servicenow

Driving Cybersecurity Excellence in Asia Pacific Governments

A roadmap for government organisations

REPORT

Introduction

With caches of sensitive and classified data often protected by inadequate cybersecurity systems in outdated IT platforms, government bodies are major targets for cyberattacks.

Nowhere is this more evident than in the Asia-Pacific (APAC) region, which is highly exposed to cyberattacks due to geopolitical tensions, supply-chain risks, regulatory differences, and the rapid shift to digital usage during the pandemic.

To understand the cybersecurity challenges that government organisations face in the region and how they overcome them, ServiceNow and ThoughtLab surveyed leaders in 175 local, regional, and national entities in APAC. We found that an elite group of government organisations are well ahead of others in keeping their data safe from cyberattacks. Their example can guide other government bodies as they strive to develop effective cybersecurity strategies to combat escalating risks in the region.

ServiceNow and ThoughtLab surveyed leaders in:

175

local, regional, and national entities in APAC

About the research

We conducted our survey in 2024. The 175 respondents included technology and management executives representing local, state or provincial, and national level agencies of different budget sizes in Australia, India, and Singapore. (See appendix for the full respondent profile.)

As part of the research, we created a cybersecurity maturity framework to identify "Pacesetters"— government organisations that are most advanced in implementing a set of cybersecurity best practices. Of our sample of 175 organisations, 20% qualified as Pacesetters, 57% as intermediates, and 23% as beginners in cybersecurity maturity. (See the methodology in the appendix.)

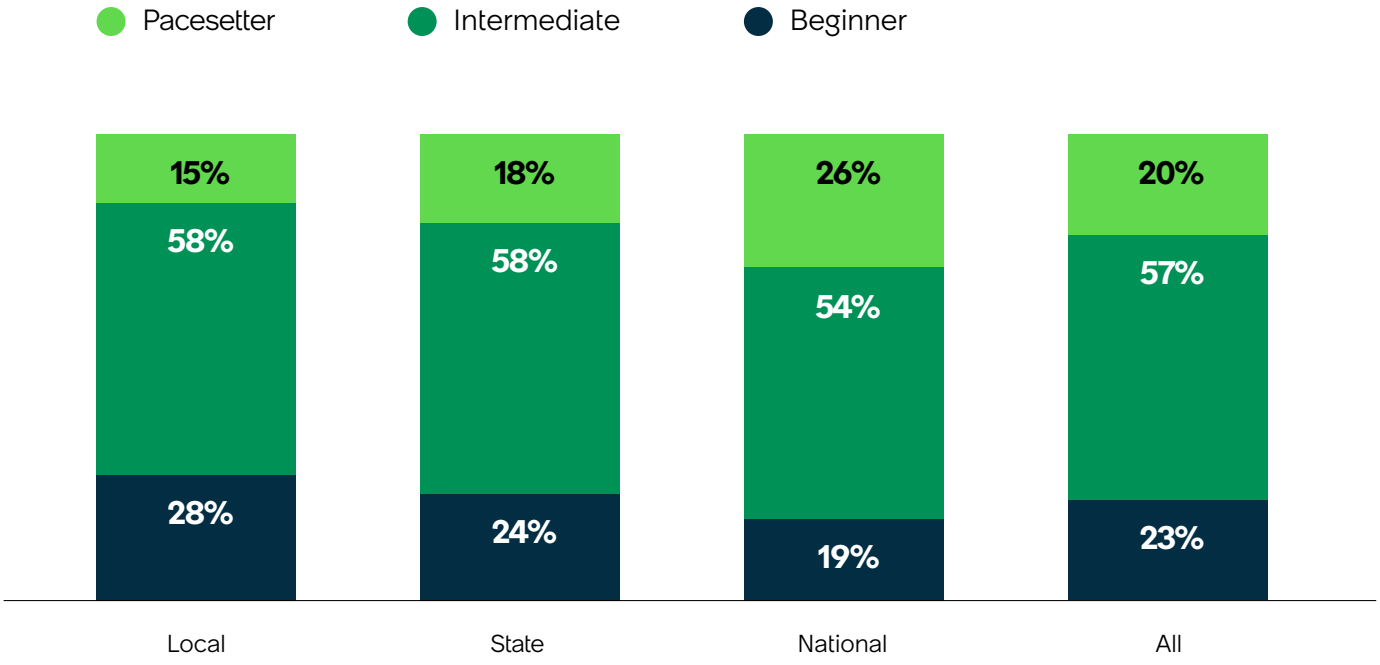
Our survey revealed that most government organisations in APAC are still in the beginning or intermediate stages of cybersecurity maturity. That is especially true of local and state agencies, which have more limited cybersecurity budgets and skills than national bodies. Only 15% of local entities—city and county governments—are Pacesetters. Slightly more state and provincial government organisations, at 18%, qualify as Pacesetters. National organisations, with greater human resources and spending power, have the largest share of Pacesetters, at 26%.

