gemalto
security to be free

Global Study on the State of Payment Data Security

Introduction

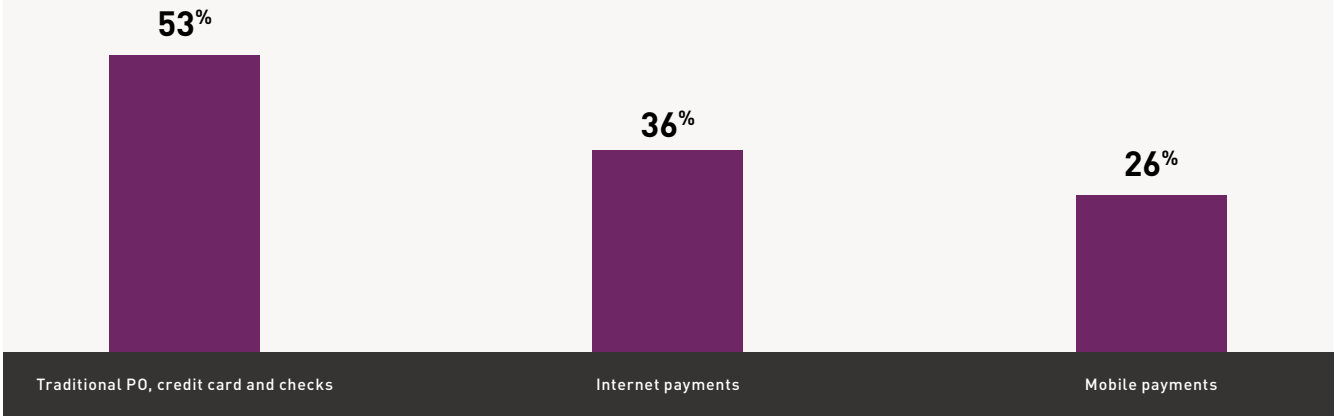
We are pleased to present the findings of **The Global Study on the State of Payment Data Security Study** conducted on behalf of Gemalto by the Ponemon Insitute. The purpose of this research is to focus on the approach organizations are taking to secure payment data. As the research reveals, IT professionals believe the risk to payment data is increasing because of new payment methods such as mobile payments, contactless payments and e-wallets.

The majority of companies represented in this study (**54 percent** of respondents) have **had a security or data breach involving payment data an average of four times in the past two years**. Based on the study, companies need to take steps to improve the security of data in new payment methods or they will continue to experience breaches. This is especially critical because the acceptance of mobile payments is expected to double from nine percent of all payments today to 18 percent of all payments in the next two years.

We surveyed **3,773 IT and IT security practitioners** in the following countries: United States, United Kingdom, Germany, France, Belgium, Netherlands, Japan, India, Russian Federation, Middle East and South Africa. All respondents are familiar and involved in their companies approach to securing payment data. Most respondents are involved in setting priorities (54 percent of respondents) and selecting vendors and contractors (44 percent of respondents) in their companies' payment ecosystem.

We asked respondents to rate the effectiveness of their ability to secure the various payment methods. Figure 1 shows those respondents who rated their ability to secure payment data as very effective (7+ on the scale of 1 = ineffective to 10 = very effective). Specifically, the majority of respondents (53 percent) believe they are far more effective in securing traditional point of sale, credit card and checks than mobile payments and Internet payments.

Figure 1.
How effective is your company in securing payment data?



Other key takeaways in this research include the following:

- The uncertainty of knowing the location and storage of their payment data is a major risk for companies. Eighty percent of respondents say this is a very high (42 percent) or high (38 percent) risk to payment data. Sixty-two percent of respondents say if data is not stored in the cloud it is mainly stored in a centralized storage facility (within data centers).
- Payment data is at risk due to the new payment methods such as mobile payments, contactless payments and e-wallets. However, these new payment methods are difficult to implement because of authentication risk.
- The majority of companies represented in this study are planning to accept such next-generation payment platforms such as Apple Pay, contactless payments, Samsung Pay or MasterCard and Visa' cloud-based payments but do not believe existing security protocols are capable of supporting these platforms.
- Fifty-three percent of respondents agree that EMV and chip & pin cards improve security significantly.
- Security personnel and technologies are not sufficient to effectively protect payment data according to the majority of respondents.
- Payment data is most at risk when it is either stored or in transit between a company and financial institutions and payment processors.
- More payment data will move to the cloud but only 45 percent say they use encryption, tokenization or other cryptologic tools to protect data in the cloud.
- Only 44 percent of respondents say their company uses end-to-end encryption for payment data as it moves from the POS terminal and then transmitted to the financial institutions. Thirty-two percent say they only encrypt data as it is sent to the financial institution or when it is stored (29 percent of respondents). However, 70 percent of respondents say they use encryption or tokenization to protect data as it is captured at the point of sale.
- To protect payment data, most companies use firewalls (93 percent of respondents), anti-virus/anti-malware (92 percent of respondents) or intrusion detection and prevention systems (75 percent of respondents).
- Multi-factor authentication is used more often for internal employees (66 percent of respondents) than vendors or third parties (34 percent of respondents).
- Ownership of payment data security is disparate and not centralized. No single function is clearly accountable for protection of payment data.
- Compliance with PCI DSS is not considered sufficient for ensuring the security and integrity of payment data, according to 31 percent of respondents. In fact, only 17 percent of respondents say PCI DSS is essential and 18 percent of respondents say it is very important to achieving a strong payment data security posture.

