CYBERSECURITY STANDOFF AUSTRALIA

WHY LEADERSHIP ALIGNMENT IS ESSENTIAL TO SECURE DIGITAL SUPPLY CHAINS ACROSS AUSTRALIA
Each day, digital transformation sees the introduction of new ways for people, businesses and government to connect and interact. Thanks to technology, daily processes and experiences, from buying a cup of coffee to completing an international business transaction, feel almost effortless.

To achieve this seamless digital environment requires a web of interconnected digital and physical suppliers, each adding their own layer of expertise, resources and unfortunately, risk.

Our ever-increasing reliance on data and connected technologies is firmly embedded in most aspects of our lives, from public safety and economic security to our daily wellbeing; and this makes us extremely vulnerable.

Unisys sought the insights and opinions of Chief Executive Officers (CEOs) and Chief Information Security Officers (CISOs) from Australia’s private and public sectors to better understand the perceived role and value of cybersecurity at a business level.

The survey sample reflected the Australian business landscape which is dominated by small to medium enterprises (SME). The Australian government estimates 97 per cent of Australian businesses employ less than 200 people¹.

The Australian government has also committed to sourcing 10 per cent of all contracts, and 35 per cent of contracts up to $20 million, from SMEs². As a result, they provide many of the services and products used by large businesses and government to deliver their own services. And in today’s hyper-connected world, any view of cybersecurity in business needs to span this entire ecosystem.

The results of our research highlight that, in many instances, cybersecurity is still considered to be an ‘IT concern’ and that CEOs and CISOs are at odds with each other regarding the role of cybersecurity within the organisation.

For example, 69 per cent of CISOs believe that cybersecurity is viewed as part of the organisation’s business plans and objectives; however, just 27 per cent of CEOs agree with this statement.

For a quarter (25 per cent) of the organisations surveyed with a board, cybersecurity is not reported on a regular basis and just six per cent of respondents agreed that their cybersecurity platform enables business and supports growth.

Alarmingly, many leaders are concerned they are not doing the basics when it comes to privacy laws. Nearly half (47 per cent) believe their organisation does not make it clear to customers or citizens when they are collecting personal data.

To thrive in this challenging cybersecurity landscape requires a new mindset and unified approach from all members of the supply chain and at all levels of business.

Information security professionals must start speaking the language of business to position cybersecurity as a way to mitigate risk and add value to the organisation. For business leader’s, cybersecurity is a clear competitive advantage in the new data economy.

Gergana Kiryakova
Industry Director Cyber Security for Unisys, Australia and New Zealand
Cybersecurity state of play in Australian organisations*

*Combined CEO & CISO responses

- See cybersecurity as part of the organisation’s business plans and objectives: 43%
- Do not report cybersecurity opportunities and concerns to the board on a regular basis: 25%
- View the purpose of their cybersecurity framework is to enable business and support growth in a cyber-secure manner: 6%
- Believe they can detect and respond to data breaches in real time: 37%
- View data breaches as a business issue: 27%
How citizens view data security
Unisys Security Index, 2019

The top three security concerns for Australians relate to **data theft**

- Of Australians are seriously (extremely/very) concerned about **unauthorised access to or misuse of their personal information**
- Of Australians are aware their **data was compromised** in the last 12 months
- Stopped dealing with the organisation responsible for losing their data
- **Publicly exposed** the organisation responsible for losing their data via social media
- Pursued legal action over personal data loss
Cybersecurity overlooked in business plans

In today’s digitally-led world, an IT outage makes headlines because of the flow-on impact to individuals and businesses.

For example, when Telstra suffered a network outage in July this year, media reports focused on how families couldn’t buy their groceries at Woolworths, drivers were powerless to pay for petrol at Caltex and HICAPS medical claims couldn’t be processed.

This demonstrates how much we rely on digital connectivity in our business and personal lives. One technical challenge can have a domino effect crippling commerce (and business reputations) and stopping the business of living among citizens.

Imagine then the chaos that could be generated by targeted malicious cyber-attacks designed to take over control of a network or steal customer data?

