IRON MOUNTAIN®

2025 London | Washington | Davos | **Sydney**

Information security executive panel series

The end of cybersecurity

Our expert panel - Sydney

Chris Inglis

Chris Inglis served as the first Senate-confirmed National Cyber Director and advisor to the former President Joe Biden on cybersecurity. He previously worked as a U.S. Naval Academy Looker Distinguished Visiting Professor for Cyber Studies, as a managing director at Paladin Capital, a member of the boards of several public and private corporations, and as a Commissioner on the U.S. Cyberspace Solarium Commission.

Marcus Thompson

Marcus Thompson is a retired Major General in the Australian Army where he finished with his final post as inaugural Head of Information Warfare for the Australian Defence Force. He has held numerous leadership positions in both conventional and special military units, and the Department of Prime Minister and Cabinet. Today Marcus holds numerous Board and advisor roles in the space of data and cyber.

Melissa Osborne

Melissa Osborne is the former Head of National Security & Defence for Amazon Web Services (AWS) in Australia and New Zealand, and former Chief Technology Officer for Dell Technologies, Australia and New Zealand. Prior to this, Melissa spent 24 years of her career in National Security, Intelligence, and Defence roles for the Australian Government.

Kevin Thomas

Kevin Thomas is Senior Vice President Resilience, Geopolitical Strategy and Incubation at Iron Mountain. Prior to joining Iron Mountain, Kevin worked for the United States federal government for career, the last nearly two decades at CIA. A Distinguished Career Intelligence Medal recipient, Kevin most recently led all operations for CIA's Transnational and Technology Mission Centre.

In the modern era of cybercrime, the likelihood of any organisation falling victim to an attack is not a matter of if, but when.

With nation states actively weaponising cyber-attacks as part of their ongoing information warfare activity, and criminal gangs exploiting cutting edge artificial intelligence (AI) technologies to launch increasingly sophisticated attacks, defenders face a variety of threats that are complex in their execution and relentless in their volume.

If any organisation is to withstand this onslaught, it must view cyber threats as a critical business risk and develop a defensive strategy that extends beyond detection and protection to encompass response and recovery.

That also means ceasing to view cyber risk as somehow being different to any other risk that an organisation faces.

To put it bluntly, it's time to stop talking about cyber security, and start talking about business resilience.

Standing strong in the face of cybercrime was the core focus of an executive security discussion conducted by Iron Mountain in Sydney in March 2025. Featuring leading representatives from the Australian and international cyber security community, the discussion covered the extent of current threats and the best-practice approaches that organisations could take to strengthen their defences.

> The good organisations treat it as a genuine business risk, and it starts with recognising that the threat is real, active, and wishes you harm. This risk cannot be outsourced to the IT team.
>
> **Marcus Thompson**

Cyber security as a business strategy

Digital systems are the beating heart of twenty-first century organisations, and any disruption can quickly unfold into an existential crisis. Their defence warrants the same attention as any other significant business risk.

But for many organisations, a distinction remains between how they manage business risk and cyber risk, with responsibility for cyber consigned to specialised teams that are far removed from broader risk management activities.

Aligning business and cyber risk strategies is a challenge that all parties must own, but which can be made easier by building bridges between people with different responsibilities, knowledge, and skill sets, to create areas of shared interest. This often starts with finding a common language.

> I would stop having conversations about 'cyber security' and start having conversations about what I want to do with my business and the dependencies that come from that. Digital infrastructure can then be aligned to those business objectives in the same way that we have always done for people, intellectual property, and strategy(ies). A conversation that starts with the business plan is a conversation that everyone understands.

Chris Inglis

A conversation that starts with the business plan allows digital systems and their defence to be viewed within the context of how they contribute to the organisation's goals. All parties can understand the importance of digital systems as well as their vulnerabilities. They can create risk management strategies that represent the true risk to the business, and then make better decisions regarding defensive strategies and investments.

