Decoding a hacker's playbook in public sector cybersecurity

verizon

Produced by

InnovationAus.com

Introduction

Public entities are prime targets for cybercriminals. Bastien Treptel's journey from teenage hacker to cybersecurity expert sheds light on why these agencies attract such attention with their wealth of sensitive data and critical infrastructure. As Mr Treptel noted, "Anyone with an IP address is vulnerable to simple net biohacks."

Mr Treptel joined Rob Le Busque, Verizon's Regional Vice President, and InnovationAus.com publisher Corrie McLeod to discuss how decision-makers in the public sector traverse a landscape very different from their private sector peers.

They're challenged daily, including working with diverse standards and policies, managing legacy systems, and grappling with infrastructure shaped by years of efficiency dividends and shifting priorities. This situation is often compounded by the need to support a distributed workforce, leading to a fragmented IT architecture and significant technical debt.

The human element and cyber risk

Threats to public entities come from a broad spectrum of adversaries, particularly when viewed through former hackers like Mr Treptel, who are masters at using social engineering to penetrate local, state, and federal IT systems, even as zero-trust environments take shape.

He outlines how local councils experience technological inertia and resistance to change. Recent hacking incidents targeting municipal and government institutions are skyrocketing—courthouses, libraries, hospitals, schools, and government service agencies are vulnerable.

In 2017, WannaCry ransomware crippled the UK's NHS, costing over $100 million and disrupting services. Highlighting government unpreparedness underscored the public sector's vulnerability to undetected, prolonged cyber-attacks.

Threat diversity

Security risks within government communication systems are varied and nuanced. Mr Treptel gives an example: "We can listen to you from your printer's radio frequency signal and reprint the documents you're printing at a highly secure place."

From individual hackers to state-sponsored actors, each brings different tactics and objectives, making the cybersecurity landscape complex.

Individual hackers are often driven by personal goals like curiosity, fame, or revenge, using essential hacking tools or scripts found online. They may exploit vulnerabilities in public sector websites for personal satisfaction or to demonstrate skills.

Financially motivated criminals want monetary gain by directing ransomware attacks, data theft for selling on the dark web, or banking fraud. Examples could include criminal groups targeting hospital systems with ransomware, encrypting sensitive data, and demanding payment.

Activist groups or "Hacktivists" are driven by political or social causes, intent on sending a message or disrupting activities they deem unjust. Tactics could include denial-of-service attacks or defacing websites to make political statements.

Organised crime groups are like illegal businesses, highly organised and involved in big cybercrimes like data breaches and identity theft. For instance, they run advanced phishing schemes to steal people's personal information and commit fraud.

State-sponsored actors with significant resources, typically the most sophisticated, aim for espionage, disruption, or influencing geopolitical dynamics. Skilled in disrupting critical infrastructure, they may infiltrate another country's government networks to steal classified information or disrupt elections.

“There are agents from China and Russia or even America who live in Australia and are getting information about our organisations,” said Mr Treptel. These insider threats are challenging to detect as they involve individuals deeply integrated into an organisation.

Adversarial AI

He shared insights on exploiting trust within systems, mentioning how easy it is to infiltrate council organisations by posing as cleaners or other staff: “I do have a police record, and yet I’m still in there cleaning.”

AI has significantly lowered the entry barrier for diverse cyber criminals.

“Even people with no development experience can write a zero-day exploit,” said Mr Treptel. Now, it’s more accessible for attackers to launch sophisticated cyber threats, placing an added burden on cash-strapped agencies.

AI systems monitor platforms like LinkedIn to target new employees in an organisation: “We know on LinkedIn that they’ve started a new role, and then we have an AI system just monitoring that.”

AI tools can also monitor public sector email communication: “It creates an agent for every single person using that email system... learning everything about your role.” The algorithms manipulate emails subtly for malicious purposes, demonstrating a significant shift in email security threats.

Talent, technical debt and resources

Mr Le Busque’s observation on resource disparities among government departments – “There’s the great big fish like DFA... and then there’s pesticides regulators who throw their hands up and declare nobody loves us” – further illustrates the need for tailored cybersecurity strategies across various government sectors.

Meanwhile, outdated technology hinders the attraction of skilled personnel; it’s hard to attract people when agencies are not working on transformative tech like AI, mobile apps, cloud applications, machine learning, and robotics.

It creates a cycle where technical debt limits talent acquisition.

Often, large government agencies need to pay more attention to creative, asymmetrical thinkers and non-traditional candidates.

“Despite being recognised for my expertise in cybersecurity in the private sector, I found it challenging to secure a financially comparable advisory role in the government sector,” said Mr Treptel.

