Enhancing Threat Protection in 2022, Australia

Perspectives from senior security leaders during Dataminr's Threat Intelligence roundtable, November 2021

Dataminr®

Corinium

Contents

Click below to navigate

Executive Summary

With disruption rife across many industries over the past 24 months, shoring up risk management frameworks and processes has become a major priority for a number of organisations.

To stay ahead of and prepare for such disruption — including emerging risks and high-impact events — business leaders need access to real-time information on the incidents and crises that could negatively affect their organisation.
The growing need for this risk intelligence was the focus of a November roundtable hosted by real-time information discovery platform provider Dataminr, in partnership with Corinium.

In attendance were Australian security leaders from both the cyber and physical domains, who used the forum to discuss how they are advancing their threat intelligence strategies in 2022.
Additional discussion topics include how:

- Risk intelligence has been shaped by the COVID-19 pandemic.
- Organisations have brought teams from corporate security, risk and cyber together.
- Information security leaders are organising, and gaining executive sponsorship for, their risk intelligence programs.

In this report, we highlight many of the insights that came from the roundtable discussions.
Note that some insights have been edited for clarity and length. ■

Contributors

Luke Coley
APAC Sales Director,
Dataminr

John Donohoe
Group Intelligence Manager,
Woolworths

George Abraham
Chief Information Security Officer,
Novatti Group

Abhijith Nair
Cloud Security Architect,
Transport for NSW

Security Teams Step Up

Security leaders are providing expertise on broader business issues

Given the events over the past 24 months, including the COVID-19 pandemic and its effect on supply chains, customer behaviours, remote work and cyber attacks like ransomware, shoring up threat detection processes has become a topic of great interest and investment within the fields of risk and corporate and cyber security.

Dataminr Sales Director for APAC Luke Coley says since the pandemic, there have been dramatic changes across the threat landscape, in corporate, physical and cyber security.

"I'm seeing a lot of organisations developing cybersecurity and corporate security teams and aligning those to combat emerging threats. I'm keen to know how other teams are forming up and communicating across the business," he says.

As a large Australian retail organisation, Woolworths, has had both physical and cyber security functions collaborate to manage intelligence and risk during the pandemic.

John Donohoe, Group Intelligence Manager with Woolworths Group, says having a chief risk officer in the executive committee has been a huge benefit in terms of leadership to drive a risk mindset in decision making across the company.

"When COVID vaccination requirements were announced for staff, several risks flowed downstream from it," he says.

"Advice was able to flow up to decision makers in a cohesive manner from the right areas before decisions were made, and then flow back to inform how to manage the risks following those decisions. This helped instil confidence that decisions were made in line with our appetite for risk having taken a range of conflicting issues into account."

"Advice was able to flow up to decision makers in a cohesive manner from the right areas before decisions were made, and then flow back to inform how to manage the risks following those decisions"

John Donohoe
Group Intelligence Manager,
Woolworths

Bringing Issues to the Board

Dataminr's Luke Coley says having a direct line of influence into the board of directors has been increasingly important for organisations responding to the need for holistic risk intelligence.

"Cyber threats are a risk, staff safety is a risk. It makes sense over time that we will see these things fall under a chief risk officer or be reported directly to the board," he says.

George Abraham, Chief Information Security Officer at Novatti Group, an ASX-listed fintech company and payments handler, says his role has a dotted line into the board, which promotes risk awareness and communication.

"Every quarter I present to the board, and that makes it easier for me to push initiatives," he says. "In my previous role it was quite similar. While I'd report into the executive team, being able to also present to the board each quarter helps to make the whole organisation more cyber aware." ■

Facing Business Disruptions

New risk topics emerge and close collaboration becomes critical

Consumer behaviours influenced by hybrid and remote working models, and increased online consumption has influenced disruptions in processes and supply chains.

Dataminr's Luke Coley says in 2021 there had been a natural increase in security concerns throughout the pandemic as working from home and restrictions were put into place. Cybersecurity incidents rose sharply, misinformation was abundant and the amount of technology-enabled fraud and scams spiked.

"Phishing attempts, ransomware and also public safety and unrest have become increasingly topical," he says.

