2012 Payment Security Practices Survey: United States

Research sponsored by CyberSource & Trustwave

Independently Conducted by Ponemon Institute LLC

July 2012

Ponemon Institute© Research Report

2012 Payment Security Practices Survey: United States

Part 1. Introduction

We are pleased to present the findings of the *2012 Payment Security Practices Survey: United States*, sponsored by CyberSource and Trustwave. The study also was conducted in the United Kingdom and the findings from that research are available in a separate report.

A secure payment process is essential to maintaining customer confidence and trust when making online purchases and sharing financial information. Managing payment security involves securing payment data across an organization's full order lifecycle, from the point of payment acceptance through fraud management, fulfillment, customer service, funding and financial reconciliation and transaction record storage.

The strategies and practices employed by an organization have a dramatic impact on its ability to adequately manage security, minimize operational complexity and scale its business. This report highlights the strategies adopted by the best performing organizations and compares them to the practices of organizations that have yet to achieve an optimal approach to this area of their operations.

In this study, we focused on organizations that range from having at least one million transactions to more than six million transactions annually (Level1 & 2 Merchants). We surveyed 474 individuals in IT and IT security in these organizations. Most of the respondents report to the chief information officer and chief information security officer.

The key topics in this research conducted by Ponemon Institute are:

- Characteristics of organizations that have experienced none or only one data breach in the past 24 months versus those that have had multiple incidents
- Current state of merchant payment security practices
- Considerations associated with securing the payment process
- Trends in enabling technologies for the payment process

Based on the findings of this study, it is absolutely possible for merchants to manage security in a way that mitigates risk and reduces operational complexity, but not all merchants have adopted practices that ensure such control and scale. It is clear that a majority of merchants recognize the importance of managing payment security. In fact, 66 percent of respondents believe just one data breach would impact their organization's reputation, marketplace image and brand value and 68 percent of respondents say just one such incident would diminish their customers' trust and confidence.

In this research, we identify high-performing organizations as those that had one or no data breaches in the past 24 months. Thirty-two percent of organizations represented in this study are considered high performing and 53 percent are considered low performing. The remaining organizations provided no comment to this question. The following are key characteristics of high-performing organizations:

- Most likely to have sufficient resources to achieve a secure payment process and to have ample security technologies to secure the payment process. On average, high-performing organizations' security budget is $1.21 million greater than low-performing organizations. Further, C-level executives are more likely to view a secure payment process as a core business objective.

- More likely to be compliant with PCI DSS requirements for all applications and databases across the enterprise.

- Less likely to retain and store permanent account numbers (PAN) and more likely to agree that to reduce the impact of a breach it is a good idea to centralize the organization's payment data and substitute PAN with payment tokens.

- More likely to agree that populating customer records with a payment token reduces the exposure of payment data, thereby creating a more secure payment environment.

Here are some of the most interesting findings:

- More than 70 percent of respondents believe attacks against their payment processes are on the rise, with about one-third saying the attacks are increasing in both frequency and severity. However, 49 percent of respondents believe their security budgets will stay the same, which presents a challenge to improving the effectiveness of their payment security.

- Seventy-six percent of respondents strongly agree or agree that minimizing employee interaction with raw payment data creates a more secure payment environment.

- Sixty-one percent agree or strongly agree that replacing customer records with a payment token creates a more secure payment environment.

- The most difficult or very difficult payment security process, according to 56 percent of respondents, is maintaining a firewall configuration to protect confidential data and applications. This is followed by 48 percent who say it is maintaining secure payment applications.

- Today, 45 percent of organizations use in-house encryption to protect stored payment data. In 24 months, this will decline to 39 percent. Tokenization through a service provider will grow from 19 percent today to 27 percent over a two-year time period, indicating a shift in technology strategies.

- Forty-four percent of organizations currently use some kind of in-house point-to-point encryption technology to secure the capture and transmission of payment data. In the next 24 months, this percentage will decline to 38 percent of organizations represented in this study. However, encryption through a service provider will increase from 25 percent today to 34 percent. Today, 26 percent of respondents use hosted payment acceptance and that number will remain unchanged.

The research also reveals the following implications for merchants:

- Hardening organizational security and enabling organizational scale requires a combination of the right technologies, employees with the appropriate expertise and a governance process.

- Organizations might consider engaging a managed services firm to assist in ensuring a secure payment process. In other words, it might be best not to go it alone when trying to mitigate the risk to customers' financial information.

- Emerging channels such as mobile payment are becoming increasingly popular but can pose some risk if not managed properly. The advice is to not jump in without having the necessary security protocols in place.

- In the event of a data breach, seize the opportunity to re-examine existing protocols, overhaul outdated systems and seek incremental resources to upgrade the organization's security practices to meet current requirements.

Part 2. Key Findings

In this section, we analyze in greater detail the key findings from the research. The complete audited findings are presented in the appendix of this paper. We organized the results according to the following themes:

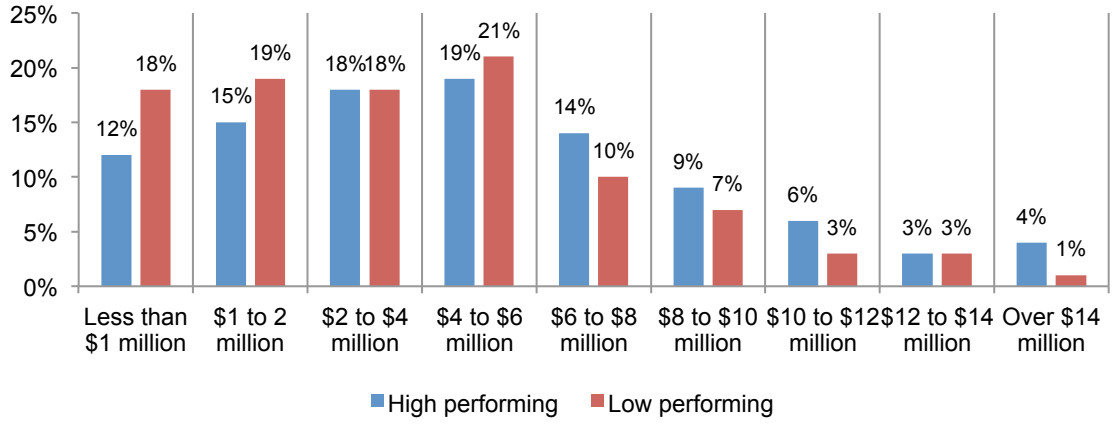
- Characteristics of organizations that have experienced none or only one data breach in the past 24 months versus those that have had multiple incidents
- Current state of merchant payment security practices
- Considerations associated with the payment process
- Trends in enabling technologies for the payment process

Characteristics of high-performing organizations

In this research, we identify high-performing organizations as those that had none or just one data breach. Thirty-two percent of organizations represented in this study are considered high performing and 53 percent are considered low performing organizations. The remaining organizations provided no comment to this question. The following are key characteristics of high-performing organizations.

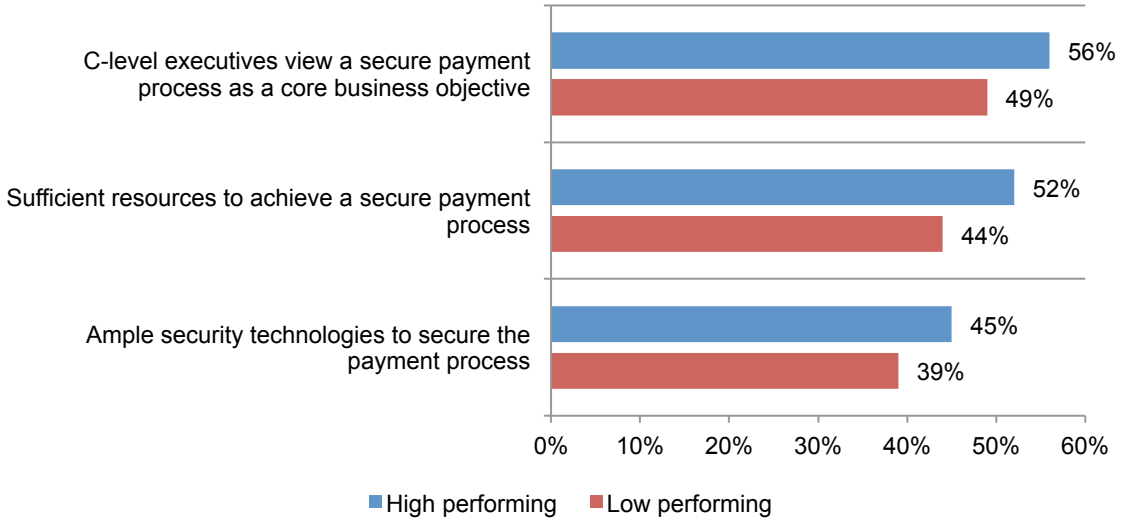
Adequate resources and technologies are less of a concern in high-performing organizations. As shown in Figure 1, high-performing organizations are most likely to have sufficient resources to achieve a secure payment process and to have ample security technologies to secure the payment process. Based on an extrapolated average, high-performing organizations' security budget is $1.21 million greater than low-performing organizations (Figure 1).

Figure 1. Differences in security budget between high and low-performing organizations



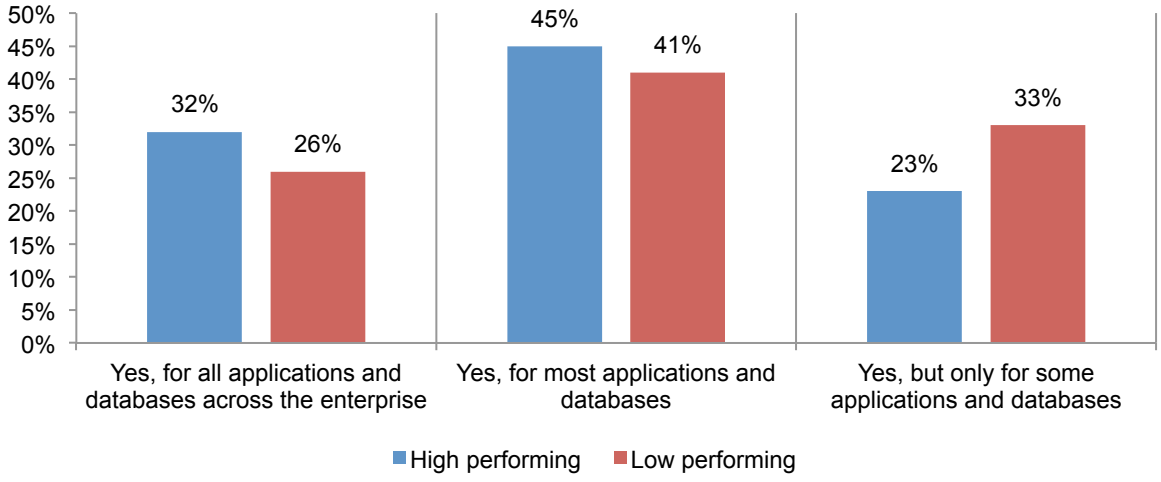
C-level support exists in more high-performing organizations. As shown in Figure 2, C-level executives in high-performing organizations are more likely to view a secure payment process as a core business objective. They also are more likely to have knowledgeable or expert staff dedicated to securing the payment process and sufficient resources.