Key Findings

In this section, we provide an analysis of the key findings. Payment data is susceptible to data breaches

- Trends in payment methods
- Payment security and governance practices

Payment Data Is Susceptible to Data Breaches

Payment data has been breached multiple times. Fifty-four percent of respondents say their organization has had a breach involving payment data in the past two years. On average, these organizations have had approximately four such breaches in the past two years, as shown in Figure 2.

Figure 2.
How frequently has your company's payment data been breached?
Extrapolated average 3.9

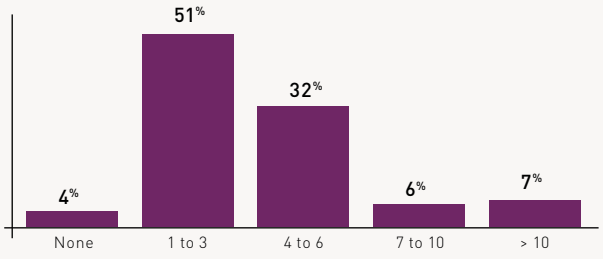
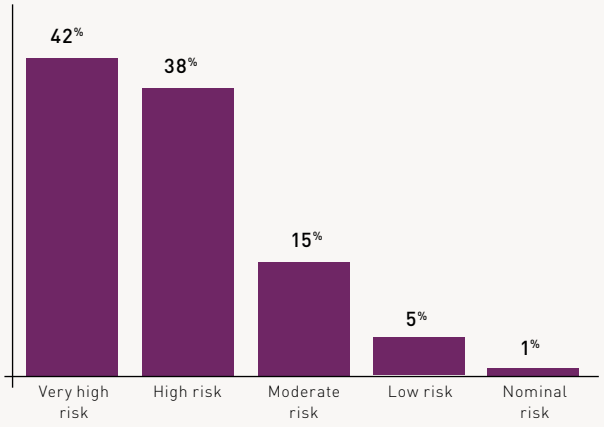


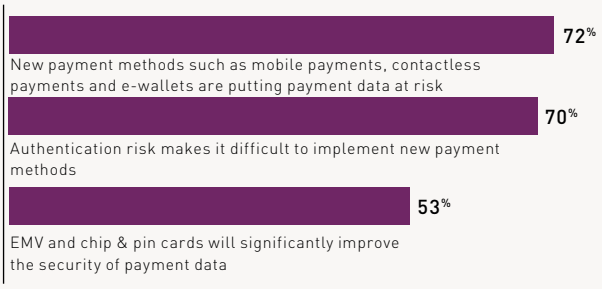
Figure 3.
What best describes the inherent risk of data loss or theft as a result of not knowing where payment data is stored or located?



Where is payment data stored or located? A problem companies need to confront is determining the location and storage of their payment data. According to Figure 3, the majority of companies (55 percent of respondents) represented in this study do not know where all their payment data is stored or located and this is considered either a very high risk (42 percent of respondents) or high risk (38 percent of respondents).

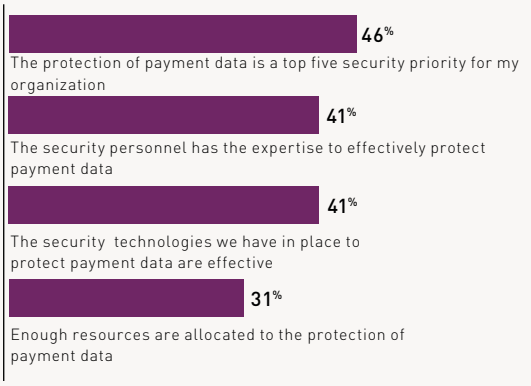
Can companies address the security of new payment methods? As shown in Figure 4, 72 percent of respondents believe new payment methods such as mobile payments, contactless payments and e-wallets are putting payment data at risk and 70 percent of respondents say authentication risk makes it difficult to implement new payment methods. However, EMV and chip & pin cards are considered by 53 percent of respondents to significantly improve the security of payment data.

Figure 4.
Why payment data is believed to be at risk
Strongly agree and agree response combined



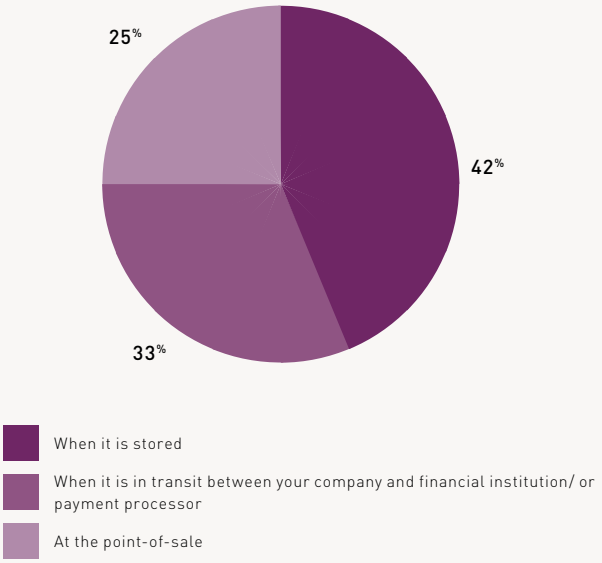
A barrier to payment data security is that only 46 percent of respondents say the protection of payment data is among the top five security priorities for their companies and only 31 percent of respondents say their organization allocates enough resources to the protection of payment data, as shown in Figure 5. Moreover, only 41 percent of respondents say their security technologies and security personnel are in place to protect payment data.

