QUEENSLAND
FUTURES INSTITUTE

QLD POLICY LEADERS' FORUM

LEADING CYBER SECURITY

23 OCTOBER 2024

LEADING CYBER SECURITY

PANELISTS:

KARLA DAY

Chief Technology and
Transformation Officer
QBANK

IVAR VAN DEN BERGE

Head of Cyber Security
Sime Darby Industrial Australasia

BRUCE IRWIN

Principal Consultant
Cyber Security and Risk
Business Aspect

PROFESSOR RYAN KO

Chair & Director
UQ Cyber Research Centre
The University of Queensland

MODERATOR
CAT MATSON

CEO & Lead Facilitator
Impactful Presenters

QFI THANKS ITS SPONSORS

Data#3

BUSINESS ASPECT

Snapshot

The 2024 Queensland Futures Institute's Leading Cyber Security Panel highlighted the critical need for robust cyber security across all organisations. The discussion outlined the increasing risks of cyber security incidents and data breaches – emphasising that effective cyber security requires a proactive approach led by people and processes, rather than just through compliance.

The Panel highlighted that organisations must build a risk-aware culture around cyber security, and that this must be led by strong governance and leadership to protect against threats and build resilience in today's rapidly evolving digital landscape.

Summary of Panel Comments

- Cyber security is critical for organisations of all sizes – particularly small and medium businesses, 60% of which would go bankrupt following a cyber security incident.
- In managing this risk, effective practices, governance and a focus on people and processes are critical for organisations, while the technology aspect of cyber security will follow.
- Building a cyber security culture which builds security awareness into daily practices is key.
- This is important in building an environment which encourages early reporting of cyber security incidents, which is vital for rapid response and resolution.
- This requires leadership from the top of organisations. Additionally, governance and accountability structures are critical in managing risks and aligning security priorities within organisations.
- Balancing reactive risk management with proactive measures is essential, and clear risk assessments and quantifying potential impacts in terms of financial value can aid in decision-making.

Panel Comments

Cat Matson

- From 2014 to 2020, I served as Brisbane's Chief Digital Officer, focusing on leading digital transformation of the City's economy.
- This involved supporting a startup ecosystem and exploring how innovations like the sharing economy (e.g., Uber) would impact Brisbane.
- Back then, cyber security was seen as a 'big company' issue, not something that small businesses needed to worry about.
- However, the situation is very different today; two-thirds of small businesses would fail if they were targeted by a ransomware attack. This highlights the urgency of cyber security.

Karla Day

- As Chief Technology and Transformation Officer at QBANK in Brisbane, cyber security is critical to my role given the bank's regulatory and compliance obligations, and critical accountability function.
- QBANK's members are people who serve our community. Safeguarding data and finances is a top priority.
- To do this, I'm passionate about fostering innovation across the organisation and ensuring everyone can effectively collaborate to deliver secure, high-quality services and products. This is a challenging but essential task, to protect our members and fulfill our responsibilities at QBANK.

Bruce Irwin

- As the Principal Consultant for Cyber Security Risk at Business Aspect and having been in the IT industry for over 30 years, I've witnessed a major shift in security being an afterthought, to becoming a central concern for organisations.
- Business Aspect helps other organisations like QBANK to protect their stakeholders.
- My primary passion lies in privacy – which it critical for organisations, society and government institutions, now and in the future.
- Privacy is at the heart of the challenges we're facing. Overcoming this challenge will require strong governance, effective practices and a focus on people and processes. Once this is achieved, the technology solutions will follow.

Panel Comments

Professor Ryan Ko

- UQ Cyber is an interdisciplinary research centre that bridges industry, IT departments, research and teaching. We bring together around 13 entities from four faculties, a research institute and a research centre, covering a breadth of topics including quantum computing, policy and cryptography.
- Our team includes about 60 academics and nearly 100 PhD students working on diverse aspects of cyber security.
- My passion in cyber security research focuses on people and processes, as this is where the frontiers of threat prevention lie, more so than in technology.
- Small and medium businesses, which comprise over 90% of developed nations, often lack resources for cyber security.
- As such, we aim to address these challenges by identifying research questions and solutions tailored to small and medium enterprises.
- To support this, I co-founded Cyber Security Certification Australia, an industry council dedicated to creating standards and certifications for these businesses.