In light of this, protecting the intellectual property of the business, control of its services and customer data should be a tier one business priority for every organisation across Australia. Yet, less than half (43 per cent) of Australian organisations surveyed consider cybersecurity to be an integral part of the organisation’s strategic plans and objectives.

Dig a little deeper and it is clear those at the helm of business, CEOs, predominantly see cybersecurity in tactical terms as either an IT issue (14 per cent), compliance requirement (16 per cent) or a matter for operations to manage (18 per cent). Less than a third (27 per cent) of CEOs view cybersecurity as part of the organisation’s business plans.

When asked to rank their organisations, current business priorities, protecting critical internal data was listed last.

Furthermore, the fact that a quarter (25 per cent) of all organisations do not report cybersecurity priorities or concerns to their board shows a dangerous lack of understanding regarding the value of the organisation’s data, and the risks and potential liabilities they could face if it were compromised.

Reporting appears to be a particular concern among SMEs where just 58 per cent of those with a board report on cybersecurity matters on a regular basis, compared with 72 per cent of government or large-scale entities.

**AT A GLANCE: HOW DIFFERENT INDUSTRIES VIEW CYBERSECURITY**

<table>
<thead>
<tr>
<th>Cybersecurity mindset</th>
<th>Industries that hold this view</th>
</tr>
</thead>
</table>
| Cybersecurity is part of the organisation’s business plans and objectives | • Information & communication technology (79%)  
• Administration of office support (50%)  
• Financial Services (33%) |
| Cybersecurity is a compliance requirement | • Accounting (57%)  
• Healthcare and pharmaceutical (43%)  
• Accommodation and food services (67%) |
| Cybersecurity is an operations concern | • Real estate or property (50%)  
• Manufacturing & logistics (50%)  
• Mining, resources or energy (100%) |
| Cybersecurity is part of our enterprise risk framework | • Sports and recreation (20%)  
• Sales (18%)  
• Agriculture (20%) |
| Cybersecurity is something for IT to deal with | • Financial Services (33%)  
• Manufacturing & logistics (50%)  
• Construction or engineering (20%) |
The data divide: CEOs vs CISOs and SMEs vs large organisations

As organisations increase the digital enablement of core business functions, the type and volume of data collected, stored and used grows significantly.

The survey reveals that awareness of what information is being collected, and how, is not necessarily understood at a leadership level. There is a clear disconnect between the way CEOs and CISOs view the business risk of data security and their ability to prevent or manage data breaches.

For example, when asked how the volume or type of data collected by their organisation had evolved over the last ten years, 68 per cent of CEOs declared there has been no change, whereas only 19 per cent of CISOs held this view.

Just 11 per cent of CEOs state that their organisation now collects customer or citizen financial data, compared with a significant 57 per cent of CISOs.

CEOs are almost twice as confident that their organisation’s data collection policies are clear to consumers or citizens (51 per cent) than CISOs (26 per cent). CEOs (14 per cent) are also more likely to believe that their organisation adheres to the Australian Privacy Principles for data collection than CISOs (7 per cent).

When it comes to data collection, SMEs (49 per cent) are more confident that their policies are clearer than those from large scale enterprise (40 per cent).

When asked about how their organisation manages compliance, those in the SME sector are the least likely to believe their approach is based on recognised industry frameworks.

"Those in the SME sector are the least likely to believe their cybersecurity approach is based on recognised industry frameworks."

Start-ups (46 per cent) and large-scale enterprise (45 per cent) predominantly base their compliance on a framework that uses known industry standards such as ISO³, NIST⁴ or ASD⁵, compared with just 33 per cent of SMEs.

Of those surveyed, SMEs were the most likely to have a reactive approach to managing compliance (30 per cent). However, there is also potential knowledge gap between CEOs and CISOs on this issue: CEOs (32 per cent) are much more likely to say their organisation has a reactive approach to compliance, where just six per cent of CISOs agreed that this is their approach.

CEOs: overconfident and out of the loop

In business, confidence can be a powerful asset, unless the topic at hand relates to cybersecurity.