Figure 5.
Barriers to payment data security
Strongly agree and agree response combined



Where is payment data at most risk? According to Figure 6, payment data is considered most at risk when it is either stored (42 percent of respondents) or when in transit between the company and financial institution/ or payment processor (33 percent of respondents). Only 25 percent of respondents say it is at the point-of-sale. The most important payment data elements to protect are password/PIN, credit card and debit card and security codes.

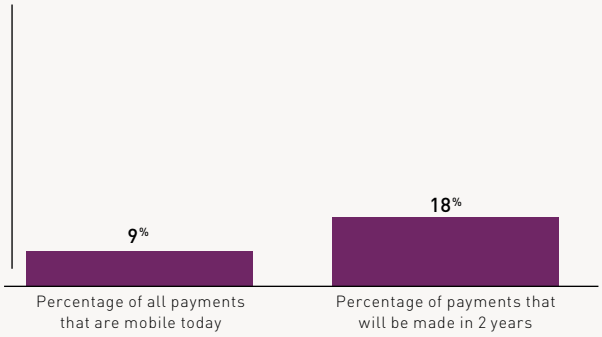
Figure 6.
Where do you think payment data is most vulnerable to security threats?



Trends in Payment Methods

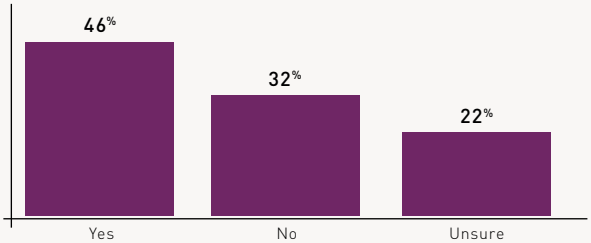
The acceptance of mobile payments will double in the next two years. Currently, 74 percent of respondents do not accept mobile payments. As shown in Figure 7, if companies do accept mobile payments, the average percentage of all mobile payments is 9 percent and this will increase to 18 percent in the next two years.

Figure 7.
Acceptance of mobile payments today and in two years
Extrapolated average



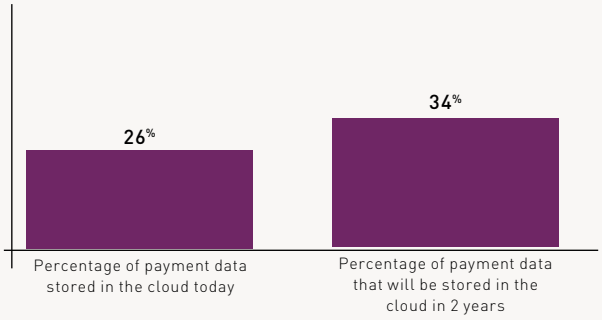
What are the trends in the use of next-generation payment platforms? Seventy-six percent of respondents say their companies accept Chip and PIN or Chip and Signature credit cards. Only 14 percent of respondents say their organization currently offers Apple Pay, contactless payments, Samsung Pay or MasterCard and Visa's cloud-based payments. But 51 percent of respondents say their organization is planning to accept these next-generation payment platforms. However, as shown in Figure 8, 54 percent of respondents say they do not believe (32 percent of respondents) or are unsure (22 percent of respondents) that their organization's existing security protocols are capable of supporting these platforms.

Figure 8.
Do you believe your organization's existing security protocols are capable of supporting next-generation platforms?



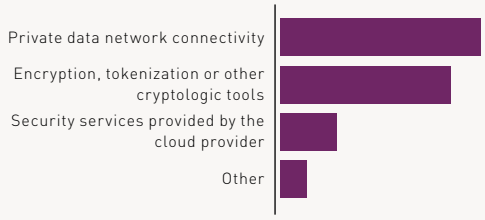
The movement of payment data to the cloud will increase. According to Figure 9, today, 44 percent of respondents say their companies on average store 26 percent of all payment data in the cloud and this is expected to increase to an average of 34 percent.

Figure 9.
Percentage of all payment data is stored in the cloud today and in two years
Extrapolated average



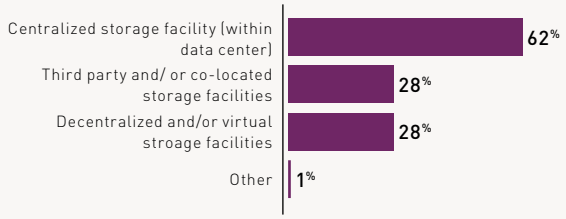
As shown in Figure 10, to protect payment data in the cloud, 53 percent of respondents say they use private data network connectivity followed by encryption, tokenization and other cryptologic tools (45 percent of respondents). Only 15 percent of respondents depend upon the security services provided by the cloud provider.