The cybersecurity readiness of government agencies varies widely by country. For example, the percentage of cybersecurity Pacesetters in Singapore is considerably higher than that in other countries. Among the reasons is the nation's commitment to cybersecurity, its robust legal framework, and its focus on cybersecurity training, supported by such initiatives as the Cybersecurity Industry Employee Grant. In contrast, India and Australia have the fewest Pacesetters. In the case of India, the country's fragmented cybersecurity approach and inconsistent enforcement of cybersecurity rules hold many agencies back.

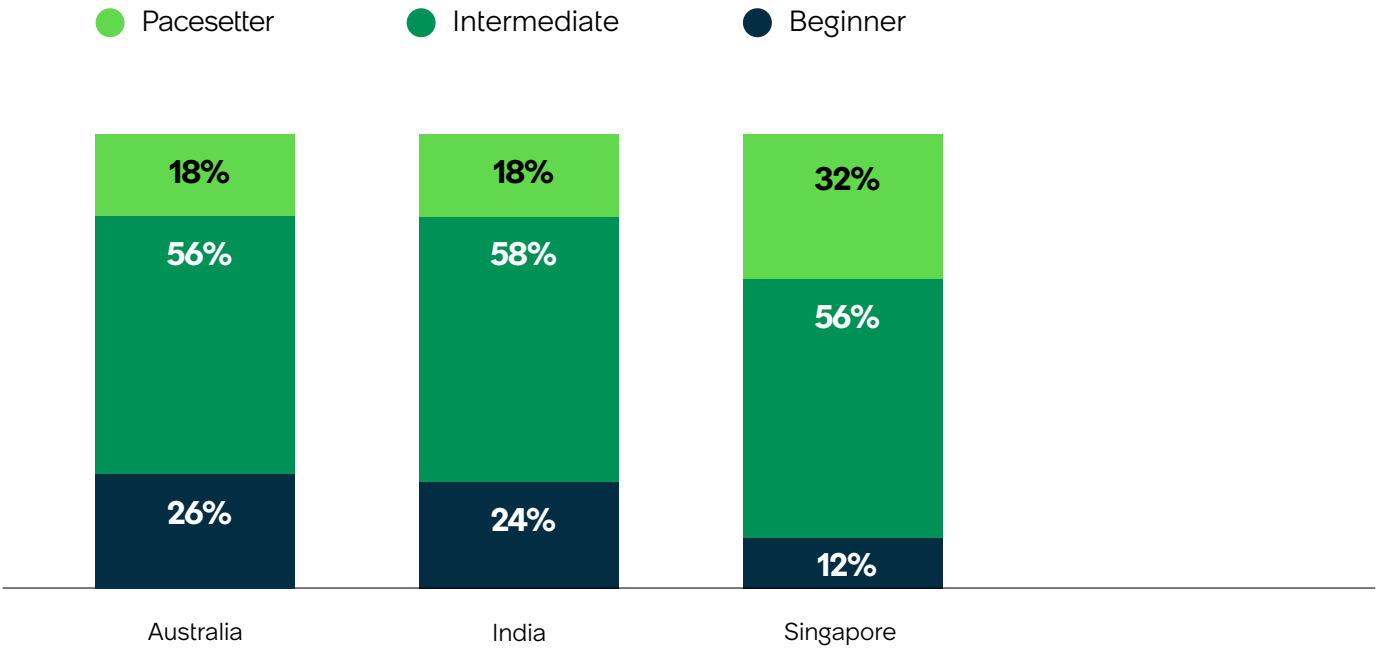
Acknowledging the "cyber slumber" in Australia in past years, Cyber Security and Home Affairs Minister Clare O'Neil released the 2023-2030 Australian Cyber Security Strategy late in 2023, committing A$586.9 million to strengthening cybersecurity in the country.

servicenow

Stages of maturity by government type



Stages of maturity by country



The evolving threat landscape in Asia-Pacific

Government agencies in APAC are often prey to cybercriminals, hackers, and nation-state actors.

According to Positive Technologies, a cybersecurity service company, APAC was the most attacked region in 2022, accounting for 31% of attacks globally. The most frequent victims were government agencies—representing 22% of total attacks on APAC organisations.

Aside from the insufficient defences of government organisations, a major reason for the rise in attacks is the span of highly motivated threat actors.

At the top of the list, according to public-sector executives, are cyber adversaries capitalising on underdeveloped links in complex supply chains and services from government contractors. Such attacks, such as the SolarWinds Attack and the Accellion File Transfer Attack, are particularly difficult for governments to detect since they can be embedded deep into supply chains or in poorly designed digital vendor solutions.

According to Mark Anderson, Chief Security Officer with Microsoft for Australia and New Zealand, government bodies need a solid third-party risk management strategy because of their reliance on third parties. "With the use of digital products and services growing, I can only see the use of third parties increasing for government," says Anderson.

To minimise such risks, he advises government organisations to buy hardware and software only from low-risk, reputable organisations; put in place good support contracts; and ensure that third parties comply with industry standards and beyond. At the same time, Anderson cautions that not all suppliers are the same, and that a "one-size-fits-all" vendor management strategy doesn't always work.

