IoT SMM: Retail Profile for Point-of-Sale Devices

omg/2020-08-01

Authors

Frederick Hirsch (Upham Security), Andy Mattice (Lexmark), Bart McGlothin (Cisco), Leonid Rubhakin (Aptos), Ekaterina Rudina (Kaspersky), Ron Zahavi (Microsoft)

Technical Editor

Stephen Mellor (IIC staff)

CONTENTS

The retail landscape is changing with digital transformation, evolving technologies, and increasing risks associated with greater connectivity and integration. The retail industry is deploying Internet connected devices to reach and serve customers better, ranging from new point of sale (also known as point of service) payment devices such as radio-frequency identification (RFID) and signature scanners, to audit-logging devices such as printers, cash dispensers and other systems such as lights and cameras. With the proliferation of mobile devices and other technologies, retailers are intentionally and, perhaps, unintentionally, collecting more and more data about their customers. New threats constantly emerge, and attackers are becoming more capable and organized. At the same time, compliance requirements around data protection and security are becoming more significant. These trends increase the urgency and importance of addressing security and data protection concerns in a systematic and effective manner.

The Object Management Group's (OMG) Retail Domain Task Group[1] (with members previously in the ARTS community[2]) has recognized these issues and previously produced primers about security and data protection threats and associated controls. Trust is essential to the customer relationship with the retailer. The challenge is to figure out how much security is needed, how much to invest to fit certain scenarios and which controls to deploy, given the complexity of the retail environment. All aspects must be considered including governance, technology and operations. The IoT Security Maturity Model (SMM) helps organize and manage these concerns, enabling various stakeholders to communicate and determine appropriate maturity targets, assess the current status, and create action plans to address gaps.

The SMM defines general considerations to form a foundation from which communities can consider their specific needs and concerns and extend the SMM by creating profiles that consider industry and device specific concerns. This document is a profile for the point of sale (POS) retail community.

This document, the "IoT Security Maturity Model: Retail Profile," is an industry profile extension to the "IoT Security Maturity Model: Practitioners Guide" that provides details on the SMM. It draws on the detailed analysis in the ARTS Cybersecurity Primer[3] and the ARTS Data Privacy Primer[4]. The material in Payment Card Industry (PCI) standards are relevant, in particular the Data Security Standard,[5] Payment Application Data Security Standard,[6] and the PIN Transaction Security Devices standard.[7]

---

[1] https://www.omg.org/retail/

[2] Association for Retail Technology Standards (ARTS) in the National Retail Federation (NRF), *https://nrf.com/insights/retail-technology*

[3] See [ARTS-CYBERP2015]

[4] See [ARTS-DATAP2015]

[5] See [PCI-DSS]

[6] See [PCI-PADSS]

[7] See [PCI-PTS]

1 THE IOT SECURITY MATURITY MODEL

The goal of a SMM is to provide a path for Internet of Things (IoT) providers to know where they need to be and how to invest in security mechanisms that meet their requirements without over-investing in unnecessary security mechanisms. It seeks to help organizations identify the appropriate approach for effective enhancement of these practices where needed. Deciding where to focus limited security resources is a challenge for most organizations given the complexity of a constantly changing security landscape.

As an informed understanding of the risks and threats an organization faces is the foundation of choosing and implementing appropriate security controls, the model provides a conceptual framework to organize the myriad considerations. The framework helps an organization decide what their security target state should be and what their current state is. Repeatedly comparing the target and current states identifies where further improvement can be made.

Not all IoT systems require the same strength of protection mechanisms and the same procedures to be deemed secure enough. The organization determines the priorities that drive the security enhancement process, making it possible for the mechanisms and procedures to fit the organization's goals without going beyond what is necessary. The implementation of security mechanisms and processes are considered *mature* if they are expected to be effective in addressing those goals. It is the security mechanisms' appropriateness in addressing the goals, rather than their objective strength, that determines the maturity. Hence, *security maturity* is the degree of confidence that the current security state meets all organizational needs and security-related requirements. *Security maturity* is a measure of the understanding of the current security level, its necessity, benefits and cost of its support. Factors to weigh in such an analysis include the specific threats to an organization's industry vertical, regulatory and compliance requirements, the unique risks present in an environment and the organization's threat profile.

Security level,[1] on the other hand, is a measure of confidence that system vulnerabilities are addressed appropriately and that the system functions in an intended manner. The SMM does not say what the appropriate security level should be; it provides guidance and structure for organizations to identify considerations for different maturity levels appropriate for their industry and system. It provides guidance for defining and accounting for different levels of comprehensiveness and alignment with industry sector and system, including non-industrial systems. Some users of the model will apply its guidance to create industry- and system-specific profiles, which can then be used by a broader audience, in concert with the model, to help assess maturity in a specific vertical or use case.

The audience for this document includes owners of IoT systems, decision makers, security leaders in various verticals, business risk managers, system integrators, architects, security assessors, analysts, policy and regulatory authorities, and other stakeholders concerned about the proper

[1] According to [IEC-62443-33]

strategy for the implementation of mature security practices tailored to the needs and constraints of the specific IoT system.

Those using this SMM should be able to determine and clearly communicate to management the answers to the following questions:

- Given the organizational requirements[1] and threat landscape, what is my solution's target maturity state?
- What is my solution's current maturity state?
- What are the mechanisms and processes that will take my solution's maturity from its current state to its target state?

