

Accelerating Physical – Cyber convergence

AIPIO Conference

20 Aug 2019





**Wayne
Forgesson**

- ▷ **Chief Executive Officer and Co-Founder of Signal Corporation Limited**, a New Zealand based organization that designs, develops and maintains the Signal online application.
- ▷ Signal is a Software as a Service application that enables organisations to discover relevant information from a variety of sources including social media, public internet sites, the Dark and Deep web.
- ▷ Signal customers include Fortune 500 Corporations (U.S), Australia/New Zealand Companies, Emergency Management and Public Safety Agencies
- ▷ Prior to Signal Corporation, Wayne was co-founder of Interagen, a multi award winning New Zealand based systems integrator.

Signal

Intelligence gathering solution

for organisations with distributed workforces,
regulatory compliance requirements

and that care about employee safety, cyber security
and intellectual property.

Playing your part in Cyber – Physical convergence

Physical Security: What's changing

- ▶ Access
 - ▶ Credentials – electronic/online
 - ▶ Building security – video/online
- ▶ Safety
 - ▶ Employee Safety – social/personal data
 - ▶ Executive security – online threats/attacks
- ▶ Physical
 - ▶ Environment – information at the speed of data
 - ▶ Company locations – virtual/work from home



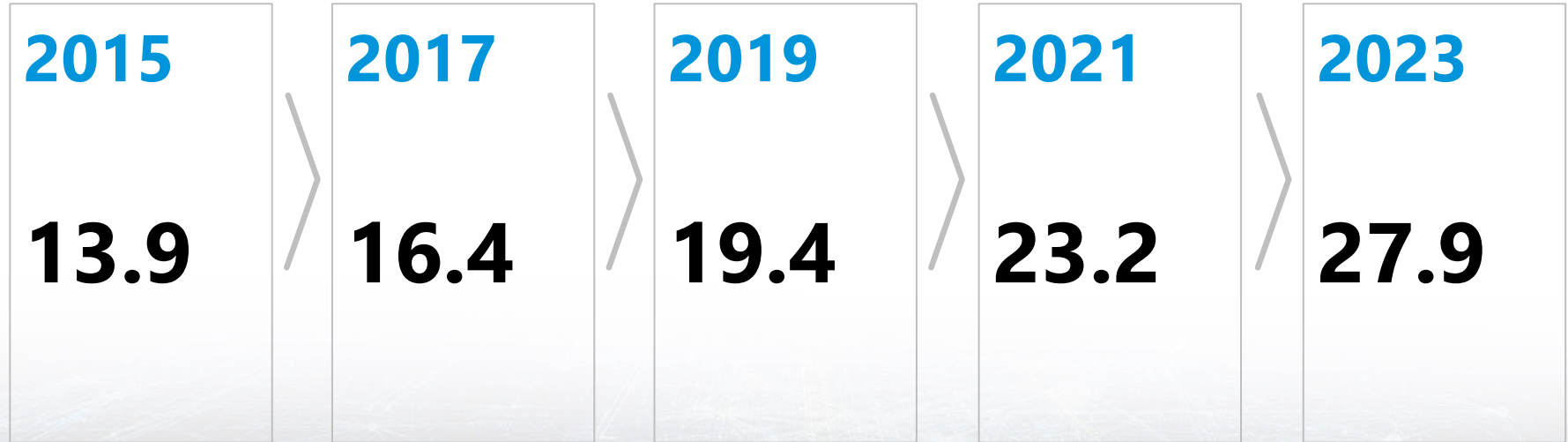
Cyber Security: What's changing

- ▶ Defence
 - ▶ Local and Wide area networks – BYOD
 - ▶ Internet connections – Café's/remote workers
 - ▶ Data protection – collaboration
- ▶ Detection
 - ▶ Intrusion detection – advanced warnings
 - ▶ Identity and access management – published online
 - ▶ Anti-virus/malware – personal devices



Rapid pace of change: Internet Connected devices

Internet device connections (in billions)



