How Secure Are You?

Australia & India will contribute about 25% each to the region's cybersecurity spending this year

By Raju Chellam

Digital trust is quite hard to find,
With scams and hacks of every kind.
We type in our info,
Hoping it won't go,
To some cybercriminal mastermind.

If that limerick made you wonder, these stats should make you ponder: The Indo-Pacific region outside of Japan will spend a whopping US$36 billion to beef up cybersecurity this year, up 12.3% over 2023, according to IDC (International Data Corp) estimates. That spend includes security hardware, services, and software. IDC expects spending on security to grow at a five-year CAGR (compound annual growth rate) of 12.8% between 2022 and 2027 to reach US$52 billion by 2027.

"The surge in cyberthreats utilizing AI – such as deepfakes, pretexting, and identity theft – has spurred a heightened demand for comprehensive security solutions in the region that include threat detection, automated remediation, and behavioral analysis capabilities," says Sharad Kotagi, an IDC regional market analyst. "The demand for security in complex IT environments, including networks, cloud services, and endpoints, remains high amid a cybersecurity talent shortage."

That's a slew of opportunities for vendors to provide a range of security services, especially managed services, which could form nearly 40% of overall security spend. "Regulatory requirements and data protection laws will be a catalyst for spending on security consultation and integration services," says Benjamin Ten, an IDC research analyst for IT services. "The managed security services market will be buoyed by the increasing complexity of IT environments and the shortage of cybersecurity talent."

HOT SECTORS

The "hot" sectors? BFSI (banking, financial services, insurance), government agencies, and telco. Together, these sectors will account for more than half of the total security spend this year. "Companies are investing strategically to keep up with tech advancements such as open banking, digital payments, e-governance, modernization of IT infrastructure, and regulations," IDC says.

On the other side, are governments doing enough to keep their citizens and nations safe? Nope. Take the US as an example. Gartner predicts 75% of US Federal agencies will fail to implement zero trust security policies over the next two years, due primarily to funding and talent deficits.

Gartner defines zero trust as a security paradigm that starts from the baseline of trusting no end user. It explicitly identifies users and grants them the precise level of access necessary to accomplish their tasks. Zero trust is not a specific technology, product, or service. Instead, it is a set of security design principles that contrasts with the traditional perimeter-based security approach.

"With the September 2024 deadline for specific zero trust requirements for US Federal agencies being established, requirements are broad for all agencies," says Mike Brown, a Gartner vice president. "One of the main impediments is a skills shortage. Government agencies are challenged to compete with the private sector for staff with necessary skills. To address these shortages, agencies should be working simultaneously with service contracts, to reskill existing staff and to recruit new staff."

Failure to meet policy deadlines will continue to leave Federal agencies exposed to risks that could be cascaded downstream, especially because of the big new elephant on the scene: AI. Hackers have been able to leverage AI and GenAI way more innovatively and insidiously than scrupulous users.

COOL FRAUDS

In a survey by the US-based Association of Financial Professionals, 65% of respondents admitted that their organizations had been victims of attempted or actual payments fraud in 2022. Of those who lost money, 71% were compromised through email. Larger organizations with annual revenue of US$1 billion were the most susceptible to email frauds, according to the survey.

Here is an alarming example: A finance employee in Hong Kong received a message from the firm's UK-based CFO (chief financial officer) asking for a US$25.6 million bank transfer. Though initially suspicious that it could be a phishing email, the employee's fears were allayed after a video call with the CFO and other colleagues whom he recognized. It was only after he checked with HQ that he discovered the deceit: Everyone on the call was deep faked. But by then the money was transferred.

"Everyone present on the video calls except the victim was a fake representation of real people," South China Morning Post reported on February 4, 2024. "The scammers applied deepfake tech to turn publicly available video and other footage into convincing versions of the meeting's participants. Police said they were highlighting the case as it was the first of its kind in Hong Kong and involved a large sum. They did not reveal details about the company, or the employees involved."