Other major threats come from persistent highly skilled actors, including organised cybercriminal groups and nation-state actors. State-sponsored attackers have been particularly prolific in targeting countries across the region, including Taiwan, India, Malaysia, and Singapore. North Korea is also known for its aggressive cyberattacks against South Korea.

Government agencies are exposed to a host of other cyber perpetrators with less sophisticated methods. These include unsophisticated hackers, malicious insider threat actors, and hacktivists, who often hack and deface government websites and services to disrupt government activities or to express political views and discontent.

servicenow

RICHARD BERGMAN

Global Cybersecurity Transformation Leader, EY

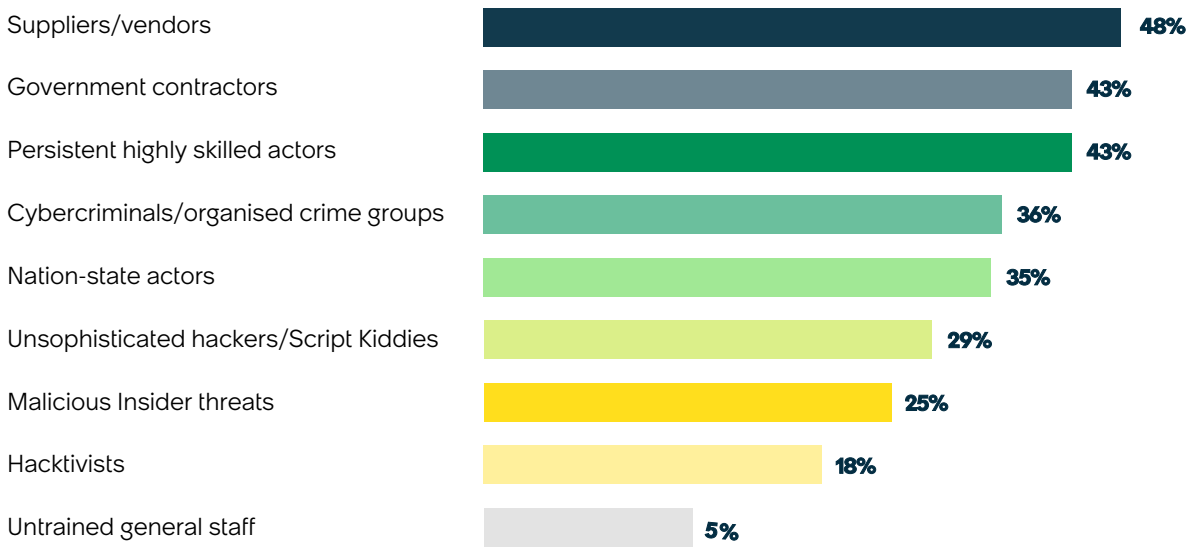
—

“We’re still sitting in a world where over 80% of cyberattacks are caused by a human clicking on a link or a phishing email or opening an attachment.

Although 43% of survey respondents recognise that their agencies’ cybersecurity training programs are ineffective, only 5% see untrained general staff as a source of risk. This may be a critical oversight. While untrained staff may not technically be a direct threat actor, they can open the door to cybercriminals by clicking on malicious links or using a weak password. According to various sources, such as the World Economic Forum and IBM, the vast majority of cybersecurity incidents are caused by human error.

Threat actors creating the largest risks

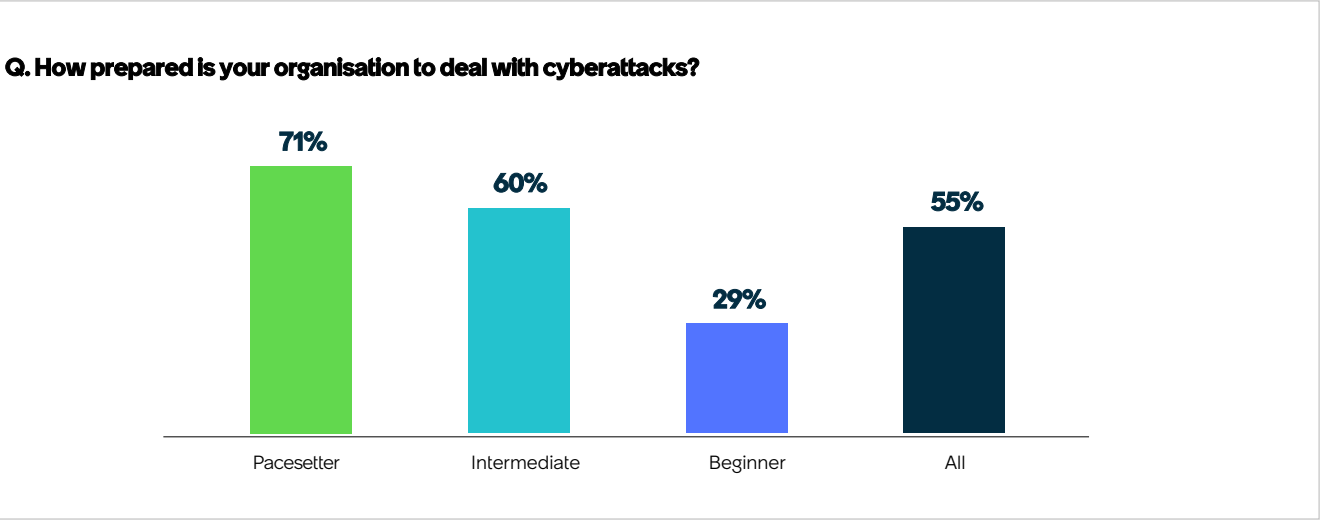
Q. Which of the following parties create the largest risks for your organisation either directly or indirectly?



