# nCipher Security

## Trust. Integrity. Control.

www.ncipher.com

# New technologies introduce new risks

- **Larger attack surface and more opportunities for mistakes**
  - Cloud misconfigurations continue to regularly lead to data breaches

Example

**1.8 billion** intelligence data objects exposed in Amazon S3

  - IoT devices create new paths into protected networks

Example

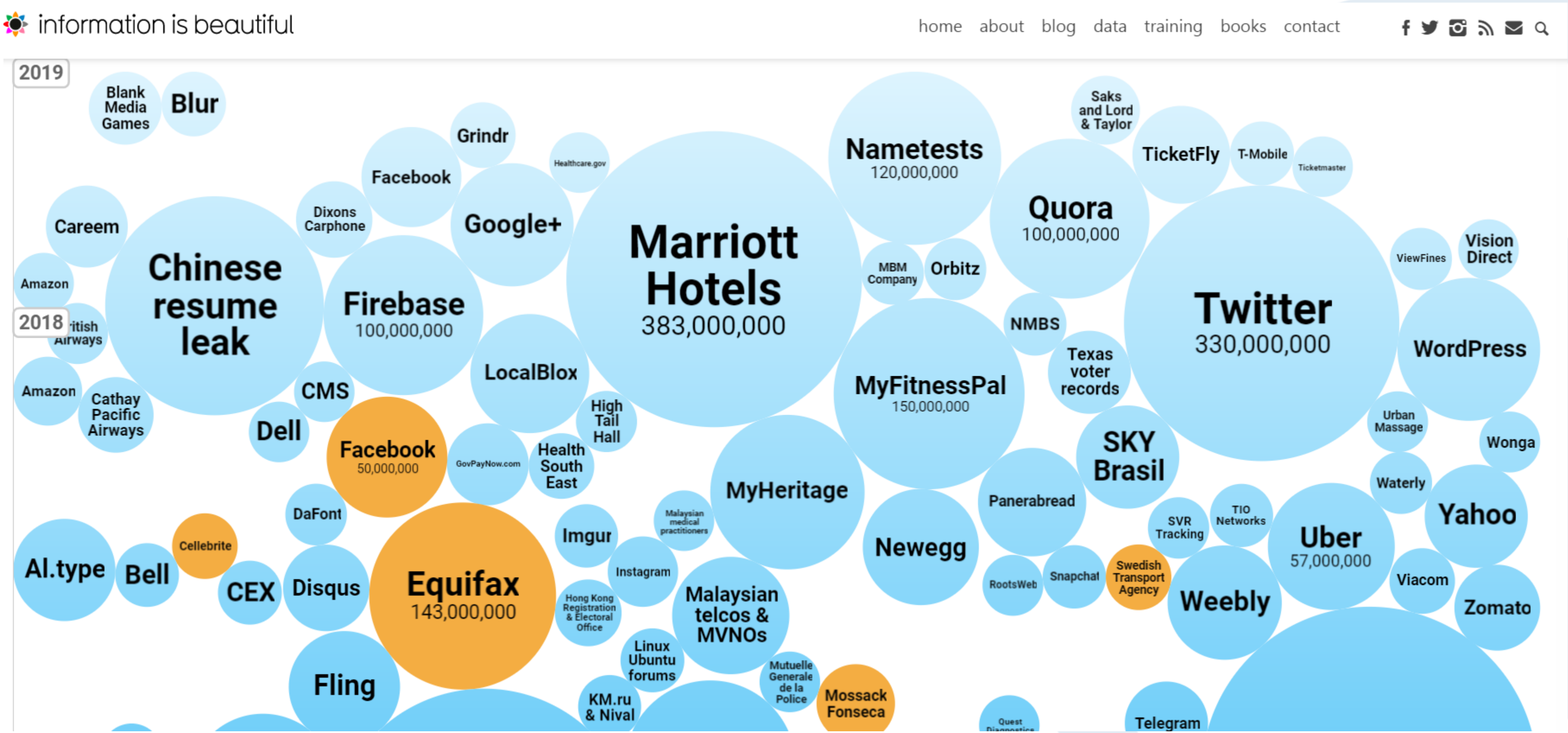
**10 GB** data stolen from casino via connected fish tank thermometer

- **Isolated, hardware-based protection is a proven method to minimize risk and exposure**

