BY JOE SKORUPA

BUSINESS-DRIVEN SECURITY

Solving a two-fold challenge: prioritizing problems from a business perspective and creating a holistic roadmap

Today's retail security challenges can seem too large, too broad and too numerous for even the most well-funded IT departments. The challenge is two-fold: prioritizing problem areas from a business perspective and creating a capability roadmap that ensures security solutions work together. This roadmap should not only encompass all security solutions that are in place today, but those that will be added later.

In the current treacherous cybersecurity climate retailers are rebuilding or upgrading their security solutions, but since this is the retail industry they face a unique problem in terms of prioritization. Like it or not, a large chunk of a retailer's security focus must be on the Europay, MasterCard, Visa (EMV) mandate and Payment Card Industry Data Security Standard (PCI DSS) compliance.

Left alone, retailers might have chosen to invest more heavily in such areas as mobile application security or perimeter protection, two of the lowest ranked areas of knowledge and expertise in today's retail organization — just 13% of retailers say they are at an advanced level in mobile application security, and just 13% say they are advanced in perimeter protection. (See Figure 1.)

Since retailers must focus on PCI and EMV instead of other areas, we find that 38% of retailers say they are at an advanced level for PCI compliance and 35% for EMV. Both of these numbers are up from levels recorded last year in a similar Custom Research report on security. At that time the advanced level of PCI was claimed by 35%, and advanced EMV claimed by 23%.

The Hacker Way

The hacker's chief weapon is continuous iteration, evidence of which we can clearly see by looking at the top three areas cited by retailers as posing the greatest security risk. (See Figure 2.)

Last year, the top three areas of greatest security risk were hackers using unauthorized credentials (chosen by 51%), internal misuse (51%) and partner/third-party risk (43%). None of these areas appear on this year's top-three list, which now includes malware (58%), point-

Figure 1

Level of knowledge and expertise in the key areas of data and payment security

	Weak	Rudimentary	Adequate	Advanced
EMV Mandate	10%	10%	45%	35%
PCI DSS	14%	17%	31%	38%
Tokenization	13%	20%	37%	30%
P2P encryption	13%	20%	40%	27%
E-commerce data security	10%	14%	52%	24%
Data-centric security	13%	30%	40%	17%
Field-level encryption	17%	28%	41%	14%
Perimeter protection	20%	30%	37%	13%
Mobile application security	29%	42%	16%	13%

Figure 2

Areas that pose the greatest security risk to your organization

2015	
Hackers using unauthorized credentials	51%
Internal misuse	51%
Partner/third-party risk	43%
2016	
Malware	58%
POS intrusions	55%
Credit-card skimming	52%

Figure 3

Technologies that pose the greatest security risk to your organization

2015	
POS software	51%
WiFi in stores	51%
Worldwide Web	49%
2016	
POS software	74%
POS hardware	45%
WiFi in stores	42%

Figure 4

Effectiveness of P2P encryption and tokenization

24%	52%	14%	3%	7%
Will block hackers during payment processes	Will effectively de-identify credit card data throughout payment processes	Effective tool but hackers will crack it	Need more information, plan to evaluate	Not sure and have no plans to evaluate

Figure 5

24%

Only a quarter of retailers believe P2P encryption and tokenization will secure sensitive payment and customer information which is a sharp drop from 44% a year ago.

Figure 6

How data security concerns affect cloud strategy

43%	25%	14%	14%
Cautious speed ahead due to lack of full confidence	Full speed ahead with confidence in managing risks	Will only use non-sensitive data to avoid risk	Evaluation underway, includes major security concerns

Figure 7

Data sources clearly identified and included in organization's data security plan

100%	Payment transactions data and payment card information (PCI)
83%	Personally identifiable information (PII)
59%	Loyalty programs customer data sets
48%	Health/protected health information (PHI – healthcare records)
21%	Social media data
21%	Location data (GPS, in-store, telecoms etc.)

Figure 8

Rate the following technologies for value and risk in terms of providing business opportunity and competitive edge vs. data breach/security risk.

	HV/HR	HV/LR	LV/HR	LV/LR
Mobile payments	41%	31%	21%	7%
Cloud computing	34%	55%	10%	0%
Big data analytics	21%	69%	3%	7%
Opt-in mobile apps	14%	25%	14%	46%
Near-field (Bluetooth) payments	14%	24%	48%	14%
WiFi in stores	14%	24%	41%	21%
Beacon technology/ Location data in-store	10%	21%	21%	48%
Text messaging	7%	38%	7%	48%

(HV stands for High Value. LV stands for Low Value. HR stands for High Risk. LR stands for Low Risk.)

of-sale (POS) intrusions (55%), and credit card skimming (52%).

