nCipher: French organizations lead the world in protecting consumer information with encryption, finds 2019 Encryption Trends Study

PARIS – Nov. 6, 2019 – nCipher Security, an [Entrust Datacard company](#) and provider of trust, integrity and control for business-critical information and applications, announces the French results of its [2019 Encryption Trends Study](#) from the Ponemon Institute. As they seek to protect consumer information and comply with external security and privacy requirements, organizations in France have increased their adoption of enterprise-wide data protection strategies, with almost half (46%) embracing encryption.

Data protection drivers and threats
Organizations in France lead their global counterparts in protecting personally identifiable information (PII) with encryption. The most common types of PII data encrypted by French organizations is customer information (66%) and healthcare information (57%), with the latter being significantly higher than the global average of 24%. Outside of PII, French organizations also encrypt intellectual property and payment-related data more than anywhere else in the world.

At 53%, compliance is the top driver for encrypting data. This figure, along with the encryption of PII, may be attributable to the long-standing and stringent French data protection and privacy laws enforced by the French regulatory body Commission Nationale de L'informatique et des Libertés (CNIL). Also impacting compliance standards is the EU's General Data Protection Regulation (GDPR) requirements.

Similar to other countries, 61% of French organizations rank employee mistakes the top threat to data – a number that is 7% higher than the global average and a significant increase from 27% in each of the past two years. Organizations in France also rate the threat from malicious insiders higher than any other country (28% vs. the global average of 21%).

"The use of encryption is at an all-time high, driven by the need to address compliance requirements such as GDPR 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."

Data discovery the number one challenge
With the explosion and proliferation of data that comes from digital initiatives, cloud use, mobility and IoT devices, data discovery continues to be the biggest challenge in planning and executing a data encryption strategy, with 68% of respondents in France citing this as their number one challenge. Training users to leverage encryption appropriately is also listed as a challenge by 20% of respondents, a number that has jumped from 12% in the past two years. Three-quarters of organizations list 'no clear ownership' as the top barrier for effectively managing keys and

certificates, a number that is 11% higher than the global average.

"Organizations are under relentless pressure to protect their business-critical information and applications and meet regulatory compliance, and French organizations appear to be getting the message. But the proliferation of data, and concerns around data discovery and policy enforcement, makes this a challenging environment, " said Geoffrey Portier, regional sales manager, France 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:

- Almost half (46%) of organizations in France transfer sensitive or confidential data to the cloud, with another 32% planning to do so in the next 12 months
- Over half (54%) of organizations in France rate hardware security modules (HSMs) as important to their key management or encryption strategy today while 73% rate HSMs as important in the next 12 months (this highest across all regions surveyed)
- One-third plan to deploy HSMs for IoT root of trust in the next 12 months, compared with 14% currently; this is the largest planned increase globally
- France reports the lowest overall pain associated with managing keys or certificates
- 'A lack of skilled personnel' is lowest in France at 31%, compared with a 62% global average

Download the 2019 France 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