Figure 2. Attributions about payment security practices
Strongly agree and agree response combined



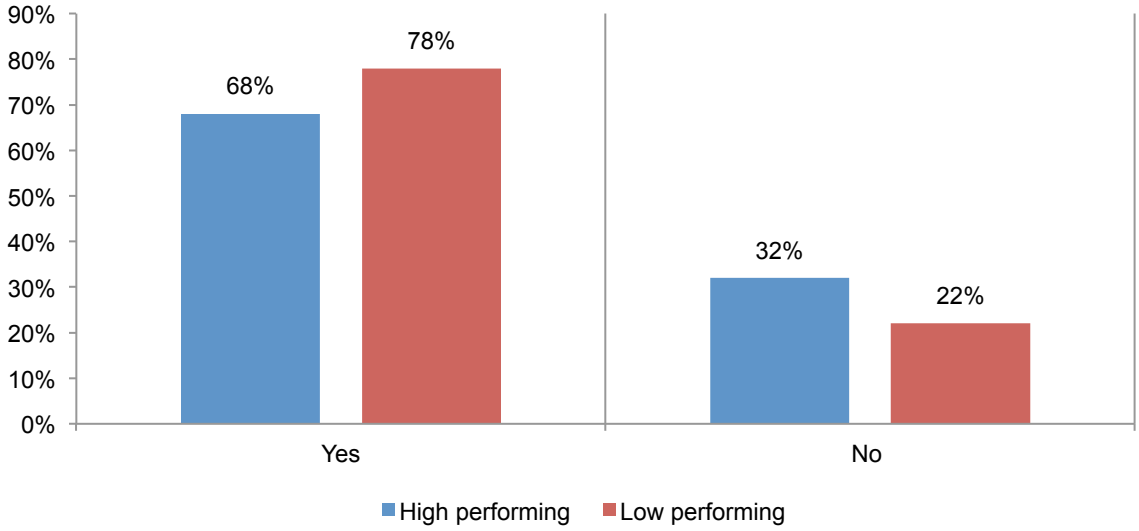
PCI DSS compliance is more prevalent in high-performing organizations. According to Figure 3, high-performing organizations are more likely to be compliant with PCI DSS requirements for all applications and databases across the enterprise. They are also less likely to fail a PCI DSS audit or assessment: 11 percent for high-performing organizations vs. 17 percent for low-performing organizations (not shown in the figure below).

Figure 3. Compliance with PCI DSS requirements



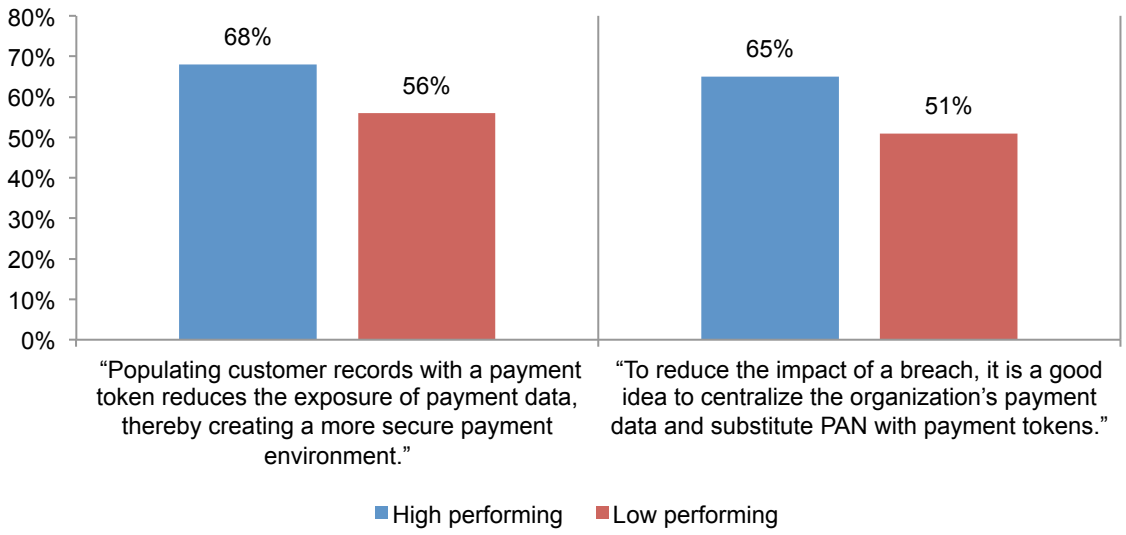
Less likely to retain and store PAN. As shown in Figure 4, high-performing organizations are not as inclined to retain and store PAN.

Figure 4. Does your organization retain and store PAN



Tokenization is more popular in high-performing organizations. Figure 5 reveals that high-performing organizations are more likely to agree that populating customer records with a payment token reduces the exposure of payment data, thereby creating a more secure payment environment. They also have a strong belief that in order to reduce the impact of a breach, it is a good idea to centralize the organization's payment data and substitute PAN with payment tokens.

Figure 5. Attributions about creating a more secure payment environment

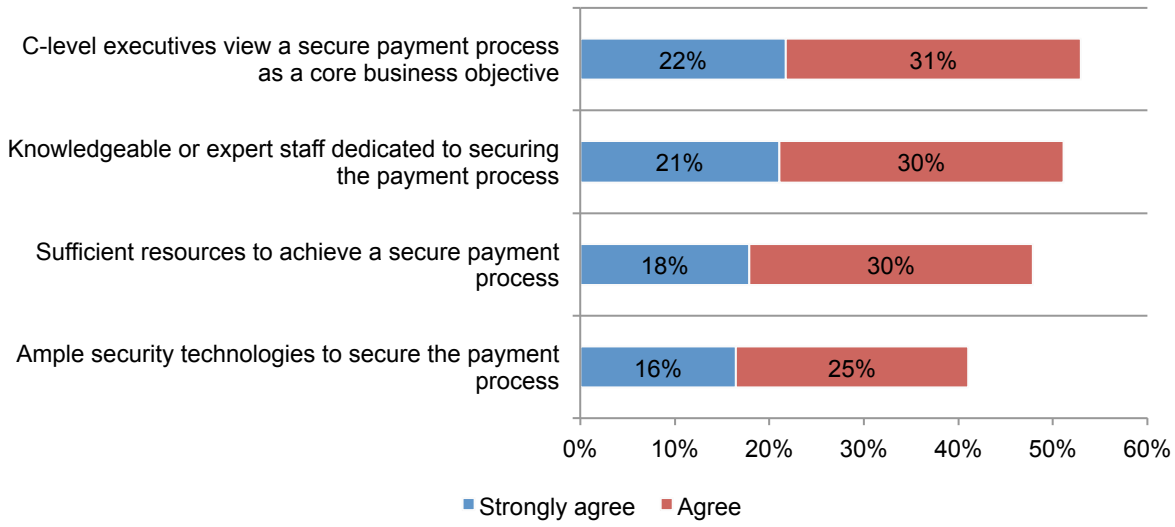


Current state of merchant payment security practices

Despite the importance of a secure payment process, organizations are lagging behind in allocating sufficient resources and investing in technologies. According to Figure 6, more than half (53 percent) of respondents believe their organization's C-level executives view a secure payment process as a core business objective and 51 percent agree that they have knowledgeable or expert staff dedicated to securing the payment process.

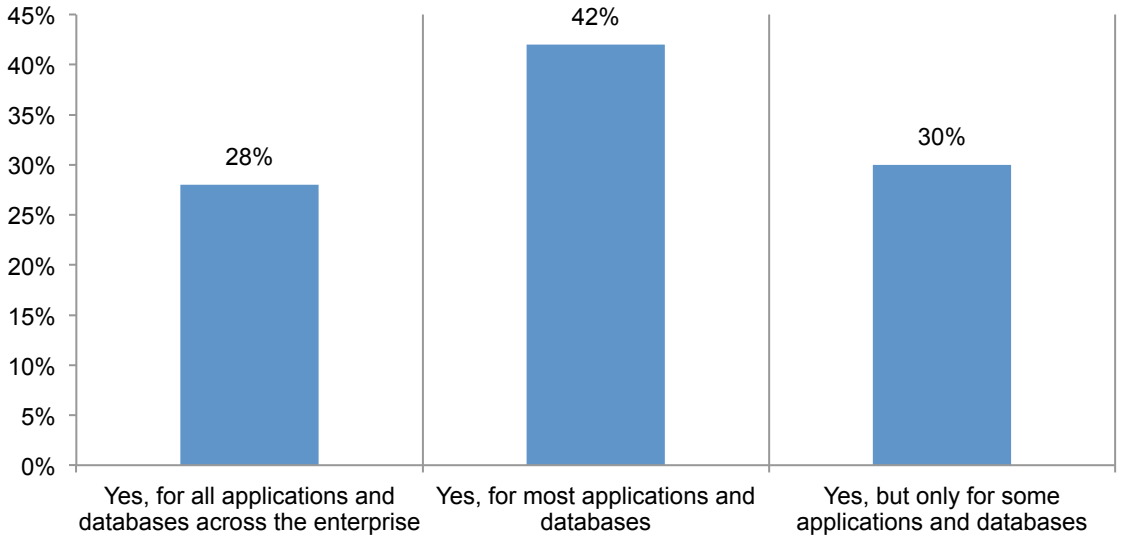
However, less than half of respondents believe their organization has sufficient resources to achieve a secure payment process or ample security technologies to secure the payment process (48 percent and 41 percent, respectively).

Figure 6. Attributions about secure payment processes



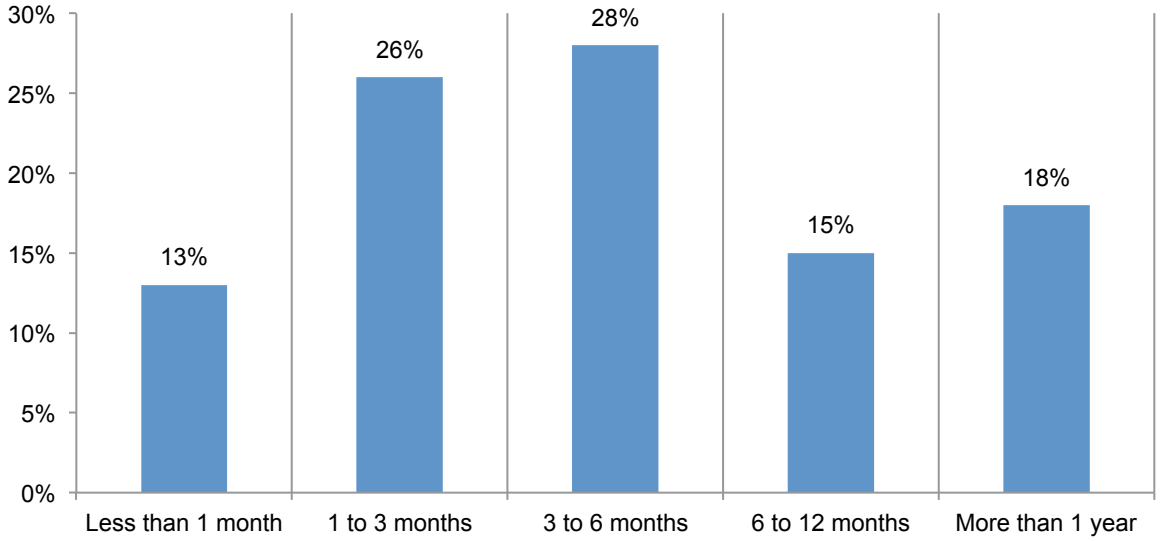
Progress is being made to be PCI DSS compliant. Figure 7 reveals that 70 percent say that their organizations are in substantial compliance with PCI DSS. Twenty-eight percent say they are PCI DSS compliant for **all** applications and databases across the enterprise and 42 percent say they are compliant for **most** applications and databases.

