Press release

nCIPHER
AN ENTRUST DATACARD COMPANY

Customer personal information is the number one data protection priority globally, but in Australia compliance is king

nCipher 2020 Global Encryption Trends Study finds organisations globally racing to protect sensitive data as it proliferates across cloud, IoT devices and 5G networks

Sydney, Australia – 15 July, 2020 – As organisations accelerate digital initiatives such as cloud and the internet of things (IoT), and data volumes and types continue to rise, IT professionals around the world cite protection of customer personal information as their top driver for data encryption, according to the 2020 Global Encryption Trends Study from the Ponemon Institute. However, Australian respondents cite regulatory compliance and internal policies as their top prioroties, with privacy and data security regulations as their top motivators, over protection of customer data.

Drivers and priorities

For the first time in the Global Encryption Trends Study, protecting consumer personal information is the top global driver for deploying encryption (54% of respondents), outranking compliance, which ranked fourth (47%).

Australian respondents, however, think differently. Only 29% of Australian respondents rated protecting customer personal information as their number one data protection priority, which is the lowest rate globally and 25% lower than the global average.

- 57% of Australian organisations said regulatory compliance is top driver for encrypting data. That's 10% higher than the global average, and up from 47% two years ago
- For the third straight year, Australia chose the driver 'to comply with internal policies' more than any other region (43% vs. the global average of 23%)

"I'm actually not surprised by these results," says James Cook, Regional Sales Director, Australia for nCipher Security, an Entrust Datacard company. "There has been a raft of new regulations and regulatory changes impacting this market over the past couple of years such as Consumer Data Right (CDR), and a critical focus on the financial sector in particular, so it is only natural for respondents to have a keen focus on compliance."

"Organisations that move beyond encryption for the sake of compliance understand and value their data protection credentials as a genuine selling point," Cook says. "Australian enterprises have an opportunity to transform their outlook on encryption from checking the compliance boxes to protecting customer information in ways that improve customer retention, profitability and competitiveness."

Negligent insiders pose the greatest threat to sensitive data

For 62% of Australian respondents, 'employee mistakes' are considered the biggest threat to sensitive data, which is 8% higher than the global average. Local respondents rate the threat of 'temporary or contract workers' lowest and the 'risk of hackers' second-lowest.

Data discovery the number one challenge

Thanks to the proliferation of data from digital initiatives, cloud use, mobility, IoT devices and the advent of 5G networks, data discovery continues to be the biggest challenge in planning and executing a data encryption strategy, with 70% of respondents in Australia citing this as their top concern (67% globally). And that is likely to increase, with a pandemic-driven surge in employees working remotely, using data at home, creating extra copies on personal devices and cloud storage.

Blockchain, quantum computing and adoption of new encryption technologies

The study indicates that 52% of organisations in Australia have adopted encryption strategies across their enterprises (48% globally). With encryption deployment steadily growing, how are organisations looking ahead? In the near term, 59% plan to use blockchain, with cryptocurrency/wallets, asset transactions, identity, supply chain and smart contracts cited as the top use cases.

As encryption use has grown, Australian respondents rate specific encryption features notably higher in importance than their global counterparts, including 'support for emerging algorithms' such as elliptic-curve cryptography (80% in Australia vs. 59% globally; up from 65% last year). Other much-hyped technologies are not on IT organisations' near-term radar, based on global results. Most IT professionals see the mainstream adoption of multi-party computation at least five years away, with mainstream adoption of homomorphic encryption more than six years away, and quantum resistant algorithms over eight years out.

Trust, integrity, control

The use of hardware security modules (HSMs) continues to grow, with 42% of Australian respondents deploying HSMs to provide a hardened, tamper-resistant environment with higher levels of trust, integrity and control for both data and applications. Organisations in Germany, the United States and Middle East are more likely to deploy HSMs, with Australia, Germany and the United States most likely to assign importance to HSMs as part of their encryption or key management activities.