And as retailers grow increasingly digital to keep up a competitive pace in the omnichannel race, they become even more susceptible to savvy cyber-thieves. (See Figure 3.). While cyber-criminals' favorite technology entry points last year were POS software and in-store WiFi (51% respectively) followed by the Worldwide Web (49%), this year's list includes some changes. POS software still tops the list of security risks (74%), however retailers have become increasingly concerned with POS hardware (45%) and in-store WiFi networks (42%).

Determined to fight back, the first step retailers are taking to protect sensitive customer-specific and mission-critical information is adopting point-to-point (P2P) encryption and tokenization. These processes are believed by more than half (52%) of retailers to effectively de-identify credit card data throughout the payment process. (See Figure 4.)

Getting Strategic

Cloud computing is gaining more traction in retail thanks to its ability to efficiently scale to need. However, only 25% of retailers are confident about adopting cloud-based technologies and moving forward full speed ahead. (See Figure 6.) Nearly half (43%) of retailers still lack full confidence in cloud security and 14% still only trust the cloud with non-sensitive information. Clearly, the majority of retailers are still hedging their bets on cloud platforms due to security concerns.

Besides adding security technologies in the right places, retailers also need to clearly identify their most susceptible data sources. (See Figure 7.) All companies (100%) indicate they are focused on payment transaction data and payment card information (PCI) by including it in their data security plan. Another data area widely included is personally identifiable information (PII), such as addresses, driver's license data, and other personal details (83%). The other two high priorities include customer data sets associated with loyalty programs (59%) and protected health information (PHI) or healthcare records (48%).

Retailers must be equally concerned about new solutions they are deploying in an increasingly digital world and how vulnerable they are to cyber-criminals. (See Figure 8.) Retailers say mobile payments (41%), multichannel integration points (38%) and cloud computing (34%) provide the highest opportunities for their organizations, but they also feel these solutions pose the highest risks.

Another challenge for retailers is the struggle to balance security for low value technologies. For example, retailers may not consider near-field/Bluetooth-enabled payments (48%), in-store WiFi (41%), and mobile payments (21%) as high-value, mission-critical solutions, since each of these fell into the "low value" category. But without effective security technologies in place they can quickly become entry points for hackers.

Figure 9
Status of the key security technologies

	Up to date	Working on now	Begin by end of year	Begin in 2017
PCI DSS	62%	24%	0%	14%
P2P encryption	52%	31%	3%	14%
Ecommerce security	52%	34%	7%	7%
Field-level encryption	48%	14%	7%	31%
Tokenization	45%	34%	3%	17%
Perimeter protection	41%	31%	7%	21%
Data-centric security	41%	38%	7%	14%
Encryption key management	41%	21%	10%	28%
Mobile application security	38%	21%	7%	34%
EMV mandate	24%	59%	7%	10%

Figure 10
Organizational position regarding security breaches

Figure 11
What is your organization's EMV strategy?

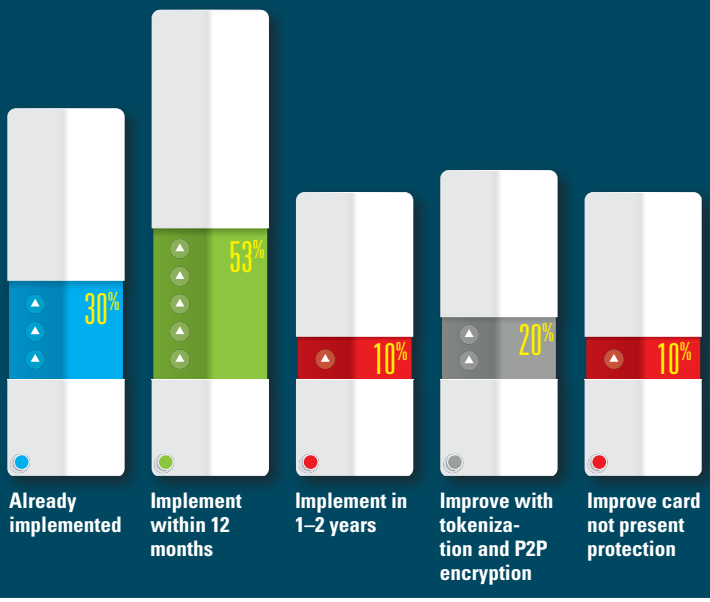
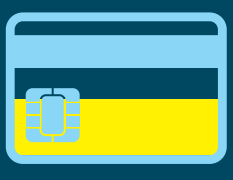


Figure 12



30% Less than a third of retailers say they have already implemented EMV technology, which isn't a lot but it is double the amount (14%) from last year.