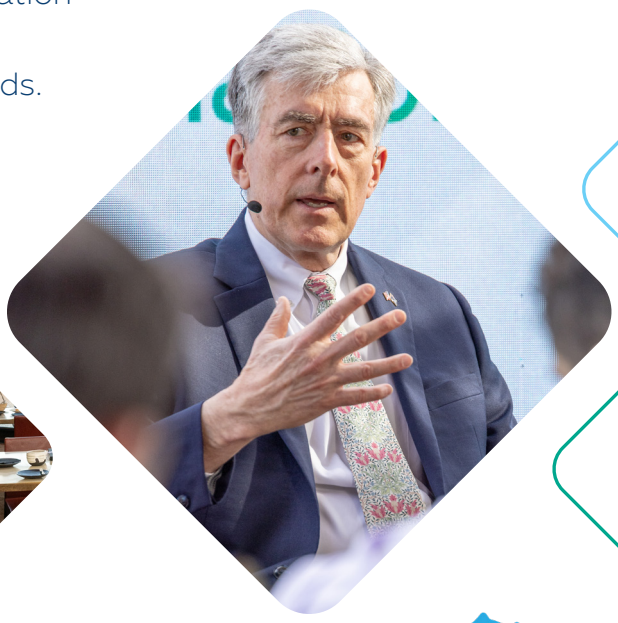
Importantly, this alignment reduces the likelihood of cybersecurity becoming an impediment to innovation. When cyber controls are implemented in line with business strategy, they can become an enabler of faster and safer transformation.

> Security need not be a barrier to the organisation's speed and agility.

Melissa Osborne

Defining a cyber strategy in this top-down fashion ensures it is understood and managed at the highest level, in the same manner as any other risk.

Cyber defence is not about defending an organisation's IT infrastructure. It is about extending and empowering the business in a world that is dependent on IT.



The post-protection world

> Nearly every company will be subject to some sort of breach in the next year or two. It is incumbent on each and every company to acknowledge that fact to appreciate what comes next – which is to prepare their organisation to protect, detect, respond and recover.
>
> **Kevin Thomas**

While the chances of falling victim to a cyber-attack might be an inevitability, recent experience has shown that the damage they inflict depends greatly on the speed and effectiveness of the response.

This means an effective cyber strategy cannot rely exclusively on absolute prevention, but must also incorporate a strong capability for response and recovery. The earlier an organisation is aware of an attack, the sooner it can enact strategies to minimise the damage, such as isolating compromised systems and informing relevant parties, while also accelerating the activation of recovery programs.

Organisations that have a rapid understanding of what has happened can minimise their losses.

Achieving this capability requires intentional thinking and targeted investment, and a willingness to constantly test and assess the state of their defences and recovery processes.

> The goal is not just to 'prevent' since that implies a degree of perfect security that is simply unattainable. The goal is to create defensible systems and to then figure out how to detect and interdict threats that make it past your front line defenses, and then focus on response and recovery to seize back the initiative from transgressors.
>
> **Chris Inglis**

Stronger together

Massive growth in cybercrime is a product of the low cost of launching attacks and the high potential reward from their execution.

Despite the resultant deluge of attacks, no organisation is alone in its fight against cybercrime.

Indeed, the sheer volume of attacks presents a silver lining in the form of the amount of data being received by defenders. This collected intelligence and experience has generated a wealth of knowledge regarding best practice for security architectures and infrastructure development.

This knowledge is often represented in the tools and practices of cybersecurity service providers, who assist organisations in implementing best practice strategies. This includes guidance for managing the lifecycle of the data assets that criminals are seeking to exfiltrate, such as recommendations for the destruction of redundant, obsolete and trivial data – an action that can also help ensure an organisation is compliant with regulatory requirements such as Australia's privacy regulations.

Those organisations that are part of a larger information sharing coalition also tend to be those that prevail in times of challenge. This ability has been demonstrated by Ukraine, which had hardened its digital infrastructure in the face of attack from Russia, while also utilising a coalition of co-defenders including organisations within its cyber defence supply chain. These actions all made the task for its adversary so much harder.