Figure 7. Compliance with PCI DSS requirements



Also shown in Figure 7, 30 percent say they are compliant only for **some** applications and databases. According to Figure 8, 67 percent of respondents in these organizations predict that it will take six months or less to achieve substantial compliance.

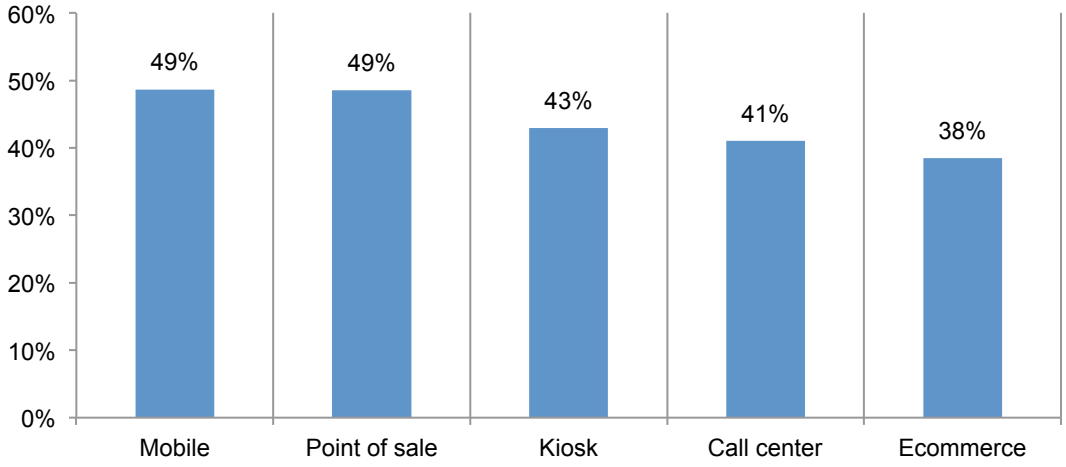
Figure 8. Length of time it will take to achieve substantial compliance with PCI DSS



Considerations associated with securing the payment process

The most difficult payment channels to secure are mobile and point of sale. Figure 9 reveals that approximately half (49 percent) say that both mobile and point of sale channels are the most difficult to secure. Significantly fewer respondents (38 percent) say ecommerce is very difficult or difficult.

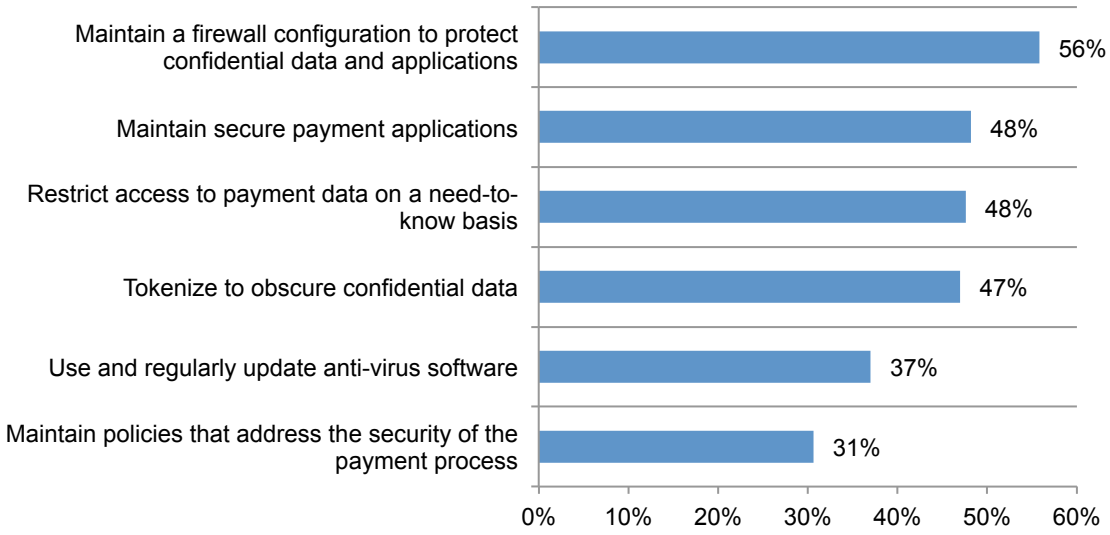
Figure 9. Payment channels difficult to secure
Very difficult and difficult response combined



Certain security initiatives are more of a challenge. Security practices that are most difficult to accomplish are shown in Figure 10. By far it is maintaining a firewall configuration to protect confidential data and applications (56 percent).

Others that are difficult to accomplish include: maintaining secure payment applications (48 percent), restricting access to payment data on a need-to-know basis (48 percent) and tokenizing to obscure confidential data (47 percent). Using and regularly updating anti-virus software (37 percent) and maintaining policies that address the security of the payment process are considered least difficult. The complete list of security practices referenced in this question with frequency of response is in the appendix to this report.

Figure 10. Security practices difficult to accomplish
Very difficult and difficult response combined

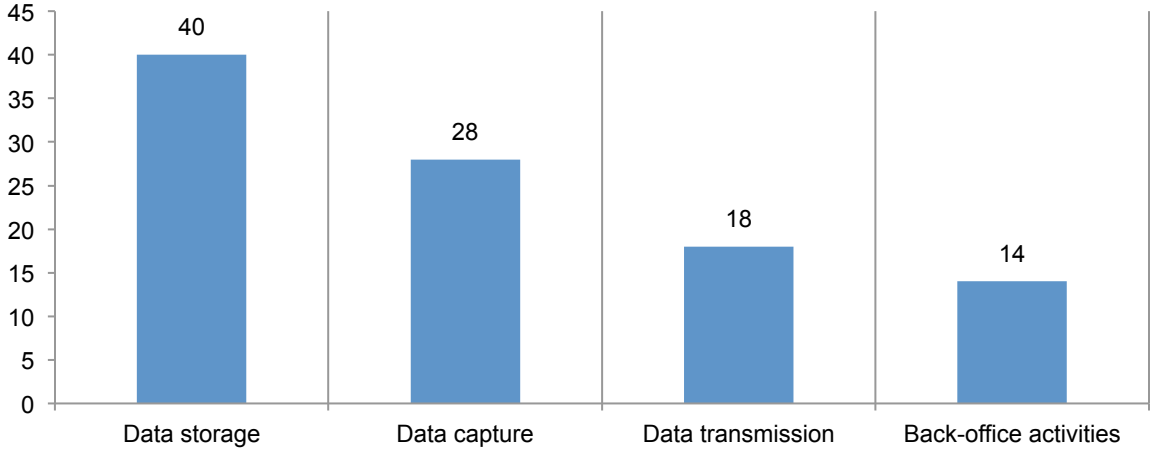


Lack of resources and inability to understand risks are barriers to achieving a secure payment process. The challenges organizations face are lack of resources and ability to assess and prioritize risks. The complexity of regulations is the least significant barrier to overcome (Figure 11). This is consistent with the findings in Figure 6 that point to gaps in available resources and technologies necessary to secure the payment process.

Figure 11. Barriers to achieving a high level of security
Two choices permitted

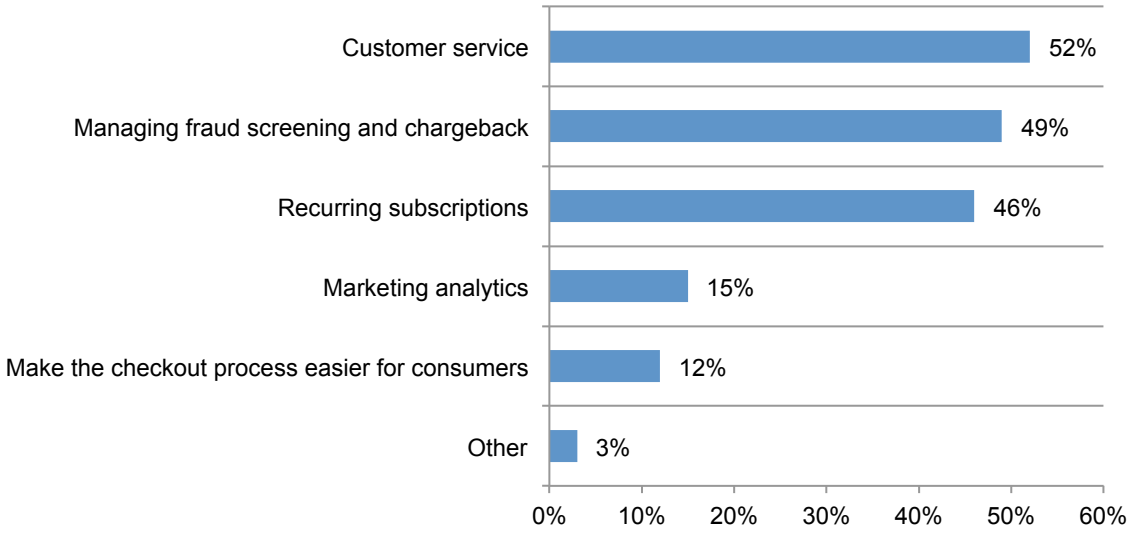
The most serious risk is in data storage. According to Figure 12, by far the most serious threat in the payment data lifecycle is when data is stored. This is followed by when it is captured. With respect to the security of payment data, the greatest threats are the negligent insider followed by the hacker or cyber criminal. The back office activity that poses the greatest risk of data loss or theft is accounting followed by customer service (not shown in figure below).

Figure 12. When payment data is most vulnerable
Total points sum to 100



The practice of retaining and storing permanent account numbers (PAN) is putting organizations at risk for a data breach. Seventy-three percent of organizations in this study retain and store PAN. They do this primarily to support customer service, manage fraud screening and chargebacks and to handle recurring subscriptions, according to Figure 13.

Figure 13. Why organizations retain and store PAN
Two choices permitted



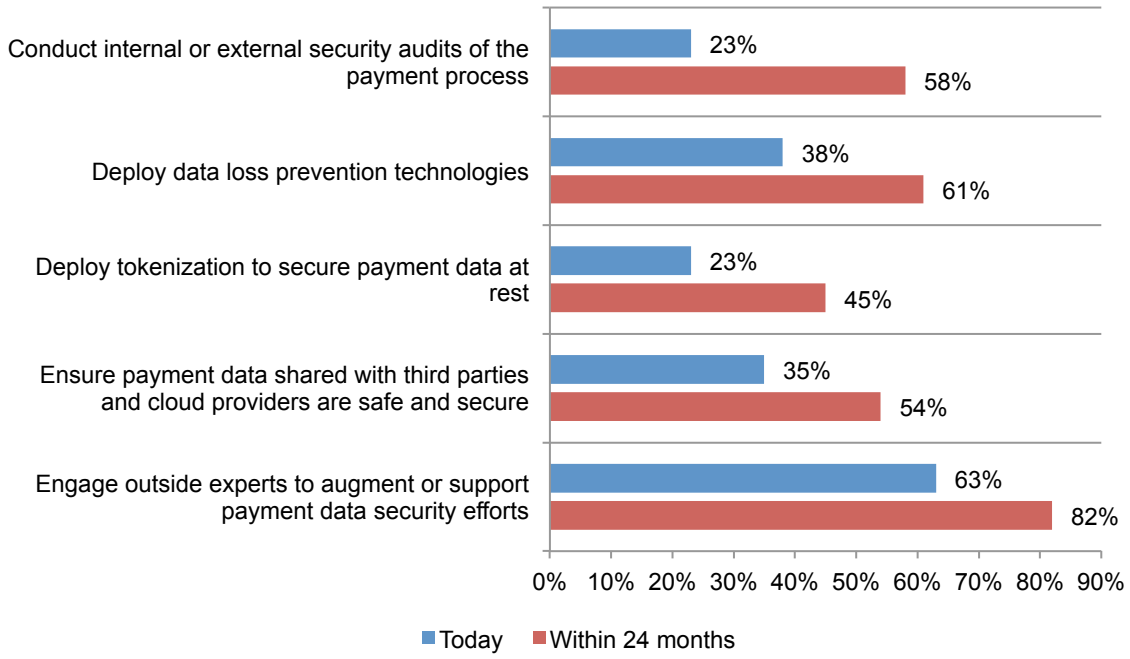
As a security measure, the majority of respondents (56 percent) believe it is a good idea to centralize the organization's payment data and substitute PAN with payment tokens. Sixty-one percent also believe populating customer records with a payment token reduces the exposure of payment data, thereby creating a more secure payment environment (not shown in the figure).