The reality is that each new application, network, partnership or business integration presents a new opportunity for hackers to exploit or increases the chance of accidental data loss through human error.

Of those surveyed, just 27 per cent believe their organisation suffered a data breach in the last 12 months. However, CEOs appear to be in the dark about data loss with just six per cent acknowledging a breach, compared to 63 per cent of CISOs.

CEOs are also more likely to be optimistic about their organisation’s ability to detect and respond to a data breach. According to the survey, 44 per cent of CEOs believe their organisation can detect and respond to a data breach in real-time, compared with just 26 per cent of CISOs.

When looking at the impact of a data breach, however, CISOs are more likely to underplay its significance to the business. A third of all CEOs (33 per cent) would regard a data breach as a business issue, compared to just 17 per cent of CISOs.

Most CISOs view a data breach as an issue to be managed by the IT or information security team only (46 per cent), or by their IT security vendor (26 per cent). Shockingly, no CISO surveyed saw the need to inform staff, clients, customers or partners that could be impacted by a non-reportable data breach, compared with 14 per cent of CEOs.

One of the biggest disconnects the survey reveals is that both CEOs and CISOs have their attention focused on different threats.

Of those who have experienced a data breach, human error (64 per cent) was agreed by both CEOs and CISOs as the most likely cause. This was followed by targeted attacks by hackers (56 per cent), malware/spyware (54 per cent), deliberate data breaches by staff (33 per cent) and a breach through partners or suppliers (18 per cent).

Despite human error being seen as the top threat, When asked what the biggest cybersecurity threat is to their organisation, just 18 per cent of CEOs and 44 per cent of CISOs felt that a lack of staff knowledge on how to protect data should be their chief concern. Instead, they cited malicious attacks as the greatest concern with 64 per cent of CEOs and 69 per cent of CISOs agreeing that this is their biggest risk.

From here however there is a significant disconnect regarding perceived cyber risks. While CISOs are concerned about state-sponsored spying (52 per cent versus eight per cent of CEOs and corporate espionage (28 per cent versus 14 per cent of CEOs); CEOs (27 per cent) believe that out-of-date technology is placing their organisation at risk (compared with just seven per cent of CISOs).

### IDENTIFYING DATA BREACHES

<table>
<thead>
<tr>
<th>Method</th>
<th>What CEOs think</th>
<th>What CISOs say</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actively search for breaches via dark web scanning</td>
<td>11%</td>
<td>44%</td>
</tr>
<tr>
<td>Wait for anti-malware/endpoint security software to pick up any suspicious activity</td>
<td>48%</td>
<td>69%</td>
</tr>
<tr>
<td>Daily sweeps of all networked devices</td>
<td>32%</td>
<td>59%</td>
</tr>
<tr>
<td>Breaches are identified after the fact by employees</td>
<td>10%</td>
<td>20%</td>
</tr>
<tr>
<td>Breaches are identified after the fact by customers</td>
<td>7%</td>
<td>9%</td>
</tr>
<tr>
<td>Not sure</td>
<td>18%</td>
<td>2%</td>
</tr>
</tbody>
</table>

**Industries most likely to be concerned about state-sponsored spying include:**
Information or communication technology, Accommodation or food service

**Industries most likely to be concerned about corporate espionage include:**
Banking and insurance, Science and technology
Public sector vs private sector

The public sector is more likely to view **cybersecurity as part of the organisation’s business plans** (41% vs 34% of non-government)

The private sector is almost twice as likely to see **cybersecurity as an operations concern** (8% vs 15%)

Those in the public sector are more likely to see **cybersecurity as an IT issue** (16% vs 10%)

Realtime reactions to detect and manage a data breach are evenly matched between the public and private sectors (35% vs 34%)

Compared with ten years ago, the public sector is more likely to **collect biometric data from customers or citizens** (46% vs 27%)

Only the private sector views **cybersecurity as part of the enterprise risk framework** (10%)

Those in the public sector are almost twice as likely to be concerned that **the collection of personal information isn’t made clear by their organisation** (43% vs 25%)
Adopting a unified approach to cybersecurity

In the United States, cybersecurity has been placed on the national agenda through a program called, Cybersecurity Moonshot.