Figure 10.
How does your organization protect data stored in the cloud?
More than one response permitted



If payment data is not stored in the cloud, it is most likely stored in a centralized storage facility within the data center (62 percent of respondents) followed by 28 percent of respondents who say it is stored in a decentralized and/or virtual storage facility or third party and/or co-located storage facilities (28 percent of respondents), according to Figure 11.

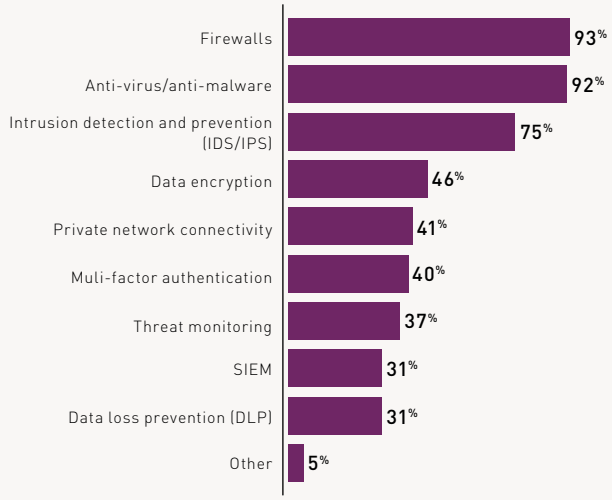
Figure 11.
Where is payment data stored within your organization?
More than one response permitted



Payment Security and Governance Practices

Security measures currently used to secure payment data. Figure 12 presents the security measures most often used to protect payment data are: firewalls (93 percent of respondents), anti-virus/anti-malware (92 percent of respondents), intrusion detection and prevention (75 percent of respondents) and data encryption (46 percent of respondents).

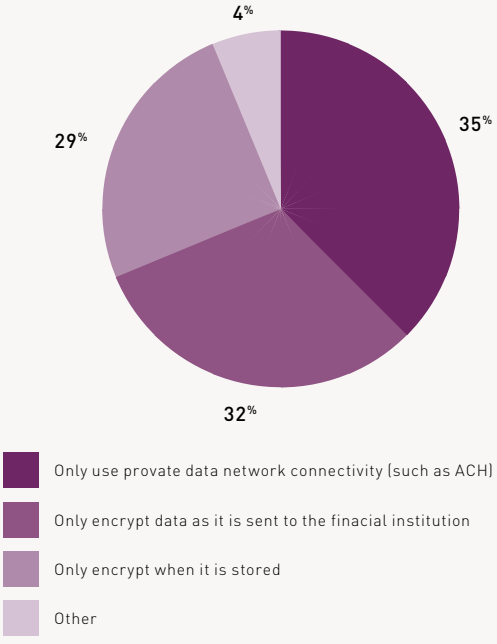
Figure 12.
What security measures do you currently use to protect payment data?
More than one response permitted



How encryption is used to protect payment data. Forty-four percent of respondents say their company uses end-to-end encryption for payment data as it moves from the POS terminal and then transmitted to the financial institution. As shown in Figure 13, if they do not use encryption to protect sensitive information, including payment data, 35 percent say they only use private data network connectivity (such as ACH), 32 percent say they only encrypt data as it is sent to the financial institution (32 percent of respondents) and 29 percent say they only use encryption when the payment data is in storage.

Figure 13.

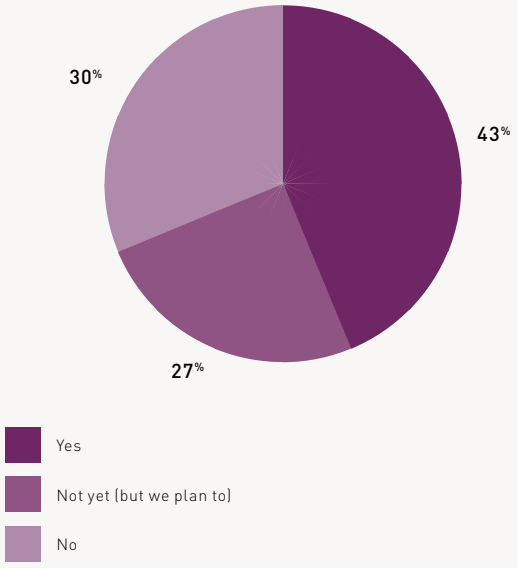
How does your company use encryption to protect sensitive information, including payment data?



Only about half of companies use encryption at the POS. Figure 14 reveals that 43% percent of respondents say their company uses encryption and/or tokenization to protect data is captured at the point of sale or plan to do so.

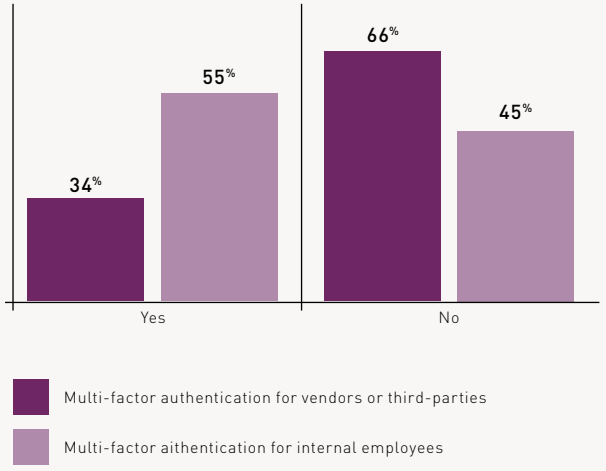
Figure 14.