Trends in enabling technologies to secure the payment process

Over the next 24 months, organizations plan to increase the steps taken to secure the storage of payment data and minimize back office exposure in all payment channels. In this section, we discuss the most significant changes in order to improve security in all channels. Generally, the activities that seem most likely to be increased over the next 24 months in order to secure data in all channels are: conducting internal or external security audits, deploying data loss prevention technologies and deploying tokenization to secure payment data at rest. The complete list of activities now in place and expected to be taken within the next 24 months is presented in the appendix of this paper.

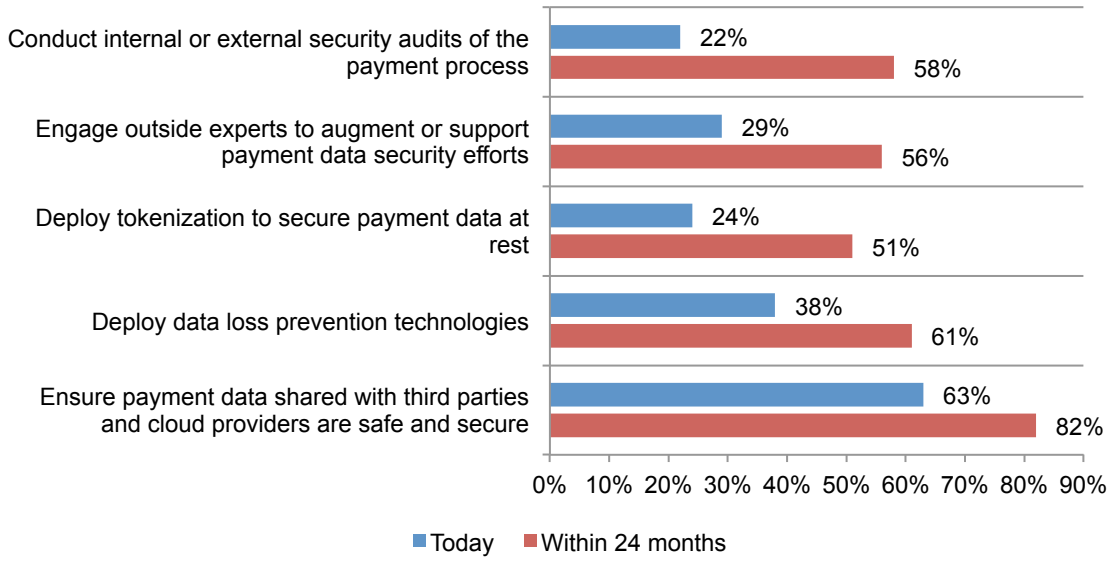
As shown in Figure 14, the greatest increases in ecommerce security will be made in conducting internal or external security audits of the payment process (35 percent increase), deploying data loss prevention technologies (23 percent increase), deploying tokenization to secure payment data at rest (22 percent increase), ensuring payment data shared with third parties and cloud providers are safe and secure (19 percent increase) and engaging outside experts to augment or support payment data security efforts (19 percent).

Figure 14. Steps taken to increase ecommerce security



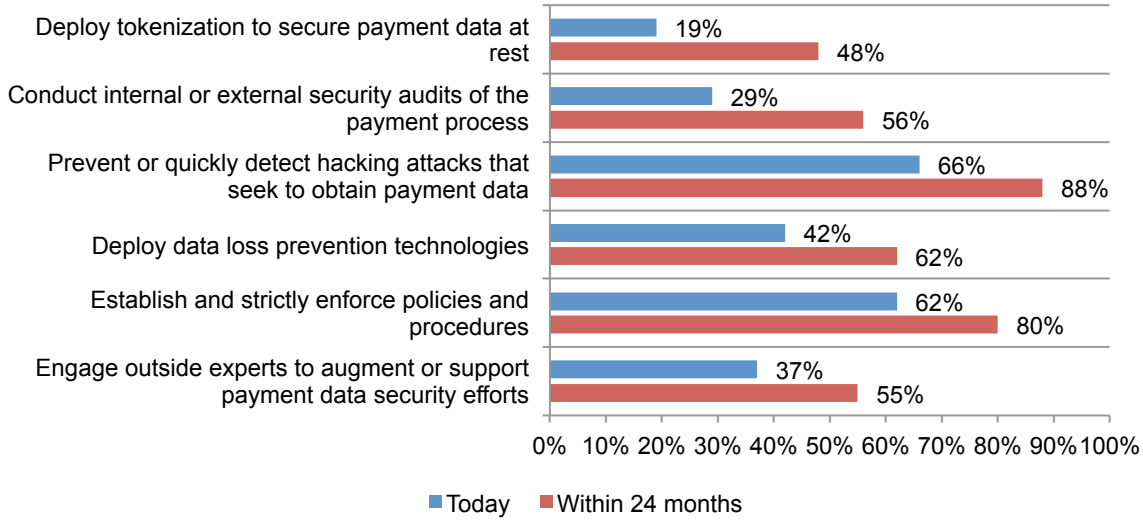
Call centers will see the greatest increases in conducting internal or external security audits of the payment process (36 percent increase), engaging outside experts to augment or support payment data security efforts (27 percent increase), deploying tokenization to secure payment data at rest (27 percent increase), deploying data loss prevention technologies (23 percent increase) and ensuring payment data shared with third parties and cloud providers are safe and secure (19 percent increase), according to Figure 15.

Figure 15. Steps taken to increase call center security



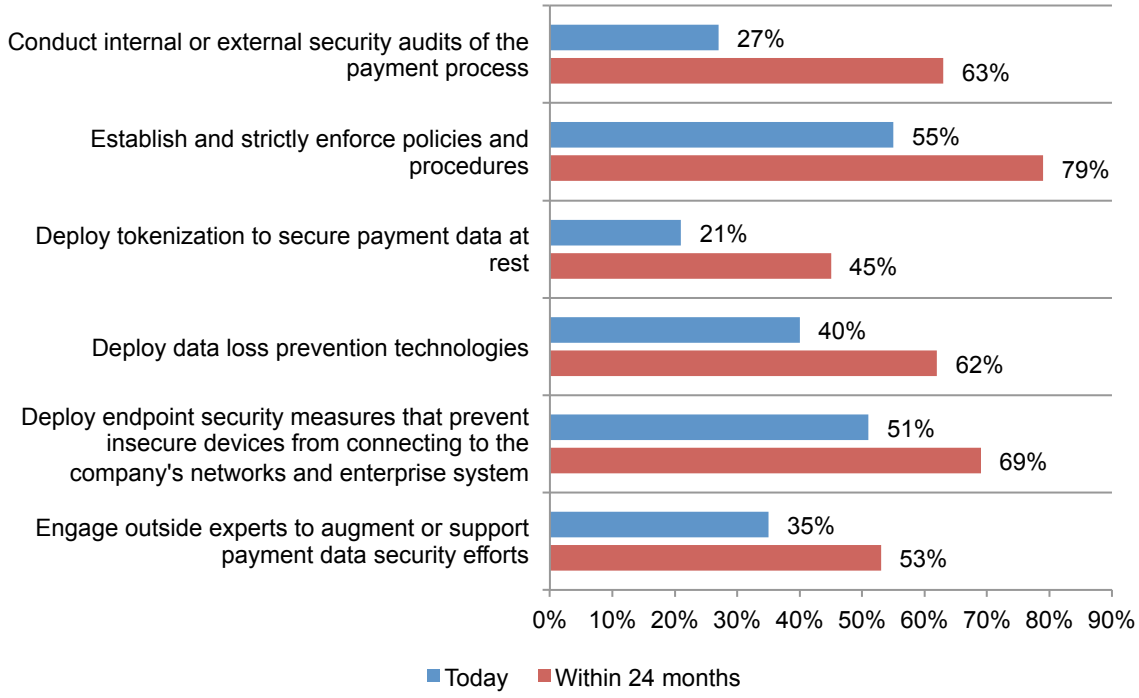
Point of sale channels will see the greatest increases in the following steps: deploying tokenization to secure payment data at rest (29 percent increase), conducting internal or external security audits of the payment process (27 percent increase), preventing or quickly detecting hacking attacks that seek to obtain payment data (22 percent increase), deploying data loss prevention technologies (20 percent increase) and establishing and strictly enforcing policies and procedures (18 percent increase), as shown in Figure 16.

Figure 16. Steps taken to increase point of sale security



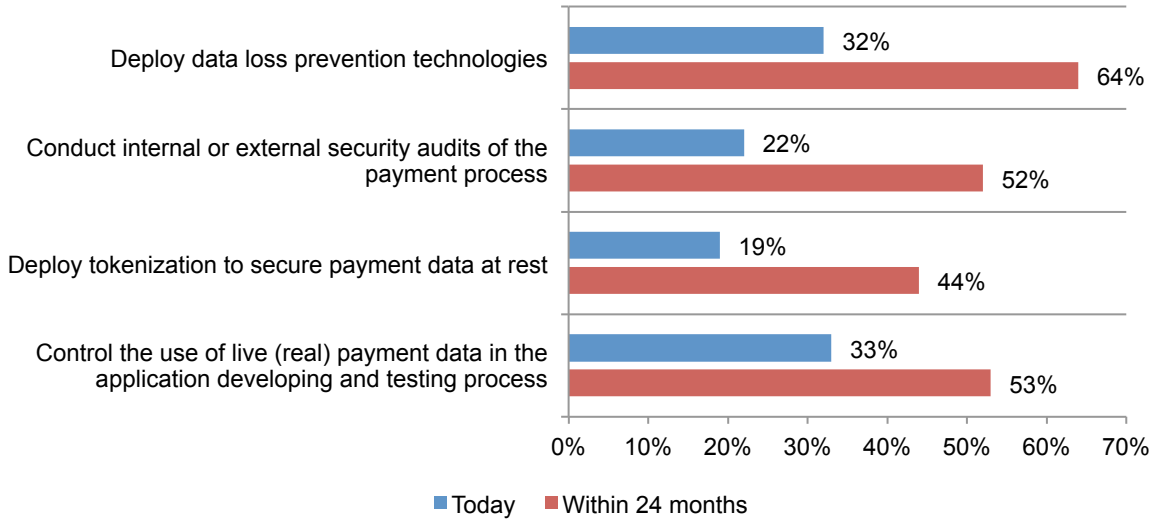
According to Figure 17, mobile payment channels will see the greatest increases in: conducting internal or external security audits of the payment process (36 percent increase), establishing and strictly enforcing policies and procedures (24 percent increase), deploying tokenization to secure payment data at rest (24 percent increase), deploying data loss prevention technologies (22 percent increase), deploying endpoint security measures that prevent insecure devices from connecting to the company's networks and enterprise system (18 percent increase) and engaging outside experts to augment or support payment data security efforts (18 percent increase).

