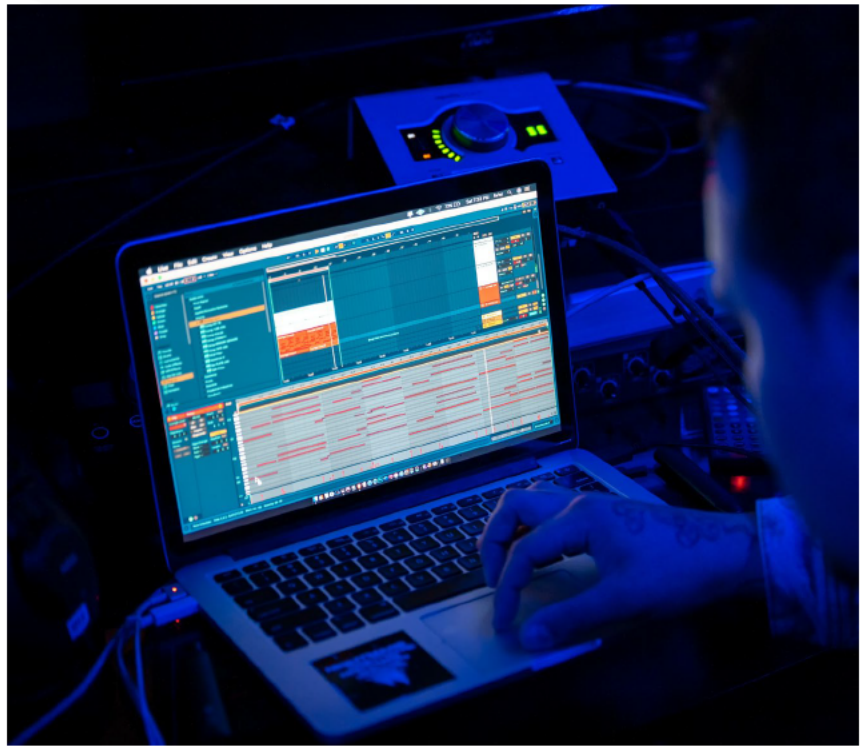
RSAConference2020 APJ

A Virtual Learning Experience

Sell Side – Cyber Security Due Diligence

Supply Chain

- Software
  - Do they have external software development
  - Where is the code?
  - Who has access to it?
  - How secure is the code?
  - Are you acquiring a product that is manifestly insecure?
- Hardware
  - Do they have hardware developed by external parties?
  - With hardware comes software risks as well.
  - How is this monitored and controlled?
- Services
  - Do they have outsourced parties with privileged access to their environments?
  - How is remote access and privileged access management controlled



Data

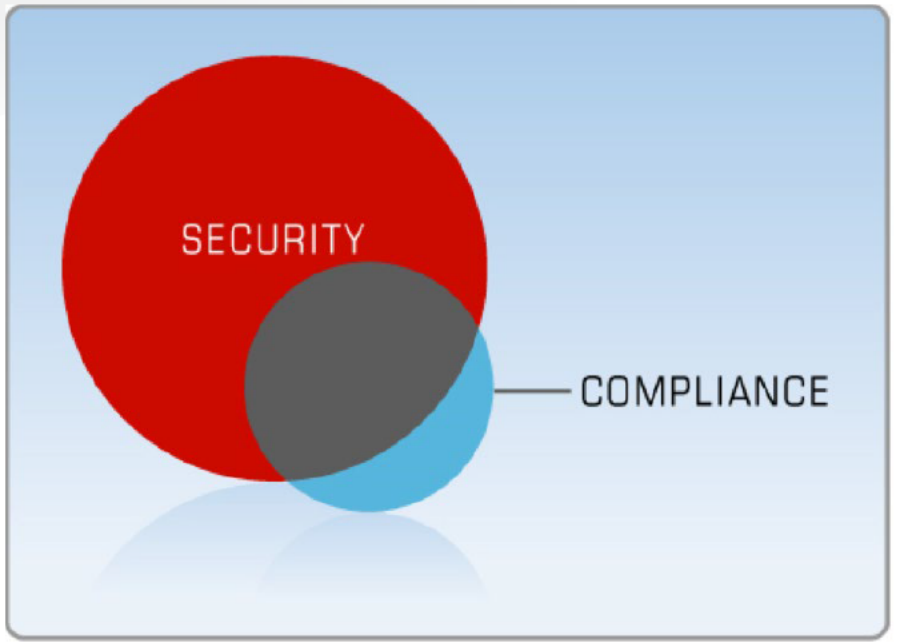
- Do they have good control of their data?
- Data management models?
- Data custodians?
- Data protection management
- Where is the data?
- How is it protected?

- Extremely complicated with Cloud environments, replicated environments, mobile workers, mobile devices, laptops etc

Sell Side – Security Testing Validation

- Supply previous pen tests?
- Can you rely on them? There are Pen Tests and there are PEN TESTS
- Was the scope adequate?
- Can you conduct your own tests?
- Can you conduct a Red Team Test?
- Do you have the time?