Ivar van den Berge

- Sime Darby Australasia is a large Malaysian organisation operating across the Asia-Pacific. The organisation fully embraces cyber security beyond mere compliance, which is a major motivator.
- Sime Darby provides equipment for the mining and resource industries, so we must prioritise strong protections to ensure quick recovery and continuity in case of a cyber incident; when our operations stop, it impacts other companies across Queensland and Australasia that rely on our services.
- While technology is essential, people and processes are a critical element in cyber security. To achieve success, we must foster a cultural shift – moving away from a strict compliance mentality to one that values proactive security. To do this requires leadership from the top.

Panel Questions

What are the real and emerging cyber security risks that we're now navigating?

Karla Day

- Identity theft has long been a challenge, particularly for the banking industry.
- With AI and deepfake technology, the threat level has significantly escalated, making it harder to verify peoples' identities. For example, someone can even submit a video of themselves, making it difficult to detect identity theft from a physical or even technical perspective.
- As such, combating identity theft, fraud and scams is a major challenge in the industry. This is highlighted by the $2.7 billion lost to scams last year, which highlights the ongoing risk to our members and bank customers.
- While government support, initiatives and accords aim to tackle scams, it remains essential to educate our members on recognising and preventing these threats.

Cat Matson

- The $2.7 billion figure highlights the scale and complexity of the scam industry. We have moved from these threats coming from unorganised actors to becoming large organisations.

Bruce Irwin

- We've recently seen extensive media coverage on AI and its impact on organisations. Karla mentioned AI impersonation, and I've observed early instances of video impersonation attempts on Teams calls.
- While AI brings risks, it also has opportunities. It is critical to prepare organisations to use it effectively and securely, just like past technological developments.
- Given AI accelerates data processing, it has the potential to reveal flaws in processes and data security, or 'spill' data faster, which can lead to rapid data leaks.
- As such, organisations must be cautious with the adoption of this technology to avoid unintended vulnerabilities.

Professor Ryan Ko

- Ransomware and scams are highly prevalent issues faced by people and organisations today.
- One of my research areas is tracking cryptocurrency payments to identify criminal activity. We have found through analysis and tracing of cryptocurrency payments that in the last two years, scam payments have surged to nearly five times the volume of ransomware payments globally.
- This growth reflects how organised and opportunistic criminals are targeting the 'lowest hanging fruit' – ordinary people rather than heavily protected organisations or entities.
- However, this also reflects on the above discussion around small and medium businesses – given that around 60% of small and medium businesses go bankrupt following a data breach, ransomware attack or scam.

Panel Questions

Ivar van den Berge

- Ransomware and scams result because of tactics which employ social engineering through email, to get into organisations or businesses, leading to business email compromise and identity theft.
- Malicious actors now use AI to gather personal information from the internet, building detailed profiles and crafting highly targeted messages. This makes it increasingly easy to fall for these scams due to this personalised approach.
- To protect against this, I believe the best approach is to 'fight AI with AI', as AI-based solutions are becoming more accessible and affordable, enabling both large and small businesses to protect themselves more effectively.

Karla Day

- On the topic of 'fighting AI with AI' – from my perspective, this would rely on partnering with the right organisations to support our cyber security needs.
- This adds complexity around third-party security, as we must ensure the trustworthiness and security of third-party vendors. Another challenge is the overwhelming number of vendors offering solutions across these emerging technologies, making it hard to choose the right fit.

How are you building a culture of security in your organisation?

Ivar van den Berge

- Setting the tone at the top is important for leaders, as it reflects that cyber security is as a business-wide responsibility.
- Most organisations use phishing simulations to educate employees. This is a good method of supporting employees to learn but should not focus penalties for employees who click on the simulated problem emails.
- AI has led to phishing emails becoming increasingly sophisticated and frequent, making it critical to combine technology and user awareness approaches to protect against these threats.
- In my organisation, we borrowed the concept of 'safety shares' from Zero Harm physical safety protocols to create 'cyber safety shares' in meetings.
- This has sparked a positive ripple effect and led to others in meetings sharing their cyber security experiences.
- This example highlights how the culture can be shifted in businesses, and how cyber security can be made relatable and actionable by emphasising people, family and the community.