Commenting on the new threats and challenges arising for Australian CISOs, Transport for NSW Cloud Security Architect Abhijith Nair says the shift to remote work has required the need for data to become accessible to all staff, irrespective of their work location.

"When everyone started working from home, productivity increased. Everybody wanted to get the work done and wanted access to all the tools required to do that work, which required new processes, features, and developments around security that we had to enable or develop," he says.

"The amount of cumulative risk increased many-fold. Because of that, the attack vectors increased. Our intelligence variables also increased. The challenge is to have a mechanism to digest this data and produce actionable information."

> *"When everyone started working from home, productivity increased. Everybody wanted to get the work done and wanted access to all the tools required to do that work, which required new processes, features, and developments around security that we had to enable or develop."*
>
> **Abhijith Nair**
> Cloud Security Architect,
> Transport for NSW

Finding Fusion to Fight Risk

In response to new and emerging risks, another security executive from a large Australian retail enterprise suggested recent disruptions had driven an even greater need for fusion between the corporate, physical and cyber security teams. They would then have better oversight of all the systems and touchpoints in place and be able to collaboratively manage risk for the business and customers.

Transport for NSW's Abhijith Nair says with the need for organisations to offer enhanced services comes increased collaboration. In Nair's experience, the Service NSW app, which brings together many of the state's government services into one portal for citizens, was a key example of this.

"The Service NSW app started to get used very widely for COVID check-ins. A lot of teams that traditionally would work in silos became more aligned," he says.

"In an app development lifecycle, sometimes the approach is to build and then fix, but the pandemic has impacted turnaround times. So, building securely first became the approach. The constant interaction of all teams responsible for the project and delivery resulted in a secure and usable application. Continuous communication and acknowledgement of the significance of each other's contribution was the key." ■

Measuring the Impact of Investments on Risk Intelligence

Spending can be justified by showing process or predetermining outcomes

Whether it's in creating or hiring new roles, standing up new technology or launching specific projects, many organisations have made various investments to help improve their risk intelligence capabilities in light of COVID-19.

"A Gartner study recently stated that 78% of CISOs had 16 or more tools in their cyber ecosystem, while 12% had 46. That complexity, and the people to support those tools and programs and move it forward is considerable," Dataminr APAC Sales Director Luke Coley says.

"Given that, I want to understand how cybersecurity leaders are demonstrating to the board the value in security investments and how they approach it."

One unique aspect of security as a business function, be it cyber or physical, is that when managed well, it can go unnoticed by the wider organisation. While this is helpful in keeping business focused on core goals, it can make understanding the effectiveness of security investments difficult to understand.

Security leaders are addressing this by starting conversations about investment and risk appetite.

"It can be tricky to define risk appetite in practical and meaningful terms. Particularly in security," Woolworths' John Donohoe says. "Everyone is against downside risk, but too much risk aversion in a general sense without zooming in a bit closer to really understand what that means can limit opportunities.

"Instead of saying, 'We want to spend this much money on software and solutions' to limit exposure, the conversation starts at what the risk appetite is and what a reasonable response is to demonstrate with confidence we are operating in line with that appetite. Then business cases for investing in preventative and reactive controls should become a lot more clear."

"Everyone is against downside risk, but too much risk aversion in a general sense without zooming in a bit closer to really understand what that means can limit opportunities."

John Donohoe
Group Intelligence Manager,
Woolworths

Goal and Outcome-Based Converged Security Spending

Novatti Group Chief Information Security Officer George Abraham says putting a business case behind an investment is all about risk appetite.

"I explain this in a different way, I compare cyber to health and fitness. I ask where the organisation wants to be," he says.

"Do they want to run a marathon, for example? If that's the level they want to be, they do need the 40 cyber tools, have threat intelligence coming in from three different sources, and have a 24/7 security operations centre. If they want to play at that level, that investment is necessary.

"If you just want a healthy BMI, good blood pressure and be generally healthy, then you probably don't need $3 million in investment."

Another strategy that CISOs discussed involved introducing a security outcomes approach to managing investment.