Governments are not well prepared

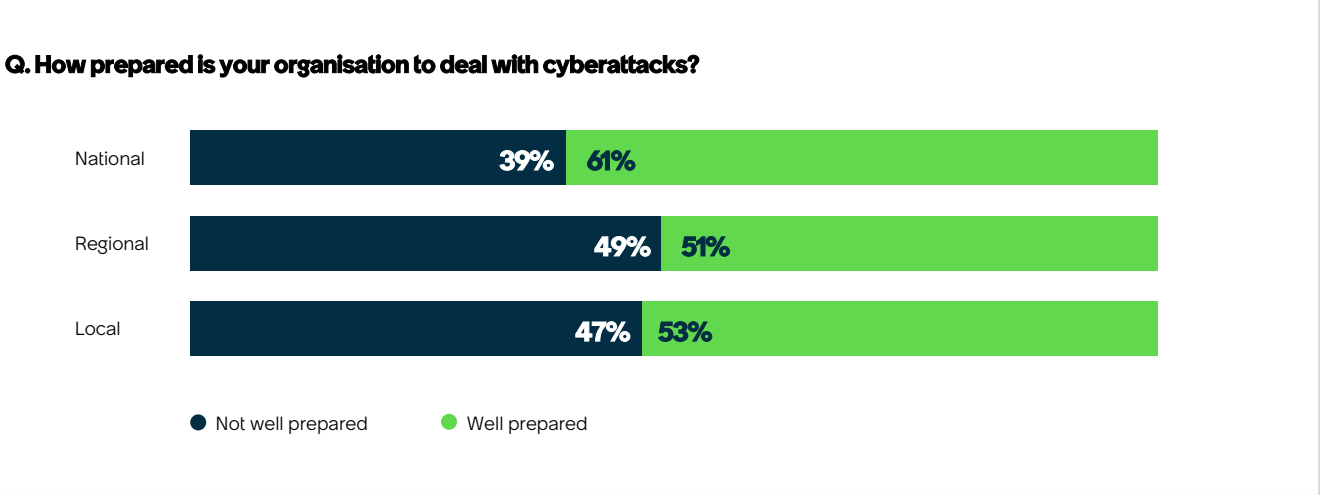
Some 45% of respondents in APAC admit that their government organisations are ill-prepared to deal with cyberattacks. Pacesetters, however, show the state of the art in cybersecurity, with close to three quarters well or very well prepared.

More Pacesetters are well prepared

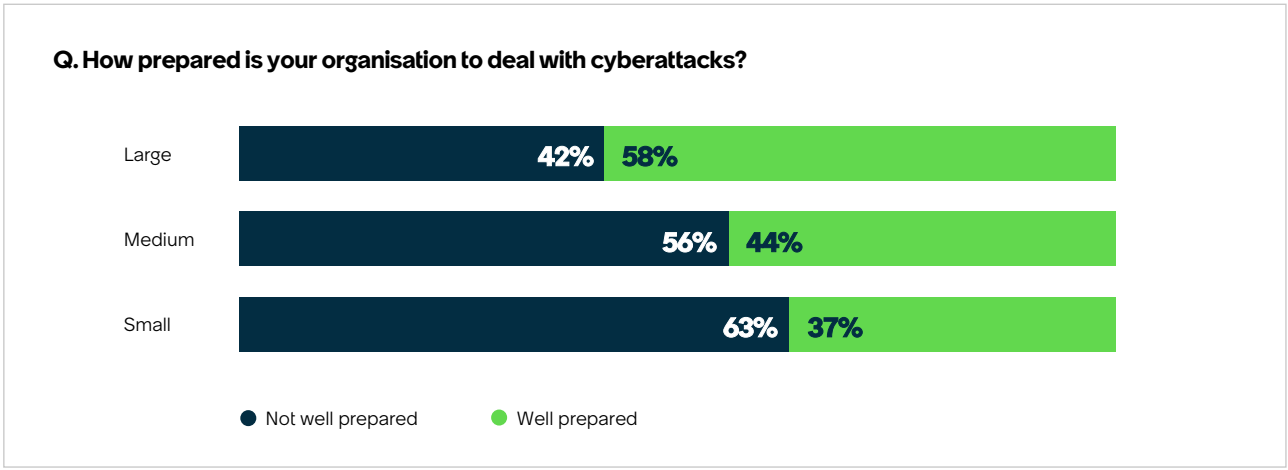


There is also a gap by type of organisation. More entities at the national level (61%) say they are well prepared than regional (51%) or local agencies (53%). The latter two groups generally have smaller budgets and staffs, and more limited access to cybersecurity talent. The data underscores that larger entities with bigger budgets are better prepared. Not only do they have deeper pockets—they also have more to lose.