HSM usage is no longer limited to traditional use cases such as public key infrastructure (PKI), databases, application and network encryption (TLS/SSL). The demand for trusted encryption for new digital initiatives has driven significant HSM growth for big data encryption (up 17%) code signing (up 12%), IoT root of trust (up 10%) and document signing (up 7%). Additionally, 35% of respondents report using HSMs to secure access to public cloud applications. In Australia, 52% say that in the next 12 months their organisations will be using HSMs for payment transaction processing, including point-to-point encryption (P2PE).

The race to the cloud

More than 80% of Australian respondents report transferring sensitive data to the cloud, or planning to do so within the next 12 to 24 months.

In the next 12 months, respondents predict a significant increase in the ownership and operation of HSMs to generate and manage Bring Your Own Key (BYOK), and integration with a Cloud Access

Security Broker (CASB) to manage keys and cryptographic operations.

Global respondents cited the most important cloud encryption features as:

- support for Key Management Interoperability Protocol (KMIP) (67%)
- security information and event management (SIEM) integration (62%)
- granular access controls (60%)
- key usage audit logs (55%), and
- privileged user access controls (50%)

Australia shows a stronger preference than other regions for encryption solutions with:

- Support for emerging algorithms (e.g. ECC): 80% vs. 59% globally
- System scalability: 73% vs. 58% globally
- Separation of duties and role-based controls: 69% vs. 54% globally

"Consumers expect brands to keep their data safe from breaches and have their best interests at heart. The survey found that IT leaders are taking this seriously, with protection of consumer data cited as the top driver of encryption growth for the first time," says Dr Larry Ponemon, chairman and founder of Ponemon Institute. "Encryption use is at an all-time high with 52% of respondents in Australia saying their organisation has an overall encryption plan applied consistently across the entire enterprise, and a further 33% having a limited plan or strategy applied to certain application and data types."

Other key trends:

- The fastest growing encryption use cases for respondents in Australia include public cloud services (49%, up from 32% last year), IoT devices (31% from 22% over the past two years) and Docker containers (26%, up from 19% last year)
- The highest prevalence of organisations with an enterprise encryption strategy is in Germany (66%) followed by the United States (66%), Sweden (62%), Hong Kong (60%), Netherlands (56%) and the United Kingdom (54%). Australia is at 52%.
- Globally payment-related data (54% of respondents) and financial records (54% of respondents) are most likely to be encrypted. 71% of organisations in Australia encrypt payment-related data, jumping up from 44% just two years ago.
- In Australia, organisations have continued to encrypt employee/HR data (58% vs 52% globally) and customer information (54% vs 44% globally) at higher rates than global counterparts.

Download the 2020 Australia Encryption Trends Study

2020 Global Encryption Trends Study methodology

The 2020 Global Encryption Trends Study, based on research by the Ponemon Institute, and now in its fifteenth year, captures how organisations around the world are dealing with compliance, increased threats, and the implementation of encryption to protect their business critical information and applications. 6,457 IT professionals were surveyed across multiple industry sectors in 17 countries/regions: Australia, Brazil, France, Germany, India, Japan, Hong Kong, Mexico, the

Middle East (which is a combination of respondents located in Saudi Arabia and the United Arab Emirates), the Russian Federation, Southeast Asia (Indonesia, Malaysia, Philippines, Thailand, and Vietnam), South Korea, Taiwan, the United Kingdom, the United States and two new regions for the first time, Netherlands and Sweden.

About nCipher Security

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organisations by delivering trust, integrity and control to their business-critical information and applications. Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our same proven technology that global organisations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business-critical applications, ensure the integrity of your data and put you in complete control – today, tomorrow, always. www.ncipher.com
Follow us on LinkedIn, Twitter, Facebook and Instagram – search nCipherSecurity.

Media Contact:
Richelle Gillett
Giant Squid Inc for nCipher Security
+61 418 781 610
rg@giantsquidinc.com.au