McKinsey says organizations should be aware of four primary sources of inbound risk from the adoption of GenAI:

- **Security Threats:** These result from the increased volume and sophistication of attacks from GenAI-enabled malware.
- **Third-Party Risk:** These emerge from challenges in understanding where and how third parties may be deploying GenAI, creating potential unknown exposures.
- **Malicious Use:** These arise from the potential for bad actors to create compelling deepfakes of company representatives or branding that could result in significant reputational damage.
- **IP Infringement:** These result from intellectual property (including images, music, text) being scraped into training engines for underlying large language models and made accessible to anyone using the technology.

"The essential starting point for organizations deploying GenAI use cases is to map the potential risks associated with each case across key risk categories to assess the potential risk severity," McKinsey advises. "For example, use cases that support customer journeys – such as GenAI-enabled chatbots for customer service – may raise risks such as bias and inequitable treatment across groups (by gender and race, for example). Others are privacy concerns from users inputting sensitive information, and inaccuracy risks from model hallucination or outdated information."

> “ACCORDING TO IDC, CHINA LEADS REGIONAL SECURITY INVESTMENTS, COMPRISING OVER 40% OF TOTAL SPENDING IN 2024, WITH A CAGR OF 13.5% FROM 2022 TO 2027. AUSTRALIA AND INDIA ARE NEXT, ACCOUNTING FOR MORE THAN 25% TO THE REGION'S SECURITY SPENDING.

DESIRABLE DOZEN

So then, how secure are you and your enterprise? How can your business cultivate a robust cybersecurity environment for your employees, partners, and customers? Here are a dozen desirable recommendations from me, in alphabetical order:

- **Audit:** Regularly. Particularly in the areas of cybersecurity and sustainability. This will expose weaknesses and enhance both security and eco-conscious initiatives, potentially elevating your digital trust scores for your stakeholders to continue to do business with you.
- **Build:** Transparency. Make it clear how you gather, utilize, and safeguard customer data. Your company's privacy policy should be defined, easily accessible and comprehensible to your users.
- **Communicate:** Policies and practices. Share your privacy policies, data protection strategies, and security protocols. This can instill confidence in your end-users and suppliers, reassuring them that their privacy is well-protected.
- **Deploy:** Certifications and standards. Implement third-party certifications (like SSL) and follow standards (as recommended by ISO or your national standards organizations) to validate your security and data protection efforts.
- **Encourage:** Feedback. Welcome customer feedback and treat any issues or complaints with seriousness. This shows your suppliers and customers that their input is valued and acted upon.
- **Foster:** Data protection policies. Stress the significance of safeguarding sensitive data to your staff and stakeholders. Internal breaches can be just as, if not more, damaging than external ones.
- **Generate:** Trust. Cultivate a culture of trust within your business and make trust a fundamental value. This encourages staff to adhere to best practices and be conscious of security and privacy.
- **Handle:** Data responsibly. Treat customer data ethically and responsibly. Refrain from using customer or partner information in ways that could potentially harm or exploit them.
- **Invest:** In endpoint security, information and data security applications, and identity and digital trust software. Boost network security, including firewalls, intrusion detection and prevention, unified threat management, and the use of VPNs (virtual private networks).
- **Justify:** Robust security measures. Enforce strong security measures within your organization. Employees should be required to use strong passwords, multifactor authentication, encryption, and other security measures to ensure data safety.
- **Keep:** Systems and policies updated. Maintain your software and systems, especially with the most recent security patches and updates. This can reduce the risk of cyberattacks and prompt you to implement mitigation strategies.
- **Learn:** From mistakes and mishaps. Accept responsibility when things go wrong and act swiftly to rectify the situation. This can foster trust by showing a commitment to accountability.

Why bother at all? Because cyberattacks are increasing in intensity and breadth across the region. This requires a shift in addressing cyberthreats. According to IDC, China leads regional security investments, comprising over 40% of total spending in 2024, with a CAGR of 13.5% from 2022 to 2027. Australia and India are next, accounting for more than 25% to the region's security spending.

And finally, since we started with a scary limerick on cybersecurity, let us end with a scarier one:

Members of the board gathered around,
To decide cybersec strategy, which was sound.
“Encrypt all the things,
So no data leak springs!”
But the secure password was lost; never found.

Raju Chellam is a former Editor of Dataquest and is currently based in Singapore, where he's the Editor-in-Chief of the AI Ethics & Governance Body of Knowledge, and Chair of Cloud & Data Standards.

maildqindia@cybermedia.co.in