Source – IOT-analytics.com 2018

Rapid pace of change: Attack footprint is increasing

- ▶ If 'Everything is a Computer'
- ▶ Everything is a target
- ▶ "Data is the new oil" – The Economist
- ▶ The worlds most valuable resource is now data

- ▶ Medium time to detect cyber breaches

146 days



Cyber : Example – Capital One

- ▶ Hack published 21 April
- ▶ Hacker boasted online social media & forums
- ▶ Capital One alerted 17 July by GitHub user
- ▶ 106 Million individuals impacted including social security numbers
- ▶ Estimated cost \$150 million USD
- ▶ Previous Capital One breaches;
 - ▶ November 2014,
 - ▶ July 2017,
 - ▶ September 2017

87 days



Cyber : Business impact

- ▶ Average data breach cost has risen to \$3.92 million

**\$3.92
million**

(IBM 2019 cost of
data breach report)

Cyber : the Most Devastating Cyberattack in History?

- ▶ 27 June 2017 NotPetya Malware strikes
- ▶ Within 2 hours ALL Maersk computers and digital phones turned off
- ▶ 800 Maersk's seafaring vessels – tens of millions of tons of cargo – dead in the water
- ▶ Unintended consequences of Russian Cyber War on Ukraine
- ▶ Maersk IT basically built a new infrastructure from the ground up
- ▶ Merck, TNT Express, Saint-Gobain, Mondelez, Reckitt Benckiser

**\$10 billion
worldwide
damages (est)**

Maersk IT systems are down

We can confirm that Maersk IT systems are down across multiple sites and business units due to a cyber attack. We continue to assess the situation. The safety of our employees, our operations and customer's business is our top priority. We will update when we have more information.



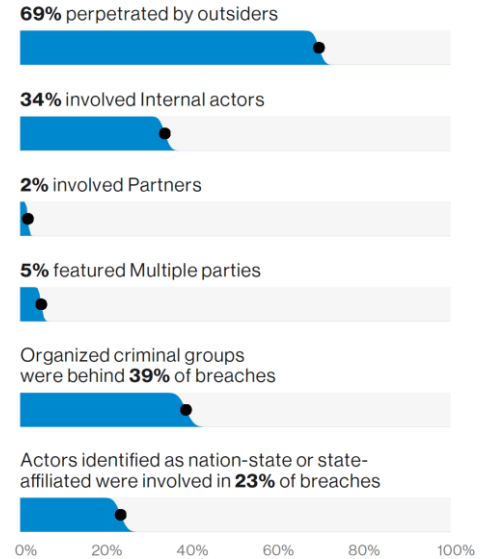
Follow our Twitter feed for more information.

[Read the post](#)

Cyber : Beware the insider

- ▶ 34% of breaches involved Internal actors

> 1 in 3



Breaches

Figure 4. Who's behind the breaches?

Source – 2019 Verizon Data Breach Investigations Report

Cyber : Beware the insider

- ▶ 34% of breaches involved Internal actors

10 hours ago
Westpac Australia worker Hello, I'm looking for someone on the inside to provide me with some info. I have a competitor that banks with Westpac and I want to know where he get his supply from. Just go through his statement, write down the name of the companies he make his payment to. That's all.

- ▶ Air NZ - accidental by staff
 - ▶ 112,000 customers – All their top flyers
 - ▶ 9 days to notify customers
 - ▶ Access to internal documents via phishing attack



Cyber : We are safe, only the banks are targets!

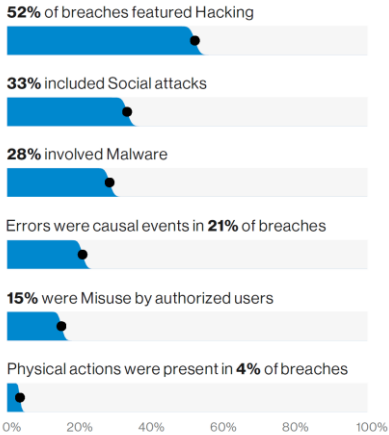
- ▶ “Nothing of value at Government Agencies”
- ▶ “Small Companies are immune”



Figure 2. Who are the victims?