The Cybersecurity Moonshot subcommittee (of which Unisys is a key member) has developed recommendations for a “whole of nation approach” for a safer, more resilient internet to deliver government and critical infrastructure services.

The name ‘moonshot’ references the audacious, but strategic original Moonshot challenge given to American scientists by President John F. Kennedy to land humans on the moon within the space of a decade.

This time, the stretch goal is a safer, more resilient use of connected devices to deliver government and critical infrastructure services securely.

The recommendations and learnings from the Cybersecurity Moonshot program can be used by organisations of all sizes across Australia to strengthen and unify their approach to cybersecurity. They are distilled into six key pillars:
TECHNOLOGY

While just 20 per cent of Australian CEOs and CISOs believe out of date technology is compromising their cybersecurity, investing in technology should be a priority for organisations.

As organisations cite accidental data breaches as their biggest source of risk, technology should be deployed to create a zero-trust environment where the default is always to verify permission: from both within and outside of the IT environment.

Zero-trust technology demands strong user authentication processes (such as biometrics), machine authentication through digital certificates and can be bolstered by technology such as Unisys’ Stealth dynamic isolation to allow priority communications to be concealed from those not authorised to access them.

HUMAN BEHAVIOUR

Data breaches from insider threats, whether accidental (64 per cent) or deliberate (33 per cent), make employees and supply chain partners one of the biggest risks to an organisation’s cybersecurity outlook.

Organisation’s need to shift from a defend and protect stance to a more proactive approach that identifies potential breaches or risks as they happen.

For example, user and entity behaviour analytics are critical to understanding what standard behaviours take place in the environment; so abnormal behaviour such as large file uploads can be quickly identified and immediately addressed.

EDUCATION

As each person and device within an organisation can present a cybersecurity risk, a whole or organisation approach to cybersecurity is required, from the top executives to casual staff and suppliers.

Without this approach, the supply chain is at risk.

From covering the basics of ‘how to identify a phishing scam’ to ensuring that the organisation has a clear ‘no exceptions’ culture for security best practice.

ECO-SYSTEM ROLES AND RESPONSIBILITIES

Unisys recommends establishing an environment that enables the organisation to predict, protect, detect and respond to potential threats.

By adopting a proactive approach (unlike the majority of survey respondents who respond to data threats retrospectively) organisations can get on the front foot of the cybersecurity war.

This layered approach can be applied to five potential risks: email and web attack, malware download, machine takeover, privilege escalation and data exfiltration to provide a robust defensive system.

PRIVACY

Respecting customer or citizen data is not only essential to an organisation’s reputation, it’s the law.

Executives and those responsible for collecting, managing or accessing customer data must be confident that correct procedures are being followed.

POLICY

Unless there are clear policies in place, organisations cannot expect their staff to know what they can and cannot do with the data they have access to on a daily basis.

A robust policy that is clearly explained to all staff members, partners and suppliers is essential to creating a cybersecure culture and providing the organisation with an avenue to act should a data breach occur.
Conclusion

To keep pace with ever-evolving cyber risks and threats will require the rapid adoption of new thinking, behaviours and practices. Best practice is to address the six core pillars of technology, human behaviour, education, eco-system roles and responsibilities, privacy and policy in the cybersecurity approach.

Organisations at all points in the supply chain have a responsibility to protect the private information of their staff, customers, stakeholders, partners and suppliers, along with their IP.

Cyberattacks are inevitable. Organisations who take a proactive and unified approach to managing their data will be best placed to identify and stop threats before they impact business continuity, partners, customers or citizens.

RESEARCH METHODOLOGY: Unisys’ Cybersecurity Standoff Australia research sought the insights and opinions of CEOs and CISOs from Australia’s private and public sectors to better understand the perceived role and value of cybersecurity at a business level. The online survey was conducted by Pure Profile during September 2019, surveying 88 CEOs and 54 CISOs from Australia’s private and public sectors. Reflecting the Australian business landscape, 90% of responses were from small-medium enterprises (less than 200 employees).