Figure 17. Steps taken to increase mobile payments security



Kiosk channels will see the following steps increasing: deploying data loss prevention technologies (32 percent increase), conducting internal or external security audits of the payment process (30 percent increase), deploying tokenization to secure payment data at rest (25 percent increase) and controlling the use of live (real) payment data in the application developing and testing process (20 percent increase), as shown in Figure 18.

Figure 18. Steps taken to kiosk security



Access governance systems are important to securing the payment process. As mentioned earlier, insiders and hackers pose the greatest threat to payment data and data in storage or at rest is most vulnerable. Accordingly, when asked to select their five most important technologies to securing the payment process directly or indirectly respondents selected the following: access governance systems (44 percent), P2P encryption (41 percent), security intelligence systems including SIEM (39 percent), identity & access management systems (39 percent) and encryption for data at rest (38 percent) (Figure 19).

Figure 19. Most important enabling security technologies
Five choices permitted

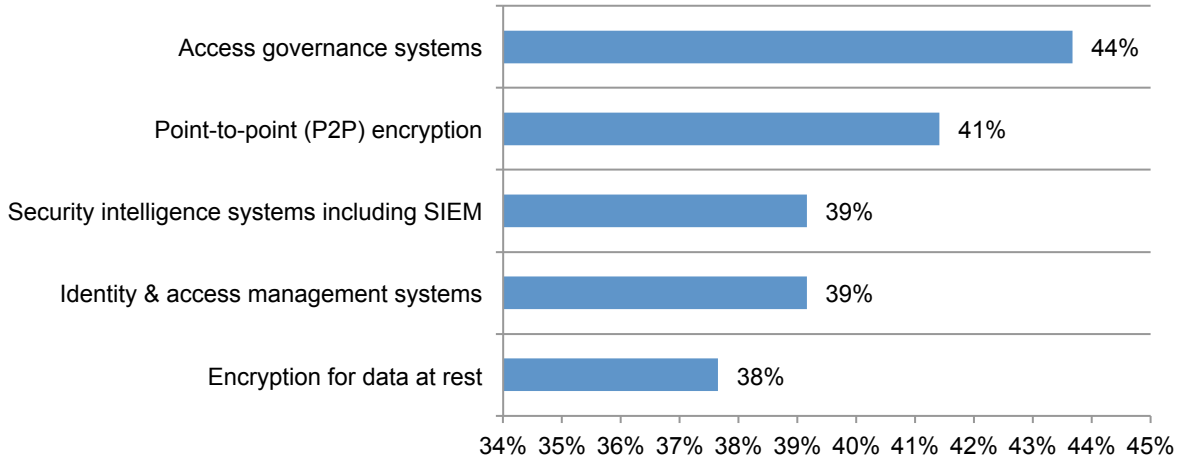
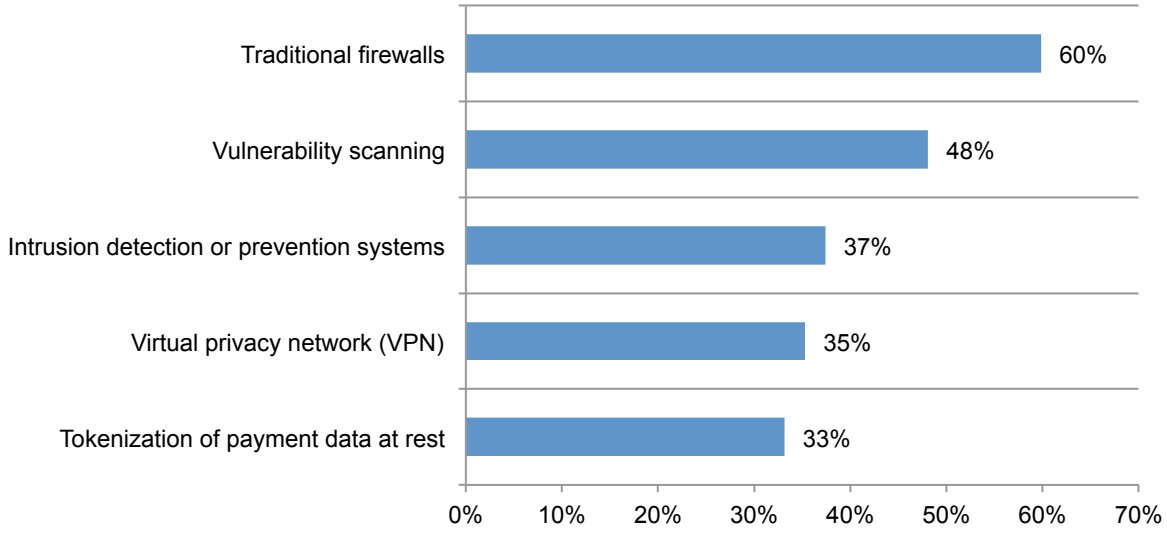


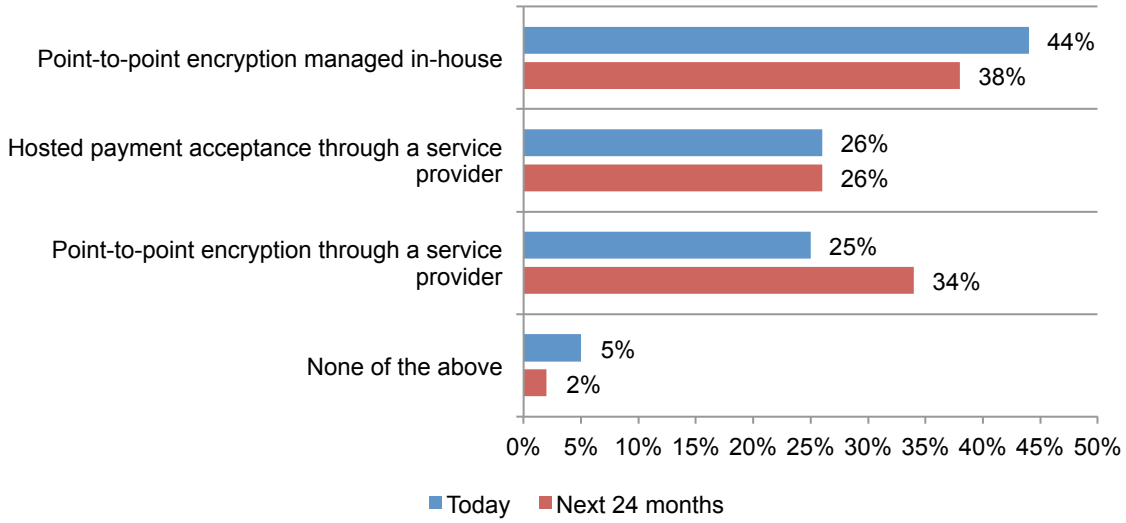
Figure 20 reveals that the following five technologies were selected by respondents as being the least important to ensuring a safe and secure payment process: traditional firewalls (60 percent), vulnerability scanning (48 percent), intrusion detection or prevention systems (37 percent), virtual privacy network (35 percent) and tokenization of payment data at rest (33 percent).

Figure 20. Least important enabling security technologies
Five choices permitted



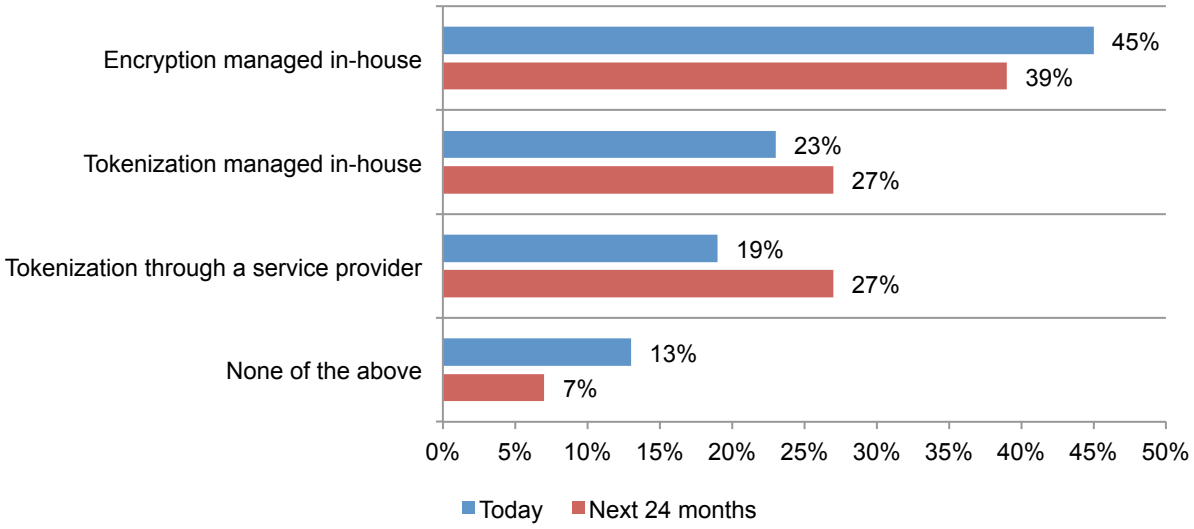
Security strategies for data capture/transmission and storage are changing. The majority (77 percent) of organizations represented in this study do not change their security strategies for capture/transmission and storage according to channel. As shown in Figure 21, the strategy for data capture/transmission is moving from point-to-point encryption managed in-house to point-to-point encryption through a service provider.

Figure 21. Security strategy for data capture/transmission



In the case of data storage, security strategy is moving from encryption managed in-house to tokenization managed in-house and tokenization through a service provider, according to Figure 22.

Figure 22. Security strategy for data storage



Part 3. Conclusion

As revealed in this study, organizations face challenges to reducing the risk to payment data. Many of the respondents in this study agree it is their organizations' inability to prioritize risks and deal with the complexity of technologies that are roadblocks to achieving an effective and efficient secure payment process program. Addressing these challenges is critical because 70 percent of respondents say that attacks on their payment processes are increasing.

We recommend that organizations consider the following actions to protect sensitive information in the payment process:

- Create policies and procedures that state the importance of protecting sensitive information in the payment process.
- Train employees to mitigate the security risk specific to the payment process to make sure sensitive and confidential information is not threatened. This is especially important because respondents ranked negligent insiders as the greatest threat to the security of payment data.
- If appropriate, establish a function dedicated to governance oversight of the payment process.
- Provide customers with the ability to provide feedback about the payment process and have any complaints or concerns promptly addressed.

Based on the findings of this study, it is absolutely possible for merchants to manage security in a way that mitigates risk and reduces operational complexity. In fact, respondents are consistent in what they believe should be done to secure data in all channels. These are: conducting internal or external security audits, deploying data loss prevention technologies, and deploying tokenization to secure payment data at rest. Other factors that lead to better security, based on the practice of high-performing organizations, are C-level support combined with ample resources and budget. They also are more likely to be PCI DSS compliant and less likely to retain and store PAN.