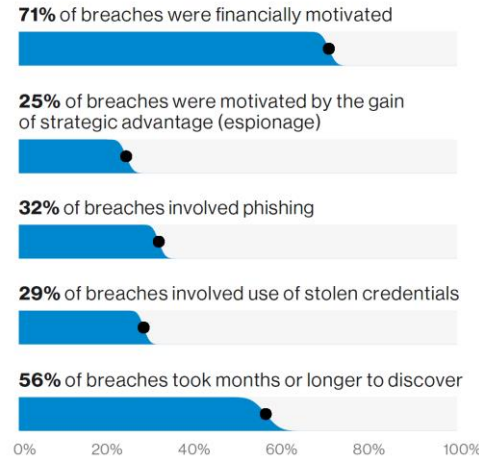
Source – 2019 Verizon Data Breach Investigations Report

Stats: 2019 Verizon Data Breach Investigations Report



Breaches

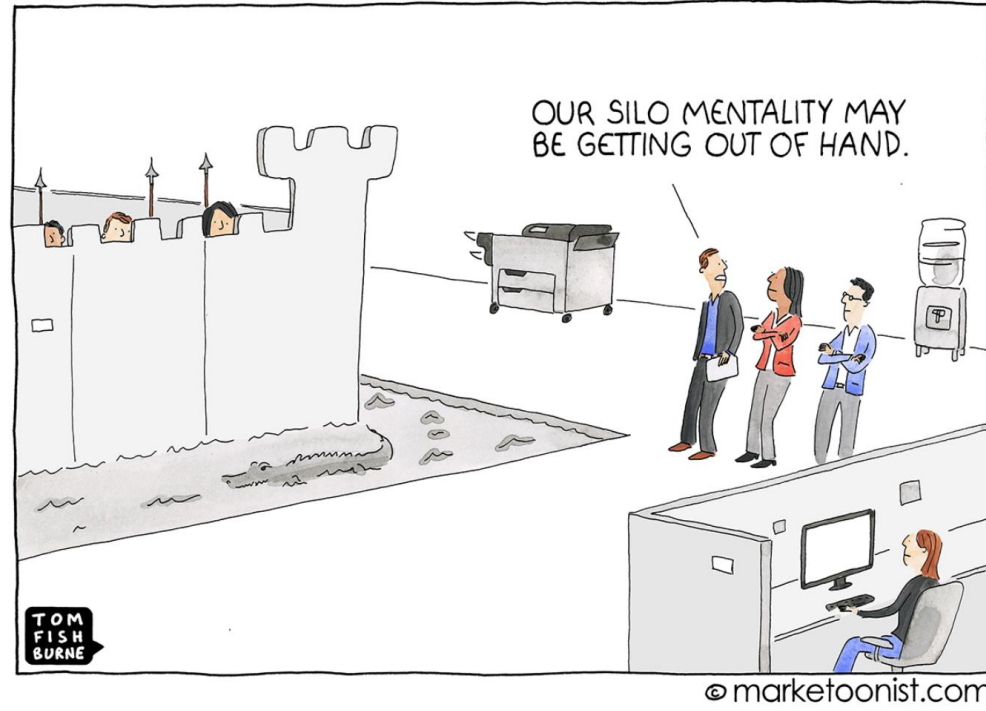
Figure 3. What tactics are utilized?