Does your organization currently use encryption and/or tokenization to protect data as it is captured at the POS?



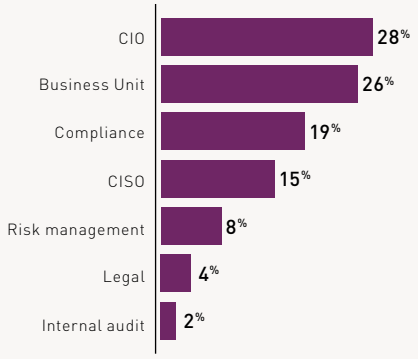
Multi-factor authentication is mainly used for internal employees and rarely for third parties or vendors. Security measures for vendors or third parties with access to payment applications and data should be strengthened. According to Figure 15, 59 percent of respondents say their organizations permit third parties to have such access but only 34 percent of respondents say their organizations use multi-factor authentication for third parties and vendors. Fifty-five percent say they use such technology for internal employee's access to payment applications and data.

Figure 15.
Does your company use multi-factor authentication for vendors and/or employees?



Ownership of payment data security is disparate and not centralized. As shown in Figure 16, no single function or role is leading the effort to secure payment data. Twenty-eight percent of respondents say it is the CIO and 26 percent say the business unit is responsible for the security of payment data collected and stored in their companies.

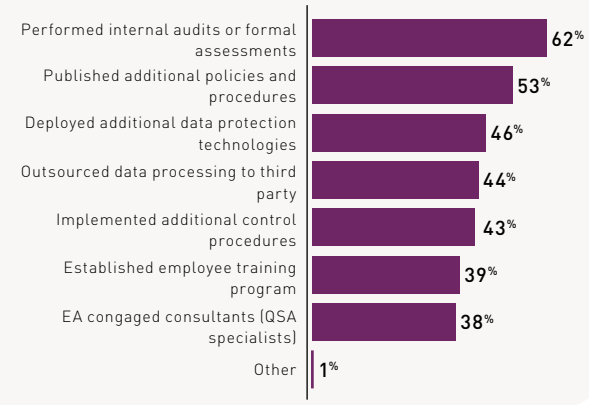
Figure 16.
Who is most responsible for ensuring payment data is protected?



What is the role of PCI DSS compliance in the security of payment data? Compliance with PCI DSS is not considered sufficient for ensuring the security and integrity of payment data, according to 31 percent of respondents. In fact, Only 17 percent of respondents say PCI DSS is essential and 18 percent of respondents say it is very important to achieving a strong payment data security posture.

Seventy-four percent of respondents say their companies are not fully compliant (38 percent) or only partially compliant (36 percent). For those companies partially compliant but interested in becoming fully compliant, the steps most often taken, as shown in Figure 17, are internal audits or formal assessments (62 percent of respondents), published additional policies and procedures (53 percent of respondents), deployment of additional data protection technologies (46 percent of respondents) and outsourced data processing to a third party (44 percent of respondents).

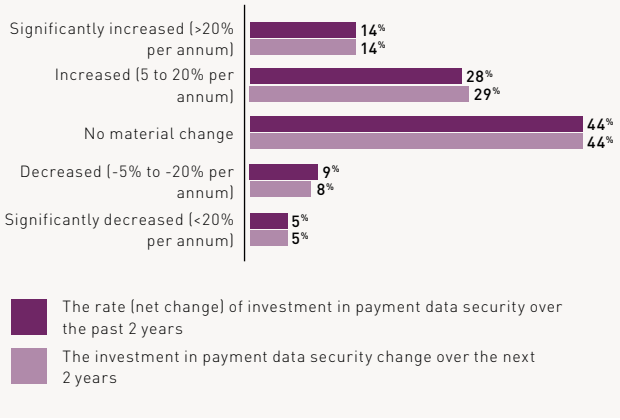
Figure 17.
What steps is your organization taking to become fully compliant?



Is the investment in payment data security sufficient?
On average, companies are investing 15 percent of the overall IT budget in data protection and security and an average of 13 percent of the data protection and security budget is allocated to securing payment data.

As shown in Figure 18, the rate of investment in payment data security is not expected to change significantly. Only 14 percent of respondents say they significantly increased the budget for payment data security in the past 2 years and the same percentage say their companies are expected to increase their percentage significantly.

Figure 18.
How investment in payment data security changed the past two years and will change over the next two years?