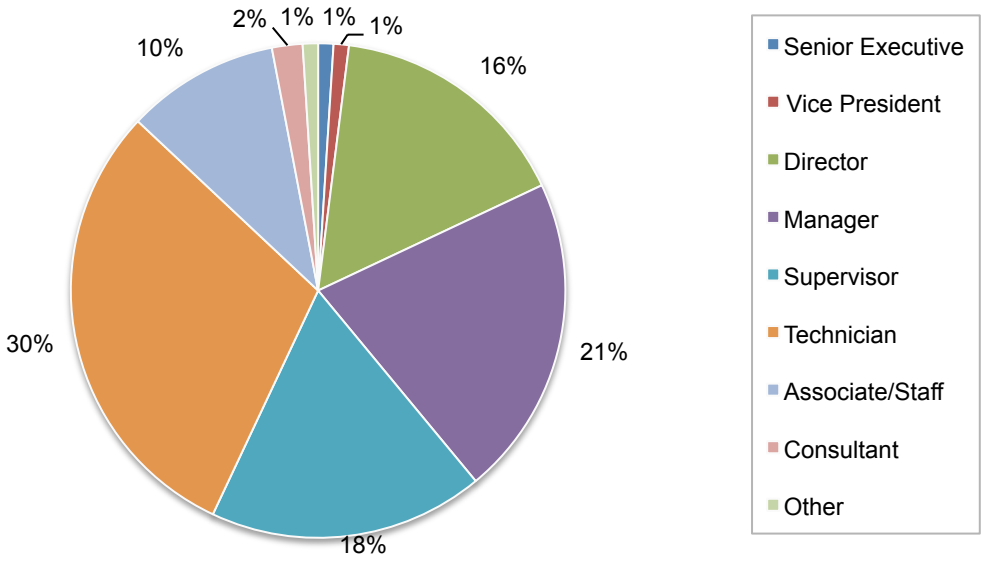
Part 4. Methodology

Table 1 reports the sample frame of 17,898 individuals who have bona fide credentials in IT and IT security. In total, 742 respondents completed the survey. Of the returned instruments, 48 surveys failed reliability checks. A total of 474 surveys were used as our final sample, which represents a 2.6 percent response rate.

Table 1. United States Sample response	Freq.	Pct%
Sampling frame	17,898	100.0%
Total responses	742	4.1%
Screened surveys	220	1.2%
Rejected surveys	48	0.3%
Final sample	474	2.6%

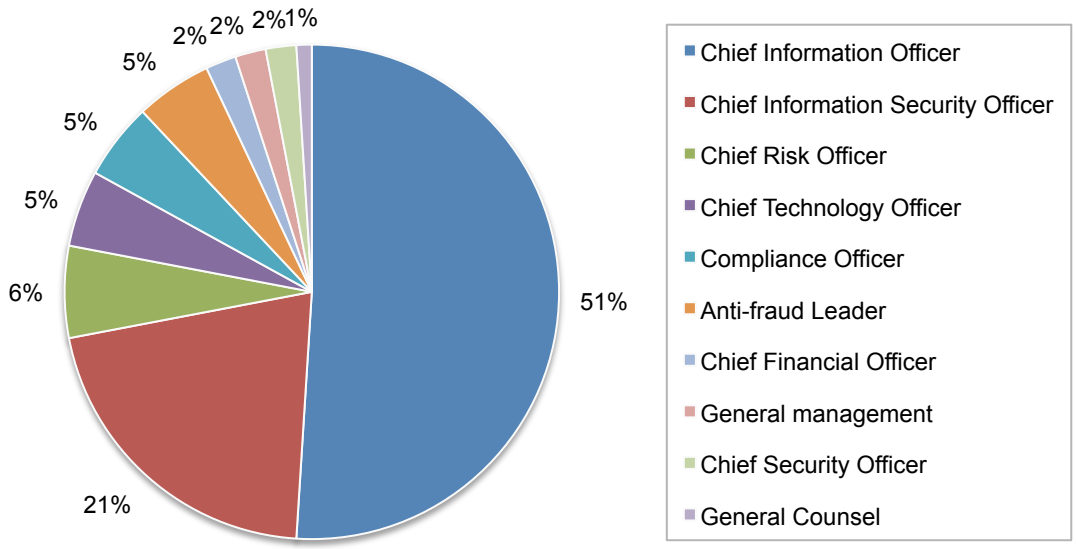
Pie Chart 1 summarizes the approximate position levels of respondents in our study. The majority (57 percent) of respondents are at or above the supervisory level. The average years of business experience is 9.86 years.

Pie Chart 1. Distribution of respondents according to position level



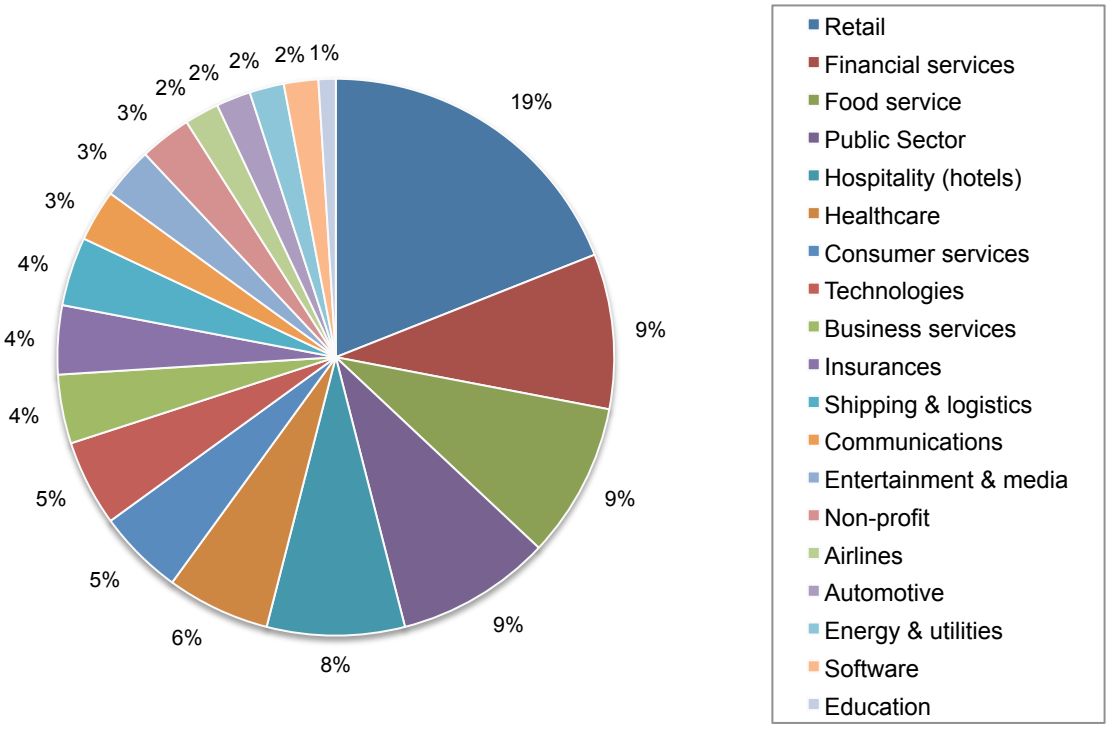
Pie Chart 2 shows that more than half of the respondents (51 percent) report to the Chief Information Officer and 21 percent report to the Chief Information Security Officer.

Pie Chart 2. Distribution of respondents according to position level they report to



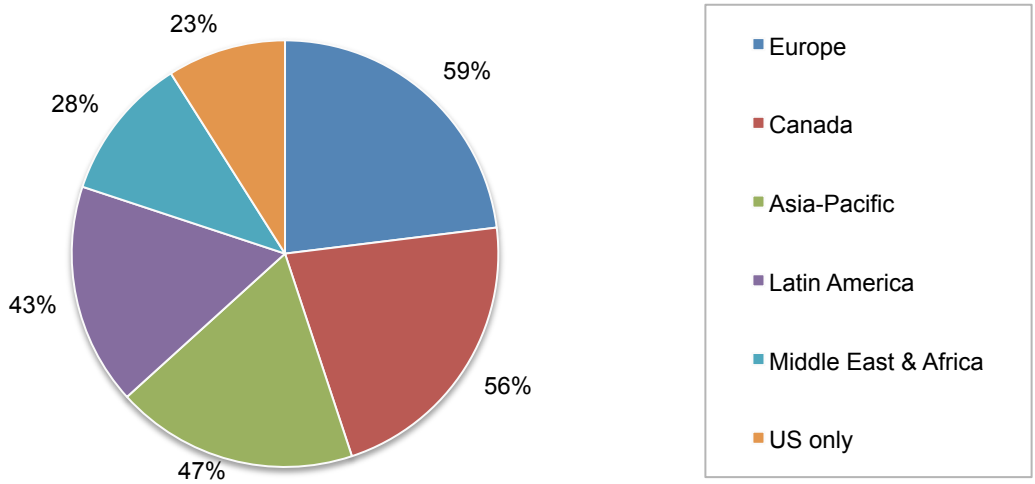
Pie Chart 3 reports the respondents' primary industry segments. Nineteen percent of respondents are in retail and nine percent are in the financial services, which includes banking, investment management, insurance, brokerage, payments and credit cards. Another nine percent are also in the food service sector and public sector organizations, including central and local government.

Pie Chart 3. Distribution of respondents according to primary industry classification



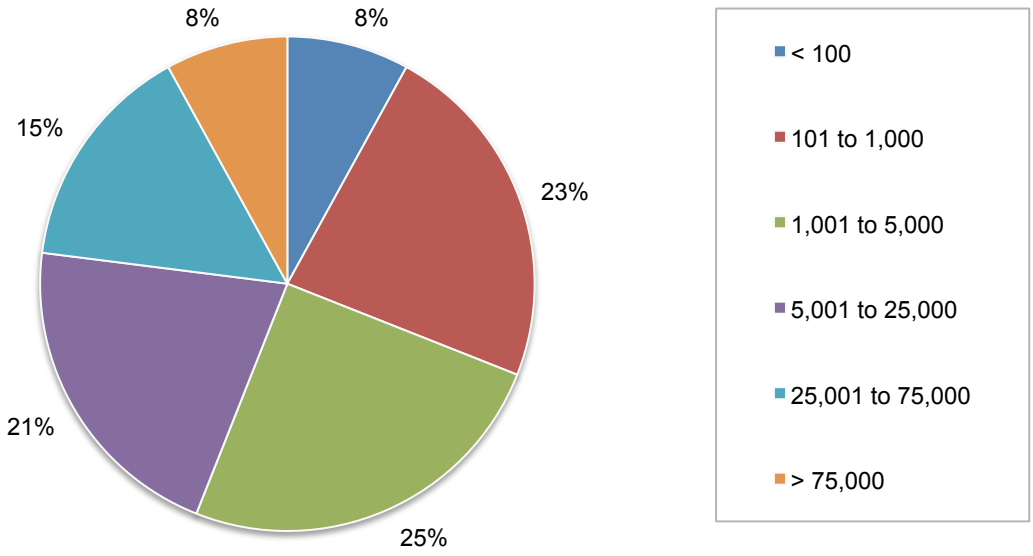
As shown is Pie Chart 4, 59 percent of respondents reported employees located in Europe and 56 percent reported employees are located in Canada.

Pie Chart 4. Location of employees
More than one choice permitted



The majority of respondents (69 percent) are from organizations with a global headcount of over 1,000 employees, as shown in Pie Chart 5.

Pie Chart 5. Global headcount



Part 5. Caveats

There are inherent limitations to survey research that need to be carefully considered before

drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in March and April 2012.

Sample response	Freq	Pct%
Total sample frame	17,898	100%
Total responses	742	4.1%
Screened surveys	220	1.2%
Rejected surveys	48	0.3%
Final sample	474	2.6%

Part 1. Screening.

