COMMVAULT

Transforming Cyber Security

The Emergency Services CXO Imperative

Brad Howarth, Moderator

James Fell, Department of Premier and Cabinet Victoria

Simon Newman, Cyber Resilience Centre for London

Matt Palmer, Community Emergency Response Team (CERT), Jersey

Jonathan Hatchuel, Commvault

Australia's emergency services have had a lot to contend with this decade, but aside from the constant onslaught of natural disasters, more insidious threats are waiting. The growing dependency of frontline responders on digital services means cybersecurity is now a critical consideration, especially given the chaos that could ensue should any agency suffer a cyber-related outage. The cyber threats to frontline responders and techniques for protecting them was the key focus for a recent discussion hosted by 6 Degrees Media and Commvault. Industry leaders including the Emergency Services Sector CISO at Department of Premier and Cabinet Victoria, **James Fell**, and international speakers **Simon Newman** from the Cyber Resilience Centre for London and **Matt Palmer** from Jersey's CERT, joined with Commvault's Director for Enterprise and Public Sector **Jonathan Hatchuel** and other cyber CXOs to discuss the threat landscape and the latest techniques for keeping critical workers safe from cyber threats.

Australia's emergency services and first responders have built their reputations around the ability to respond quickly to whatever situations come their way, and they invest in the latest technology and training to ensure they maintain that strength. That same thinking is coming to define their response to cyber threats, with agencies today investing in new processes and technologies to minimise cyber risk and maximise the effectiveness of their response.

According to the Emergency Services Sector CISO at the Department of Premier and Cabinet Victoria, James Fell, the Victorian Government was constantly looking for innovative ways to protect emergency services. In one instance he said the realisation that 80 per cent of incidents commenced with some form of phishing attack had led the government to implement an advanced secure machine learning gateway, which detected these attacks and either alerted recipients to the suspicious behaviour, or blocked the attacks outright.

Fell said another successful initiative had been the implementation of a password blacklist solution, which enabled staff to maintain non-expiring passwords by preventing them from using weak and publicly breached passwords. "One thing that everyone doesn't want to have to do all the time is change their passwords," Fell said. "It's this brilliant double-edged sword, where it increases security but it's better for the user."

Another new addition to the state's arsenal had been next generation anti-virus and extended detection and response (EDR) capabilities. "We did a whole heap of independent testing just to ask if it is actually better, and the answer is yes, it is," Fell said. "It also is significantly better for the performance of your machines, so you get a performance benefit, which is brilliant."

A Team Effort

Phishing has also been a constant problem on the British island of Jersey. The Director of the Community Emergency Response Team (CERT) for Jersey Matt Palmer noted that these attacks had become more sophisticated in nature, including one that had recently targeted the island's commercial sector, and required a coordinated approach.

"When we looked at this in another level of detail, what it turned out to be was a business email compromise of a number of companies all around the world," Palmer said. "We were able to stop that, because a couple of them got reported into us. We notified the rest of the industry and that allowed others to identify when they were being attacked.

"One of the things that we've learned from that is that it's important to really be ahead of the game. We're in a position where we're looking at the cyber issues on the island, and more broadly, and can understand and talk about it in a shared way before it actually becomes an issue."

This idea of community and communication was also being adopted by the Cyber Resilience Centre for London, where Interim CEO Simon Newman said success had come through bringing different emergency services teams together to improve interoperability.

Newman said the speed and frequency of attacks now was leading emergency services organisations in the UK to consider an approach to cyber security called defence-in-depth, which he likened to treating an organisation like a medieval castle.

"You've got your really sensitive, delicate information right in the keep in the middle of the castle, but you've got a series of walls and perhaps a moat outside as well," Newman said. "It's about having the right mechanisms in place to keep your data as secure as you can."

Delivering Social Strategies

Not all solutions to the cyber crisis are technical, and the need to strengthen security practices had led attendees to more actively consider the culture within their organisations might be influenced to reinforce more secure practices.

Fell said it was important to first acknowledge that culture of an organisation was set by the people in the organisation, and the best way to influence them was to start with the people at the top.

"Across the Victorian government, and in the emergency services, we've started with board level training and executive training," Fell said. "The training teaches them to ask the right questions, and if they're asking the right questions for you, then hopefully the training and culture initiatives will answer those questions."

Newman agreed that culture was critical, as it was ultimately an organisation's staff who would prove to be the strongest link in the defensive chain.

James Fell, Department of Premier and Cabinet Victoria

> **"Across the Victorian government, and in the emergency services, we've started with board level training and executive training. The training teaches them to ask the right questions, and if they're asking the right questions for you, then hopefully the training and culture initiatives will answer those questions."**
>
> – James Fell, Department of Premier and Cabinet Victoria

Simon Newman, Cyber Resilience Centre for London

> **We need to create cultures in organisations which actually reward positive behaviour, because we know that the quicker that we can respond to someone clicking on a malicious link, the better chance that we've got on reducing the impact on an organisation.**
>
> – Simon Newman, Cyber Resilience Centre for London

"We need to create cultures in organisations which actually reward positive behaviour, because we know that the quicker that we can respond to someone clicking on a malicious link, the better chance that we've got on reducing the impact on an organisation," Newman said. "We want to encourage people to report to their internal managers and IT staff as quickly as possible, so regular training is really good. This is where the role of the CISO is really importantly, in terms of promoting the right culture in an organisation."

