Thought Leadership White Paper

A Perspective on Retail Payments Security

TOGETHER COMMERCE™

TOSHIBA
Leading Innovation >>>

The following paper outlines a point-of-view and examples of products and services available from Toshiba Global Commerce Solutions. A set of best-in-class solutions is presented and is not tailored to any one customer environment. All customer situations differ and the solutions represented may not be optimal for your company's needs. Please contact your Toshiba Global Commerce Solutions representative so that we may provide you with an idea of solutions that will meet your company's unique needs.

The Bottom Line: Retailer Implications

- At a recent conference, Jeff Wilson (Principal Security Analyst at Infonetics), indicated that many of the major breaches in 2014 were identified (with over 2 weeks lead time) by security scanning tools. However, the reaction time and evaluation of alert messaging was stymied by process—inadequate noise filtering, escalation procedures, and communications channels resulted in the right people not knowing if new alerts were different from all the other alerts they were receiving on a daily basis relative to potential severity and risk.
- Since new viruses and malware are created on an ongoing basis and scanning tools cannot necessarily identify or scan for viruses and malware that have not previously been identified, categorized, and studied, it is possible that many corporate systems have already been compromised without the knowledge of security teams.[1]
- Thus, while the bad news is that it is probably not realistic to be able to prevent and mitigate every single threat to enterprise security, the good news is that there are a few basic steps that can be taken to reasonably protect customer payment data, which comes with the important benefit of mitigating potential financial losses and reputational damage.

The Realities of Payments Security

It comes as no surprise—according to security firm Risk Based Security—that 2014 was the worst year ever for corporate data breaches. In the first nine months of 2014, 904 million records were breached versus the 813 million in all of 2013.[2] Some of the better known examples from 2014 include:

- **Home Depot:** Pending litigation over 56 million cards potentially compromised over a 5 month period
- **eBay:** Facing class action lawsuits over failure to properly secure customer information which was obtained through unauthorized access to company systems
- **Target:** Found negligent (by Minnesota District Court) in data breach which resulted in the compromise of 40 million cards and the personal information of 70 million shoppers, leaving the door open for liability compensation and financial restitution to financial institutions and consumers
- **Sony Pictures:** Five feature films stolen and posted along with other sensitive files containing employee compensation, social security numbers, personal e-mail correspondence, celebrity phone numbers, etc. Additionally, employees were locked out their work computers and the company's network.
- **JPMorgan:** 76 million households affected by compromised employee credentials which allowed hackers to access personal information

Between (i) the multitude of news articles glorifying the billions of dollars generated via successful technology company exits (greatly elevating the status of being a "computer geek"), (ii) the variety of television shows and movies showcasing the ingenuity and value of skilled computer professionals and hackers (e.g., *Scorpion, 24, Person of Interest, CSI, Leverage, Die Hard 4, Hackers,* etc.), and (iii) the lack of strong economic opportunity for younger citizens in many parts of the world (i.e., Europe, Middle East, etc.), it is no surprise that people are choosing to mesh interest in technology with the goal of financial betterment in the form of computer hacking and cybercriminal activity. Thus, with regard to payments security, it's best to keep the following points in mind:

- The bigger and more public your company is, the more attractive of a target it becomes for cybercriminal activity—simply put, too much money flows through retail and corporate systems for criminals to NOT target your company
- Per a recent report from Nilsen, US-based companies are particularly vulnerable—the US accounted for 47 percent of over $11 billion in international payment fraud despite having only 23.5 percent of total international card volume[3]
- Cybercriminals have become more organized, sophisticated, and international relative to the early days of the internet—with the large potential for financial gain in the digital world as well as the increase in state-sponsored corporate espionage and cyberterrorism activity[4] it's not a stretch to assume that cybercriminals will often be more knowledgeable and motivated than incumbent corporate IT staff (e.g., Guardians of Peace versus Sony Pictures)
- As a result, companies in the retail industry must constantly maintain a high level of vigilance relative to enterprise security with a particular focus on payments