S1. Are you involved in your organization's payment security process including compliance efforts with PCI DSS?	Freq	Pct%
Yes	611	88%
No STOP	83	12%
Total	694	100%

S2. What function in your organization is most responsible for payment security? Please choose only one.	Freq	Pct%
Legal	27	4%
Compliance	24	4%
Finance	89	15%
Operations	200	33%
Information Technology (IT)	97	16%
Shared responsibility among two or more functions (please specify these functions)	127	21%
Other (please specify)	11	2%
Unsure STOP	36	6%
Total	611	100%

S3. The PCI Security Standards Council has defined four organizational levels based on the volume of credit, debit or prepaid card transactions on an annual basis. What Level best describes your organization?	Freq	Pct%
Level 1 Merchant – more than 6 million transactions from all channels annually	259	45%
Level 2 Merchant – between 1 and 6 million transactions from all channels annually	215	37%
Level 3 Merchant – between 20,000 to 1 million transactions from all channels annually STOP	35	6%
Level 4 Merchant – less than 20,000 transactions from all channels annually STOP	27	5%
PCI Level is not specified STOP	21	4%
Level 1 or 2 Service Provider STOP	18	3%
Total	575	100%

Final sample used in the following questions	474

Block allocations by channel for Q6 and Q15	Freq	Pct%
Ecommerce	178	38%
Call center	116	24%
Point of sale	95	20%
Mobile	53	11%
Kiosk	32	7%
Total	474	100%

Part 2. Attributions. Please rate each one of the following six statements using the scale provided below each item. Strongly agree and agree response.	Strongly agree	Agree
Q1a. My organization has sufficient resources to achieve a secure payment process.	18%	30%
Q1b. My organization has ample security technologies to secure the payment process.	16%	25%
Q1c. My organization has knowledgeable or expert staff dedicated to securing the payment process.	21%	30%
Q1d. My organization's C-level executives view a secure payment process as a core business objective.	22%	31%
	Strongly agree	Agree
Q1e. A data breach would impact my organization's reputation, marketplace image and brand value.	32%	34%
Q1f. A data breach would diminish customer trust and confidence in my organization.	33%	35%

Part 3. General Questions

Q2. Within the table provided below, please allocate 100 points to approximate the distribution of payment data captured by your organization in the following five sales channels: online, call center, point of sale, mobile and Kiosk. Note that the total points allocated must sum to 100.	Allocated points
Ecommerce	37
Call center	22
Point of sale	23
Mobile	12
Kiosk	6
Total points	100

Q3a. At present, is your organization compliant with PCI DSS requirements?	Pct%
Yes, for all applications and databases across the enterprise [Go to Q4]	28%
Yes, for most applications and databases [Go to Q4]	42%
Yes, but only for some applications and databases	30%
No	100%

Q3b. How long will it take your organization to achieve substantial compliance with PCI DSS requirements?	Pct%
Less than 1 month	13%
Between 1 and 3 months	26%
Between 3 and 6 months	28%
Between 6 and 12 months	15%
More than 1 year	18%
Total	100%

Q4. Did your organization ever fail a PCI DSS audit or assessment?	Pct%
Yes	15%
No	85%
Total	100%

Q5. Does your organization use a PCI DSS certified service contractor to help it achieve compliance requirements?	Pct%
Yes, we presently use a PCI DSS certified service contractor	30%
No, but we plan to use a PCI DSS certified service contractor within the next 12 months	17%
No, but we have employees who are PCI DSS certified	21%
No	32%
Total	100%

Q6. How difficult or "challenging" is the deployment of the following controls to ensure a safe and secure payment process within your organization? For the **one channel** assigned, please rate each control using the following four-point scale provided below each control from very difficult to deploy to the stated control is not deployed at present.

Q6a, Maintain a firewall configuration to protect confidential payment data and related applications	Very difficult	Difficult
Ecommerce	19%	22%
Call center	25%	29%
Point of sale	31%	33%
Mobile	35%	37%
Kiosk	23%	25%
Average	27%	29%

Q6b. Encrypt payment data during its transmission across open, public networks	Very difficult	Difficult
Ecommerce	17%	23%
Call center	15%	22%
Point of sale	20%	22%
Mobile	22%	19%
Kiosk	20%	24%
Average	19%	22%

Q6c. Encrypt payment data stored (at rest)	Very difficult	Difficult
Ecommerce	18%	21%
Call center	21%	22%
Point of sale	31%	24%
Mobile	29%	21%
Kiosk	17%	23%
Average	23%	22%

Q6d. Tokenize to obscure confidential data	Very difficult	Difficult
Ecommerce	19%	20%
Call center	25%	26%
Point of sale	27%	29%
Mobile	28%	23%
Kiosk	17%	21%
Average	23%	24%

Q6e. Use and regularly update anti-virus software	Very difficult	Difficult
Ecommerce	18%	17%
Call center	15%	18%
Point of sale	18%	19%
Mobile	20%	21%
Kiosk	18%	21%
Average	18%	19%

Q6f. Maintain secure payment applications	Very difficult	Difficult
Ecommerce	20%	21%
Call center	19%	25%
Point of sale	29%	26%
Mobile	33%	25%
Kiosk	20%	23%
Average	24%	24%

Q6g. Restrict access to payment data on a need-to-know basis	Very difficult	Difficult
Ecommerce	18%	23%
Call center	17%	24%
Point of sale	28%	31%
Mobile	20%	23%
Kiosk	26%	28%
Average	22%	26%

Q6h. Limit physical access to payment data	Very difficult	Difficult
Ecommerce	21%	22%
Call center	21%	20%
Point of sale	32%	31%
Mobile	17%	21%
Kiosk	21%	22%
Average	22%	23%

Q6i. Monitor access to network resources	Very difficult	Difficult
Ecommerce	16%	24%
Call center	19%	22%
Point of sale	20%	17%
Mobile	17%	24%
Kiosk	17%	22%
Average	18%	22%

Q6j. Test payment security applications and processes	Very difficult	Difficult
Ecommerce	19%	19%
Call center	19%	23%
Point of sale	18%	19%
Mobile	31%	34%
Kiosk	20%	25%
Average	21%	24%

Q6k. Maintain policies that address the security of the payment process	Very difficult	Difficult
Ecommerce	11%	15%
Call center	11%	13%
Point of sale	13%	16%
Mobile	15%	20%
Kiosk	16%	23%
Average	13%	17%

Q7. How many data breaches has your organization experienced involving the loss or theft of credit card, debit card or other customer payment data during the past 24 months?	Pct%
None (Go to Q9)	9%
Only 1 incident	23%
Between 2 to 5 incidents	31%
Between 6 to 10 incidents	13%
Between 11 to 15 incidents	5%
Between 16 to 20 incidents	3%
More than 20 incidents	1%
No comment (Go to Q9)	15%
Total	100%
Extrapolated number of data breach incidents	4.4

Q8. In your opinion, did security practices improve after these data breaches were experienced by your organization?	Pct%
Yes, a significant improvement	25%
Yes, but only nominal improvement	41%
No improvement	25%
Unsure	9%
Total	100%

Q9. With respect to security risk, where are serious threats to payment data located? Within the table provided below, please allocate 100 points to approximate the distribution of overall security risk in the following four phases in the payment data life cycle. Note that the total points allocated must sum to 100.	Allocated points
Data capture	28
Data transmission	18
Back-office activities	14
Data storage	40
Total points	100

Q10. With respect to the security of payment data, where do you see the greatest threats? Please rank order the following six choices, where 6 = the most serious threat to 1 = the least serious threat.	Average rank	Rank order
Negligent insiders	4.38	6 = most
Malicious insiders	2.64	3
Hackers/cyber criminals	3.85	5
Hardware or software glitches	3.19	4
Third-party mistakes	1.95	1 = least
Lost or stolen computing devices	2.43	2
Average	3.07	

Q11. With respect to the security of payment data, which back-office activity poses the greatest risk of data loss or theft? Please rank order the following five choices, where 5 = the most risky back-office activity to 1 = the least risky back-office activity.	Average rank	Rank order
Order review/fraud management	2.59	3
Accounting	4.21	5 = most
Customer services	3.17	4
Fulfillment	2.37	2
Chargeback management	1.96	1 = least
Total	2.86	

	Strongly agree	Agree
Q12a. Attribute (strongly agree and agree rating): “Minimizing employees’ interaction with raw payment data creates a more secure payment environment.”	40%	36%
Q12b. Attribute (strongly agree and agree rating): “Populating customer records with a payment token reduces the exposure of payment data, thereby creating a more secure payment environment.”	28%	33%

Q13. Please choose one statement that best describes the frequency and severity of attacks that impact the security of your organization’s secure payment processes.	Pct%
Attacks are increasing in both frequency and severity	31%
Attacks are increasing in frequency, not severity	13%
Attacks are increasing in severity, not frequency	27%
Attacks are not increasing	29%
Total	100%

Q14a. Does your organization retain and store PAN?	Pct%
Yes	73%
No (Go to Q15)	27%
Total	100%

Q14b. If yes, why does your organization retain and store PAN? Please select the top two business reasons.	Pct%
Recurring subscriptions	46%
Managing fraud screening and chargeback	49%
Customer service	52%
Marketing analytics	15%
Make the checkout process easier for consumers	12%
Other (please specify)	3%
Total	177%

	Strongly agree	Agree
Q14c. Attribution (strongly agree and agree rating): "To reduce the impact of a breach, it is a good idea to centralize the organization's payment data and substitute PAN with payment tokens."	25%	32%

Q15. What steps is your organization taking to secure the storage of payment data and minimize back office exposure? For the **one channel** assigned, please check if your organization is doing it today or plans to do it within the next 24 months. Leave blank if your organization has no plans to do this step.

Ecommerce: Steps taken to secure payment data	Today	Within 24 months
Conduct data inventory to identify the location of payment data	20%	24%
Implement a payment data classification scheme	31%	33%
Conduct training and awareness activities for all employees and contractors that access payment data	28%	32%
Deploy encryption to secure payment data at rest	43%	46%
Deploy tokenization to secure payment data at rest	23%	45%
Deploy data masking or other suppression to secure payment data at rest	13%	19%
Deploy endpoint security measures that prevent insecure devices from connecting to the company's networks and enterprise system	52%	68%
Identify and authenticate all end users before granting them access to payment data	76%	82%
Ensure payment data shared with third parties and cloud providers are safe and secure	63%	82%
Ensure storage devices including routers and servers containing payment data are properly secured	65%	78%
Prevent or quickly detect hacking attacks that seek to obtain payment data	67%	83%
Control the use of live (real) payment data in the application developing and testing process	34%	50%
Establish and strictly enforce policies and procedures	62%	78%
Conduct internal or external security audits of the payment process	23%	58%
Engage outside experts to augment or support payment data security efforts	35%	54%
Deploy data loss prevention technologies	38%	61%
Deploy application security measures including the use of web application firewalls	58%	62%

Call center: Steps taken to secure payment data	Today	Within 24 months
Conduct data inventory to identify the location of payment data	17%	22%
Implement a payment data classification scheme	30%	35%
Conduct training and awareness activities for all employees and contractors that access payment data	28%	33%
Deploy encryption to secure payment data at rest	43%	46%
Deploy tokenization to secure payment data at rest	24%	51%
Deploy data masking or other suppression to secure payment data at rest	10%	21%
Deploy endpoint security measures that prevent insecure devices from connecting to the company's networks and enterprise system	51%	65%
Identify and authenticate all end users before granting them access to payment data	74%	86%
Ensure payment data shared with third parties and cloud providers are safe and secure	63%	82%
Ensure storage devices including routers and servers containing payment data are properly secured	64%	80%
Prevent or quickly detect hacking attacks that seek to obtain payment data	65%	83%
Control the use of live (real) payment data in the application developing and testing process	39%	55%
Establish and strictly enforce policies and procedures	60%	75%
Conduct internal or external security audits of the payment process	22%	58%
Engage outside experts to augment or support payment data security efforts	29%	56%
Deploy data loss prevention technologies	38%	61%
Deploy application security measures including the use of web application firewalls	62%	65%