Local and state government organisations are less prepared



Smaller entities are less prepared



Challenges governments must overcome

Government organisations face many hurdles that prevent them from building cybersecurity proficiency. Some of the biggest problems come from neglecting basic cybersecurity measures, such as providing effective training programs, implementing organisation-wide governance structures, prioritising cyber risk management across the organisation, and identifying key risks. The latter, the first prerequisite of the NIST cybersecurity framework, is particularly crucial, according to Microsoft's Anderson: "Identification of risks and impact of the risk being realised are absolutely key. Identifying key systems and then the key risks and potential vulnerabilities should be the top priority because then you can align the limited resources you have at your disposal accordingly."

Because of their inadequate budgets, government bodies struggle to invest in the latest digital solutions needed to protect, detect, and respond to cybersecurity attacks, especially when compared against well-funded cyber adversaries, which are better equipped to capitalise on advances in technology and keep up with the pace of automation.

The organisational structure and culture of government institutions can also expose them to greater cyber risks. For example, siloed organisational structures and a paucity of skilled cybersecurity professionals make it difficult for government agencies to fend off more nimble adversaries.

33%

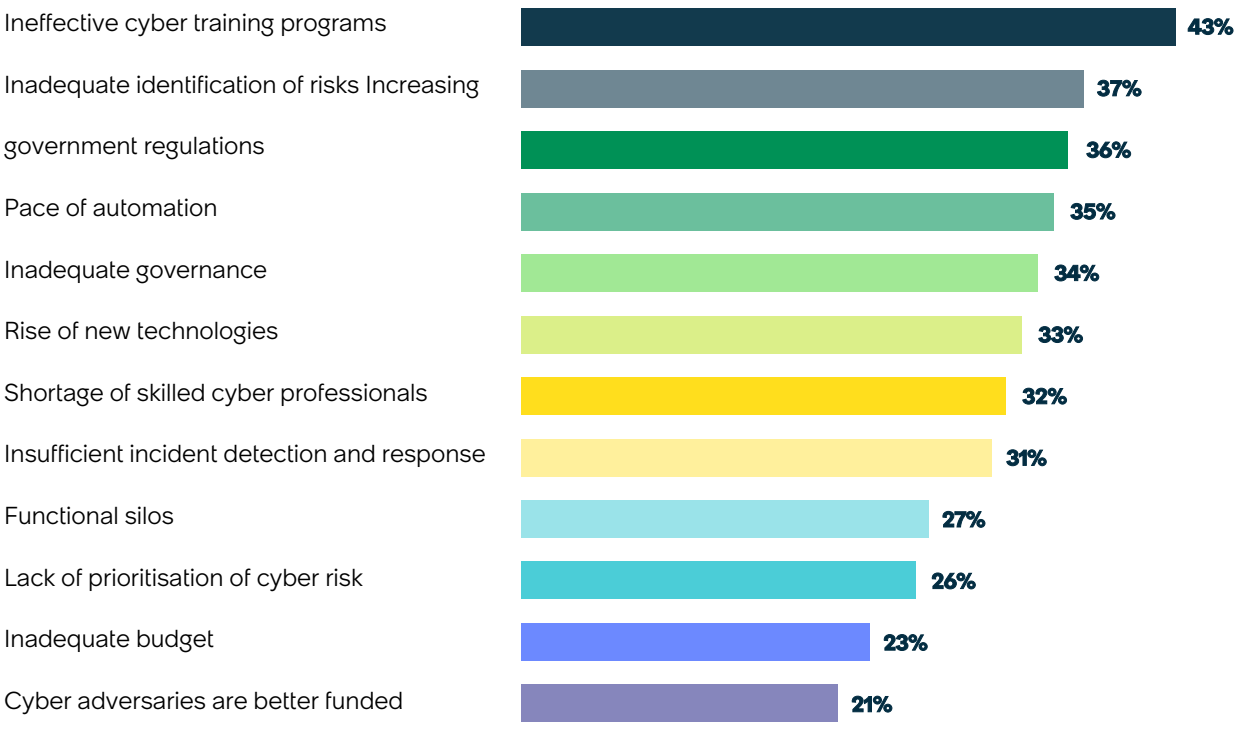
of organisations are challenged by the rise of new technologies

21%

believe they are losing the arm's race with cyber adversaries

Top 12 challenges that government organisations face

Q. Which are the biggest cybersecurity challenges that your organisation now faces?



Pacesetters show the way forward

Pacesetters are far more advanced than others in adopting cybersecurity best practices.

For example, almost twice as many Pacesetters as others are midway or advanced in risk detection, continuously screening for risks through advanced detection processes and technologies. Almost twice the percentage of Pacesetters are similarly ahead in using zero-trust programs, a sophisticated technique requiring strict identity verification for every person and device trying to access resources on a network, regardless of location.