A former Senior ASD analyst notes that the war on talent means the government should not make salary the benchmark for attracting top candidates. They can compete with unique purpose-driven missions directly contributing to the public interest. Public sector leaders should focus their recruitment and retention on “What is the unique contribution that an employee will make to the community/state/country that is exclusive to our organisation?”.

Legacy security gaps

Over time, Mr Treptel has noticed greater disengagement and outdated practices in the public sector. "Hundred per cent worse... people are disengaged doing things like data entry. Why in the world in 2023?"

Now a white-hat hacker, he also questions the continued reliance on passwords and champions more secure methods. "Why does anyone use passwords anymore?" he asks, advocating for technologies like passkeys.

He noted the government's slow adoption of technology compared to the private sector is understandable. "Government is designed to be slow...But how do you mobilise those guardians of sensitive information?"

Affordable digital transformation

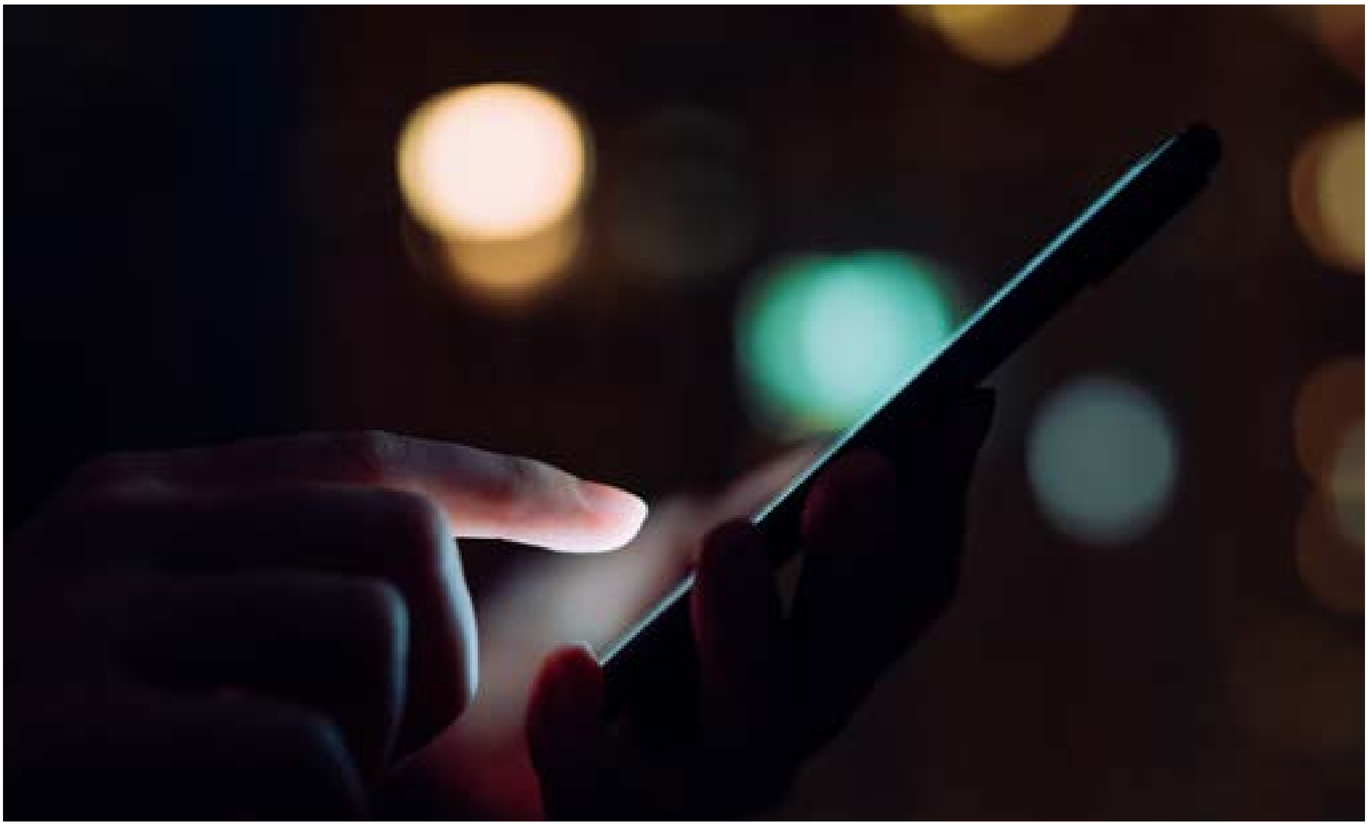
Australian public sector entities are, to varying degrees, pursuing digital transformation. A core goal is improving citizen and employee experiences through modernised IT infrastructure. Currently, 53% of the focus is on the former, with the rest on building resilience.