Cat Matson

- From my experience in delivering safety leadership training, I've seen how safety shares can keep a high level of awareness for daily safety practices.
- With new psychosocial wellbeing regulations, there's growing pressure to introduce 'psychosocial shares', and cyber security can easily be a part of this. For example, cyber safety shares could help reduce the mental anguish that employees might feel if they accidentally click a harmful link, knowing the potential consequences for the organisation.

Panel Questions

Bruce Irwin

- In building a security culture within organisations, it is important to measure the right things. Organisations often focus on counting how many people clicked a phishing link during tests but should be focused on how quickly the first person reported the phishing attempt, as this is what enables IT to eliminate the threat.
- Rewarding that first responder reinforces the right culture by encouraging proactive reporting, rather than punishing people for honest mistakes.

Karla Day

- Early reporting is essential, so organisations should remove scare tactics and a blame mentality from their approach. If people are afraid to report incidents, they won't share when they've made a mistake – and this will lead to the threat not being resolved.
- Cyber threats tend to strike when we're busiest, often using urgent, distracting tactics to catch even the most vigilant person off guard. Additionally, phishing attempts often play on emotions, mentioning things like family, which makes people more likely to fall for them.
- Organisations must create a blame-free environment to encourage employees to report incidents immediately, allowing them to quickly and effectively resolve any threat.

How do you balance managing the risk (i.e., a reactive response) and eliminating it all together (i.e., through proactive measures)?

Karla Day

- Effective cyber security relies on robust risk assessment processes to identify and understand any potential risks.
- It is critical for organisations to articulate what each risk would look like if it were to happen and develop mitigation strategies and response plans.
- However, this ultimately comes back to education and ensuring visibility across the business to ensure preparation and support for any risk management protocols.
- Vendor risk management is also a significant challenge – especially for small businesses that often lack the resources to manage these risks independently.

Ivar van den Berge

- Governance structures play a critical role in risk management. In some cases, after completing a risk assessment, the approach could be to implement temporary controls and hold off on further investment – for example if an upgrade or technology replacement is planned soon.
- Formal risk acceptance takes place at the highest level, aligning decisions with organisational priorities and accountability.

Panel Questions

Bruce Irwin

- It is critical to clearly articulate risk assessments to stakeholders – such as the audit committee or board.
- Because technical statistics such as firewall data can confuse these discussions, security leaders should quantify the risk burden, showing the value of data within the organisation for these stakeholders.
- For example, a new platform might carry $30 million in privacy risk due to potential breach costs, which would then justify a $175,000 investment in protection.
- This approach shifts the conversation to a clear cost-benefit analysis which supports balancing risk management and elimination for decision-makers.

Professor Ryan Ko

- Traditional risk management often focuses inwardly on the organisation, but it is important to also consider external risks. This can include looking at potential vulnerabilities across the supply chain – including from IT suppliers, vendors, security service providers, and even lawyers and accountants.
- It is critical to assess and manage these external risks as well as those within internal operations to comprehensively protect the organisation.

What is the one thing that you want our audience to leave with when it comes to cyber security?

Ivar van den Berge

- Cyber security must be made tangible, by framing it around the actual risk to teams, business units, and the organisation. This enables effective risk management and prioritisation.

Professor Ryan Ko

- Use basic measure such as multifactor authentication to protect against cyber threats and attacks.

Bruce Irwin

- Put people at the centre of your approach, using empathy and care.

Karla Day

- Understand your business and your stakeholders and bring them along on the journey.

Audience Questions

How do we prioritise cyber security in a world where everyone is always busy?

Professor Ryan Ko

- To build a strong cyber security culture, it is important to lead by example.
- At UQ, we launched a program called UQ Cyber Champions, which is a cultural initiative which has seen each department designate a Cyber Champion who meets with others to share experiences, challenges and insights.
- The program began with only four members and has grown to over 200 champions out of UQ's 7,000+ employees, seeing strong representation across departments.
- Building this culture takes time and initial effort, but with the support of leadership, it has gained momentum and spread across the organisation.

Karla Day

- Leadership plays a role in defining 'busy', examining what is occupying our time and defining priorities.
- A 'security first' mindset – similar to what has been developed for visible hazards – can be used. This would see cyber security issues treated equally as critical as physical hazards.
- Education is key to embedding this mindset so that we prioritise security over simply being 'busy'.
- This shift in mindset requires leadership, board support and consistent reinforcement from the executive level to reach everyone across the organisation.

