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

Contents

Click below to navigate

Executive Summary

The vulnerability and patch management landscape is under renewed focus because of increasing compliance pressures and demand for organisational resilience and visibility over systems.

Cybercriminals remain fixated on discovering exploits within hardware and software systems. In the interest of Australians everywhere, the importance of maintaining and improving vulnerability and patch management processes within Australian government departments is considerable.

Informed by insights from security experts with experience in Australian government agencies, this report will explore how cybersecurity leaders develop and run successful, modern vulnerability, asset and patch management practices.

Over three chapters we will consider the state of the vulnerability management landscape from a government perspective, identify major challenges cybersecurity professionals might expect to come against in applying good patch management, and discuss useful considerations for ongoing resilience. ■

Contributors

Jonathan Owen, Acting Chief Technology Officer, Australian Capital Territory Government

Julian Valtas, Acting Chief Information Security Officer, Australian Capital Territory Government

Jamie Norton, Former Chief Information Security Officer, Australian Taxation Office, Partner, McGrath Nicol

Kathryn Green, Director Digital Technology, CIO & CISO, Australian Radiation Protection and Nuclear Safety Agency

Asaf Ahmad, Former Chief Information Security Officer, NSW Fire & Rescue, President, ISACA Sydney Chapter

Walter Manyati, Director Technical Account Management, ANZ, Qualys

Vulnerability Management from a Public Sector Perspective

Government cybersecurity leaders face an extra level of accountability

Running vulnerability assessments and patching operating systems, applications and devices has always been a critical practice for cybersecurity leaders in ensuring the security of systems.

The increasing sophistication of cyber-attacks as well as the importance and volume of data entrusted to government organisations has only reinforced the need to have effective vulnerability and patch management processes embedded within government departments.

In 2020, the Australian Government revealed organisations, including those at "all levels of government" were being targeted by a state-based actor with "significant capabilities". 2021 has also already seen several examples of zero-day exploit discoveries.

Threats have driven stronger regulation around cybersecurity compliance, including tightened rules around patch management. In 2017 The Australian Cyber Security Centre published the Essential 8, a revised set of mitigation strategies recommended for organisations to defend against cyber threats.

Included in those baseline strategies was 'patch operating systems' and 'patch applications' as recommendations. In July 2021 an update to the strategy classified patching as mandatory for government departments.

The profile of security and in particular, patch and vulnerability management, has increased recently in response to both threat and compliance demands, according to Australian Capital Territory Government acting Chief Technology Officer Jonathan Owen.

"From my perspective, some of the high-profile cases have given more opportunity for governments like us or internal providers to actually have higher level conversations across government," he says. "We may otherwise not necessarily have been sitting at the board table having the conversation with people around cybersecurity being one of the top five risks around across government."

Owen says the Federal Government's acknowledgement of a state actor in 2020 was a particularly important example of security in government being widely publicised.

"Having front page headlines has certainly prompted business owners to ask questions about their security posture as well as what kinds of things organisations need to be concerned about," Owen says.

> *"Some of the high-profile cases have given more opportunity for governments like us or internal providers to actually have higher level conversations across government."*
>
> **– Jonathan Owen**
> Acting CTO,
> ACT Government

Risk Position and Considerations

Government organisations in Australia are not vastly different from private commercial enterprises in terms of their exposure to bad actors looking to exploit vulnerabilities. But with scrutiny from both parliament and the public, as well as certain reporting requirements, they are uniquely positioned in their accountability.

ACT Government acting Chief Information Security Officer Julian Valtas says while the ACT Government does not hold national security classified data, it's security and technology team's remit extends to portfolios that are identified as critical infrastructure sectors, including state hospitals and transport services.

Consequences of risks being realised against a number of directorates' critical outputs and processes supported by ICT systems, has drawn needed attention to vulnerability management.

"We've seen a big ramp-up in support from the Federal Government through the Australian Cyber Security Centre. We are getting access to a lot more threat information and we strongly live and breathe the ACSC's Essential 8," Valtas says.

Former Australian Taxation Office CISO Jamie Norton says the obligation to protect public assets was front and centre during his three-year tenure with the agency.

"For agencies like the ATO, that has data on nearly every adult citizen in Australia, not to mention every company and all the financial characteristics of those companies. It certainly wasn't lost on us," he says.

"The criticality of that data and the sensitivity of that data was not just part of my role but also owned by the executive as well. They had a strong understanding of the implications of getting anything wrong."

Given the Essential 8 is a must-do for government agencies, demonstrating compliance and being assessed is another element of the job that public sector cybersecurity leaders contend with.