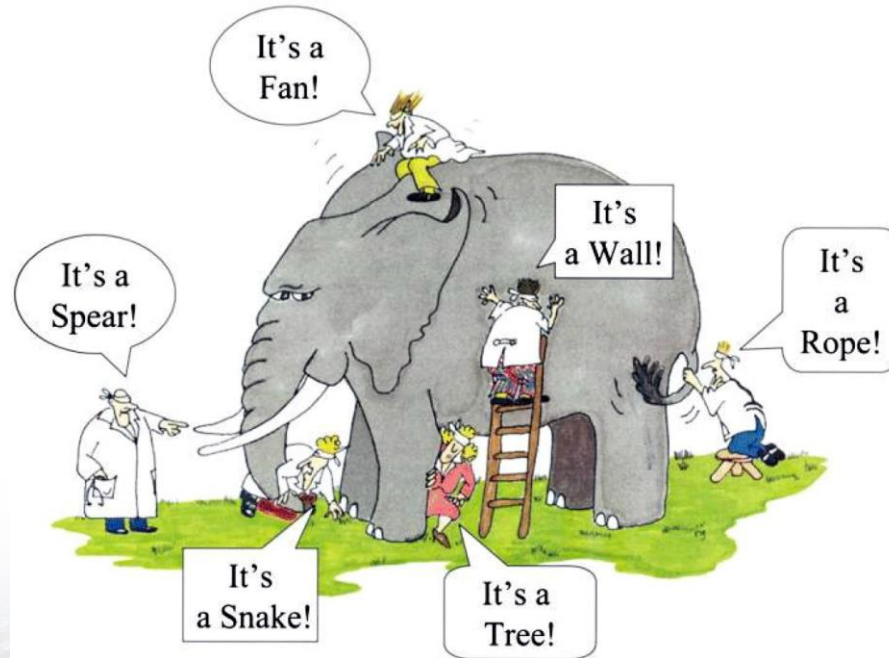
Breaches

Figure 5. What are other commonalities?

Structure: Organisations usually work in silos



Wood or Trees: This often translates to not having a total view



Customer survey: Takeaways

1) Starts at the top

▶ Convergence requires a leader

2) Desire vs Implementation

▶ Change can be hard

3) Regulation drives innovation

▶ A regulatory push can help

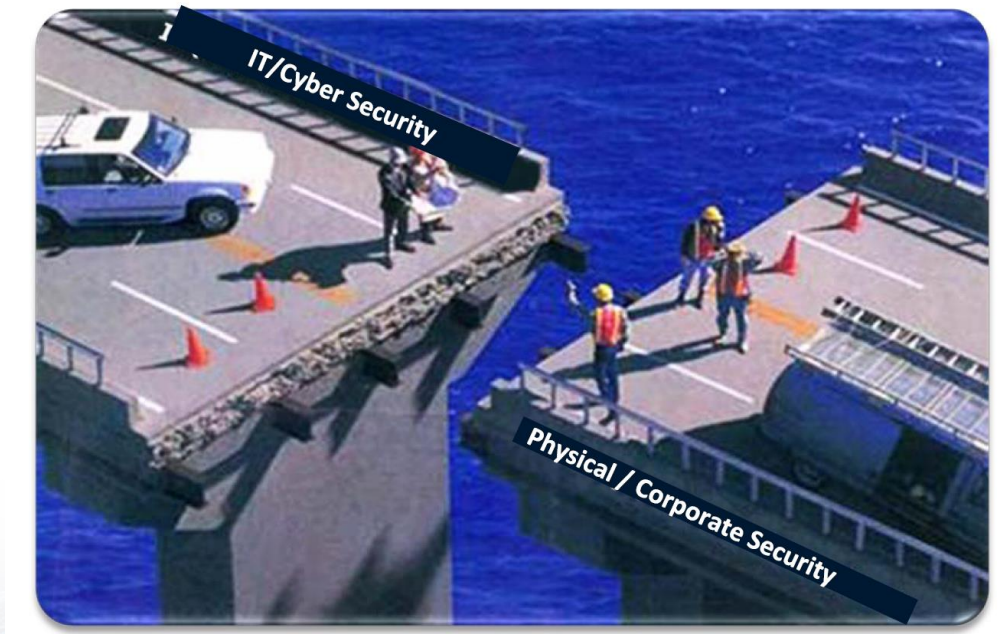
4) Leverage data & technology

▶ OSINT, integration, the Human factor

5) Value individual skill sets

▶ Specific skillsets Physical vs Cyber

Takeaways: Collaboration is critical



"We don't talk to those guys, they are in a different state"