1.1 THE SMM PROCESS

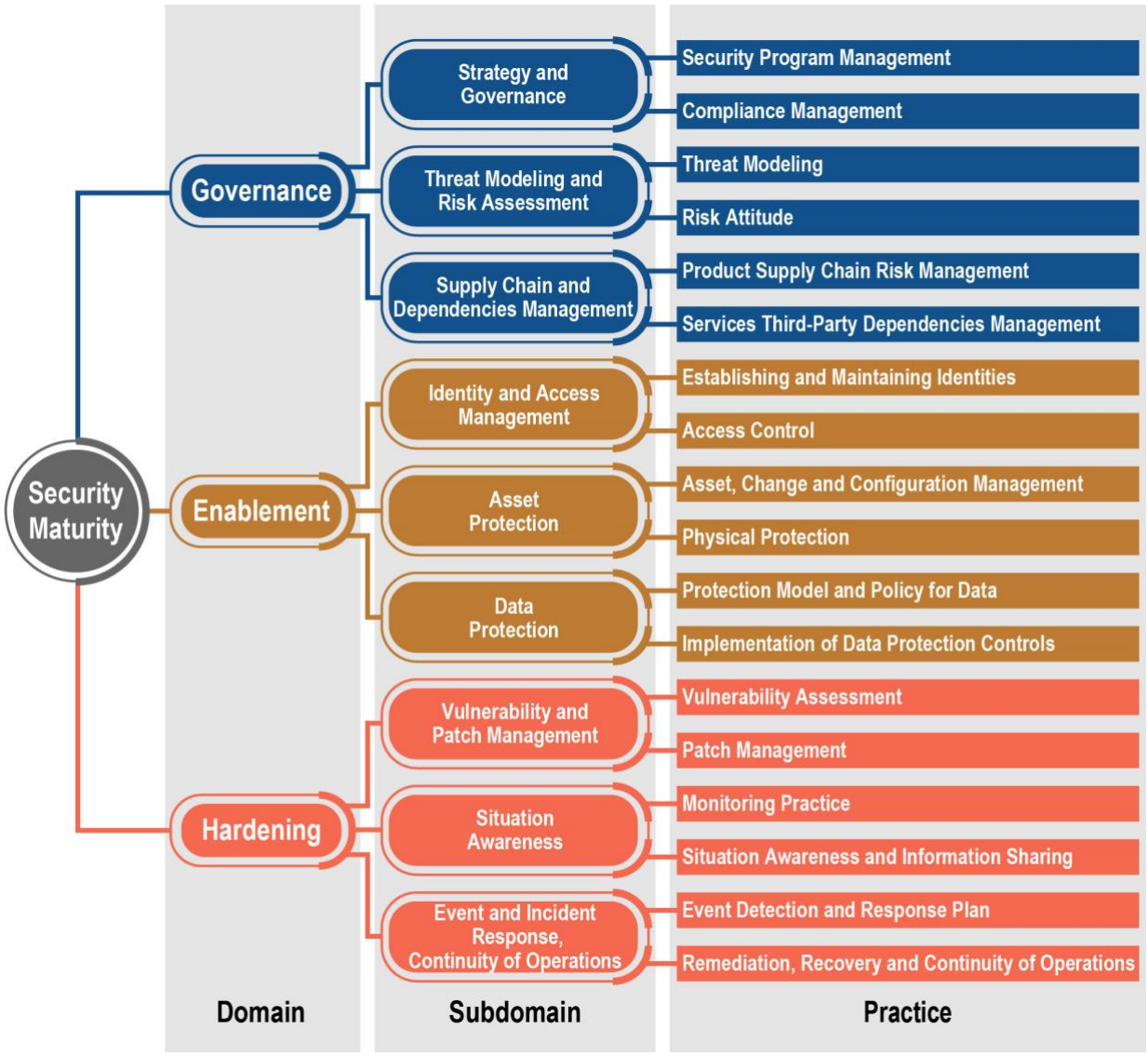
Organizational business stakeholders define goals for the security posture of the organization and the systems it owns or operates. These systems may be brand new or brownfield. These goals should be mapped to objectives that tie to the risks. Technical teams within the organization, or third-party assessment vendors, map these objectives into tangible security techniques and capabilities, identifying the appropriate target security maturity state. Establishing a target maturity state, while accounting for industry and system-specific considerations, facilitates generation of security profiles. These profiles capture target security maturity states of systems and can act as templates for evaluating security maturity of a specific area of use, common use-case or system of interest.

1.2 UNDERSTANDING THE MODEL

Figure 1-1 illustrates the structure of the SMM and the breakdown of security maturity domains. *Domains* are the high-level views that capture the key aspects of security maturity: governance, enablement and hardening. Each of the domains has different key aspects to it, called *subdomains*. For example, the hardening domain includes subdomains vulnerability and patch management, situational awareness and event and incident response. Each domain may use a variety of practices, both technical and organizational, to achieve results related to that domain.

This hierarchical approach enables the maturity and gap analysis to be viewed at different levels of detail, from the various domains overall to the individual practices.

[1]Namely, business or mission needs, requirements from regulatory authorities, and other similar factors.



Domains are pivotal to determining the priorities of security maturity enhancement at the strategic level.

Sub Domains reflect the basic means of obtaining these priorities at the planning level.

Practices define typical activities associated with sub domains and identified at the tactical level.

At the domains level, the stakeholder determines the priorities of the direction in improving security.

At the sub domains level, the stakeholder identifies the typical needs for addressing security concerns.

At the practices level, the stakeholder considers the purpose of specific security activities.

Figure 1-1: SMM Hierarchy

1.2.1 SECURITY GOVERNANCE

Figure 1-2 below describes the elements of the governance domain of the SMM.

The security governance domain is the heart of security. It influences and informs every security practice including business processes, legal and operational issues, reputation protection and revenue generation.

Security strategy and the governance sub domain facilitates organizational drivers along with providing security, compliance with regulations, laws and contractual obligations. This also can relate to customer expectations and reputation management.

Security program management practice is vital to the clear planning and timely provision of security activities, control over the process and results and optimal decision-making procedure for fulfillment of security related demands.	**Compliance management practice** is necessary when strict requirements for compliance with evolving security standards is needed.

Threat modeling and the risk assessment sub domain identifies gaps in specific configurations, products, scenarios and technologies and prioritize countermeasures accordingly.

Threat modeling practice aims at both revealing known and specific factors that may place the functioning of a given system at risk and accurately describing these factors.	**Risk attitude practice** enables an organization to establish a strategy for dealing with risks according to risk management policy, including conditions for acceptance, avoidance, evaluation, mitigation and transference.

Supply chain and the external dependencies management sub domain aims at controlling and minimizing a system's exposure to attacks from third parties that have privileged access and can conceal attacks.

Product Supply chain risk management practice addresses the need to enable trust for contractors or suppliers and to ascertain the absence of hidden threat sources, ensuring the integrity of the supply chain.	**Services Third party dependencies management practice** addresses the need to enable trust for partners and other third parties. The ability to have assurance of the trust of third parties requires understanding of the business and trust infrastructure and possible hidden threat sources.

Figure 1-2: Security Governance

1.2.2 SECURITY ENABLEMENT

Figure 1-3 below describes the elements of the enablement domain of the SMM.

The security enablement domain is based on established security policy and addresses the business risks using the best available means. Security policy and controls are subject to periodic review and assessment.

Identity and access management sub domain aims to protect the organization and control the use of resources by the identified agents to reduce the risk of information leakage, tampering, theft or destruction.

Establishing and maintaining identities practice helps to identify and constrain who may access the system and their privileges.	**Access control practice** policy and implementation allow a business to limit access to resources to only the specific identities that require access and only at the specific level needed to meet organizational requirements.

The asset management sub domain is put in place to protect both physical and digital assets. This is an area of strong collaboration between IT and physical security teams.

Asset, Change and Configuration Management practice constrains the types of changes allowed, when those changes can be made, approval processes and how to handle emergency change scenarios.	**Physical protection practice** policies address the physical security and safety of the premises, its people and its systems to prevent theft and ensure the ongoing safe operation of equipment.

The data protection sub domain prevents unauthorized data disclosure or manipulation of data, both for data at rest, in transit and in use. This is important for security, privacy, regulatory compliance, legal and intellectual property protection.