Pacesetters are more conscientious than others in developing a cybersecurity framework to guide their organisations. They set up governance and organisational structures that lay out key processes, controls, and responsibilities. They also take early action to identify key vulnerabilities and prioritise assets that require the greatest security. And they develop risk ecosystems with law enforcement agencies and other firms that can help them manage different aspects of cybersecurity.

Pacesetters understand the best cybersecurity approach involves people, process, and technology. That is why they apply risk-based decision-making that draws on analytical models that can help identify the probability and potential trajectory of risk; upskill staff on cybersecurity best practices; and employ advanced technology to both detect and protect against risks.

Microsoft's Anderson believes that technology plays a critical role in today's cyber battleground. "When we speak of people, process, and technology in terms of cybersecurity investment, I would be controversial and go the other way around, which is technology, then, process, then people in terms of defence layers. We are relying a little too much on human and process sides to do the job, and not enough on the technology. Picking and implementing the right technology solutions to help mitigate the risks first, then the processes hopefully will work when that layer fails. The last line of defence should be the people. Organisations need to find the right balance between training their people and making sure they have the right technology in place to stop the attack dead in its tracks."

Best practices Pacesetters focus on much more than others*

Q. In which stage of maturity is your organisation in the following cybersecurity risk management processes?

	Pacesetter	Other	% difference
Risk detection: monitoring and use of advanced tech	74%	38%	95%
Zero trust: strict identity verification for all persons and devices	74%	38%	95%
Risk identification: target vulnerabilities and prioritise assets	60%	32%	88%
Governance: processes, controls, and responsibilities	80%	44%	81%
Risk-based decisions: quantitative analysis of risk probability	80%	51%	57%
Risk protection: protective technology and staff training	80%	53%	51%
Risk ecosystem: collaborate with law enforcement and others	91%	62%	47%

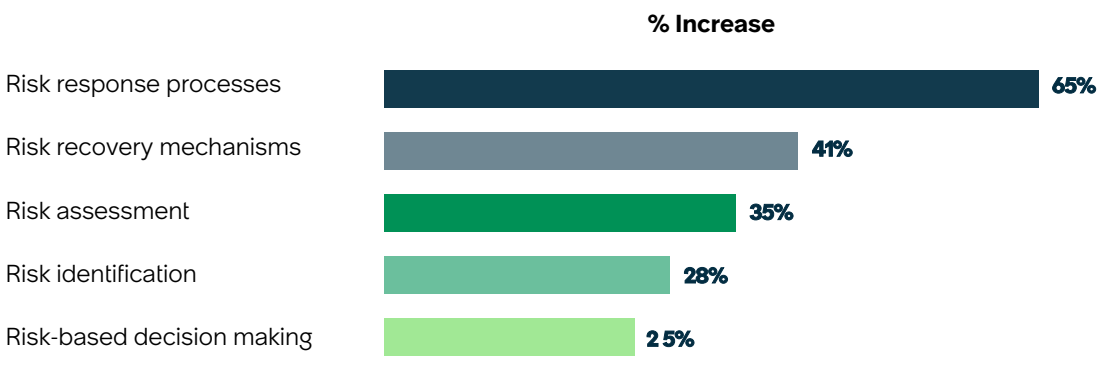
*Mid- or full implementation

Areas of focus growing most

Malicious cyber adversaries can often find their way into even the most secure IT systems. Recognising this, Pacesetters plan to beef up their risk response and recovery processes over the next three years. Pacesetters also will take risk analysis to the next level, not only increasing the regularity and sophistication of their risk assessment, risk modeling, and stress testing programs, but also paying closer attention to understanding their risk vulnerabilities and probabilities of attack.

Best practices Pacesetters will focus on much more in three years

Q. In which stage of maturity is your organisation in the following cybersecurity risk management processes? In which stage is your organisation planning to be in three years?



*Mid- or full implementation

servicenow

Winning the cyber technology arms race

Technology can be a double-edged sword for governments bodies. It can help defend against attacks, but as more processes are digitised and automated, it can expand the attack surface and open new vulnerabilities. Worse yet, threat actors are leveraging AI and automation to launch more sophisticated phishing campaigns faster than many government agencies can adapt, according to EY's Bergman.

While all APAC organisations employ cybersecurity tools and technologies, Pacesetters use more specialised solutions that help them stay ahead of their adversaries. Almost double the share of Pacesetters as others rely on security and incident response management solutions, which help them systematically detect, respond to, and recover from cybersecurity breaches. Similarly, nearly twice as many Pacesetters use sophisticated cybersecurity risk models and risk assessment platforms that allow them to quantify the probability and potential impact of cyber threats under different scenarios.

Security orchestration automation and response (SOAR) systems are another common tool for Pacesetters, which use these systems to automate, optimise, and integrate processes involved in detecting, assessing, and responding to cyber security events. Pacesetters are also more likely to focus on improving cybersecurity hygiene through regular vulnerability and patch management and more effective identity and access management measures.

Solutions that Pacesetters use more than others

Q. Which of the following cybersecurity solutions has your organisation already invested in, and which does it plan to start to invest in or continue to invest in over the next three years?