"The Australian government has certain requirements that apply to us as an agency. We have to adhere to these and regularly report on our compliance. We regularly do maturity assessments and we show the process that we're going through to improve our maturity levels," says Kathryn Green, CISO for The Australian Radiation Protection and Nuclear Safety Agency (ARPANSA).

> *"We regularly do maturity assessments and we show the process that we're going through to improve our maturity levels"*
>
> – **Kathryn Green**, CISO, Australian Radiation Protection and Nuclear Safety Agency

Managing and Oversight

Asaf Ahmad, former Fire & Rescue NSW CISO and now CISO and President of his consulting firm CyberEx, says the vulnerability management space is constantly changing. To this end, CISOs are under more pressure than ever to think strategically and get buy-in from their organisations to do the job.

"Vulnerabilities are being discovered as we go. So once a patch becomes available for deployment, a weakness is known. If you don't apply that patch, somebody could try to exploit it," he says.

ACT Government acting CTO Jonathan Owen says it's important for government CISOs to think about two levels of conversation to have within the department or organisation when it comes to managing security.

"At the executive level it's a conversation around cyber hygiene and cyber-risk. Those are ongoing things we need to be regularly educating people on and one of the key parts of hygiene is vulnerability management," he says.

"Whereas in the technical areas where we are given critical information from sources like the ACSC, they expose the real, tangible reasons behind breaches like phishing and patching. Those are immediate, practical things that if not responded to quickly put you in a lot of trouble."

Kathryn Green says part of her strategy as CISO at ARPANSA is to keep infrastructure manageable.

"To make sure our approach to vulnerability and patch management is well-organised, we have a policy of minimising the number of technologies in use by preferencing the Microsoft technology stack, in particular Microsoft Azure, Office 365 and associated security and compliance platforms," she says.

"Smaller agencies like ours, and in fact many agencies, are looking at minimising the number of technology platforms that are used and are standardising desktop environments."

Former ATO CISO Jamie Norton says having complete oversight of a network, its assets and their criticality is a top priority in cybersecurity, but it's not always a given.

"You may have pockets of space where you don't have full visibility or you may not even have much idea at all about the network depending on the maturity of your environment. Vulnerability management gives you that visibility of the environment," he says. ■

> *"Vulnerabilities are being discovered as we go. So once a patch becomes available for deployment, a weakness is known."*
>
> **– Asaf Ahmad**
> Former Fire & Rescue NSW CISO

Challenges in Vulnerability Management

From unique applications to machines that can't just be turned off, patching isn't always straightforward

With a heightened threat landscape and increasingly stringent compliance regulations, cybersecurity leaders in government are compelled to shore up vulnerability management processes.

But while resources exist that mandate what must be done in order to achieve maturity against a framework like the Essential 8, the vulnerability journey is littered with challenges.

"There's an interesting aspect to the regulatory framework in that it can sometimes create a compliance burden that doesn't necessarily reflect the risk you are trying to tackle," Former ATO CISO Jamie Norton says.

"You can get caught up in the wording and embedding because it says you have to, while losing sight of the intent of what you are trying to do. That was something we had to be really careful of."

Norton says recent changes to the Essential 8, which mandate vulnerability management as a requirement for baseline maturity and compliance, run the risk of being treated as box-ticking exercises that result in incessant scanning and data piling up that doesn't guarantee an outcome.

"That might end up earning you compliance but it's not effective," he says. "I think that's where departments can lose momentum; if teams become solely focused on the regulation and not so much about the overall effectiveness or the outcome."

Former Fire & Rescue NSW CISO Asaf Ahmad says despite the Essential 8 demanding immediate patching in cases of the most critical patch releases, this advice doesn't help for zero-day scenarios.

"Patches are classified depending on how critical they are, this helps cybersecurity leaders implement them according to their patching cycles," he says. "But in the case of zero-day vulnerabilities, wherein a vulnerability has been discovered and a patch for it doesn't exist, cybersecurity leaders need to have workarounds so that exploit can't be used to cause damage."

"There's an interesting aspect to the regulatory framework in that it can sometimes create a compliance burden that doesn't necessarily reflect the risk you are trying to tackle"

– **Jamie Norton**, Former CISO, Australian Taxation Office

Unique Systems and Isolation

While compliance or regulations represent the beginning of a vulnerability management approach, the standards don't account for each unique use case.

ACT Government acting CISO Julian Valtas says there may be situations in which it becomes bad practice to follow a piece of compliance advice to the letter, in which case cyber teams and analysts need to think strategically.

"Even some of the things that the ACSC suggest, like 48-hour patching, for example, can create a challenge. Sometimes mission-critical systems may not lend themselves to 48-hour patching with robust testing," Valtas says.

