gemalto
security to be free

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

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

NOT ALL COMPANIES KNOW WHERE PAYMENT DATA IS LOCATED.

55% of companies do not know where all their payment data is stored

PAYMENT DATA HAS MANY POINTS OF VULNERABILITY TO SECURITY THREATS

42% said when it is stored

33% said when in transit between the company and financial institution or payment processor

25% said data 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

31% 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

- **9%** of all payments are mobile today
- **18%** of all payments will be mobile in two years

HALF OF ALL COMPANIES HAVE PLANS TO ACCEPT MOBILE PAYMENTS

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

NOT ALL COMPANIES ARE CONFIDENT IN THEIR ABILITY TO SECURE NEXT GENERATION PAYMENT METHODS

54% of companies do not believe or are unsure if their existing security protocols are capable of supporting these platforms.

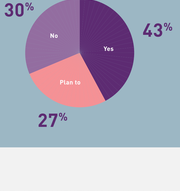
TRENDS IN PAYMENT DATA SECURITY

TOP SECURITY TECHNOLOGIES USED TO PROTECT PAYMENT DATA

Note: % of respondents who said they used these security technologies to protect payment data.

TOP SECURITY TECHNOLOGIES USED TO PROTECT PAYMENT DATA

Only **43%** of companies use encryption or tokenization at the point of sale. **27%** have plans to implement and **30%** do not use it.

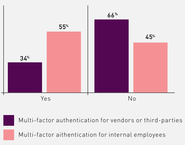


END-TO-END ENCRYPTION OF PAYMENT DATA

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.

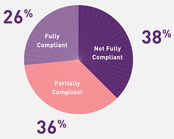
MULTI-FACTOR AUTHENTICATION IS MAINLY USED FOR INTERNAL EMPLOYEES AND RARELY FOR THIRD PARTIES OR VENDORS

- **9%** of all payments are mobile today
- **18%** of all payments will be mobile in two years



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



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