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 companies have experienced a data breach involving payment data in the last 2 years.
- **Payment Data Has Many Points of Vulnerability to Security Threats**: 42% of companies have experienced a data breach in the past, and 25% of companies are not sure where their payment data is located.
- **27% of Companies Do Not Believe or Are Unsure If Their Existing Security Protocols Are Capable of Supporting These Platforms**: Interestingly, 54% of companies do not believe or are unsure if their existing security protocols are capable of supporting these platforms.
- **Top Security Technologies Used to Protect Payment Data**: This is represented in the infographic, where we see that Firewalls are used by 93%, Anti-Virus / Anti-Malware by 92%, Data Encryption by 75%, Intrusion detection and prevention (IDS/IPS) by 46%, Multi-factor authentication by 40%, SIEM by 31%, and Data Loss Prevention by 31%.

**TOP SECURITY TECHNOLOGIES USED TO PROTECT PAYMENT DATA SECURITY**

- **Only 43% of companies use encryption or tokenization at the point of sale**. 27% have plans to implement and 30% do not use it.
- **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 CRUCIAL FOR INTERNAL EMPLOYEES AND RARELY FOR THIRD PARTIES OR VENDORS**

- **34% use multi-factor authentication for vendors or third-parties**. This is a significant finding in understanding the security strategies employed by companies.

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

- **54% of companies say that payment data security is owned by the CIO Business Unit Compliance CISO Risk Management Legal Internal Audit**, indicating a fragmented approach to data security ownership.

**MORE TRENDS IN PAYMENT METHODS**

- **Mobile Payments Will Double in the Next Two Years**: 55% of respondents say their company had a data breach involving payment data an average of four times in the past two years, while 26% said when it is stored, 28% said when in transit between the company and financial institution, and 15% said at the point-of-sale.

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

- **45% of companies do not put payment data security as a top five security priority**. 44% of companies 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 are unsure if their existing security protocols are capable of supporting these platforms.

**TOP SECURITY TECHNOLOGIES USED TO PROTECT PAYMENT DATA**

- **Today, 14% of companies accept mobile payments such as Apple Pay, Samsung Pay or other contactless payment methods**, and 51% of companies have plans to accept mobile payments in the future.

- **HALF OF ALL COMPANIES HAVE PLANS TO ACCEPT MOBILE PAYMENTS**. This highlights the growing acceptance and importance of mobile payments.

- **NOT ALL COMPANIES ARE CONFIDENT IN THEIR ABILITY TO SECURE NEXT GENERATION PAYMENT METHODS**. This is a significant concern as new payment methods are introduced.

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

- **54% of companies do not put payment data security as a top five security priority**. 44% of companies say they allocate enough resources to the protection of payment data.

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

- **54% of companies do not put payment data security as a top five security priority**. 44% of companies say they allocate enough resources to the protection of payment data.

**TRENDS IN PAYMENT METHODS**

- **Mobile payments will double in the next two years**: 55% of respondents say their company had a data breach involving payment data an average of four times in the past two years, while 26% said when it is stored, 28% said when in transit between the company and financial institution, and 15% said at the point-of-sale.

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

- **54% of companies do not put payment data security as a top five security priority**. 44% of companies 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 are unsure if their existing security protocols are capable of supporting these platforms.

**TOP SECURITY TECHNOLOGIES USED TO PROTECT PAYMENT DATA**

- **Today, 14% of companies accept mobile payments such as Apple Pay, Samsung Pay or other contactless payment methods**, and 51% of companies have plans to accept mobile payments in the future.

- **HALF OF ALL COMPANIES HAVE PLANS TO ACCEPT MOBILE PAYMENTS**. This highlights the growing acceptance and importance of mobile payments.

- **NOT ALL COMPANIES ARE CONFIDENT IN THEIR ABILITY TO SECURE NEXT GENERATION PAYMENT METHODS**. This is a significant concern as new payment methods are introduced.

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

- **54% of companies do not put payment data security as a top five security priority**. 44% of companies say they allocate enough resources to the protection of payment data.

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

- **54% of companies do not put payment data security as a top five security priority**. 44% of companies say they allocate enough resources to the protection of payment data.