The security model and policy for data practice identifies whether different categories of data exist and considers the specific objectives and rules for data protection.	**The implementation of data protection controls practice** describes the preferred application of data protection mechanisms to address confidentiality, integrity and availability.

Figure 1-3: Security Enablement

1.2.3 SECURITY HARDENING

Figure 1-4 below describes the elements of the security hardening domain of the SMM.

The security hardening domain practices support trustworthiness objectives through the assessment, recognition and remediation of risks with both organizational and technical countermeasures.

Vulnerability and the patch management sub domain policies and procedures keep systems up to date and less prone to attacks.

Vulnerability assessment practice helps to identify vulnerabilities, determine the risk that each vulnerability places on the organization and develop a prioritized remediation plan.	**Patch management practice** policy clarifies when and how frequently to apply the software patches, sets up procedures for emergency patches and proposes additional mitigations in the instance of constrained access to the system or other issues involved with patching.

The situational awareness sub domain aims at understanding the current security state enabling an organization to prioritize and manage threats more effectively.

Monitoring practice is used to monitor the state of the system, identify anomalies and aid in dispute resolution.	**Situational Awareness and Information sharing practice** helps organizations be better prepared to respond to threats. Sharing threat information keeps systems up to date.

Event and incident response, continuity of operations sub domain implemented in a combination of policy and technical preparation allows an organization to respond to incidents swiftly and minimize disruption to the rest of the system.

An event detection and response plan defines what a security event is and how to detect and assign events for investigation, escalate them as needed and respond appropriately. It should also include a communications plan for sharing information appropriately and in a timely manner with stakeholders.	**Remediation, recovery, and continuity of operations** represent a combination of technical redundancies whereby trained staff and business continuity policy help an organization recover quickly from an event to expedite returning to business as usual.

Figure 1-4: Security Hardening

1.3 APPLYING THE MODEL

Two aspects are essential for measuring the maturation progress of IoT systems and prioritizing associated security practices – comprehensiveness and scope. These are considered within the context of the target and assessment, namely the system of interest, whether end to end, a component or a sub-system under consideration.

Comprehensiveness captures the degree of depth, consistency and assurance of security measures that support security maturity domains, sub domains or practices. For example, a higher level of comprehensiveness of threat modeling implies a more automated systematic and extensive approach.

Scope reflects the degree of fit to the industry or system needs. This captures the degree of customization of the security measures that support security maturity domains, sub domains or practices. Such customizations are typically required to address industry-specific or system-specific constraints of the IoT system.

1.3.1 SCORING AND PRIORITIZATION

Any rigorous security self-assessment procedure, including the SMM, needs a scoring and prioritization method to enable evaluation of the current state and the development of a metrics-based security strategy.

Comprehensiveness and scope, which are orthogonal, help score and prioritize security maturity practices. Certain IoT systems may not require the highly sophisticated or narrowly scoped implementation of all security practices. Such implementation may be over-engineered, given the particular system and the threats that it faces. The security maturity of the system should be determined against the requirements that best meet its purpose and intended use.

1.3.2 COMPREHENSIVENESS LEVELS

There are five comprehensiveness levels for every security domain, sub domain and practice, from Level 0 to Level 4, with larger numbers indicating a higher degree of comprehensiveness of security controls. Every comprehensiveness level covers all the requirements set by the lower levels, augmenting them with additional ones.

Level 0, None: There is no common understanding of how the security practice is applied and no related requirements are implemented. (As this is null, we shall not discuss it further).

Level 1, Minimum: The minimum requirements of the security practice are implemented. There are no assurance activities for the security practice implementation.

Level 2, Ad hoc: The requirements for the practice cover main use cases and well-known security incidents in similar environments. The requirements increase accuracy and level of granularity for the environment under consideration. The assurance measures support ad hoc reviews of the practice implementation to ensure baseline mitigations for known risks. For this assurance, application of measures learned through successful references may be applied.

Level 3, Consistent: The requirements consider best practices, standards, regulations, classifications, software and other tools. Using such tools helps to establish a consistent approach to practice deployment. The assurance of the implementation validates the implementation against security patterns, design with security in mind from the beginning and known protection approaches and mechanisms. This includes creating a system with the security design considered in the architecture and design as well as definition defaults.

Level 4, Formalized: A well-established process forms the basis for practice implementation, providing continuous support and security enhancements. The assurance on the implementation focuses on the coverage of security needs and timely addressing of issues that appear to threaten the system of interest. For this assurance, a more complex approach is applied that uses semi-formal to formal methods.

1.3.3 SCOPE

The scope measurement captures the extent to which the specifics of an application, network or system of interest is taken into account during the implementation of the security facet.

There are three levels of scope for every security facet, from Level 1 to Level 3, with higher numbers indicating a narrower and more specific scope.

Level 1, General: This is the broadest scope. The security practice is implemented in the computer systems and networks without any assessment of its relevance to the specific IoT sector, equipment used, software or processes to be maintained. The security capabilities and techniques are applied as they were in the typical environment.

Level 2, Industry specific: The scope is narrowed from the general case to an industry-specific scenario. The security practice is implemented considering sector-specific issues, particularly those regarding components and processes that are prone to certain types of attacks, and known vulnerabilities and incidents that have taken place.

Level 3, System specific: This is the narrowest scope. The security practice implementation is aligned with the specific organizational needs and risks of the system under consideration, identified trust boundaries, components, technologies, processes and usage scenarios. Combining the general and domain specific objectives in a unique manner sets the requirements of this implementation.

1.3.4 SMM TEMPLATE

All IoT devices, networks and systems do not require the highest comprehensiveness and scope for all security domains, sub domains or practices. The security maturity target for the system of interest is defined as the set of all desirable values of comprehensiveness and scope characteristics for every security maturity domain, sub domain and practice.

In case of insufficient details about the system-security needs the stakeholders may initially determine the target levels of comprehensiveness and scope just for domains. These levels determine the relative priorities of security governance, enablement and hardening. The levels set for the domains will be inherited by the appropriate sub domains and then by the practices

according to the hierarchy. The stakeholders may modify the levels to match the risks more closely. This is helpful for the step-by-step recognition of an uncertain security maturity target.

The security maturity target by default is defined when referring to the comprehensiveness and scope for security maturity practices as seen in **Error! Reference source not found.**. Each practice table has four columns, one for each comprehensiveness level. The objective in each level describes the general considerations that should be met. Guidance is provided in the form of general considerations.

	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	<Objective Level 1>	<Objective Level 2>	<Objective Level 3>	<Objective Level 4>
General considerations	<List of Level 1 general considerations>	<List of Level 2 general considerations>	<List of Level 3 general considerations>	<List of Level 4 general considerations>

Table 1-1: SMM Template

1.4 SECURITY MATURITY PROFILES

The SMM is designed to be extensible across a wide array of industries and systems. It addresses the general scope, which looks at common security maturity best practices in the industry. There is an opportunity to add industry-specific and system-specific scope to any or all of the practices.