In the effort to protect these and other vulnerable technologies many retailers are investing in security solutions. Sixty two percent (62%) of retailers have committed to keeping PCI DSS standards and processes up to date, while 24% are working on upgrading them now. P2P encryption is also a top priority with 52% of retailers saying they are up to date and another 31% upgrading now. E-commerce is another heavy investment area where we see that 52% say their technology is up to date with another 34% working on improvements now. (See Figure 9.)

Key Takeaways

Additional findings in the study include:

- A majority of companies (63%) are putting these funds to good use, as they invest in solutions and processes designed to reduce their vulnerability to data breaches on a continuous basis. However, only a fifth (20%) report they have the strongest possible security measures possible in place. (See Figure 10.)
- While the EMV mandate's October 2015 deadline is a distant memory only a meager 30% of retailers say it is fully implemented. The good news is another 53% plan to be compliant within 12 months, and among these companies, 20% plan to improve EMV compliancy with tokenization and P2P encryption. (See Figure 11.)
- Less than half (47%) of retailers say they have strong top-management support with budget backing for protecting sensitive data. (See Figure 13.)
- One-third (33%) of retailers say they increased spending on security between 2% and 5% compared with last year. Another 10% increased their security budgets between 5% and 10%. (See Figure 14.)

Conclusion

Data breaches have become a sobering cost of doing business for retailers. The only successful strategy is to be vigorously proactive. However, as security challenges expand and grow more complex the task can overwhelm even the most well-funded IT departments.

The two-fold challenge retailers need to overcome is to prioritize a proactive security to-do list and then ensure that all new solutions as well as legacy solutions already in place work together in a unified way.

While retailers are allocating more technology budgets to their security strategies, a significant portion of funds remains focused on supporting the EMV mandate and PCI DSS compliance. These investments are necessary, but they are not a complete solution.

The answer, of course, is to adopt a strategy of continuous investment coupled to a clear roadmap that ensures all security components work together seamlessly. This is one area where you don't want to leave gaps. **RIS**

Figure 13

Strength of top-management understanding of data breach risk and support for sensitive data security

Strong support with budget backing	47%
Strong support without budget backing	13%
Mediocre support and budget backing	33%
Inadequate support and budget backing	7%

Figure 14

Status of your current security technology budget compared to the previous year

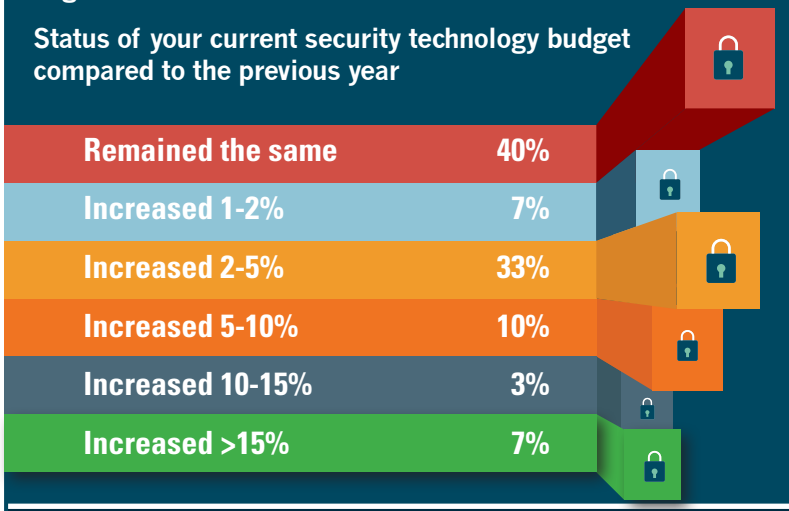


Figure 15

Annual revenue

27%	13%	17%	17%	27%
< $100 million	$100 million to $500 million	$500 million to $1 billion	$1 billion to $2 billion	> $2 billion

Figure 16

Sales revenue in the last 12 months