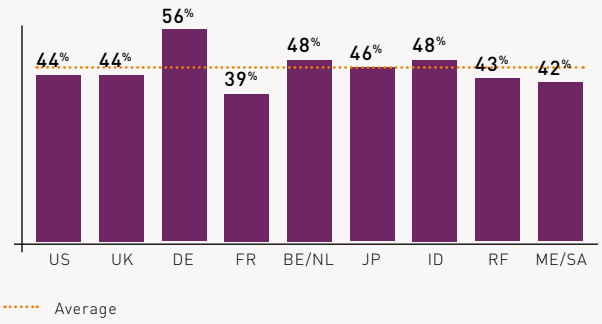
Country Differences

In this section, we provide an analysis of country differences in perceptions about payment data security. We also focus on questions regarding confidence in knowing where all payment data is stored or located and perceptions about the risk of data loss or theft when not knowing where payment data is stored or located.

Perceptions about Payment Data Security

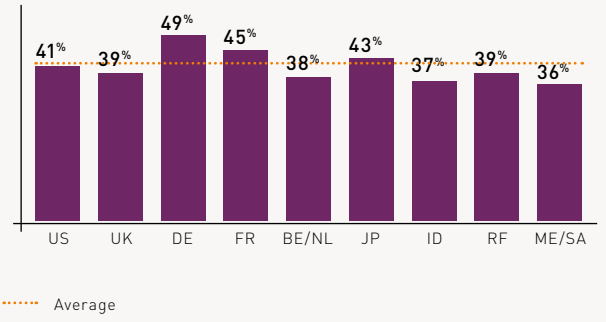
As shown in Figure 19, organizations in Germany are more likely to make the protection of payment data a top priority. France is less likely to see protection of payment data as critical.

Figure 19.
The protection of payment data is a top five priority for my organization
Strongly agree and agree responses combined



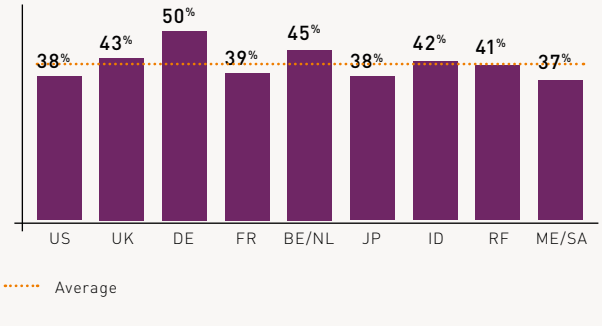
Companies in Germany are more likely to consider their security technologies to protect payment data are effective, according to Figure 20. As shown above, they are more likely to make the protection of payment data a priority. In contrast, companies in the Middle East/South Africa are least likely to believe in the effectiveness of their security solutions for payment data.

Figure 20.
The security technologies we have in place to protect payment data are effective
Strongly agree and agree responses combined



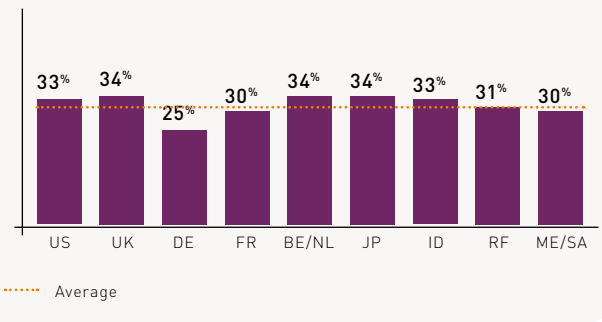
Once again, as presented in Figure 21, German companies seem to be better prepared to deal with the protection of payment data. Countries that lack the necessary in-house expertise are: US, France, Japan and Middle East/South Africa.

Figure 21.
Our security personnel has the expertise to effectively protect payment data
Strongly agree and agree responses combined



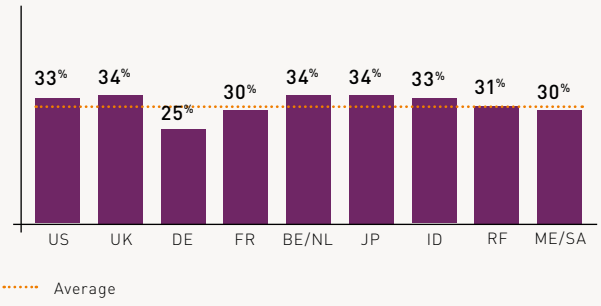
As shown in Figure 22, all countries are most likely to believe they cannot rely upon PCI DSS to ensure the security and integrity of payment data. However, Only 25 percent of respondents from German organizations believe PCI DSS is sufficient for achieving their payment data security goals.

Figure 22.
Compliance with PCI DSS is sufficient for ensuring the security and integrity of payment data
Strongly agree and agree responses combined



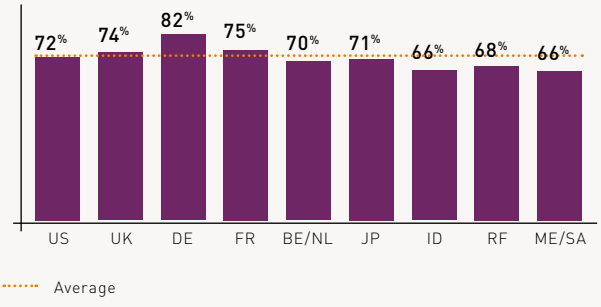
As shown in Figure 19, organizations in Germany are more likely to make the protection of payment data a top priority. France is less likely to see protection of payment data as critical.