This shift, driven by a desire for more accessible and equitable digital services, brings a crucial need to prioritise cybersecurity, especially considering the 69% year-on-year increase in attack types like ransomware.

Even with limited resources, public sector entities can still deploy effective cybersecurity strategies by focusing on strategic investments and resourceful approaches. The key is ensuring every dollar spent aligns with managing specific organisational risks and objectives, some of which have been mentioned above but bear repeating.

Zero-budget cybersecurity strategies

1. **Purpose-driven talent recruitment:** Attracting talent in cybersecurity doesn't always require high salaries. Emphasising the mission and impact of public service can draw skilled professionals. This approach leverages the unique appeal of public service to compensate for budget limitations.
2. **Promoting cybersecurity awareness:** Building a security-conscious culture is a cost-effective way to strengthen defences. Regular training in best practices and awareness of the latest threats can significantly improve an organisation's security posture, demonstrating the value of investing in education and understanding.
3. **Proactive and adaptive security measures:** Implementing a proactive cybersecurity approach, such as regular system updates and basic cyber hygiene practices, aligns with the principle of effective budget use. Public sector entities must 'assume nation-state and work backwards.' This approach fosters a defensive mindset, preparing agencies to counteract even the most sophisticated threats effectively.



4. **Collaborative defence and resource utilisation:** Collaborating with cybersecurity agencies and pooling knowledge and resources can maximise the impact of every dollar spent. Alongside partnering with industry experts, public sector entities are encouraged to engage actively with state and Commonwealth cybersecurity services. Leveraging these resources strengthens the overall defence posture.

The role of industry partnerships

Partnering with industry experts offers a viable solution for public entities to advance their cybersecurity posture rapidly. Industry partners like Verizon can assist in several key areas.

1. **Identifying assets and risks:** An external perspective can help identify digital assets and assess associated risks.
2. **Implementing policies and controls:** Leveraging industry expertise can expedite the development and implementation of effective cybersecurity policies and controls.
3. **Addressing human factors:** Partners can offer insights and training to address the human factors in cybersecurity, a critical aspect often overlooked in digital transformation initiatives.
4. **Monitoring, mitigating, and responding to threats:** Ongoing monitoring and threat response improve cybersecurity postures with the support of experienced industry partners.

The future of zero trust in the public sector

Ultimately, moving towards a zero-trust future in the public sector means acknowledging the cunning strategies of modern hackers. They'll often bypass zero trust systems through social engineering, detailed reconnaissance, and exploiting the human element in security. "I'll often go after the directors at home and then infect them and then take them into work," said Mr Treptel.

This method highlights a critical vulnerability: ***the human factor.***

Hackers can infiltrate otherwise robust systems by compromising individuals in less secure environments like their homes.

Even with advanced security measures, subtle oversights remain.

"At the federal level, while application and hardware allow listing, peripherals like keyboards often go unmonitored," he said. This gap in physical security showcases how simple devices can become tools for data exfiltration, challenging the efficacy of zero-trust strategies.

It compels cybersecurity leaders to consider asymmetrical thinking in dealing with these threats.

"We're drowning in digital identities – up to 10,000 per citizen. It's chaotic."

He advocates a seismic shift for the public sector: a single, centralised digital ID system.

Managed by birth and marriage registries, this system would issue one unique, quantum-proof identity to each individual. Limiting data sprawl echoes successful models in Norway and India, a unified approach for a more secure digital Australia.

The path forward

Real-world tools and techniques hackers aim at in the public sector are evolving rapidly. We see sophisticated AI-driven attacks and insider threats that exploit even minor security oversights.

They're targeting people, not just systems. With resources often stretched, wafer-thin pressure to adapt is immense.

Banks now operate on the ethos that harmful agents are already within their systems, focusing on monitoring and limiting damage.

This approach stems from the realisation that traditional security measures might only catch some things, especially with the sophistication of AI-driven attacks.

Despite this, there's hope.

The future lies in collaboration, creative thinking, and a shift in how we approach cybersecurity.

"We need to look beyond traditional defences," said Mr Le Busque, "small and medium-sized government agencies can lead in cybersecurity by embracing proven, innovative strategies and industry partnerships."

The public sector must prioritise cybersecurity as a technical challenge and a crucial part of its mission to serve and protect the public.

In doing so, they can transform potential vulnerabilities into strengths, ensuring a more secure and resilient digital future for all Australians.

verizon✓

Produced by
InnovationAus.com