The IIC will collaborate with a wide range of industry groups to encourage development of profiles—practice tables that go beyond general scope and include industry- and system-specific requirements for different comprehensiveness levels. For example, a retail group may create profiles of some or all practices that include best practices and regulatory requirements specific to the retail industry; they may also create system specific profiles for commonly used devices such as card readers or security cameras. A health care profile may include specific guidance related to *HIPAA*, while a system-specific profile could address considerations for, say, *FDA* pre- and post-market guidance for implanted medical devices.

Industry and system profiles need not be created for every practice in the model. An industry may decide that the general scope is sufficient for most of the governance-related practices but that a few of the enablement practices necessitate an industry-level point of view.

When extending for industry or system-specific considerations, the practice table as seen in Table 1-2 expands to include two additional rows.

<Practice-Name>				
<Practice Description>				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	<Objective Level 1>	<Objective Level 2>	<Objective Level 3>	<Objective Level 4>
General considerations	<List of Level 1 general considerations>	<List of Level 2 general considerations>	<List of Level 3 general considerations>	<List of Level 4 general considerations>
Industry-specific considerations	<List of Level 1 industry specific considerations>	<List of Level 2 industry specific considerations>	<List of Level 3 industry specific considerations>	<List of Level 4 industry specific considerations>
System-specific considerations	<List of Level 1 system specific considerations>	<List of Level 2 system specific considerations>	<List of Level 3 system specific considerations>	<List of Level 4 system specific considerations>

Table 1-2: Template with industry and system specific considerations

Industry-specific considerations include the sector-specific issues, particularly components and processes that are prone to certain types of attacks, known vulnerabilities, incidents that took place in similar systems and possible harm to this kind of operational technology as well as sector specific priorities including legal and regulatory guidance.

While the general row in the table included headings for achieving the level and indicators of accomplishment, the industry row should include a general description of the industry-specific issues as noted above and for a comprehensiveness level with industry-specific considerations:

1. what needs to be done to achieve that level and
2. relevant industry guidelines for that level.

System-specific considerations include the specific security-relevant business needs and risks for the system under consideration, identified trust boundaries, components, technologies, processes, and usage scenarios that combine the general and domain-specific objectives in a unique manner.

As the general and industry rows in the table included headings and structure described above, the system row should include a description of the system and how it is used in the larger IoT infrastructure and for a comprehensiveness level with industry-specific considerations:

3. what needs to be done to achieve that level and
4. indicators of accomplishment that can assist assessors in identifying if the organization has met the requirements of the level.

Compliance Management				
This practice is necessary when strict requirements for compliance with evolving security standards is needed.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	*See main table.*			
General Considerations	*See main table.*			
Industry Scope Considerations		**What needs to be done to achieve this level** Ensure compliance with Internal privacy and data security requirements for the business. **Indicators of achievement** Internal privacy and data security compliance are integrated as part of overall compliance program.	**What needs to be done to achieve this level** Consider regulatory guidelines relevant to retailers including: Data Security Standard (PCI-DSS), Payment Application Data Security Standard (PA-DSS, 2010), and the PIN Transaction Security Devices (PTS, 2010). …	
Device Scope Considerations			Ensure compliance with PIN Transaction Security Devices (PTS, 2010) … **Indicators of achievement** Complete set of documents verifying and assuring compliance with security-related requirements. …	

Table 1-3: Displays the industry and system specific considerations within the template.

Establishing a target maturity state, while accounting for industry and system-specific considerations, facilitates generation of security profiles. These profiles capture systems' target

security maturity and can act as templates for evaluating security maturity of a specific area of use, common use-case or system of interest.

2 RETAIL USE CASE: POINT-OF-SALE

2.1 PAYMENT SECURITY ECOSYSTEM EXAMPLE

Because of the inherent value and belief of an easy theft, today's hackers are increasingly seeing value in locating and breaching large databases of payment information rather than focusing on the theft of individual credit cards or user information (of course, intercepting and collecting individual credit card payments remains highly lucrative). Below is an example of how payment systems evolved to improve the security and PCI compliance.

Traditional retail payment systems were implemented using so-called Integrated payment architecture.

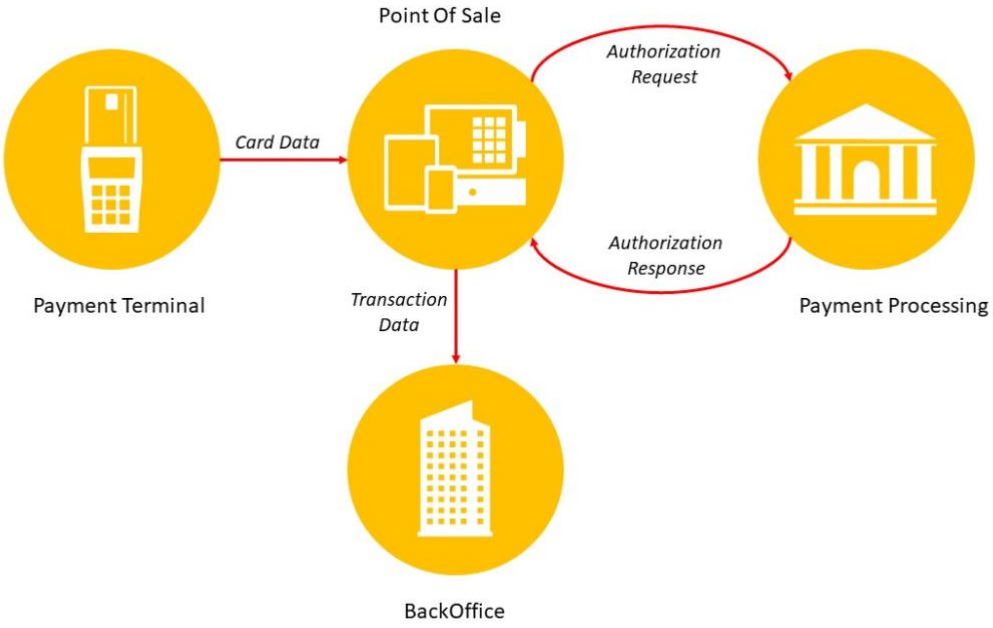


Figure 2-1: Traditional Integrated Payment

In this integrated architecture, Point-of-Sale (POS) controls the payment terminal. It builds payment messages and handles the authorization flow. Since all the significant data flows through the POS system, all the sub-systems on the diagram above have to deal with cardholder's data. Therefore, they all must be protected against determined criminal attackers. Also, the compliance with PCI regulations must be achieved at all retail locations including the back office.

A modern semi-Integrated payment architecture can help to address these challenges.