	Pacesetter	Other	% difference
Security and incident response management	31%	16%	94%
Cybersecurity risk models and risk assessment platforms	46%	24%	92%
Security orchestration automation and response	31%	19%	63%
Vulnerability and patch management	11%	7%	57%
Identity and access management solutions	34%	29%	17%

SIEMs will grow the fastest

Over the next three years, Pacesetters will rapidly expand their use of several technologies. The fastest growing one will be SIEM (Security Information and Event Management) systems, which will more than triple in use. Gathering security-related data from various sources, SIEM systems enable Pacesetters to use real-time monitoring, incident detection, compliance reporting, and post-incident analysis to protect their IT environments.

AI-enabled security analytics tools are quickly becoming a staple among Pacesetters, with over half expecting to use them over the next three years. These versatile tools will be game changers, giving organisations the ability to detect, analyse, and respond to threats in real time, as well as predict future threats and integrate intelligence from external sources.

"Irrespective of the solution or the practice area, AI and automation are playing a critical role," says Bergman.

"Organisations can gain a 35% to 45% productivity improvement with removal of the human effort involved, which boosts the detection rate."

Solutions that Pacesetters will use more in 3 years

Q. Which of the following cybersecurity solutions has your organisation already invested in, and which does it plan to start to invest in or continue to invest in over the next three years?

	Now	3 years	% growth
System information event management (SIEM)	**14%**	**46%**	**229%**
AI-enabled security analytics tools	**20%**	**54%**	**170%**
Cloud and network security	**20%**	**43%**	**115%**
Vulnerability and patch management	**11%**	**23%**	**109%**
Software security testing tech, such as penetration testing	**26%**	**49%**	**89%**
End-point security and response technology	**23%**	**37%**	**61%**
Security and incident response management	**31%**	**46%**	**48%**

Following the lead of Pacesetters will help other government organisations compete in the cyber arms race. However, the key is leveraging new technologies without exceeding budgets or overcomplicating the cyber tech stack. "The challenge is to both optimise costs and rationalise technology to reduce the number of security tools and technologies in place," says Bergman. This simplification offers benefits. "It will help drive AI and automation a lot faster and more cheaply across an organisation," he says.

servicenow

Adopting such technologies does not necessary require deep pockets. Smaller government agencies can enhance their cyber posture by considering the following:

Cyber Hygiene: Starting with cyber hygiene is crucial, as many vulnerabilities stem from human errors, such as clicking on phishing links. Basic measures like implementing MFA, strong passwords, automated patching, and regular cyber training can greatly reduce risks.

Increased Visibility: Ensuring good cyber visibility across the organisation helps in understanding and addressing the most critical vulnerabilities. This involves creating an asset inventory, viewing IT assets through a policy compliance lens, and prioritising budgeting based on risk.

Cloud Security Solutions: Utilising cloud security solutions can offer enterprise-grade protection with a flexible "as a service" model, aiding in secure backups and efficient security monitoring and response.

Collaboration and Culture: Collaboration with other agencies and fostering a cyber-aware culture within the organisation can significantly improve security outcomes. Sharing threat intelligence and participating in security communities are key strategies.

The bottom line

While latest technologies like SIEM and AI can help government organisations stay at the top of their game, it is important for government organisations to understand the role of the procured technology within the business. Knowing the capability of that technology allows the organisation to utilise it for its intended purpose, revealing gaps and allowing the business to strengthen its posture.

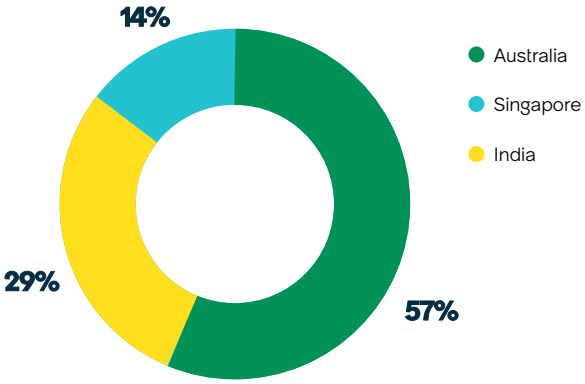
Microsoft's Anderson recommends that they focus on the foundations first. For most organisations, he says, especially smaller ones, just having good password policies, multifactor authentication, rapid and timely patching, and anti-malware solutions on their desktops and servers will solve most problems. **"Organisations shouldn't underestimate the impact of getting the fundamentals correct,"** says Anderson. "No matter what is coming down the line in the future, it's pointless to concentrate on that if you can't defend against the most rudimentary attacks of today. Once you have achieved this, then you are ready to take it to the next level and look at SIEM and AI technology"

Bergman also sees technology as only part of the solution: **"The government organisations that are getting better cybersecurity outcomes do three things differently.** They are further along in the adoption of AI and automation in fighting cybercrime. They have visibility into the attacks and their complete attack surface. And they not only have specific strategies to mitigate cybercrime; they also have whole-of-enterprise ownership of cyber risk."