Secure Elements and SIMs protect mobile apps

Trusted Platform Modules (TPM) protect desktop apps

# Today’s reality: targeted and successful data breaches



www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

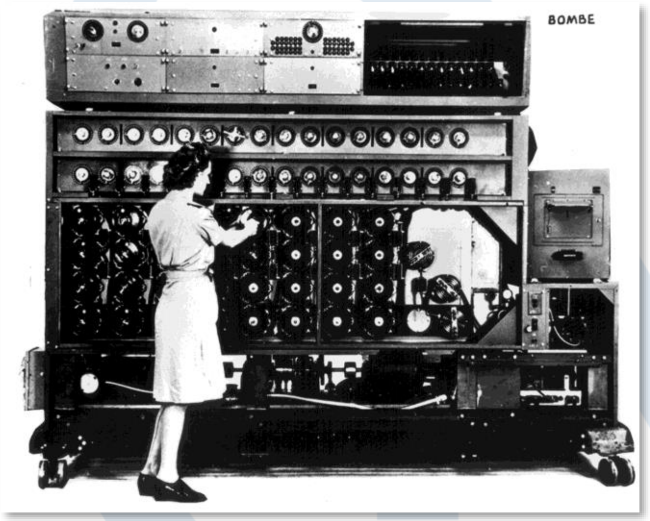
NCIPHER

# Encryption is key

- **From 1500 BCE – Mesopotamia**
  - Encrypted Cuneiform Tablet

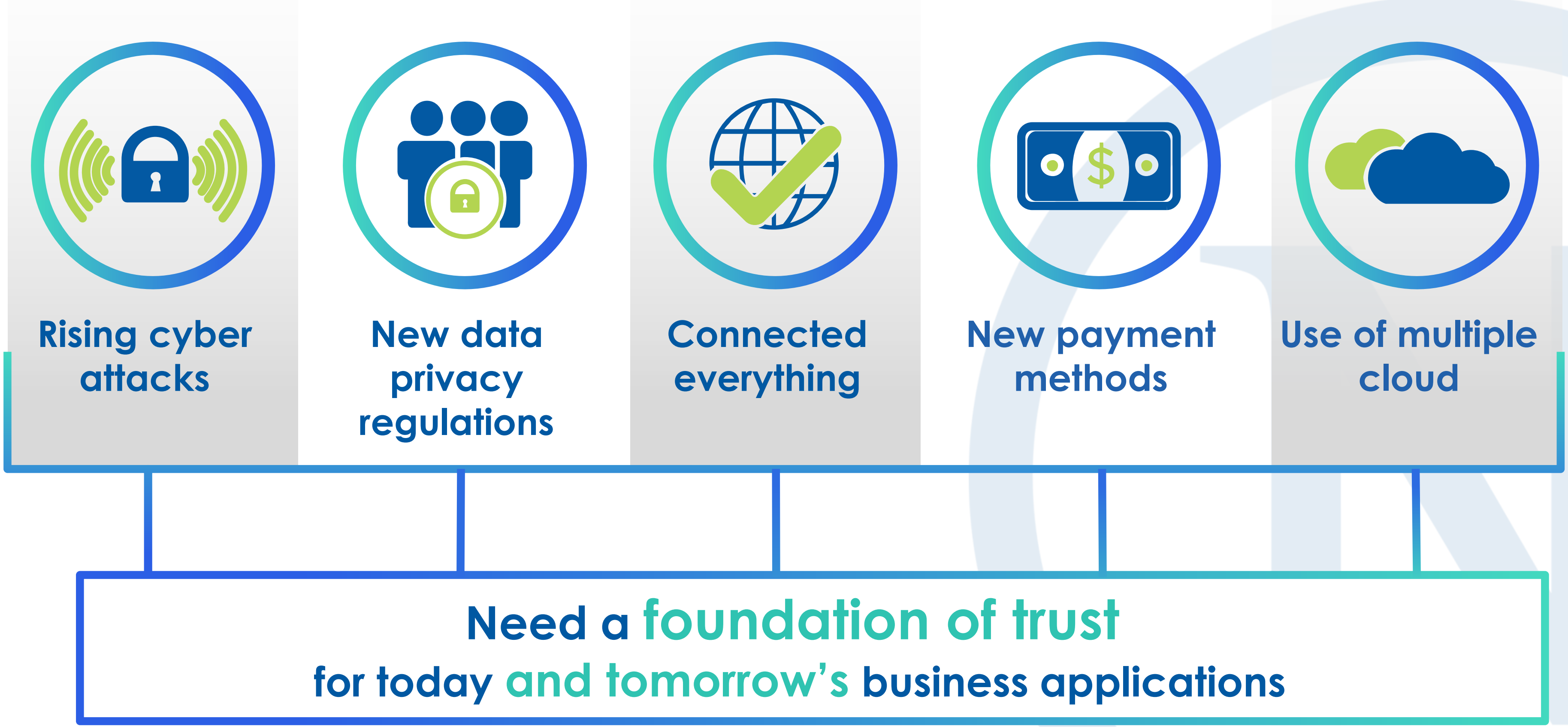
ENIGMA

- **To Late 20th Century**
  - 1970s - Financial Cryptography (DES)
  - 1980s - Commercial Cryptography & PKI
  - 1990s - Cryptography for all