Security leader – Major U.S Bank

Other examples: Doxing

DeepPaste Ajmal Latif 34 years old fake muslim from Woking Surrey UK. is a revenge porn offender and cyber stalker who has been sending his ex wife's nudes to people online and creating fake social media accounts and harassing people. This vile human has been dating married women, buying them flowers, chasing them like a dog then asking them for nudes and publishing nudes and sending them to people on their contact lists. We have received nudes from him using his dirty fake social media accounts. Information : AJMAL LATIF Born: September 9th 1983 Address : 26 Walton Road Nationality: BRITISH Country: UNITED KINGDOM County: SURREY Posttown: WOKING Postcode: GU21 5DL Country of residence: UNITED KINGDOM Origin Country: Pakistan Emails : lat_1983@hotmail.com ajmal1latif@gmail.com Sisters : Nagina Latif Sabrina Latif Amina Latif Nadia Latif Facebook : <https://www.facebook.com/rifka.rosen> <https://www.facebook.com/ajmal.latif.754> === 727595004 Instagram: https://www.instagram.com/aj_on_a_mission Work : Service Delivery Company : International SOS (London Office) ajmal.latif@internationalsos.com

Random Dox I Found
April 01, 2018 10:54PM

Name: [REDACTED]
Location: [REDACTED] North Carolina 28023, USA
SSN: [REDACTED]
Age: [REDACTED] Currently 16
Email: [REDACTED]@gmail.com
Instagram: [https://www.instagram.com/\[REDACTED\]](https://www.instagram.com/[REDACTED])
Snapchat: [REDACTED]
Facebook: [https://m.www.facebook.com/\[REDACTED\]](https://m.www.facebook.com/[REDACTED])
Current Job Address: [REDACTED] NC 28023, USA

--Phone numbers--
Mobile: [REDACTED]

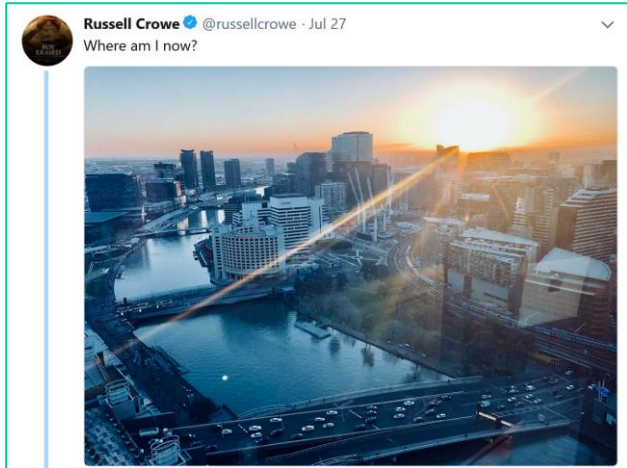
Other examples: Data for sale

ANZ AU Bank account with Security Q&A - 5-10k AUD All accounts are inactive for at least 1 month. I'm responsible for account only in moment of purchase. I'm not responsible for your or holder actions after you logged in. After your first login i will not accept any claims. I'm not replacing valid accounts. No refund. Only replace if password is wrong. After purchase you will receive login, password, security Q&A and last IP used by account owner. I'm not doing free hand-walks into. But if you