"The value of our own analysis is making an assessment about whether or not the system has out of band access. Has it got firewalls, strong authentication and other security controls?

"We try to enrich the context of what a given vulnerability means to us. For instance, if a vendor rates something as high risk, the way we've implemented that system on our network might put us at a much lower level of exposure."

ARPANSA CISO Kathryn Green says her organisation, which is a chiefly scientific agency focused on complex testing, measuring and safety assurance, says her team must also discover ways to reduce risk around hard-to-patch equipment.

"Some scientific systems are really integral to the work of the organisation, and we don't want to stop using them," she says.

"But they can be potentially vulnerable if they are not updated or patched as regularly as we would like. We always do a risk assessment when considering the frequency of patch timings and review advice from the ACSC and manage accordingly."

Another pain point for cybersecurity leaders can arise when critical applications reside on legacy hardware, which doesn't lend itself particularly well to scanning or appearing on the network, Qualys Director for Technical Account Management in ANZ Walter Manyati says.

"Legacy systems are difficult to manage simply because an organisation might have a reliance on them. For example, an old instance of a piece of enterprise resource planning software that talks to many other devices or services," he says.

"In the best environments I've seen, there's a plan in place to move away from these or to make sure that it's kept as robust and secure as possible. In the worst environments, people just say, 'Well it's there and we can't do anything about it'. With those, it's necessary to consider a good risk management process. Understanding how many of these types of assets there are, where they are, who owns them and what runs on them."

> *"Legacy systems are difficult to manage simply because an organisation might have a reliance on them. For example, an old instance of a piece of enterprise resource planning software that talks to many other devices or services."*
>
> – **Walter Manyati**, Director for Technical Account Management, ANZ, Qualys

Software Diversity and Demand

The diverse needs of the many business areas of government make the issue of scale and software demand and complexity another major challenge, according to ACT Government acting CISO Julian Valtas.

"Updating and packaging software and analysing threats and vulnerabilities takes a lot of labour effort to manage effectively, even when supported by good tooling," he says.

"The ACT Government has both the functions of a local and state government all in one. We have hundreds of discreet business units under eight directorates and whilst we all enjoy 'core' software like Office 365, browsers, video conferencing tools and media players, there is niche software required to support many business units.

"This is one of the reasons the government has a cloud-first strategy backed by governance to ensure that information has appropriate security measures."

Valtas adds while there is often demand for new software from departments, each must be considered very carefully.

"Whilst we could package up a piece of requested software for government, it would become another software package with frequent updates required for security and capability that would need to be owned by a business unit for the lifecycle of the application," he says.

"This sprawl can be a real struggle from my perspective and the total cost of ownership of effective patch and vulnerability management when the application portfolio is large."

ARPANSA CISO Kathryn Green says the agency frequently launches new projects and likes to innovate, with staff often interested in new software solutions. This presents procurement challenges.

"We need to understand how a new system works and we need to understand what impact this new system is going to have on our cyber security landscape," she says.

"Meeting our organisation's strategic objectives and solving business problems along the way is so important but being able to make new products work and fit with our cyber security landscape can be really challenging.

"Despite what some might think, cyber security people do dislike being the ones to say 'no'." ■

> ***"Sprawl can be a real struggle from my perspective and the total cost of ownership of effective patch and vulnerability management when the application portfolio is large."***
>
> **– Julian Valtas**
> Acting CISO, ACT Government

Best Practice Thinking in Vulnerability Management

Plan ahead, know your environment and make the work manageable to succeed

Meeting compliance, overseeing complex networks, avoiding downtime of critical systems and contending with procurement creates constant strategic challenges for government cybersecurity leaders.

Every government agency is different, and our expert contributors each have some familiar but reliable means of realising effective vulnerability and patch management.

Former ATO CISO Jamie Norton says, ideally, CISOs should be outcome-focused, prioritise and consider what is manageable as vulnerability management maturity is built up.

"Avoid the temptation to try and boil the ocean," he says. "Instead, deploy vulnerability management in bite-sized chunks where you can manage remediation and not become overwhelmed.

"Focus initially on the most critical risk areas, such as vulnerabilities in external-facing systems with known exploits."

ARPANSA CISO Kathryn Green says her approach starts with a formal plan.

"I'm very much a strategic person so I love a plan. I love a roadmap," she says. "You do an assessment against the variety of criteria to find out where you're lacking, what you're doing well, what you're not doing so well, and your points for improvement. You set up a roadmap of how you are going to get there, you let the executive and your leaders know what's going on and you work towards that.

"You need to rinse and repeat that too. It's common to come up with a three-year roadmap but that's quite long. "You'll probably end up getting two years in and starting a new one as you gain clarity."

