This infographic summarizes key findings of The Global Study on the State of Payment Data Security by Gemalto who surveyed more than 3,700 IT and IT security practitioners worldwide to gauge how companies are securing payment data and the security risks as new mobile payment methods grow in acceptance.

**KEY FINDINGS**

- **TRENDS IN PAYMENT DATA SECURITY**
  - **Most companies have experienced a data breach involving payment data**: 54% of respondents say their company has had a data breach involving payment data an average of four times in the past two years.
  - **Payment data has many points of vulnerability to security threats**: 42% of respondents say they have had an internal employee or a partner泄露 payment data.
  - **The security of payment data is not always a top priority**:
    - 50% of companies do not put payment data security as a top five security priority.
    - 50% say they allocate enough resources to the protection of payment data.

- **Mobile payments will double in the next two years**
  - 9% of all payments are mobile today.
  - 18% of all payments will be mobile in two years.
  - 54% of companies do not believe or unsure if their existing security protocols are capable of supporting these platforms.

- **Top security technologies used to protect payment data**
  - Firewalls: 93%
  - Anti-Virus / Anti-Malware: 92%
  - Data Encryption: 75%
  - Intrusion detection and prevention (IDS/IPS): 46%
  - Multi-factor authentication: 40%
  - SIEM: 31%
  - Data Loss Prevention: 31%
  - Other: 5%
  - Threat Monitoring: 37%
  - Private network connectivity: 41%

- **Ownership of payment data security is not centralized**

- **PCI DSS is not sufficient for ensuring the security and integrity of payment data**
  - Only 17% of companies say PCI DSS compliance is essential.
  - In fact, 74% of companies are not fully compliant or are only partially compliant.

- **End-to-end encryption of payment data**
  - 44% of companies use end-to-end encryption to protect payment data as it moves from the POS terminal and is transmitted to the financial institution.

**MULTI-FACTOR AUTHENTICATION IS MAINLY USED FOR INTERNAL EMPLOYEES AND RARELY FOR THIRD PARTIES OR VENDORS**

- Multi-factor authentication for internal employees: 66%
- Multi-factor authentication for vendors or third parties: 26%
- PCI DSS is not sufficient for ensuring the security and integrity of payment data: 38%

**PAYMENT DATA SECURITY IS NOT CONTROLLED**

- 28% of respondents say they use more than one company to manage service payments.
- 25% say they use one company and the other payment methods.

**THE SECURITY OF PAYMENT DATA IS NOT ALWAYS A TOP PRIORITY**

- 50% of companies do not put payment data security as a top five security priority.
- 50% say they allocate enough resources to the protection of payment data.

**OWNERSHIP OF PAYMENT DATA SECURITY IS NOT CENTRALIZED**

- When it came to saying who is most responsible for ensuring payment data is protected, surveyed IT professionals said the following:
  - CIO: 34%
  - Business Unit Compliance: 55%
  - CISO: 55%
  - Risk Management: 33%
  - Legal: 25%
  - Internal Audit: 118%