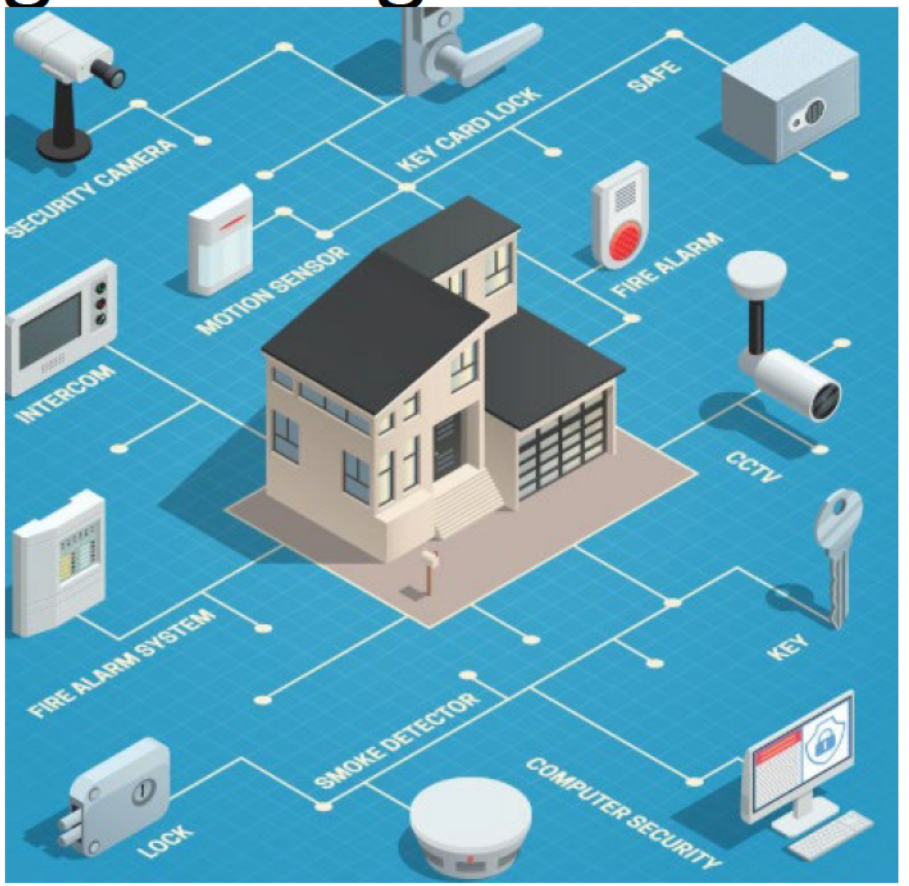
Difference between Compliant and Secure!

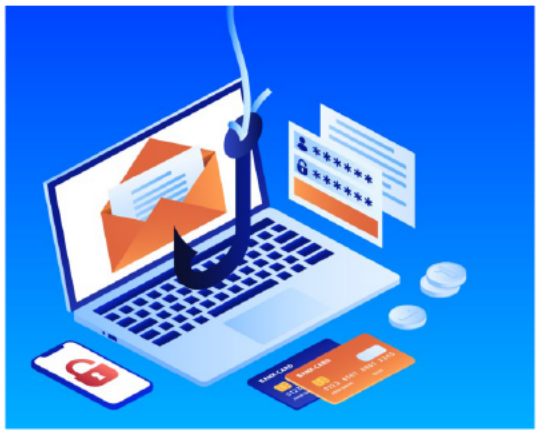


- Buyer Beware
- Compliant DOESN'T MEAN Secure
- Need to understand what compliance and certifications are in place
- E.g. Difference between PCI DSS, ISO 270001, ISM
- Scope of Compliance vs Scope of Acquisition.
- Compliance scope can sometimes be purposefully narrow

Sample Test – Dynamic Risk Assessment

- Reconnaissance incl Intelligence gathering
- Social engineering
- Physical security assessments
- Digital attack vectors





CyberCX

Sample Test – Dynamic Risk Assessment

- Goals for Persistence
- Goals for Data/IP Identification
- Determination if SecOps/Monitoring is working
- Ability to Exfiltrate data?

Cyber DD – Insights You Need to Know

- Living off the Land
- How to compromise an environment with no vulnerabilities
- Highlights Blinds Spots in Compliance
- Highlights Blinds Spots in SecOps/Outsourced Managements
- Simulates attack vectors you can expect post acquisition
- Could make Financial and Legal DD less relevant

RSAConference2020 APJ

A Virtual Learning Experience

Apply the learnings to practical outcomes

Apply – Buy Side

- Next week you should:
  - Assess data room technologies. Select based on capability, resilience, track record, authentication and access control options.
  - Identify your 3rd party footprint (Lawyers, Accountants, Advisors etc.)
- In the first three months following this presentation you should:
  - Establish firm protocols for Data Room access incl 3rd Party
  - Validate security of your 3rd party ecosystem
  - Implement robust cyber security assessment plan for acquisitions
  - Test your own incident mgt/response capability

Apply – Sell Side

- Next week you should:
  - Be prepared for the more astute buyer
  - Assess data room technologies. Select based on capability, resilience, track record, authentication and access control options.
  - Prepare your GTM approach so that buyers follow your lead
- In the first three months following this presentation you should:
  - Appoint a firm to conduct a Red Team Test
  - Validate your compliance position & map to technical controls & validate they are working
  - Demonstrate that incident mgt and response is effective
- Within six months you should:
  - Implement threat mgt and continuous monitoring to demonstrate your ongoing visibility of security issues so that there are no surprises for buyers

RSAConference2020 APJ

A Virtual Learning Experience

Murray Goldschmidt
Executive Director
CyberCX Pty Ltd
info@cybercx.com.au
Mobile: + 61 422 978 311