> If you are prepared to augment your owned resources in times of crisis by leaning on a coalition you are a part of, then you are set up to thrive and prosper under all conditions.
>
> **Chris Inglis**

Building capability

Although much effort is devoted to defending against highly complex cyber-attacks, up to 85 per cent of successful attacks are the result of simple techniques such as phishing. This suggests that more work is needed to ensure citizens and workers fully understand how to defend themselves and their organisations.

> We teach our children more about crossing city streets than we do about navigating digital infrastructure. We don't need everyone to be a python programmer or a cyber expert, but we do need them to know something more about the consequences of their choices in a world that is existentially dependent on digital infrastructure.
>
> **Chris Inglis**

The volume and sophistication of cyberattacks make it critical that those people tasked with defending organisations have the appropriate critical thinking skills needed to interpret the threat landscape and respond accordingly.

And while defensive tools are evolving to incorporate greater levels of automation using artificial intelligence, this in no way negates the need for human responsibility in decision making. Human beings will need to remain the accountable party even in an era when the speed and sophistication of attacks is only ever increasing, meaning there will be a greater need for the development of human capabilities. Hence, it is important to ensure that those people tasked with defending organisations also have the critical thinking skills needed to interpret the threat landscape and respond accordingly.

Learning from the best

The learnings from cyberattacks are embodied in maturity frameworks such as those created by the US-based National Institute of Standards and Technology (NIST) and the Australian Signals Directorate's (ASD) Essential 8, which provide detailed guidance that can be used to help organisations understand where to direct investments.

These frameworks also aid with ensuring that organisations can meet the defensive requirements expected by their regulators.

Frameworks alone are of little value however, unless their recommendations are encoded within defensive strategies and tested on a regular basis. The best-defended organisations are those that constantly practice and test their defensive strategies, to ensure they build the 'muscle-memory' within their personnel that ensures that when a crisis scenario does unfold, they have a clear understanding of the actions expected of them.

> Organisations which have little to no practice under their belt have no idea what to do or how to respond in the moment of a crisis.
>
> **Kevin Thomas**

Conclusion

Cyber defence is not a technology issue, it is a business issue, but it is one that requires both a people-based and a technology-based response. As recent successful cyber-attacks have shown, no organisation is immune to cybercrime.

A strong defence requires an intentional approach that includes robust cycles of planning, testing, and refining based on the learning from each cycle. Only in this way can an organisation ensure that its defensive measures remain fit for purpose in a world where adversarial tactics are evolving quickly.

This means also broadening capabilities away from pure defence to also incorporate response and recovery to reduce the damage from an inevitable successful attack.

> You need to lead from the top, then understand the risk appetite of the organisation and acceptable tolerances, and then engage the entire workforce.
>
> **Melissa Osborne**

In the end, cyber defence is no different to any other risk anywhere else in the business, and this means it needs to be considered at the highest levels, as would all other risks.

That means stopping the conversation about cybersecurity, and starting one about a topic that really matters – business resilience.

The Information Security Executive Panel is a global series hosted by Iron Mountain.

London | Washington | Davos | Sydney

Iron Cloud data management: Your trusted partner for strategic cloud data management throughout the data lifecycle. Whether you need to archive, back up, recover, or protect against ransomware attacks, Iron Mountain recommends a multi-tier data storage approach to better protect, preserve and unlock the full value of your data. With Iron Mountain Iron Cloud®, you can reduce risk and save on storage costs—all while retaining access to your most critical business asset: your data.

About Iron Mountain

Over 90% of the Fortune 100
trust us to protect what matters most.

Over 70 years experience
managing and protecting information.

Trusted security
68 extrabytes of data under management.

Global scale
90M sq ft, 1,450 facilities 350MW data center capacity in 60+ countries.

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organisations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centres, art storage and logistics, and cloud services, Iron Mountain helps organisations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working.

Visit www.ironmountain.com/en-au for more information.

IRON MOUNTAIN®

1300 476 668 | ironmountain.com/en-au