In that approach, certain security outcomes would be identified so the cost could be weighed against the risk. For example: a ransomware incident must not be allowed to spread to a second work site. This strategy provides a clear goal for the business and allows the cyber team to prescribe the solutions and cost to achieve it.

Dataminr's Luke Coley says hearing the various investment vs appetite strategies that different teams are considering was similar to what he had observed across the market, noting it as a positive sign.

"It's great to see the shift away from reactive," he says. "There might still be a way to go to get to be completely proactive, but there is definitely a shift away from this situation where the wallets open up only after a breach or event has occurred.

"It feels like we're moving in a more constructive direction by making risk more of a forethought considering all the disruption taking place, and that's quite positive."

Conclusion

Across Australia, organisational focus on and planning around threat intelligence and risk has accelerated since the onset of the pandemic.

While businesses may at one time have only made investments or developed strategies in risk intelligence after a disruptive event, today, progress towards proactive threat protection is being made.

Ensuring closer collaboration among risk and security experts, having a clear risk-focused position, and investing in security outcome-dependent technology are among the ways large Australian organisations will manage risk into 2022. ■

About Dataminr

Dataminr delivers the earliest warnings on high impact events and critical information far in advance of other sources.

Recognised as one of the world's leading AI businesses, Dataminr enables faster response, more effective risk mitigation and stronger crisis management for public and private sector organisations spanning global corporations, first responders, NGOs, and newsrooms.

Recently valued at $4.1B, Dataminr is one of New York's top private technology companies, with 800+ employees across seven global offices.

Learn more: https://www.dataminr.com/

Dataminr®

About the Editor

Michael Jenkin is an editor and journalist with more than a decade of experience producing content across broadcast, print and digital media. He specialises in enterprise IT and technology writing.

At Corinium, Michael develops content to inform and support data and analytics and information security executives.

To share your data story or enquire about appearing in a Corinium report, blog post or digital event, contact him directly at michael.jenkin@coriniumgroup.com

Discover More Essential Information Security Insights

As anyone who has attended our global conferences or events will know, our 300,000-strong network of information security leaders boasts many of the most forward-thinking minds in the industry.

Our new content hub, **Business of InfoSec**, brings those same essential insights direct to you and is packed with exclusive research, video podcasts, in-depth articles, interviews, and reports. Discover how other information security leaders are tackling the challenges they face today while maintaining the confidentiality, integrity, and availability of their organization's data.

For a limited time, subscribing to the **Business of InfoSec** is free. So, make sure to subscribe today for complimentary access to exclusive insights you just can't find anywhere else.

SUBSCRIBE NOW

Corinium

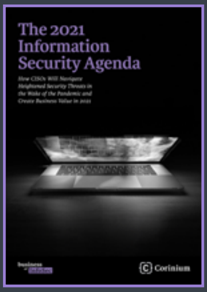
Partner with Business of InfoSec by Corinium

We'll develop industry benchmarking research, special reports, editorial content, online events and virtual summits to establish your brand as an industry thought leader.

FIND OUT MORE HERE

Supply Chain Security Trends, Australia
2022
Australian cybersecurity leaders discuss challenges in supply chain cybersecurity management and consider best practices for security teams
RAPID7
Corinium

Vulnerability Management Trends in Australian Government
The shifts Australian government cybersecurity leaders are seeing and responding to as the need for effective patching increases
Qualys.
Corinium


The 2021 Information Security Agenda
How CISOs Will Navigate Heightened Security Threats in the Wake of the Pandemic and Create Business Value in 2021
business of InfoSec
Corinium

Discover Corinium Intelligence

Corinium is the world's largest business community of more than 700,000 data, analytics, customer experience and digital transformation leaders.

We're excited by the incredible pace of innovation and disruption in today's digital landscape. That's why we produce quality content, webinars and events to connect our audience with what's next and help them lead their organisations into this new paradigm.

Find out more: www.coriniumintelligence.com

Connect with Corinium

Join us at our **events**

Visit our **blog**

Read our **reports**

Follow us on **LinkedIn**

Like us on **Facebook**

Find us on **Spotify**

Find us on **YouTube**

Find us on **iTunes**