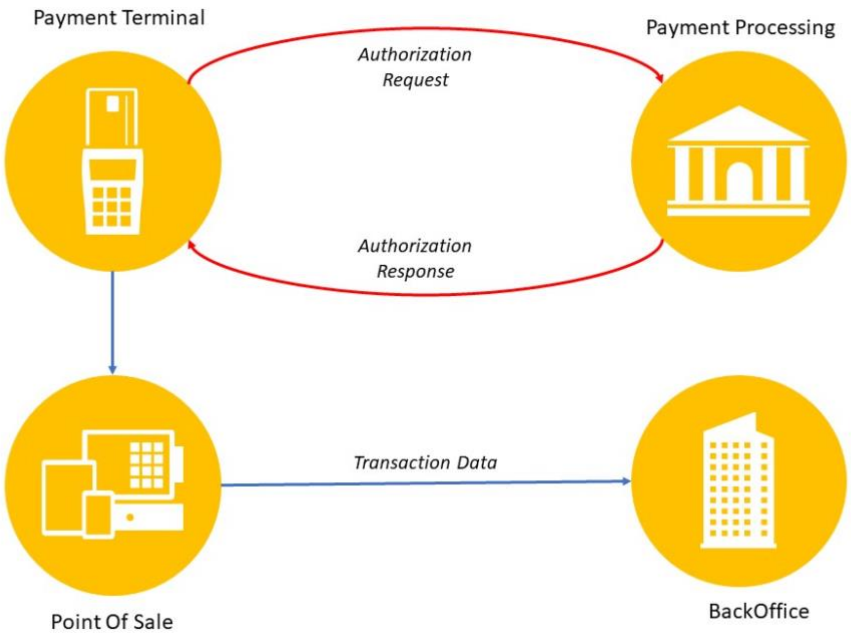


Figure 2-2: Semi-Integrated Payment

In this semi-integrated architecture, the payment terminal is still connected to the POS. However, the communication between them is limited to only non-sensitive commands. In this architecture the payment terminal also has an independent connection to authorization host system. The cardholder data only travels between the payment terminal and the authorization host. As a result, the sensitive payment data never enters the POS system. It is typical that the semi-integrated solution also uses additional payment security technologies such as Point-to-Point Encryption (P2PE) and tokenization.

Such clear separation between the payment sub-system and POS provides greater flexibility to implement different payment solutions. Semi-integrated solutions reduce the scope of PCI compliance and significantly improve security.

2.2 UPOS Device Types

The industry-level scope represents all IoT as related to UPOS that are network connected via the WS-POS standard,[1] or newer UPOS v2 API's.[2]

For device scope consideration there are four identified device types. These device types were considered in determining which requirements are general to the retail industry scope and which are specific to the device scope. The types include devices related to (1) payment or personal

[1] [WS-POS]
[2] [UPOS v2 APIS]

information (e.g., payment device), (2) audit logging and reporting (e.g., printer), (3) locally valuable assets (e.g., cash drawer) and (4) other (e.g., lighting). The examples are highlighted in

Figure 2-3: Device Types at Retail Point of Sale

- Type 1: Payment and/or PII/Identity information related
  - Biometrics
  - Check Scanner
  - Credit Authorization Terminal (CAT)
  - Electronic Value Reader/Writer
  - Individual Recognition *
  - Magnetic Stripe Reader (MSR)
  - Magnetic Ink Character Recognition Reader (MICR)
  - PIN Pad
  - Point Card Reader / Writer
  - RFID Scanner
  - Signature Capture
  - Smart Card Reader / Writer
  - Video Capture Camera *
- Type 2: Audit logging and reporting related
  - Electronic Journal
  - Fiscal Printer
  - Hard Totals
  - POS Printer
- Type 3: Locally valuable assets like cash related

  - Bill Acceptor
  - Bill Dispenser
  - Cash Changer
  - Cash Drawer
  - Coin Acceptor
  - Coin Dispenser
  - Item Dispenser
  - Keylock
- Type 4: All other, local device control related
  - Belt
  - BumpBar
  - Device Monitor *
  - Gate
  - Gesture Control *
  - Graphic Display *
  - Image Scanner
  - Lights
  - Line Display
  - Motion Sensor
  - POS Keyboard
  - POS Power
  - Remote Order Display
  - Scale
  - Scanner (Bar Code Reader)
  - Sound Player *
  - Sound Recorder *
  - Speech Synthesis *
  - Tone Indicator
  - Voice Recognition *

* = new in UPOS 1.16

3 PROFILE TABLES

The following tables add the industry and device scope to the general SMM considerations as appropriate.

Security Program Management				
This practice is critical for the planning and timely provision of security activities, control over the process and results and optimal decision-making procedure for fulfillment of security related demands.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations		**What needs to be done to achieve this level** Plan the resources for security management, communication, training and awareness. Certify fiscal reporting devices, weights and measures. Initiate background checks for newly hired associates. Document system security administration roles and responsibilities. Adhere to local retailer requirements established by cities and states. **Indicators of achievement** Documented plan for security management including communications training and awareness. Fiscal device and weights and measure yearly certification documents. Employee background check results. System administration roles and responsibilities documentation.	**What needs to be done to achieve this level** Incorporate and follow standards relevant to retailers: Data Security Standard (PCI-DSS) applied to network infrastructure Payment Application Data Security Standard (PA-DSS) - applies to POS systems PIN Transaction Security Devices (PTS) - applies to UPOS card devices HIPPA in particular for Pharmacies Develop processes to increase awareness and integrating the following into the program: FTC Start with Security, a Guide for Business The Open Web Application Security Project (OWASP) DOJ Best Practices for Victim Response and Reporting of Cyber Incidents, (DOJ, 2015). Center for Internet Security's "Critical Security Controls for Effective Cyber Defense" The SANS Institute created a list of Top 20	**What needs to be done to achieve this level** PCI Compliant with no compensating controls. Engage with retail community regarding incident sharing, situational awareness, security alerts (e.g., NRF Security Mailer). **Indicators of achievement** Systematic approaches to sharing of information and awareness with the Retail community are in place.

