Secure Payment Survey

Executive Summary

Contending with Current Challenges and Capitalising on the Opportunities
Overview

Considering the massive scale and cost of payment system breaches that have made headlines in recent months, it is clear that—if there were ever a time to take short cuts or do the bare minimum in securing sensitive payment data—this is not it. While the need to secure payment transactions and data remains critical, it doesn't seem to be getting easier. Security teams have to contend with increasingly sophisticated attacks, as well as with lean staff and budgets and a technological environment that is evolving rapidly.

How are security teams faring as they navigate these changing dynamics and escalating demands? SafeNet recently conducted a survey on these topics. This executive summary reveals the key findings from this survey, highlighting how approaches and environments are evolving. In addition, this document features some insights into opportunities for overcoming some of the most significant challenges.

Compliance: A Massive Effort for Many

Of the total survey group, which included respondents from across industries, about one-third spend more than six weeks a year complying with card schemes’ regulations. Of those who say their organisations are concerned with Payment Card Industry (PCI) standards, the numbers rise to 50%. Of that same group, the same percentage, 50%, also spend more than six weeks complying with financial services regulations every year.

In other words, if your organisation is concerned with PCI standards, there's a 50/50 chance your organisation has staff spending 12 weeks, one-quarter of every year, on card schemes and financial services regulations.

**Key Takeaways**

These statistics speak to the rigor of these regulatory standards, and they also highlight that, whether leadership teams feel compelled by obligations or threatened by fines for non-compliance, these requirements are being taken seriously. It also seems clear that the efforts associated with compliance are overwhelming existing staff.

**The three-month compliance hit.** Of those concerned with PCI standards, more than half spend six weeks complying with card schemes regulations, and six weeks complying with financial services regulations.
Mass migration. Almost three-quarters of respondents are planning to increase their usage of virtualisation and the cloud—but security questions remain.

Security Demands Intensified by Cloud and Virtualisation

Virtualisation technologies and cloud services are growing increasingly intertwined in the technological and operational fabric of the vast majority of respondent organisations. In the next year, 73% plan to increase their usage of virtualisation or cloud technologies. When asked about their concerns surrounding this continued move to virtualised and cloud environments, by far the most consistently cited category was security, which was named by more than one-third of respondents.

73% plan to increase usage of virtualisation and cloud.

Key Takeaways

While it’s clear that there’s no stopping the adoption of virtualisation and cloud approaches, it is also clear that many continue to grapple with significant security questions and challenges as a result of this move. New computing models and services are creating the need for new security approaches and technologies, even while so many security teams are struggling to keep pace with existing demands and compliance obligations. If existing compliance and security demands can be said to be lighting a fire under security teams, these added demands introduced by virtualisation and cloud models are clearly adding fuel to the blaze.
Advantageous Encryption Alternatives
Untapped by Many

Our survey examined usage of two specific types of encryption alternatives, point-to-point encryption (P2PE) and format preserving encryption (FPE) (see the sidebar for a brief description of each). Overall, 24% of respondents are currently implementing P2PE solutions. Of those who say their organisations are concerned with P2PE, a little over half, 56%, are currently deploying a P2PE-compliant solution.

49% of respondents indicated they were not aware of FPE and another 32% said they were aware of the approach, but had no plans to use it. Only 19% of respondents indicated they were using FPE or had plans to do so.

**Key Takeaways**

P2PE and FPE represent significant opportunities that many organisations have failed to capitalise on. By leveraging P2PE or FPE, organisations can address compliance mandates, while reducing the associated workload. Through P2PE, organisations can take entire groups or even the entire business in some cases, out of the scope of PCI compliance. With FPE, organisations can leverage the security benefits of encryption, while streamlining implementation efforts.

**24% currently implementing P2PE.**

**19% using or plan to use FPE.**

**Opportunity untapped?**

In spite of the benefits P2PE and FPE provide, a significant percentage of organisations have yet to capitalise on these approaches.
Key Management: Key to Success

In recent years, many organisations have grown increasingly reliant on encryption, expanding the number and scale of their implementations. What many find is that, in the wake of this continued usage and growth, key management responsibilities continue to present an increasing burden—one that many security teams are poorly equipped to support.

Currently, many teams responsible for key management are small and distributed, which is a significant contributor to many organisations’ heavy compliance workloads. Overall, two-thirds have four or less people involved in key management, and only 39% have the staff members responsible for managing keys located in the same office.

Key Takeaways

Approaches and tools for key management can have a huge impact, not only on security, but on the amount of administrative effort required. To succeed in meeting their administrative demands and their security objectives, it is incumbent upon security teams to begin to leverage more centralised, efficient, and secure key management platforms.

Encryption Alternatives

Following are brief descriptions of two encryption alternatives the survey examined:

• Format preserving encryption (FPE). Generally, encryption alters the nature of the data being encrypted. For example, if a 16-digit credit card number is encrypted, it may be converted into a much longer string of alpha-numeric text. FPE is a form of encryption in which, if a 16-digit credit card number is encrypted, the resulting output (known as ciphertext) would also be a 16-digit number. As a result, FPE can provide many of the benefits of encryption, while minimising implementation implications.

• Point-to-point encryption (P2PE). When P2PE is employed, payment details are encrypted at the earliest point possible, generally upon the initial swipe of a payment card, until they are needed for payment clearance, often at an acquirer’s or processor’s facilities. Through these approaches, retailers can significantly strengthen security of payment details, and reduce their compliance efforts.

Two-thirds have 4 or less people doing key management.

Equipped to scale or fail?

Two-thirds of respondents have four or less people doing key management in their organisation, and 60% don’t have staff managing keys in the same office.
Conclusion

For the security teams tasked with safeguarding payment data, demands for encryption and key management are only increasing, both in scale and urgency. These realities continue to place an increased emphasis on efficiency, which means leveraging approaches like centralised key management, P2PE, and FPE will be more critical than ever.

About the Survey

This paper draws from an extensive survey conducted toward the end of 2013 and early in 2014. More than 300 individuals offered their perspectives. Participants came from many countries across the EMEA region as well as North America. Respondents also came from a number of market sectors, including financial services, business and technology consulting, manufacturing and retail.

About SafeNet

Founded in 1983, SafeNet, Inc. is one of the largest information security companies in the world, and is trusted to protect the most sensitive data for market-leading organizations around the globe. SafeNet’s data-centric approach focuses on the protection of high-value information throughout its lifecycle, from the data center to the cloud. More than 25,000 customers across commercial enterprises and government agencies trust SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.