The Most Common Cause of Data Breaches

While many companies rely on technology-based solutions such as EMV, P2PE, and tokenization to protect sensitive data, Toshiba's research shows that human oversight and failures (and not the compromise of technology-based security solutions such as EMV, P2PE, and tokenization) are the front-end cause of many security incidents. This line of thought is also corroborated in a recent Backoff Analysis Whitepaper which indicates that the first step of retail memory scraping campaigns often begin with the "locating of systems with remote desktop (or similar) tools and then brute-forcing the credential to access them, often, if possible, for an administrator account."[5] The bottom line is that most hackers are highly intelligent and practical individuals who would rather focus on the lower hanging fruit of attacking poor key management/storage practices, exploiting known security vulnerabilities that IT employees haven't yet patched, or conducting phishing and social engineering campaigns against unwitting targets versus trying to defeat strong encryption head-on. For example, in the case of a recent celebrity photo hack, multiple points of failure across a wide variety of lax human-created security practices resulted in the compromise of celebrity personal photos and other cloud-stored data without the need for hackers to defeat strong security measures (such as encryption) directly:

- Poor Authentication Management Processes

Problem	Result
Unlimited tries to enter password—no lockout after pre-specified number of attempts	Leaves accounts vulnerable to dictionary brute-force attacks
Weak knowledge-based authentication questions for password resets	Easy to find a celebrity's pet's name on the internet

- Weak Third Party Security

Problem	Result
Vendors, contractors, other sites, and other apps don't put premium or focus on security	Hackers target these individuals, sites and applications knowing that people will reuse account names and passwords—easy to obtain information which can then be used to penetrate higher value sites and apps

- Poor Celebrity Best Practices

Problem	Result
Weak passwords	Leaves accounts vulnerable to dictionary brute-force attacks
Reusing the same password for all accounts	Hacker who obtains password from less secure site/app gains access to more secure site/app

Thus, while Toshiba—like many others—is continually taking steps to harden its solutions and offerings with EMV, P2PE, and tokenization, the company believes that reliance upon technology alone is insufficient to guarantee the security of any sensitive company data (not just payment credentials). As a result, Toshiba's point-of-view is that information security should extend beyond just point-of-sale technologies and into the management of broader people and process-related security risks.

Toshiba's Five Critical Considerations for Payments Security

1. Limit and protect the amount of personal data needed to process payments—less exposure and less liability accrue with data that either does not exist or is difficult to use
2. Protect the entire transaction processing chain—also ensure that policies cover updates, patching, audits, and testing of software and services provided by third parties who may lack core competencies in security or who may not prioritize security has highly as your company
3. Create, implement, and follow an enterprise governance framework
4. Implement identity and access management tools—ensure that strong authentication management practices exist for customers, employees, contractors, and other third-parties and leverage the "least privilege principle" to minimize any damage created by compromised credentials
5. Most importantly—educate employees, vendors, and customers on policies and common risks to information security including phishing, social engineering, and improper storage of sensitive information such as account passwords, keys, or credentials

1. Limit and protect the amount of personal data needed to process payments

A retailer must consider any personal and payment data to be vulnerable whenever transmitted, processed, or stored. To protect personal and sensitive payment data, Visa, MasterCard, and Discover have agreed upon a set of minimum requirements pertaining specifically to data that are part of the broader Payment Card Industry Data Security Standard (PCI DSS)[6]:

- Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures, and processes
- Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process
- Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere)
- Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions
- Do not store the personal identification number (PIN) or the encrypted PIN block
- Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN
- Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs)
- Ensure that processes exist for the management of encryption and cryptographic processes along with associated keys

It's critical to keep in mind that while important, PCI DSS on its own only represents a minimal level of protection. However, compliance with PCI DSS in conjunction with the implementation of EMV, P2PE, tokenization, and Toshiba's five critical considerations for payments security will provide retailers with a more robust data protection plan by ensuring that sensitive customer data either does not exist or is made extremely difficult to use. Further, following all five considerations will help to mitigate additional actions (such as credential compromises) which may lead to potential back-door point-of-sale exploits.

2. Protect the entire transaction processing chain

As seen in the chart below, data must be secured across the many touch points and players in the payment value chain:

Payments Ecosystem Participants

- Consumers
- Payment terminal providers
- POS terminal and application providers
- Switch and gateway providers
- ISOs, Payment processors
- Acquiring banks
- Card brands and payment Networks(e.g., debit)
- Consumer banks
- *Mobile network providers (carriers)*
- *Mobile device OEMs*
- *Mobile wallet vendors*

To this end, several critical considerations must come into play:

- Ensuring that IT Security Governance and Risk Management accounts for the role of all players in the processing chain, with particular attention paid to the role of third-party entities and contractors who may not prioritize security as highly as your company
- Adopting and adhering to EMV and PCI compliance standards
- Implementing point-to-point encryption (P2PE) and the consideration of tokenization
- Updating, patching, auditing, and testing all software and services—this should include all software and services provided by third party vendors and contractors and verification that all updates and patches are genuine (e.g., digital signature verification)
- Implementing monitoring, scanning, and reporting processes
- Ensuring that identity and access management tools are in place and that employees, vendors, customers, etc. are able to identify basic schemes and tactics related to phishing and social engineering (covered in subsequent sections)

In particular, retailers should keep in mind that both EMV and NFC—on their own—lack native encryption capabilities which could leave sensitive and usable data vulnerable in a potential interception prior to that data reaching point-of-sale.