Security Program Management				
		Document detailing how local retailer requirements are being met.	NIST Special Publications, ISO 27002, and the HiTrust Common Security Framework (CSF). EU data protection regulations with GDPR Children's Online Privacy Protection Act (COPPA) Smart Card Alliance document and standards groups (PCI SSC, EMVCo, GlobalPlatform) Global/International Retailer Requirements - Tax, Labor, Digital Sovereignty **Indicators of achievement** Assessment reports and design documents demonstrating conformance of security management practices to the relevant standards	
Industry Scope Considerations		**What needs to be done to achieve this level** Plan the resources for security management, communication, training and awareness. Certify fiscal reporting devices, weights and measures. Initiate background checks for newly hired associates. Document system security administration roles and responsibilities.	**What needs to be done to achieve this level** Incorporate and follow standards relevant to retailers: Data Security Standard (PCI-DSS) applied to network infrastructure Payment Application Data Security Standard (PA-DSS) - applies to POS systems PIN Transaction Security Devices (PTS) - applies to UPOS card devices HIPPA in particular for	**What needs to be done to achieve this level** PCI Compliant with no compensating controls. Engage with retail community regarding incident sharing, situational awareness, security alerts (e.g., NRF Security Mailer). **Indicators of achievement** Systematic approaches to sharing

Security Program Management				
		Adhere to local retailer requirements established by cities and states. **Indicators of achievement** Documented plan for security management including communications training and awareness. Fiscal device and weights and measure yearly certification documents. Employee background check results. System administration roles and responsibilities documentation. Document detailing how local retailer requirements are being met.	Pharmacies Develop processes to increase awareness and integrating the following into the program: FTC Start with Security, a Guide for Business The Open Web Application Security Project (OWASP) DOJ Best Practices for Victim Response and Reporting of Cyber Incidents, (DOJ, 2015). Center for Internet Security's "Critical Security Controls for Effective Cyber Defense" The SANS Institute created a list of Top 20 NIST Special Publications, ISO 27002, and the HiTrust Common Security Framework (CSF). EU data protection regulations with GDPR Children's Online Privacy Protection Act (COPPA) Smart Card Alliance document and standards groups (PCI SSC, EMVCo, GlobalPlatform) Global/International Retailer Requirements - Tax, Labor, Digital Sovereignty **Indicators of achievement** Assessment reports and design documents demonstrating conformance of	of information and awareness with the Retail community are in place.

Security Program Management				
			security management practices to the relevant standards	

Table 3-1: Security Program Management

3.1 COMPLIANCE MANAGEMENT PRACTICE

Compliance Management				
This practice is necessary when strict requirements for compliance with evolving security standards is needed.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations		**What needs to be done to achieve this level** Ensure compliance with Internal privacy and data security requirements for the business. **Indicators of achievement** Internal privacy and data security compliance are integrated as part of overall compliance program.	**What needs to be done to achieve this level** Consider regulatory guidelines relevant to retailers including: Data Security Standard (PCI-DSS), Payment Application Data Security Standard (PA-DSS, 2010), and the PIN Transaction Security Devices (PTS, 2010). FTC Start with Security, a Guide for Business The Open Web Application Security Project (OWASP DOJ Best Practices for Victim Response and Reporting of Cyber Incidents, (DOJ, 2015). Consider best practices and incident next steps including: Center for Internet Security's "Critical Security Controls for Effective Cyber Defense" The SANS Institute list	

Compliance Management				
			of Top 20 HIPPA NIST Special Publications, ISO 27002, and the HiTrust Common Security Framework (CSF). GDPR Children's Online Privacy Protection Act (COPPA) Smart Card Alliance document and standards groups (PCI SSC, EMVCo, GlobalPlatform) Adhere to local retailer requirements established by countries, states, and cities. Government compliance to regulation of weights and measures. European compliance for Fiscal reporting. **Indicators of achievement** Complete set of documents verifying and assuring compliance with security-related requirements. Valid certificates and other supporting evidence.	
Device Scope Considerations			Ensure compliance with PIN Transaction Security Devices (PTS, 2010). Adhere to European fiscal reporting retailer requirements established by countries, states, and cities.	

Compliance Management				
			Government compliance to regulation of weights and measures. Adhere to HIPAA for PII and data verification at POS in retail pharmacies. **Indicators of achievement** Complete set of documents verifying and assuring compliance with security-related requirements. Valid certificates and other supporting evidence.	

Table 3-2: Compliance Management

3.2 THREAT MODELING PRACTICE

Threat Modeling				
This practice aims at both revealing known and specific factors that may place the functioning of a given system at risk and accurately describing these factors.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations		**What needs to be done to achieve this level** Establish at least weak Identity practices for Managers and Clerks to POS devices Use the Open Web Application Security Project (OWASP) and SANS institute Top 20 threat lists to identify threats. Consider barcode hacks using more resistant technology	**What needs to be done to achieve this level** Consider threats related to offline situations that increase significance of local vulnerabilities and fraud. Consider threats from risk of short well-identified credit card information and encryption key management. Consider threats to	**What needs to be done to achieve this level** Consider markdown barcode hacks and unauthorized price modifications for promotions. Cultivate a list of POS Malware (e.g., BlackPOS) and vulnerabilities Threats are shared with the retailer active threat community.

Threat Modeling				
		such as RFID. Consider threats from theft of IoT devices such as shelf labels, PDAs, barcode scanners). **Indicators of achievement** A vulnerability assessment report is available and identifies common and typical threats valid for the identified retail use cases.	Transaction logs if they contain credit card and customer information. Consider threats related to the potential loss, unauthorized access or use, destruction, modification or unintended or inappropriate disclosure of personally identifiable information (PII). Consider threats from electronic jammers that can disrupt store operations (e.g., shelf labels and mobile checkout) **Indicators of achievement** A vulnerability assessment report is available and identifies the specific threats for the identified retail use cases. Use of audit records demonstrating secure management of personally identifiable information (PII).	**What needs to be done to achieve this level** Technologies such as RFID deployed. Lists of vulnerabilities are managed and shared with the retail community.
Device Scope Considerations		**What needs to be done to achieve this level** Consider threats from theft scenarios including the printing of barcode/QR codes placed on packaging and barcodes that interfere with proper reader operations.	**What needs to be done to achieve this level** Consider threats related to PCI such as credit card skimming and MSR overlay, RAM scraping attacks, physical POS device attacks and introduction of mobile devices. Also consider	**What needs to be done to achieve this level** Cultivate a list of POS Malware (e.g., BlackPOS) and vulnerabilities. **Indicators of achievement** A vulnerability

Threat Modeling				
		Indicators of achievement A vulnerability assessment report is available and identifies mitigation for these barcode and device threats.	nefarious Bluetooth beacons infections and NFS or wireless interception. **Indicators of achievement** A vulnerability assessment report is available and identifies mitigation for these threats.	assessment report is available and identifies mitigation for these threats.

Table 3-3: Threat Modeling

3.3 RISK ATTITUDE PRACTICE

Risk Attitude				
This practice enables an organization to establish a strategy for dealing with risks according to risk management policy, including conditions for acceptance, avoidance, evaluation, mitigation and transference.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations			**What needs to be done to achieve this level** Consider impact from the June 2015 Federal Trade Commission "Start with Security" guidance. The April 2015 U.S. Department of Justice's Best Practices for Victim Response and Reporting of Cyber Incidents ("DOJ Best Practice Guidance"), and Version 6.0 of the Council on Cybersecurity Critical Controls for Effective Cyber Defense, released in October 2015 Consider the NIST Cybersecurity Framework Version 1.1 Consider the mapping between SMM and NIST framework. **Indicators of achievement** Risk-handling strategy describing avoidance, mitigation, acceptance, and transference criteria with appropriate actions.	

Risk Attitude				
Device Scope Considerations		Consider 3rd party risk for printer software libraries that enable support for many printers.		