RSA

# Now - Challenges & risks as businesses go digital



Rising cyber attacks

New data privacy regulations

Connected everything

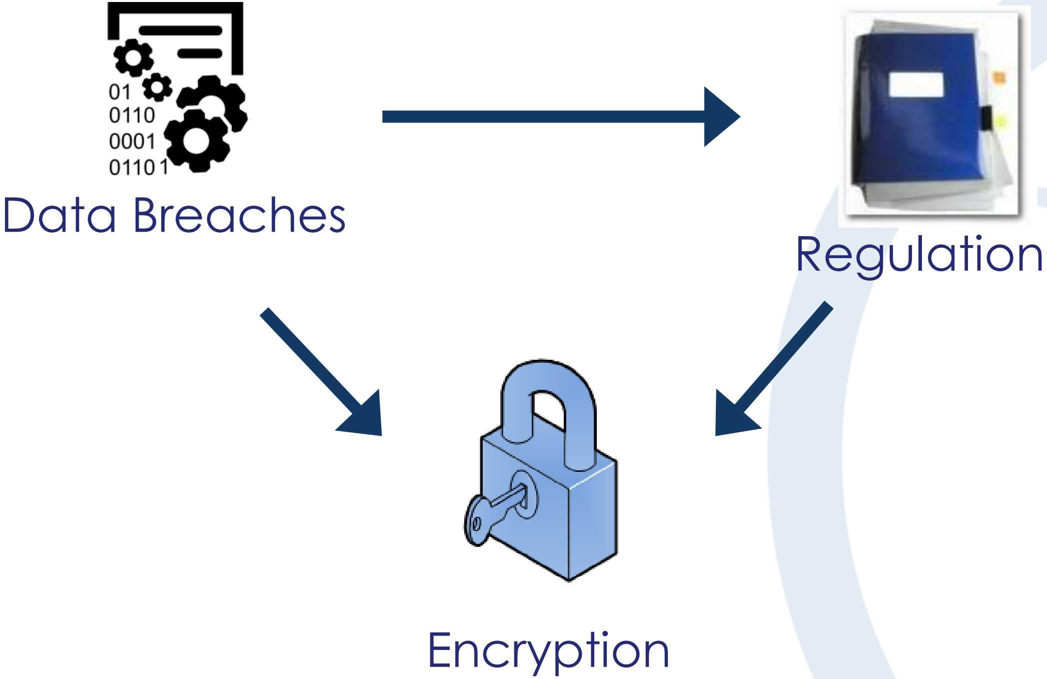
New payment methods

Use of multiple cloud

Need a foundation of trust

for today and tomorrow's business applications

# Encryption for data protection and compliance



Data Breaches

Regulation

Encryption

# Keys need strong protection

**External threats**

- ✓ Hackers
- ✓ Malware
- ✓ Trojans

**Blend of both**

- ✓Social engineering
- ✓Bribery
- ✓Corruption
- ✓Coercion

**Internal threats**

- ✓Disgruntled staff
- ✓Human error
- ✓Fraud
- ✓Duty of care
- ✓Compliance

**Auditors**

NCIPHER

# Hardware Security Modules (HSMs) provide the foundation of trust

Highest level of protection for encryption or signing keys

Implement and enforce customer-defined policy

“Harden” applications that use cryptography

Source of high quality random numbers for keys

# Tunisia

- **nCipher Security HSMs help secure Tunisia’s digital infrastructure**

- In 2015, the Tunisian government launched Digital Tunisia 2020, a plan designed to boost the nation’s digital economy by enriching online government services and electronic commerce.

- Fundamental to the success of the initiative was establishing Tunisia’s citizens’ trust and confidence in the public and private online services and electronic transactions.

# Austrian Trust Authority

- As of April 2017, a regulation known as RKSV (Registrierkassensicherheitsverordnung, or Cash Registers Security Regulation) went into effect in Austria. The regulation requires that receipts originating from businesses in the retail, hospitality and service sectors be digitally signed and stored using a unique private key assigned to each business owner. Merchants also must provide records of sales transactions that conform to specific technical standards.

www.ncipher.com

## Austrian Trust Authority provides fast, simple eIDAS digital signature security

[illegible]

BUSINESS CHALLENGE

[illegible]

TECHNICAL CHALLENGE

[illegible]

SOLUTION

[illegible]

TRUST einfach sicher

[illegible]

# Finland passport

- *nCipher hardware security modules ensure the authenticity of Finland’s e-pass*
- when Finland needed the PRC to use similar technology to issue new e-passports to comply with the latest European Union (EU) directives on electronic ID issuance, the PRC knew from experience where to turn to ensure the integrity of the process – nCipher. *ports with fingerprints secured by digital certificates*

# Conclusion

## Are your keys protected?