EMV

EMV itself does not require any sort of encryption or tokenization of a payment credential and retailers must still adhere to PCI DSS standards once EMV compliant. In addition, online EMV within the US will be slowed as the network will need the total to create the cryptogram that will authorize the user/card.

NFC

Payment credentials for NFC pass from the phone (or other device) via existing brand standards (e.g., Visa PayWave, MC PayPass, etc.), which may or may not be encrypted or tokenized. ApplePay, for example, requires biometric authorization (fingerprint) and tokenizes the credential, which is then decrypted by the network (e.g., Visa). In situations outside of the ApplePay model, credentials may be vulnerable when stored. Additionally, relative to NFC and other types of mobile payments, the keys that are stored on the Secure Element of a wireless device are potentially vulnerable to compromise if not properly protected during individual provisioning, de-provisioning, and re-provisioning processes. In some cases, data could be compromised prior to even being used in a retail setting, particularly if mobile carriers become more attractive targets for hacking and cybercriminal activity.

While arguments do exist pertaining to the feasibility and reliability of radio frequency (RF) data interception, the fact remains that limiting (i) the type of data transmitted through contactless payment means (i.e., tokens versus PANs) and (ii) the amount and type of data stored on store and company systems will expose the majority of retailers to significantly less risk and potential liability in the event that data is ever compromised. Nevertheless, while RF interception is generally considered to be more of a contactless payments issue, limiting the type and amount of data that is collected and stored through contact-type payments as well would be a prudent course of action.

Relative to tokenization, Toshiba recommends that all retailers give strong consideration to adoption and usage. Per a recent FTC whitepaper on mobile payments and tokenization[7]:

- "Under the traditional payment system, financial information on a card's magnetic stripe that is transmitted from a merchant to a bank consists of the same information sent each time a consumer makes a payment. Thus, if this information is intercepted, it can be used repeatedly for subsequent, unauthorized transactions." [Note that for card present transactions, this issue will be solved through EMV implementation and compliance].
- "Mobile payments, however, can utilize dynamic data authentication, whereby a unique set of payment information is generated for each transaction. Accordingly, even if the data is intercepted, it cannot be used for a subsequent transaction. In the mobile context, payment information also can be stored on a secure element that is separate from the rest of a phone's memory, preventing hackers who access a phone operating system from compromising sensitive financial information."

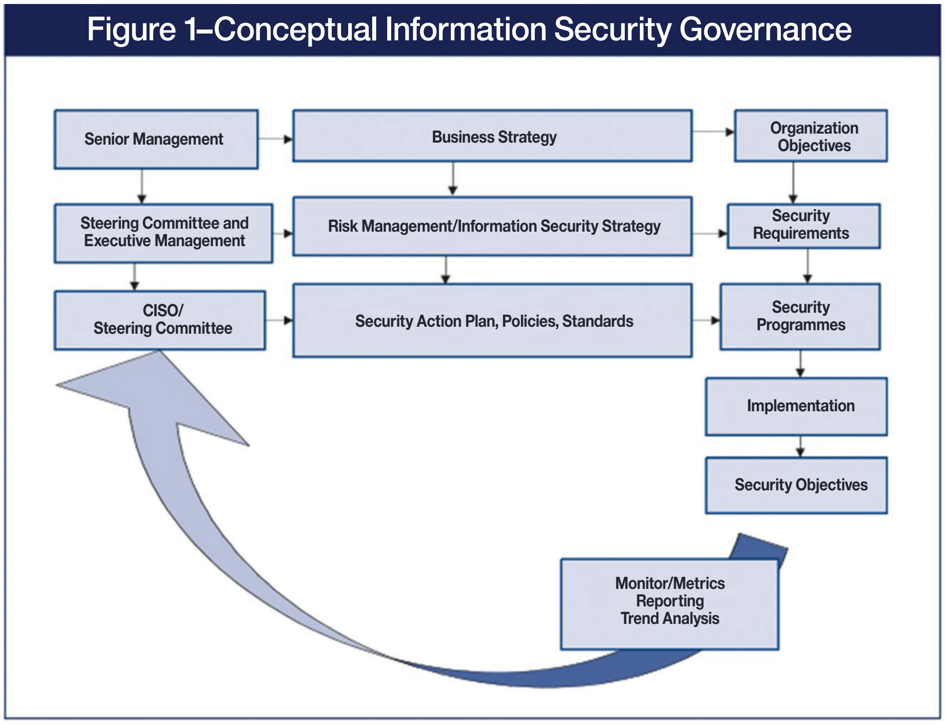
3. Create, implement, and follow an enterprise governance framework