Table 3-4: Risk Attitude

3.4 PRODUCT SUPPLY CHAIN RISK MANAGEMENT PRACTICE

Product Supply Chain Risk Management				
This practice addresses the need to enable trust for contractors or suppliers and to ascertain the absence of hidden threat sources, ensuring the integrity of the supply chain.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations		**What needs to be done to achieve this level** Deploy signed firmware images with hash checking. **Indicators of achievement** Procedures for the signed images deployment are documented.		
Device Scope Considerations				

Table 3-5: Product Supply Chain Risk Management

3.5 SERVICES THIRD-PARTY DEPENDENCIES MANAGEMENT PRACTICE

Services Third-Party Dependencies Management				
This practice addresses the need to enable trust for partners and other third parties. The ability to have assurance of the trust of third parties requires understanding of the business and trust infrastructure and possible hidden threat sources.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations		**What needs to be**	**What needs to be**	

Services Third-Party Dependencies Management				
		done to achieve this level Include KPIs in SLAs related to incident response, and reward programs managed by 3rd parties (such as early identification prior to checkout). Ensure adherence to Weights and Measures calibration. **Indicators of achievement** SLAs, KPIs are defined per established contracts.	**done to achieve this level** Ensure third parties conduct vulnerability assessments, are PCI compliant, and follow government regulations for weights and measures. **Indicators of achievement** Third-party assessment reports are provided for these processes and regulations.	
Device Scope Considerations		**What needs to be done to achieve this level** Ensure adherence to Weights and Measures calibration. Services for Video and Audio recognition analysis. **Indicators of achievement** SLAs, KPIs are defined per established contracts.	**What needs to be done to achieve this level** Ensure third parties perform device software/firmware patching for security vulnerabilities - required for PCI Compliance Monitor service providers' PCI DSS compliance status at least annually (PCI-DSS). **Indicators of achievement** Third-party assessment reports are provided for these processes and regulations.	

Table 3-6: Services Third-Party Dependencies Management

3.6 ESTABLISHING AND MAINTAINING IDENTITIES PRACTICE

Establishing and Maintaining Identities				
This practice helps to identify and constrain who may access the system and their privileges.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations	**What needs to be done to achieve this level** Ensure General Device identification is used connected to POS with Device manager. Basic store identifiers and static names and passwords are typically used. **Indicators of achievement** POS devices and stores are identified.	**What needs to be done to achieve this level** Use shared Secret PINs when attaching and connecting devices (e.g., Bluetooth). There is a Strong Password Policy and no shared passwords for clerks/managers. Use Passcards instead of simple PINs. **Indicators of achievement** PIN and password processes are documented.	**What needs to be done to achieve this level** Use UPOS to Device identification (OpenAuth "OAuth") Use OpenID Connect standards. Authenticate users and sessions. Use secure device onboarding and associated standards (e.g., FIDO) and place devices in secure segment with POS system. 802.1x standard based. Use PKI for device certificates. Identification should be used if WiFi networks exposed. **Indicators of achievement** The appropriate standards are used and documented. Centralized identity is used if WiFi exposed. WiFi access should be on a separate network than POS devices.	**What needs to be done to achieve this level** Per-transaction level of re-authentication for every device communication call/message. Short Expiration date for authentication tokens (5 events, or 60 seconds) Notification of revoked certificates/tokens. DDOS protection to ensure reliability of centralized authentications services. Highly reliable WAN infrastructure to ensure connectivity. **Indicators of achievement** The mechanisms are well established and implemented.
Device Scope Considerations	**What needs to be done to achieve this level** Identity is not	**What needs to be done to achieve this level** Use shared Secret PIN	**What needs to be done to achieve this level** Retailers require	

Establishing and Maintaining Identities				
	required for directly connected devices and for devices with no financial impact or those that do not handle privileged or private information. **Indicators of achievement** These devices may or may not have unique identities.	when attaching and connecting devices (e.g., Bluetooth) **Indicators of achievement** Connecting devices use a shared secret PIN.	offline functionality for a determined period of time (1-day) - for business critical **Indicators of achievement** Offline capabilities are deployed and well documented.	

Table 3-7: Establishing and Maintaining Identities

3.7 ACCESS CONTROL PRACTICE

Access Control				
This practice's policy and implementation allow a business to limit access to resources to only the specific identities that require access and only at the specific level needed to meet organizational requirements.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations			**What needs to be done to achieve this level** Follow practices for PCI. **Indicators of achievement** PCI use is documented.	
Device Scope Considerations			**What needs to be done to achieve this level** Use PCI for payment related devices. **Indicators of achievement** PCI use is	

Access Control				
			documented.	

Table 3-8: Access Control

3.8 Asset, Change and Configuration Management Practice

Asset, Change and Configuration Management				
This practice constrains the types of changes allowed, when those changes can be made, approval processes and how to handle emergency change scenarios.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations		**What needs to be done to achieve this level** Record and save device component changes. **Indicators of achievement** A log of device component changes exists.	**What needs to be done to achieve this level** Track device component changes and integrate and automate within the device. The change record is tamper-proof (using blockchain or similar). **Indicators of achievement** A log of device component changes exists and available over time.	**What needs to be done to achieve this level** Determine device posture based on components – for example a device that constantly connects and disconnects. **Indicators of achievement** Device monitoring is implemented to track component behavior.
Device Scope Considerations				

Table 3-9: Asset, Change and Configuration Management

3.9 PHYSICAL PROTECTION PRACTICE

Physical Protection				
This practice's policies address the physical security and safety of the premises, its people and its systems to prevent theft and ensure the ongoing safe operation of equipment.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations	**What needs to be**	**What needs to be**	**What needs to be**	**What needs to be**

Physical Protection				
	done to achieve this level Protect equipment minimally using Key locks on doors. Shared PIN or combinations are used. **Indicators of achievement** Key access is managed, and PINs and combinations are documented and distributed to appropriate personnel. Upon personnel departure or role change keys must be returned and locks changed.	**done to achieve this level** Track device component changes through manual logging. Securely attach devices to fixtures (e.g., PIN pad to cash-wrap counter). Devices are tamper-evident seals are visually inspected daily for tampering. Sensors are placed on gates and doors and anti-theft tags are placed on high value, or easily removable, assets. Anti-theft tags are added to store fixtures (shelf tags, PDAs, scanners, etc.) **Indicators of achievement** Tags are found on all relevant devices, and procedures for inspection are documented. Access is disabled upon personnel or role changes and personnel are forced to change passwords and PINs intermittently.	**done to achieve this level** Follow practices for PCI. Track sealed tamper evident seals in a database. Use video surveillance monitoring or access control (or both) to monitor physical access to restricted areas (PCI-DSS). Employees use a unique PIN/Badge based access. **Indicators of achievement** Technology is deployed for video surveillance and tracking of tamper-evident seals.	**done to achieve this level** Use integrated device alarm sensors for covers and doors. Segmented and restricted badge/card access for employees to facility (time/role based). Deploy video Analytics based alarming. **Indicators of achievement** Technology is deployed for video analytics, integrated sensors and badge/card segmentation.
Device Scope Considerations			**What needs to be done to achieve this level** Protect card-reading devices that capture payment card data via	

Physical Protection				
			direct physical interaction with the card from tampering and substitution (PCI-DSS). **Indicators of achievement** PCI use is documented.	