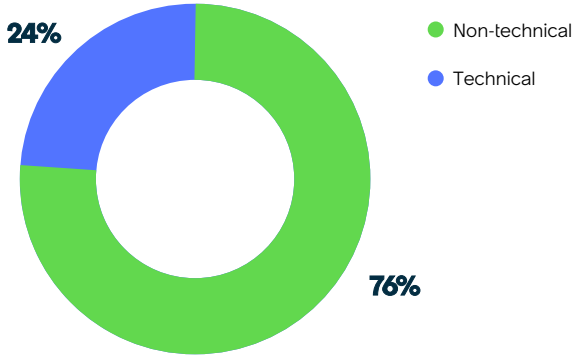
Appendix

Survey respondent profile

Respondents by country (total 175)

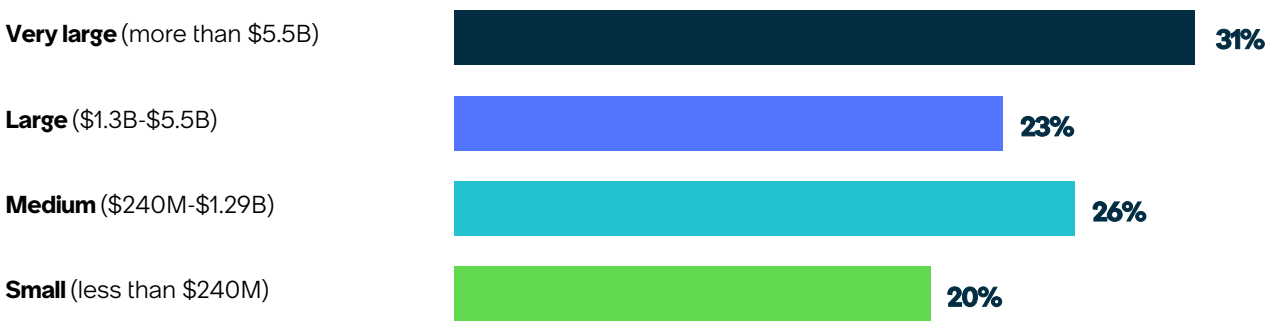


Respondents by role



Respondents by type of government organisation

Respondents by budget size



servicenow

Defining a cybersecurity Pacesetter

We used the following question in the survey to create a benchmarking model that classifies organisations by their level of cybersecurity maturity.

Q. In which stage of maturity is your organisation in the following cybersecurity risk management processes?

- **Risk identification,** targeting vulnerabilities and prioritising assets and infrastructure.
- **Governance,** implementing governance processes, controls, and responsibilities.
- **Risk protection,** using protective technology, identity access controls, and training.
- **Risk detection,** continuous monitoring and advanced detection technologies.
- **Risk response processes,** mitigating the impact of an attack and implementing predetermined response plans.
- **Risk recovery mechanisms,** restoring systems from attacks, managing PR fallout.
- **Risk-based decision-making,** making decisions based on quantitative measurement of risk probability and potential impact.
- **Risk assessment,** conducting regular risk assessments, audits, stress tests, and penetration tests.
- **Risk ecosystem development,** working closely with law enforcement agencies and other public and private entities to mitigate cyberattacks.
- **Zero trust program,** requiring strict identity verification for every person and device trying to access resources on a network.

Scoring methodology

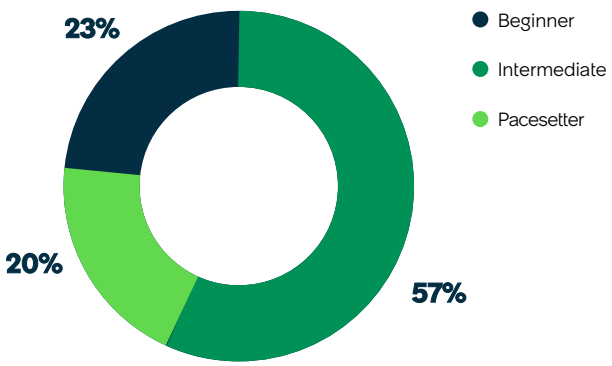
We scored their response to each cybersecurity area as follows:

- **Not considering** (0 point)
- **Planning:** Exploring options, developing plans, and building support (1 point)
- **Early implementation:** Starting to implement plans (2 points)
- **Mid implementation:** Mid-way in implementation; starting to see results (3 points)
- **Advanced:** Fully implemented, scaled across enterprise, driving results (4 points)

For each respondent, we summed the scores for each process and then grouped the respondent into one of three categories: beginners (below 25th percentile), intermediate (in 25th and 75th percentile), or Pacesetter (above 75th percentile).

We classified 23% of respondents as beginners; 57% as intermediates; and 20% as Pacesetters.

Maturity stage of respondents



About ServiceNow

ServiceNow (NYSE: NOW) makes the world of government work better for everyone. Over 1,400 government organisations globally use ServiceNow's cloud-based platform and solutions to securely automate processes and digitise services across their agencies and departments. Helping government organisations achieve their mission through improving customer experience, employee engagement, risk management, security and technology innovation. And we can all create the future of public service that we can imagine.

For more information, visit: servicenow.com