> *"It's common to come up with a three-year roadmap but that's quite long. You'll probably end up getting two years in and starting a new one as you gain clarity."*
>
> **– Kathryn Green**
> CISO, Australian Radiation Protection and Nuclear Safety Agency

Ownership, Visibility and Tools

Vulnerability management means getting visibility of systems and maintaining it, so it may sound obvious to advise cybersecurity leaders to 'do vulnerability management'. However, the alternative, in which organisations are more reactive than proactive in defending systems, has no place in government, ACT Government acting CTO Jonathan Owen says.

"It's extremely important that we have a holistic view of every asset and all of our hosted infrastructure. You can't patch what you don't know about. So we have made investments in certain tools to help us there," he says.

"We have a mature ITSM solution instance which does audited discovery of what's on the network, so we do have a good configuration management database (CMDB) of assets and what we manage."

"We also believe in the shared responsibility model for the Software as a Service and Platform as a Service offerings we consume," ACT Government acting CISO Julian Valtas adds. "In these models, vulnerability management is simplified back to a secure configuration management burden and removes that patch and verification cycle experienced with our on-premises environment."

Qualys Director for Technical Account Management in ANZ, Walter Manyati, says delegating asset ownership and patching is another way cybersecurity leaders can lighten their own workloads.

"Across Australia and New Zealand, a lot of the CISOs aren't so far removed from their people that they couldn't get a dashboard or a report with detailed asset and user information to see very quickly who's doing what," he says.

"I think it works in our favour. Some organisations have large vulnerability management teams of 50 or more people, some only have two. A good cybersecurity strategy can support asset ownership delegation and allow for dashboarding for CISOs to monitor that."

> ***"It's extremely important that we have a holistic view of every asset and all of our hosted infrastructure. You can't patch what you don't know about."***
>
> **– Jonathan Owen**
> Acting CTO, ACT Government

Involve the Executive and sit in on Procurement

One approach that has helped build confidence and success in the ACT Government's vulnerability management program has been the ability to influence organisational culture, says ACT Government acting CISO Julian Valtas.

"From a security point of view, we have made our ICT executive and technical areas know that even if they know nothing else about security, it's critically important to understand what the ACSC Essential 8 security controls are," he says.

"As vulnerability management touches two of the 8 controls (patching operating systems and patching applications) we reinforce this messaging to the 'why' along with the critical nature to ensure all stakeholders understand the requirement.

"This is done consistently in our messaging, whether at branch meetings, contributions to systems designs, change management requirements and increased reporting to support vulnerability management. We also acknowledge that patching takes a lot of effort, but once all the different teams – whether end-user compute, networks, or server team – understand the impact of getting this wrong and the role they play, it does become easier."

ARPANSA CISO Kathryn Green, who advocates for simple, standardised technology stacks for smaller agencies where possible, also advises CISOs be highly involved in procurement.

"Procurement is really important. The Federal Government has whole-of-government panels which are highly recommended for us to use," she says.

"The CISO role has been beefed up quite a bit over time and there's a responsibility for us to be across all third-party vendors as well as the organisation's supply chains.

"It's really important for us to understand the components, the technology and the scientific equipment systems as soon as they hit the network. To that end, we have to be involved in the procurement and the vendor management and the contract management." ■

"From a security point of view, we have made our ICT executive and technical areas know that even if they know nothing else about security, it's critically important to understand what the ACSC Essential 8 security controls are."

– Julian Valtas
Acting CISO, ACT Government

Conclusion

Cybersecurity professionals in government, under pressure both from the threat of intrusion as well as mandated regulatory compliance, must think strategically to achieve effective vulnerability and patch management while keeping services that serve the Australian public highly operational.

Compliance requirements are tightening, threat landscapes are widening, and resources are seldom abundant. There are indeed unique challenges realised by public sector cybersecurity leaders. The experiences and considerations presented in this report hopefully inform some thinking and strategy with respect to navigating vulnerability and patch management in government departments and beyond. ■

About Qualys

The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

More than 19,000 global businesses in more than 130 countries trust Qualys to underpin digital transformation for greater agility, better business outcomes, and substantial cost savings.

Qualys.

Find out more: https://www.qualys.com

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

2021 Global
Top 100 Leaders in
Information Security

Highlighting the Achievements of Corinium's Global Network of Information Security Leaders

Financial Services
InfoSec Trends
2021

How Financial Services Cybersecurity Leaders are Guarding Their Companies Against the Latest Information Security Threats

The 2021
Information
Security Agenda

How CISOs Will Navigate Heightened Security Threats in the Wake of the Pandemic and Create Business Value in 2021

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**