Figure 22.
Compliance with PCI DSS is sufficient for ensuring the security and integrity of payment data
Strongly agree and agree responses combined



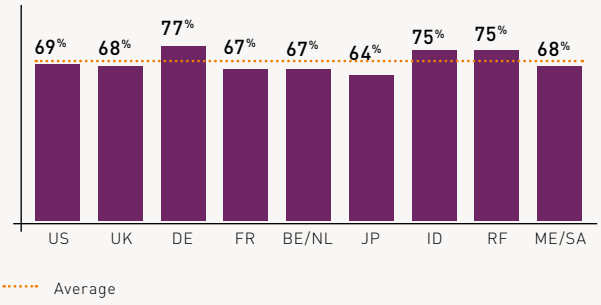
The countries most concerned about the security risks of new payment methods are Germany, France, UK and US, as presented in Figure 23.

Figure 23.
New payment methods such as mobile payments, contactless payments and e-wallets are putting payment data at risk
Strongly agree and agree responses combined



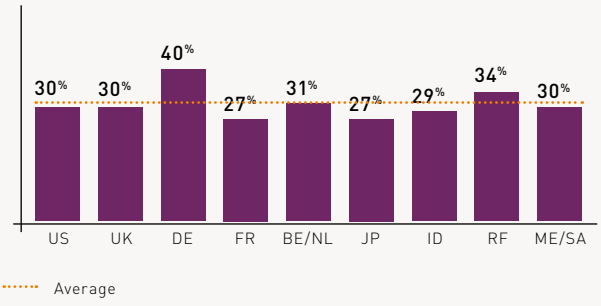
Most respondents in all countries are concerned about authentication risks with new payment methods, as presented in Figure 24. However respondents in Germany, India and the Russian Federation are more likely to agree that authentication risks are a barrier to the implementation of new payment methods.

Figure 24.
Authentication risk makes it difficult to implement new payment methods
Strongly agree and agree responses combined



Most respondents admit resources are insufficient to protect payment data. However, as shown in Figure 26, more German respondents say their organizations are allocating sufficient resources.

Figure 25.
Enough resources are allocated to the protection of payment data
Strongly agree and agree responses combined



With the exception of Belgium/Netherlands, the majority of respondents agree that EMV and chip & pin cards will significantly improve the security of payment data, according to Figure 26.

Respondents in India, Germany, US and Belgium/Netherlands are most likely to consider the risk of not knowing where payment data is stored or located as very high or high.

Figure 26.

EMV and chip & pin cards with significantly improve the security of payment data

Strongly agree and agree responses combined

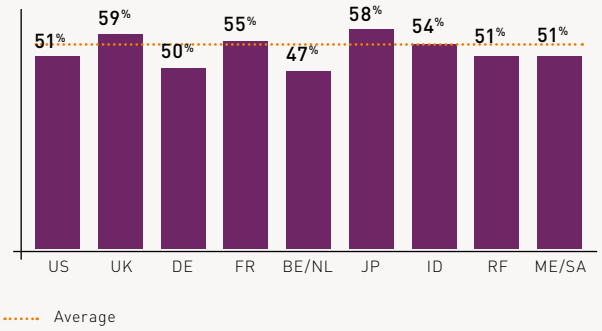
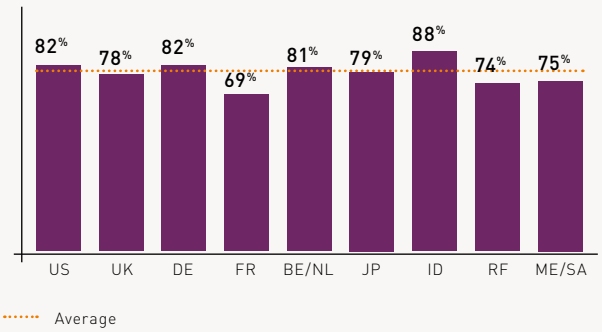


Figure 28.

Do you consider the risk of data loss or theft as a result of not knowing where payment data is stored or located very high or high?

Strongly agree and agree responses combined



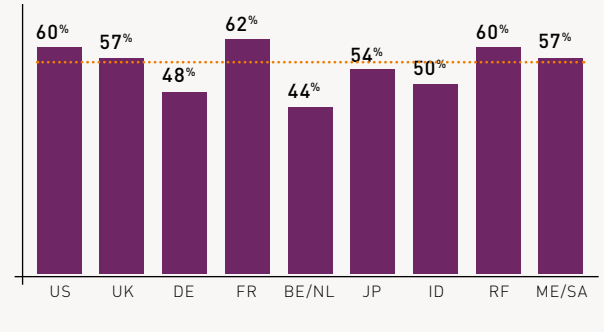
The Risk of Not Knowing Where Payment Data Is Located or Stored

When asked if they are confident they know where all payment data is stored or located, the not confident and no confidence responses are highest in France, US and Russian Federation, as shown in Figure 27.

Figure 27.