The leading industry forum for information security governance—ISACA or the Information Systems Audit and Control Association—suggests having a strong governance framework for information security. Per ISACA, "Information Security is not only a technical issue, but a business and governance challenge that involves adequate risk management, reporting and accountability. Effective security requires the active involvement of executives to assess emerging threats and the organization's response to them." As a result, successful governance starts with active leadership from senior executives and links with business strategy and operational procedures (Figure 1 – per ISACA[8]).

As seen in Figure 1, business strategy, fulfillment of customer needs, and regulatory requirements drive the creation of an information security strategy, risk identification and management program, and ultimately, specific plans, policies, and standards. Once controls and monitoring tools have been implemented, a process must be put in place to ensure incident reporting and the periodic evaluation and update of policies, standards, procedures, and risks.

At minimum, ISACA recommends the following items as key components of good information security governance framework:

Figure 1–Conceptual Information Security Governance


Senior Management
Business Strategy
Organization Objectives
Steering Committee and Executive Management
Risk Management/Information Security Strategy
Security Requirements
CISO/ Steering Committee
Security Action Plan, Policies, Standards
Security Programmes
Implementation
Security Objectives
Monitor/Metrics Reporting Trend Analysis

Key components of ISACA's information security governance framework

- An information security risk management methodology
- A comprehensive security strategy explicitly linked with business and IT objectives
- An effective security organizational structure
- A security strategy that talks about the value of information protected—and delivered
- Security policies that address each aspect of strategy, control and regulation
- A complete set of security standards for each policy to ensure that procedures and guidelines comply with policy
- Institutionalized monitoring processes to ensure compliance and provide feedback on effectiveness and mitigation of risk
- A process to ensure continue evaluation and update of security policies, standards, procedures and risks

4. Implement Identity and Access Management Tools

As alluded to previously, careless, negligent, and disgruntled humans will always "outsmart"—or perhaps "out-dumb"—the most expensive and sophisticated information security technology in existence. Simply put, even the best encryption and tokenization in the world will not protect your sensitive data if engineers and system administrators utilize poor key management and storage practices or fall victim to social engineering tactics. In addition, because it is often easier to compromise employee credentials and use them to access systems containing sensitive data than it is to directly defeat encryption, identity and access management (IAM) measures should implemented across all employees, contractors, third-party vendors, and customers for all systems that handle data. In conjunction with IAM, companies should also strive to adopt the "least privilege" principle, or the idea that users and applications should be given the least amount of rights needed to perform a given task. By implementing the "least privilege" principle, companies can greatly minimize the potential damage that could be caused by compromised employee credentials.

Relative to IAM, retailers should weigh the following considerations:

- Ensuring that all IT policies, standards, and procedures apply to all employees, contractors, and third-party vendors
- Implementing an enterprise-wide and centrally managed IAM system to help manage access to relevant applications, systems, and information sources in an efficient, uniform, and consistent manner, including the revocation of access when a user (employee or contractor) changes roles or leaves the company
- Conducting privileged user review periodically to ensure user alignment with job functions, roles, and employment status[9]
- Enabling password management programs that require strong passwords as well as password expiry timing[9]
- Utilizing identity-enabled networking (i.e. devices must be authenticated on the network to be usable on the network)[9]
- Integrating IAM with Data Loss Prevention tools[9]
- Consideration of network sequestration tactics to help disperse and mitigate risk