4303301001225356|01/21|062|██████████ 595 Burwood
Hwy|Knoxfield|VI|3180|61-437423392|NATIONAL AUSTRALIA BANK, LTD.||CREDIT|PLATINUM
5523505277062647|06/21|421|██████████ 48 Sherriff
Street|Underdale|SA|5032|61-884432600|COMMONWEALTH BANK OF AUSTRALIA||CREDIT|WORLD
4293189100363083|02/22|237|██████████ Osmond
Rd|Eastwood||5063|61-416137821|WESTPAC BANKING CORPORATION||CREDIT|BUSINESS
4303306474175061|03/20|890|██████████ Dalray
Drive|Raceview|QL|4305|61-413305848|NATIONAL AUSTRALIA BANK, LTD.||CREDIT|PLATINUM
5523505276762668|12/20|858|██████████ Mcaleer Drive|Mahomets
Flats|WA|6530|61-400228867|COMMONWEALTH BANK OF AUSTRALIA||CREDIT|WORLD
4557016900009999|04/21|117|██████████ / 7 Underwood
Street|Corrimal|NS|2518|61-417288719|NATIONAL AUSTRALIA BANK, LTD.||CREDIT|PLATINUM
5353185283426014|12/20|692|██████████ 27/29 Surfers Ave , Mermaid Beach|Gold
Coast|QL|4218|61-417672813|COMMONWEALTH BANK OF AUSTRALIA||CREDIT|GOLD
4557045537750733|09/20|794|██████████ Thomas
Street|Chatswood|NS|2067|61-94197386|NATIONAL AUSTRALIA BANK, LTD.||CREDIT|BUSINESS

Item Marriott Customers Database. Each piece contains 1 million entries including: *E-mail (Login) *Password *Name *Address *CC# *EXP *CVV *SSN *DOB *SPG (Customer Number) *DL# *Passport *Phone Geo: Worldwide If you are interested in specific geo or bulk purchase, feel free to contact me through the private messages. Ships To Worldwide

Other examples: VIP location



Famous NZ actor Cliff Curtis at Vista Conference. #avatar #avathelastairbender #pandora #morethanforest #richpeoplealsoonpandora @ SKYCITY [instagram.com/p/BuCbwCFh4hS/ ...](https://www.instagram.com/p/BuCbwCFh4hS/)

1:21 PM - 18 Feb 2019 from Auckland, New Zealand

I work at crown casino in a mens clothes store. I believe Carmella is staying at the hotel here. I'm hoping to see her!

Other examples: Potential threats

Chic fil a 2 days in a row you are all pussies
and I can easily kill you

I wish the Vegas shooter would have set up camp at **SallieMae**'s World HQ rather
than in Vegas. fuck EVERYONE who works there.

My monthly message hoping everyone
working for #Navient / #SallieMae die of
bleeding ass cancer. Fuck you, Fuck you, Fuck
you. #StudentDebt

Other examples: Misinformation (Fake news)

- ▶ Easy to propagate online
- ▶ Can quickly become viral
- ▶ Always someone that will believe – the Internet is truth
- ▶ Examples post Christchurch shooting
 - ▶ “New Zealand banning all guns”
 - ▶ “New Zealand adopting Sharia Law”
 - ▶ “NZ gun owners are uniting to fight”



You can help: Importance of intelligence

- ▶ Security is everyone's responsibility
- ▶ Protect against the threats
- ▶ Gain Cyber Threat Intelligence through commercial solutions and readily available online tools such as
 - ▶ Knowem.com, namechk.com
 - ▶ Osintframework.com
 - ▶ Textrazor.com
 - ▶ Maltego.com
 - ▶ Shodan.io
 - ▶ Tineye.com
 - ▶ Searchcode.com

Insights: Important ways to accelerate readiness

- ▶ Get access to or use existing tools
- ▶ Be part of collaborative industry groups – FSISAC (Financial Sector)
- ▶ Work with company leadership to help highlight challenges
- ▶ Offer to assist with internal policy refinement/updating
- ▶ Discuss with colleagues – even those based in other states

The background of the image is a blue-tinted photograph of a large crowd of people, possibly at a conference or event. Overlaid on this image is a white network diagram consisting of numerous small dots connected by thin lines, creating a complex web-like pattern across the lower half of the frame.

Signal

www.getsignal.info

AMERICA



RUSSIA



ENGLAND



AUSTRALIA