Cat Matson

- Cyber security can no longer be an afterthought, it must be the first consideration in business planning, given today's digitally enabled world which is highly interconnected, open and accessible.

Ivar van den Berge

- Along with education, it is critical to make the outcomes of cyber security efforts visible to staff.
- Regularly sharing statistics on cyber performance – whether improving, remaining stable or getting worse – helps staff see the real impact of their actions.

Bruce Irwin

- When we say we're "too busy" for cyber security, we should consider what is at stake and why we might not be prioritising it. Using the safety analogy, we wouldn't ignore physical safety, so if we're overlooking cyber security, our culture might need adjustment.
- Organisations need a deep understanding of who their stakeholders are and what security means to them. For example, At QBANK, our stakeholders are the people who serve our community – and protecting their financial wellbeing and privacy is essential.
- Organisations must be agile and able to adapt to new challenges by reconfiguring around its security needs. This flexibility is key to meeting future needs quickly, effectively and safely.

Audience Questions

How have you managed or mitigated risks in the past?

Bruce Irwin

- In the 2022 Australian Cyber Security Centre's annual report, Queensland reported the highest rate of cyber crime in Australia.
- Last year, New South Wales surpassed Queensland, placing us at number two. However, this still highlights that cyber crime remains a significant threat to Queenslanders and local organisations.

Professor Ryan Ko

- If there's time, I'd like to share a global example involving the Lazarus Group, a mercenary hacking organisation. They were behind a high-profile hack of the Bangladesh Central Bank, where they infiltrated the system over two years, exploiting a lack of basic security measures like patching and multifactor authentication.
- This resulted in the attempt to transfer $1 billion to New York, though not all of it succeeded. This operation was backed by North Korea, which used hacking to bypass international sanctions.
- Another example involves scam companies posing as legitimate investment platforms, targeting vulnerable demographics of people. These scam companies use professional call centres and appear in sports sponsorships to build credibility, pressuring victims to invest more.
- This prompts the simple advice: if an investment opportunity seems too good to be true, it probably is.

Bruce Irwin

- An example of an incident involves a business which developed fundraising software. On a Sunday, an administrator in the data centre broke protocol by checking Gmail on a server and clicked a malicious link.
- This led to the encryption of both their production and disaster recovery data centres, leaving them unable to access systems for weeks. They had to negotiate to unlock their backup tapes and faced significant financial hardship, eventually going out of business.
- This incident shows how quickly everything can unravel from a single lapse in protocol.

Karla Day

- Cyber security education isn't about 'if' a cyber incident will happen; it's about 'when' it will happen.
- Education should focus on preparedness across the organisation – across staff and up to the board. This must involve tabletop exercises and clear policies and procedures to follow in the event of a breach.
- Cyber security is about people and processes, but also about recovering quickly and effectively when an incident occurs.

CORPORATE PARTNERS

BDO gadens

MEMBERS

ANZ
Australia Pacific LNG
Australian Retirement Trust
Brighter Super
Brisbane Airport Australia
Brisbane Girls Grammar School
Coaching Centre
CSIRO
Data#3
eDL
EY Building a better working world
Griffith University Queensland, Australia
Hastings Deering CAT
Independent Schools Queensland choice & diversity
Innovation Central Brisbane
Jobs Queensland
KPMG
Mackay Regional Council
City of Moreton Bay
Newsreel. From the source
novo nordisk
People First Bank
Port of Brisbane Here for the future
PMSA Presbyterian and Methodist Schools Association
QCAA Queensland Curriculum & Assessment Authority
QIC
Queensland Hydro
Queensland Treasury Corporation
Queensland Government
QUT
Redland City Council
St Vincent de Paul Society Queensland good works
south bank corporation
sra Sugar Research Australia
Suncorp
tafe Queensland
TRIO Translational Research Institute Australia
The University Of Queensland Australia
University of Southern Queensland
University of the Sunshine Coast

QUEENSLAND
FUTURES INSTITUTE

FOR FURTHER INFORMATION

Steve Greenwood | Chief Executive Officer
steve.greenwood@futuresinstitute.com.au

www.futuresinstitute.com.au
Level 11, 111 Eagle Street Brisbane QLD 4000