Finally, having multiple points of identity authentication also decreases the potential for data compromise. In this vein, the biometrics component of the latest Apple devices renders a lost or stolen phone less susceptible to misuse than a lost or stolen debit card which can be reset via voice response units (or VRUs) using accessible knowledge such as birthdates, social security numbers, mothers' maiden names, and first pet names. For consumers, ISACA recommends that companies implement at least two of the authentication measures listed in the chart to the top right to limit potential fraud or misuse:

For consumers, ISACA recommends at least two of the following:

- Knowledge: something that only the user knows—such as a password or PIN
- Ownership: something that only the user has—such as a token, smart card, or phone
- Inherence: something that the user is—such as a fingerprint

5. Educate employees, vendors, and customers on policies and common risks to information security including phishing, social engineering, and "not-so-smart" practices

Retailers must ensure that their employees, critical vendors, and customers know how to identify phishing and social engineering tactics. While IAM tools and the "least privilege" principle help to mitigate direct hacking attempts, they cannot solve for instances where employees, vendors, contractors, customers, and other third-parties:

- Voluntarily provide cybercriminals with credentials that allow for access of sensitive systems and data
- Neglect updates and patching which allow for the use of known security exploits
- Store sensitive data (such as network account passwords or encryption keys) on unencrypted documents or spreadsheets that are placed in easily found or easily searchable locations

At minimum, retailers should emphasize the implementation of awareness programs which include the following critical security topics

Importance of endpoint security	Protection of personal and sensitive data and smart security design	Overviews of common social engineering and phishing scams
The best corporate security measures will be rendered ineffective if endpoints such as mobile devices, tablets, and PCs have been compromised through lack of software updates, patching, anti-virus protection, and/or the download of malicious software	PINs Passwords social security numbers, etc. Employee awareness of OWASP, etc. and smart security principles to limit potential hacker exploits	Unsolicited calls offering help you never asked for and "free lunches" are usually opportunities to obtain data

Final Takeaways

- The complexity of securing modern information systems has increased dramatically, and expectations of being able to keep everything out your computing environment while also being able to remove anything that happened to "slip by" are no longer realistic
- While some hackers and cybercriminals may be able to defeat technologies such as P2PE and tokenization directly, most hacking incidents still begin with either phishing and social engineering attempts or the exploits of known and existing software vulnerabilities
- As a result, retailers, their management teams, and their boards must proactively assume responsibility for managing their information systems and computing environments and cannot rely completely on outside or third-party technologies to resolve all of their security needs
- To date, the vast majority of retail hacks have centered around the procurement of customer payment data, where security can be enhanced through a combination of EMV, P2PE, tokenization, and the application of a few security considerations related to people, process, and governance

For more information

To learn more about payment security, please contact your Toshiba representative or Toshiba Business Partner, or visit the following website: **toshibacommerce.com**

Additionally, Toshiba Global Commerce Solutions can help credit-qualified clients acquire the IT solutions that your business needs in the most cost-effective and strategic way possible through our global financing partner.

References

[1] http://thestack.com/mimicry-in-malware-giovanni-vigna-081014

[2] Risk Based Security report, 2014

[3] http://www.marketwatch.com/story/global-credit-debit-and-prepaid-card-fraud-losses-reach-1127-billion-in-2012-up-146-over-2011-according-to-the-nilson-report-2013-08-19

[4] http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/

[5] Matrix Global Partners, Backoff White Paper, 2014

[6] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

[7] http://www.ftc.gov/sites/default/files/documents/reports/paper-plastic-or-mobile-ftc-workshop-mobile-payments/p0124908_mobile_payments_workshop_report_02-28-13.pdf

[8] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Information-Security-Governance-Guidance-for-Boards-of-Directors-and-Executive-Management-2nd-Edition.aspx

[9] http://www.ey.com/Publication/vwLUAssets/Identity_and_access_management_-_Beyond_compliance/$FILE/Identity_and_access_management_Beyond_compliance_AU1638.pdf

Premier Business Partner IBM™

TOSHIBA
Leading Innovation

Toshiba Global Commerce Solutions, Inc.
3038 E. Cornwallis Road,
Research Triangle Park, NC 27709, USA

The information in this document is provided on an as is basis. Toshiba products are warrantied solely in accordance with the applicable Toshiba limited warranty or license agreement.

The information included in this publication could include technical inaccuracies or typographical errors. All such information is provided "AS IS" without warranties of any kind, express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose.

Not all Toshiba products and services are available in every country.

All statements regarding Toshiba's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The Toshiba Global Commerce Solutions home page on the internet can be found at **toshibacommerce.com**

♻ Please Recycle