Not confident or no confidence in knowing where all your organization's payment data is stored or located

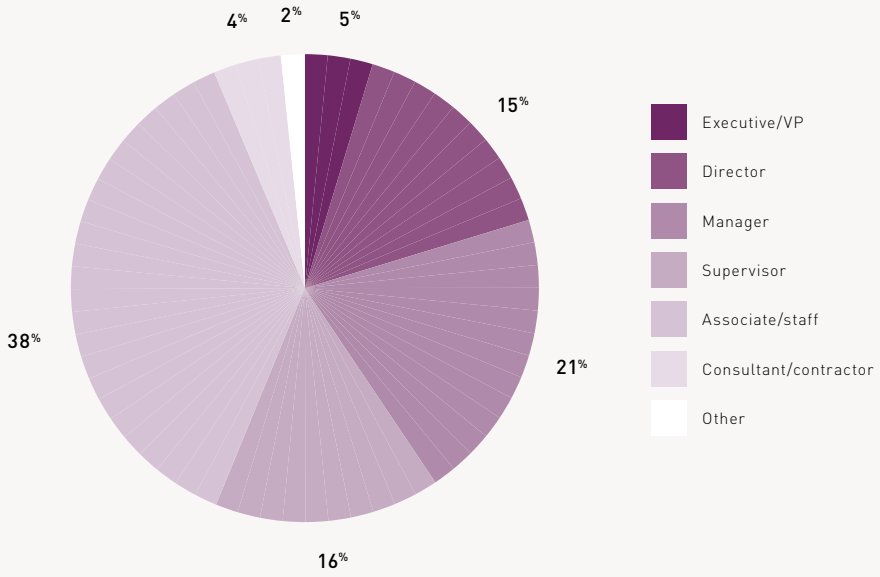
Strongly agree and agree responses combined



Demographics

Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half of respondents (57 percent) are at or above the supervisory levels.

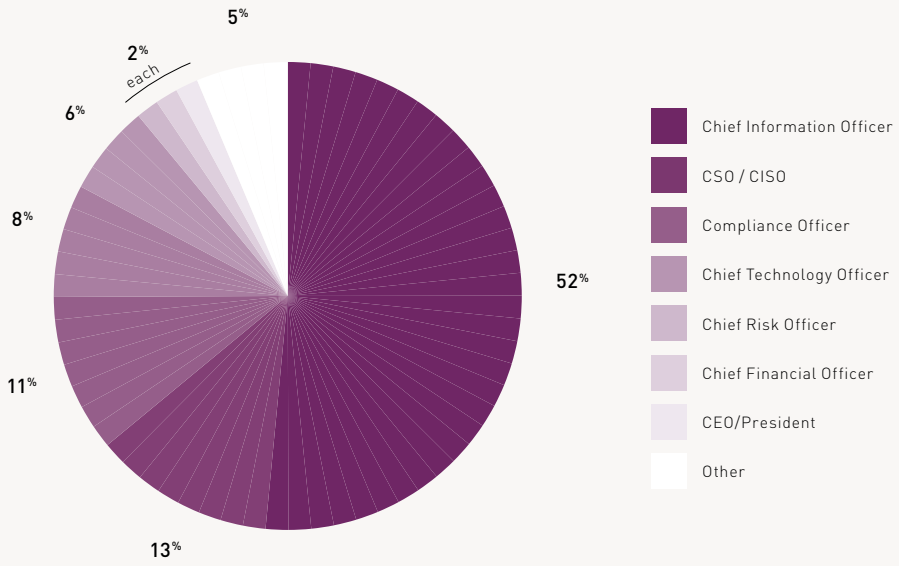
Pie Chart 1.
Current position or organizational level



As shown in Pie Chart 2, 52 percent of the respondents indicated they report directly to the CIO and another 13 percent report to the CSO/CISO.

Pie Chart 2.

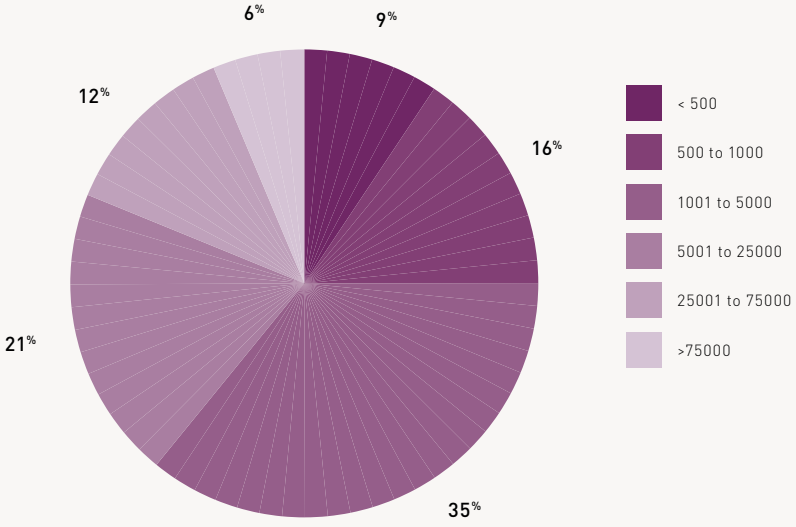
Primary Person you or your supervisor reports to



As shown in Pie Chart 3, 74 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 3.

Global employee headcount



Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments and data – from the edge to the core. Gemalto's portfolio of SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

GEMALTO.COM

gemalto
security to be free