nCipher: Use of encryption to protect consumer information soars in Mexico, but two-thirds of organizations still don't protect their data

2019/2020 Encryption Trends Study find payment-related data most common type of information encrypted by Mexican organizations (59%), followed by financial records (52%)

MEXICO CITY – Nov. 12, 2019 – nCipher Security, an [Entrust Datacard company](#) and provider of trust, integrity and control for business-critical information and applications, announces the results of its [2019/2020 Mexico Encryption Trends Study](#) from the Ponemon Institute. As organizations in Mexico seek to protect consumer information and limit exposure from data breaches, they have increased their adoption of enterprise-wide data protection strategies, with over one-third (36%) embracing encryption. While this is below the global average of 45%, Mexico's encryption growth rate of 20% exceeds the global growth rate and is the second highest (behind Australia) across regions surveyed.

Data protection drivers and threats
The top priority for encrypting data in Mexico is to protect customer information, with over half (56%) of organizations citing it as a driver. This is followed closely by limiting liability from data breaches or inadvertent disclosure, which at 41% is much higher than the global average of 23%. Payment-related data is the most common type of information encrypted by organizations in Mexico (59% of respondents), followed by financial records (52%).

These findings may indicate a greater overall awareness of the financial and reputational damage resulting from data breaches and the potential exposure of personally identifiable information (PII). There may also be concerns about compliance with Mexico's [Federal Law on the Protection of Personal Data held by Private Parties](#), which regulates the processing of personal data (e.g. customer information) for private entities.

Similar to other regions, organizations in Mexico rate employee mistakes as the highest overall threat to data (41%, up from 35% last year). This is followed by malicious insiders (27%).

"The use of encryption is at an all-time high, driven by the need to address compliance requirements and the need to protect sensitive information from both internal and external threats as well as accidental disclosure," said Larry Ponemon, chairman and founder of the Ponemon Institute. "Encryption usage is a clear indicator of a strong security posture, with organizations that deploy encryption being more aware of threats to sensitive and confidential information and making a greater investment in IT security."

Challenges and advantages
With the explosion and proliferation of data that comes from digital initiatives, cloud use, mobility and IoT devices, data discovery is cited as the biggest challenge when planning and executing an encryption strategy in Mexico (56%). Initially deploying the encryption technology is the next highest challenge at 48%, versus the 42% global average.

Compared with other regions, organizations in Mexico report the highest overall pain associated with managing encryption keys or certificates. When identifying the reasons why key management is painful, respondents rank 'lack of skilled personnel' at the highest rate globally, 82% vs. 62%. The use of hardware security modules (HSMs), which provide a hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, has grown to 32%, and while this is 11% below the global average, it represents an increase of 39% in HSM use over the past year.

"Sophisticated threat actors, coupled with inadvertent errors from employees, has made the protection of sensitive data imperative – and it appears organizations in Mexico are getting the message," said Jose Rivera, director of sales, LATAM, at nCipher Security. "nCipher empowers customers by providing a high assurance security foundation that ensures the integrity and trustworthiness of their data, applications and intellectual property."

Other key findings:

- While 49% of organizations in Mexico currently transfer data to the cloud, an additional 26% plan to do so in the next 12-24 months
- Since last year, HSM use has increased for several use cases, including code signing (up 250%, from 6% to 21%); big data encryption (more than doubled from 9% to 19%); document signing (doubled from 9% to 18%); and internet of things (IoT) root of trust (up 56%, from 16% to 25%)

Download the 2019/2020 Mexico Encryption Trends Study.

2019 Global Encryption Trends Study methodology
The 2019 Global Encryption Trends Study, based on research by the Ponemon Institute, captures how organizations around the world are dealing with compliance, increased threats, and the implementation of encryption to protect their business critical information and applications. 5,856 individuals were surveyed across multiple industry sectors in 14 countries/regions: Australia, Brazil, France, Germany, India, Japan, Mexico, the Middle East (which is a combination of respondents located in Saudi Arabia and the United Arab Emirates), the Russian Federation, South Korea, the United Kingdom, the United States and, two new regions in Asia for the first time, Southeast Asia (Indonesia, Malaysia, Philippines, Thailand, and Vietnam) and Hong Kong and Taiwan.

Follow us on LinkedIn, Twitter, Facebook and Instagram – search nCipherSecurity.

About nCipher Security
nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations 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 organizations 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

For more information, please contact:

nCipher Security
Megan Nemeh megan.nemeh@ncipher.com +1 408 887 5064
Liz Harris liz.harris@ncipher.com +44 7973 973648