Point of sale: Steps taken to secure payment data	Today	Within 24 months
Conduct data inventory to identify the location of payment data	20%	23%
Implement a payment data classification scheme	30%	33%
Conduct training and awareness activities for all employees and contractors that access payment data	28%	29%
Deploy encryption to secure payment data at rest	40%	47%
Deploy tokenization to secure payment data at rest	19%	48%
Deploy data masking or other suppression to secure payment data at rest	16%	19%
Deploy endpoint security measures that prevent insecure devices from connecting to the company's networks and enterprise system	52%	68%
Identify and authenticate all end users before granting them access to payment data	80%	79%
Ensure payment data shared with third parties and cloud providers are safe and secure	64%	80%
Ensure storage devices including routers and servers containing payment data are properly secured	70%	77%
Prevent or quickly detect hacking attacks that seek to obtain payment data	66%	88%
Control the use of live (real) payment data in the application developing and testing process	40%	49%
Establish and strictly enforce policies and procedures	62%	80%
Conduct internal or external security audits of the payment process	29%	56%
Engage outside experts to augment or support payment data security efforts	37%	55%
Deploy data loss prevention technologies	42%	62%
Deploy application security measures including the use of web application firewalls	54%	57%

Mobile: Steps taken to secure payment data	Today	Within 24 months
Conduct data inventory to identify the location of payment data	16%	27%
Implement a payment data classification scheme	30%	30%
Conduct training and awareness activities for all employees and contractors that access payment data	27%	34%
Deploy encryption to secure payment data at rest	42%	47%
Deploy tokenization to secure payment data at rest	21%	45%
Deploy data masking or other suppression to secure payment data at rest	14%	19%
Deploy endpoint security measures that prevent insecure devices from connecting to the company's networks and enterprise system	51%	69%
Identify and authenticate all end users before granting them access to payment data	78%	88%
Ensure payment data shared with third parties and cloud providers are safe and secure	66%	80%
Ensure storage devices including routers and servers containing payment data are properly secured	66%	80%
Prevent or quickly detect hacking attacks that seek to obtain payment data	69%	83%
Control the use of live (real) payment data in the application developing and testing process	38%	54%
Establish and strictly enforce policies and procedures	55%	79%
Conduct internal or external security audits of the payment process	27%	63%
Engage outside experts to augment or support payment data security efforts	35%	53%
Deploy data loss prevention technologies	40%	62%
Deploy application security measures including the use of web application firewalls	54%	61%

Kiosk: Steps taken to secure payment data	Today	Within 24 months
Conduct data inventory to identify the location of payment data	15%	20%
Implement a payment data classification scheme	23%	30%
Conduct training and awareness activities for all employees and contractors that access payment data	26%	34%
Deploy encryption to secure payment data at rest	40%	42%
Deploy tokenization to secure payment data at rest	19%	44%
Deploy data masking or other suppression to secure payment data at rest	15%	23%
Deploy endpoint security measures that prevent insecure devices from connecting to the company's networks and enterprise system	52%	68%
Identify and authenticate all end users before granting them access to payment data	76%	81%
Ensure payment data shared with third parties and cloud providers are safe and secure	62%	82%
Ensure storage devices including routers and servers containing payment data are properly secured	70%	74%
Prevent or quickly detect hacking attacks that seek to obtain payment data	68%	82%
Control the use of live (real) payment data in the application developing and testing process	33%	53%
Establish and strictly enforce policies and procedures	63%	74%
Conduct internal or external security audits of the payment process	22%	52%
Engage outside experts to augment or support payment data security efforts	39%	56%
Deploy data loss prevention technologies	32%	64%
Deploy application security measures including the use of web application firewalls	61%	64%

Q16. Following are 21 enabling security technologies that may be used by your organization to secure the payment process either directly (in-house) or with the assistance of a hosted (third party) solution. Please select no more than five (5) technologies that you perceive as most useful in achieving a safe and secure payments process. Then, select no more than five (5) technologies that your organization perceives as least useful in achieving a safe and secure payments process.	Most important	Least important
Application testing (including mobile apps)	11%	25%
Hosted payment page	10%	16%
Access governance systems	44%	2%
Anti-virus & anti-malware solution	9%	12%
Configuration and log management	11%	26%
Data loss prevention systems	18%	10%
Database scanning and monitoring	12%	25%
Encryption for data at rest	38%	14%
Encryption for data in motion	37%	27%
Point-to-point (P2P) encryption	41%	5%
Tokenization of payment data at rest	32%	33%
Traditional firewalls	9%	60%
Next generation firewalls	18%	25%
Web application firewalls	22%	19%
ID & credentialing system	7%	20%
Identity & access management systems	39%	6%
Intrusion detection or prevention systems	14%	37%
Security intelligence systems including SIEM	39%	28%
Virtual privacy network (VPN)	38%	35%
Vulnerability scanning	21%	48%
Endpoint security management	30%	28%
Total	500%	500%

Part 4. Budget

Q17. What dollar range best defines your organization's security budget in the present fiscal year? In the context of the security budget, please include all technologies, staffing and service costs incurred by your organization to secure information assets, protect the IT infrastructure, and prevent fraud.	Pct%
Less than $1 million	15%
Between $1 to 2 million	17%
Between $2 to $4 million	18%
Between $4 to $6 million	21%
Between $6 to $8 million	12%
Between $8 to $10 million	8%
Between $10 to $12 million	4%
Between $12 to $14 million	2%
Between $14 to $16 million	1%
Between $16 to $18 million	0%
Between $18 to $20 million	0%
Over $20 million	2%
Total	100%
Extrapolated value (million dollars)	$4.81

Q18. How will be security budget for your organization change in 24 months? Your best guess is welcome.	Pct%
Budget decrease	
More than 20%	0%
Between 16% and 20%	4%
Between 11% and 15%	2%
Between 6% and 10%	1%
Between 1% and 5%	1%
No change expected	41%
Budget increase	
More than 20%	1%
Between 16% and 20%	2%
Between 11% and 15%	10%
Between 6% and 10%	13%
Between 1% and 5%	25%
Total	100%

Approximately, what percentage of your organization's security budget is dedicated to the following activities in the **current year**? Your best guess is welcome.	
Q19a. Security technology/services	Pct%
< 5%	0%
5 to 10%	3%
11 to 20%	7%
21 to 30%	24%
31 to 40%	25%
41 to 50%	26%
> 50%	15%
Total	100%

Q19b. PCI certification/validation	Pct%
< 5%	0%
5 to 10%	16%
11 to 20%	21%
21 to 30%	26%
31 to 40%	21%
41 to 50%	8%
> 50%	8%
Total	100%

Q19c. Staff devoted to IT security	Pct%
< 5%	0%
5 to 10%	5%
11 to 20%	13%
21 to 30%	45%
31 to 40%	16%
41 to 50%	15%
> 50%	6%
Total	100%

Q19d. Engaging auditors and outside consultants (beyond that required for PCI DSS certification	Pct%
< 5%	10%
5 to 10%	35%
11 to 20%	41%
21 to 30%	9%
31 to 40%	5%
41 to 50%	0%
> 50%	0%
Total	100%

Q20. On a full-time equivalent basis, approximately how many staff members are dedicated to your organization's current payment security process?	Pct%
Less than 1 employee	19%
Between 1 to 5 employees	28%
Between 6 to 10 employees	29%
Between 11 to 15 employees	17%
Between 16 to 20 employees	6%
More than 20 employees	1%
Total	100%
Extrapolated value (FTE headcount)	6.8

Q21a. What best describes your organization's security strategy for data capture/transmission and data storage? Please choose one option for today and in the next 24 months for each table.		
Capture/transmission	Today	Next 24 months
Point-to-point encryption managed in-house	44%	38%
Point-to-point encryption through a service provider	25%	34%
Hosted payment acceptance through a service provider	26%	26%
None of the above	5%	2%

Storage	Today	Next 24 months
Encryption managed in-house	45%	39%
Tokenization managed in-house	23%	27%
Tokenization through a service provider	19%	27%
None of the above	13%	7%

Q21b. Does your organization's security strategy outlined above change by channel?	Pct%
Yes	23%
No	77%
Total	100%

Q21c. If yes, why? Please explain.	Contextual

Q22. In your opinion, what is the primary purpose of payment security compliance efforts such as PCI DSS and other related initiatives? Please choose the one statement you believe to be true about compliance.	Pct%
Not essential	3%
Only “CYA”	12%
Helps achieve consistent security practices across the enterprise	14%
Obtains buy-in from management	16%
Secures security budget and funding	33%
Prioritizes security requirements	6%
Helps achieve a strong security posture	6%
Preserves customer trust	5%
Protects the organization’s reputation	5%
Other (please specify)	0%
Total	100%

Q23. In your opinion, what are the main barriers to achieving a high level of security in the payments process within your organization? Please select your top two choices.	Pct%
Lack of resources	43%
Lack of knowledgeable or expert staff	26%
Lack of enabling and managing security technologies	11%
Lack of organizational leadership	19%
The complexity of regulations	5%
The complexity of enabling security technologies	30%
Ability to assess and prioritize risks	43%
Internal buy-in and sponsorship	13%
Other (please specify)	0%
Total	190%

Part 5. Your role

D1. What organizational level best describes your current position?	Pct%
Senior Executive	1%
Vice President	1%
Director	16%
Manager	21%
Supervisor	18%
Technician	30%
Associate/Staff	10%
Consultant	2%
Other	1%
Total	100%

D2. Check the **Primary Person** your IT security leader reports to within the organization.	Pct%
CEO/Executive Committee	0%
Chief Financial Officer	2%
General management	2%
General Counsel	1%
Chief Information Officer	51%
Chief Technology Officer	5%
Chief Information Security Officer	21%
Compliance Officer	5%
Human Resources Leader	0%
Chief Security Officer	2%
Chief Risk Officer	6%
Anti-fraud Leader	5%
Other	0%
Total	100%

D3. Total years of business experience	Mean	Median
Total years dealing with customer payments, cyber security and/or fraud prevention	9.86	10.00
Total years in current job	4.89	5.00

D4. What industry best describes your organization's industry focus? Please check only one.	Pct%
Airlines	2%
Automotive	2%
Business services	4%
Communications	3%
Consumer services	5%
Education	1%
Energy & utilities	2%
Entertainment & media	3%
Financial services	9%
Food service	9%
Healthcare	6%
Hospitality (hotels)	8%
Insurances	4%
Non-profit	3%
Public Sector	9%
Retail	19%
Shipping & logistics	4%
Software	2%
Technologies	5%
Other	0%
Total	100%

D5. Where are your employees located? (Please check all that apply):	Pct%
US only	23%
Canada	56%
Europe	59%
Middle East & Africa	28%
Asia-Pacific	47%
Latin America	43%

D6. What is the worldwide headcount of your organization?	Pct%
< 100	8%
101 to 1,000	23%
1,001 to 5,000	25%
5,001 to 25,000	21%
25,001 to 75,000	15%
> 75,000	8%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**,we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.