Protection in Practice

While technology and training were critical, even the best strategies could prove ineffective if they weren't tested on a regular basis. According to the director for enterprise and public sector clients at Commvault, Jonathan Hatchuel, this meant that the best time to test if a strategy actually worked was before it was needed.

"It's no use testing your restoration at the point of an incident – you have to have active restore tests all the time," Hatchuel said. "Testing your immutable copies and your recoverability on an ongoing basis will give you some peace of mind that even if a bomb was planted a while back, you've caught it, you've eradicated it, and you can restore back to a known point in time."

Fell said his team had taken a targeted approach to cyber incident response training that focused not just on the theory, but its execution from a a technical perspective.

"Desktop exercises are great, and you can have a lot of fun with them as well because you can do the worst-case scenarios," Fell said. "But at the end of the day, they're really only testing the comms and the words on the plan, they're not actually testing how to technically respond to that incident."

In Jersey, Palmer said he and his peers had scaled up their incident response exercises to look across the island's entire economy to see how a single incident could affect multiple sectors.

"You're not going to see something that just targets one organisation - you've got to work through what are those scenarios, such as what happens if we lose comms capabilities or our cloud support infrastructure is affected," Palmer said. "What I've found really makes a difference is having that collaboration ahead of time and having it in a really structured way."

What's Next

All attendees agreed that one of the common challenges they faced was the difficulty in attracting and retaining cybersecurity talent. This was especially problematic for Palmer, being located on an island with a population of just 100,000 people, and has led him to take some novel approaches to bridging the skills gap.

"I pretty much know all the cybersecurity professionals on the island," Palmer said.

"Rather than just trying to hire people who are already employed with cybersecurity roles, one of the things that we've done is launch an apprenticeship program. They do four days a week with us, and one day a week they go and study with a leading university off in the UK.

"I know at the end of that, that apprentice will then go on and work somewhere else. That's absolutely fine, because I'm increasing the number of skills going into that sector. I don't have a problem with that at all, as long as everybody else is also investing."

The high likelihood that skills will remain in short supply for the foreseeable future made it all the more important that security leaders continued to examine the emerging technology landscape. According to Hatchuel, automation was a field that should be of particular interest to skills-pressured security leaders.

"The capability in the products today is significantly ahead of where it was even 18-24 months ago, so staying on top of what's new in the sector is really important," Hatchuel said. "New capabilities and automation can help you make the most of the skills and talent you have in the organisation today."

Fell said his team had chosen so-called SOAR tools, which provide capabilities in security orchestration, automation, and response, to boost their cyber defences.

"These are highly sophisticated but extremely effective with automating manual tasks," Fell said. "The way that we've done it is pretty innovative. We're looking to share threat intelligence out across the entire government, and search for potential compromises automatically within our departments and entities' databases and other common technology platforms, like next generation anti-virus."

Riding the Wave

With the threat of cyberattacks increasing daily for all industries, the likelihood of suffering a cyber incident is not a question of if, but when. Emergency services agencies are no exception, but must nonetheless take a much more stringent approach to security practices than other industries thanks to the criticality of their work.

According to Hatchuel, this adds an extra dimension to their cyber strategies. "It's not a case of if or when, it's a case of how quickly they can recover," Hatchuel said. "Obviously identification and threat prevention are critical, but of equal importance is the ability to recover really, really quickly."

The reasoning is simple, and according to Fell, it comes from the knowledge that should a frontline agency fall victim to a cyber incident during an emergency, the result could be catastrophic.

"It could be particularly devastating for the requirement to be both rapid and always available," Fell said. "We're seeing an increase of attacks, but we're also actually seeing attacks that we didn't see previously."

Matt Palmer, Community Emergency Response Team (CERT), Jersey

"Rather than just trying to hire people who are already employed with cybersecurity roles, one of the things that we've done is launch an apprenticeship program. They do four days a week with us, and one day a week they go and study with a leading university off in the UK."

– Matt Palmer, CERT

Jonathan Hatchuel, Commvault

"Obviously identification and threat prevention are critical, but of equal importance is the ability to recover really, really quickly."

– Jonathan Hatchuel, Commvault

COMMVAULT

About Commvault

Commvault is a global leader in data management. Our Intelligent Data Services help your organisation do amazing things with your data by transforming how you protect, store, and use it. We provide a simple and unified Data Management Platform that spans all your data – regardless of where it lives (on-premises, hybrid, or multi-cloud) or how it's structured (legacy applications, databases, VMs, or containers). Commvault solutions are available through any combination of software subscriptions, integrated appliances, partner managed or Software-as-a-Service via our Metallic portfolio. In addition, integrations are available for O365, Salesforce, ServiceNow, and other leading business applications. Throughout 25 years, more than 100,000 customers have relied on Commvault to keep their data secure, assessable, and ready to drive business growth. Learn more at www.commvault.com

---

6 DEGREES MEDIA
WHERE LEADERS CONNECT

About 6 Degrees Media

6 Degrees Media was established by Angela Horvat, former Editor and Publisher of award-winning publications including *Computerworld*, *Information Age*, *My Business*, *The Who's Who of Financial Services* and Founder of FST Media; and Emma Charter, one of Australia's most connected and respected media and events strategists with more than 15 years' experience in delivering C-Level engagement strategies for clients in Australia and the UK. Together, they lead a team of Australia's most talented and driven conference producers, technology and business journalists and event managers to create content-driven experiences across C-level roundtables, custom events and large-scale conferences. For more information, please visit 6degreesmedia.com.au