Table 3-10: Physical Protection

3.10 PROTECTION MODEL AND POLICY FOR DATA PRACTICE

Protection Model and Policy for Data				
This practice identifies whether different categories of data exist and considers the specific objectives and rules for data protection.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations		**What needs to be done to achieve this level** Manage PII and sensitive data based on consent, transparency, data minimization, use limitations and consider reuse and retention policies. **Indicators of achievement** Data use policies are documented and followed.	**What needs to be done to achieve this level** Consider regulatory guidelines relevant to retailers including: PCI The Open Web Application Security Project (OWASP) HIPPA GDPR Children's Online Privacy Protection Act (COPPA) Reward program - agreements to early identification prior to checkout (mobile, WiFi, IoT, video analytics, other sensors) Global Rules Engine for Privacy Policies	**What needs to be done to achieve this level** Blacklist and wipe a device when it leaves the premises so it is not useable if re-introduced. **Indicators of achievement** Procedures for device deactivation are documented and followed.

Protection Model and Policy for Data				
			Indicators of achievement Complete set of documents verifying and assuring compliance with security-related requirements.	
Device Scope Considerations		**What needs to be done to achieve this level** Encryption of privileged information such as credit card numbers, credentials and information used to connect to database. Manage keys and keep equipment up to date. **Indicators of achievement** The identified information is encrypted.	**What needs to be done to achieve this level** Follow practices for PCI-DSS **Indicators of achievement** PCI-DSS use is documented.	

Table 3-11: Protection Model and Policy for Data

3.11 IMPLEMENTATION OF DATA PROTECTION PRACTICES PRACTICE

Implementation of Data Protection Practices				
This practice describes the preferred application of data protection mechanisms to address confidentiality, integrity and availability.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations		**What needs to be done to achieve this level** Implement data quality and integrity. Encrypt privileged	**What needs to be done to achieve this level** Consider regulatory guidelines and associated	

Implementation of Data Protection Practices				
		information such as credit card numbers. Deploy practices for key management. Deploy signed firmware images with hash checking. **Indicators of achievement** Procedures for data quality and integrity and key management are documented. Procedures for the signed images deployment are documented.	frameworks relevant to retailers including: PCI (for payment systems), HIPPA (for pharmacies and HR/employee data), HiTrust Common Security Framework (for HIPPA). Follow general best practices and PCI-DSS related to minimal data collection and minimal retention periods. Follow Quarterly Process to identify and securely delete cardholder data held beyond retention period (PCI-DSS) Ensure reward programs managed by 3rd parties (such as early identification prior to checkout) follow the required regulations. **Indicators of achievement** Procedures are documented and certifications are provided for internal and 3rd party compliance.	
Device Scope Considerations			**What needs to be done to achieve this level** Follow PCI practices from PCI-DSS, PA-DSS, PTS. **Indicators of achievement**	

Implementation of Data Protection Practices				
			PC practice use (PCI-DSS, PA-DSS, PTS) is documented.	

Table 3-12: Implementation of Data Protection Practices

3.12 VULNERABILITY ASSESSMENT PRACTICE

Vulnerability Assessment				
This practice helps identify vulnerabilities, determine the risk that each vulnerability places on the organization and develop a prioritized remediation plan.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations		**What needs to be done to achieve this level** Deploy signed firmware images with hash checking. **Indicators of achievement** Procedures for the signed images deployment are documented.	**What needs to be done to achieve this level** Track device component changes. logging **Indicators of achievement** A log exists of component changes.	
Device Scope Considerations				

Table 3-13: Vulnerability Assessment

3.13 PATCH MANAGEMENT PRACTICE

There are no retail-specific system- or device-scope considerations for the patch management practice.

Patch Management				
This practice clarifies when and how frequently to apply the software patches, sets up procedures for emergency patches and proposes additional mitigations in the instance of constrained access to the system or other issues involved with patching.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations				

Patch Management				
Device Scope Considerations				

Table 3-14: Patch Management

3.14 MONITORING PRACTICE

Monitoring Practice				
This practice is used to monitor the state of the system, identify anomalies and aid in dispute resolution.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations		**What needs to be done to achieve this level** Deploy signed firmware images with hash checking. **Indicators of achievement** Procedures for the signed images deployment are documented.	**What needs to be done to achieve this level** Follow practices for PCI Review on daily basis logs of critical system components, those that perform security functions, security event logs, and logs of system components that store, process, or transmit Cardholder Data and/or Sensitive Authentication Data (PCI-DSS). Include software and applications in log-monitoring processes. **Indicators of achievement** Processes are documented.	
Device Scope Considerations			Review logs of system components that store, process, or transmit Cardholder Data or Sensitive Authentication Data (PCI-DSS) daily. Periodically inspect card-reading device	

Monitoring Practice				
			surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). (PCI-DSS). Similarly, for reviewing fiscal devices (e.g., fiscal printers).	

Table 3-15: Monitoring Practice

3.15 SITUATIONAL AWARENESS AND INFORMATION SHARING PRACTICE

Situational Awareness and Information Sharing				
This practice helps organizations be better prepared to respond to threats. Sharing threat information keeps systems up to date.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations			**What needs to be done to achieve this level** Follow practices for sharing breach information from GDPR and other regulations. **Indicators of achievement** Processes are documented.	
Device Scope Considerations				

Table 3-16: Situational Awareness and Information Sharing Practice

3.16 Event Detection and Response Plan Practice

Event Detection and Response Plan				
This practice defines what a security event is and how to detect and assign events for investigation, escalate them as needed and respond appropriately. It should also include a communications plan for sharing information appropriately and in a timely manner with stakeholders.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations			**What needs to be done to achieve this level** Follow practices for PCI.	
Device Scope Considerations			Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data; All actions taken by any individual with root or administrative privileges and others noted in (PCI-DSS).	

Table 3-17: Event Detection and Response Plan

3.17 Remediation, Recovery and Continuity of Operations Practice

Remediation, Recovery and Continuity of Operations				
This practice is a combination of technical redundancies whereby trained staff and business continuity policy help an organization recover quickly from an event to expedite returning to business as usual.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Industry Scope Considerations			**What needs to be done to achieve this level** Retailers require offline functionality for a determined period of time (1-day) for business-critical	**What needs to be done to achieve this level** Fallback gracefully to selected (lower) level of security when offline.

Remediation, Recovery and Continuity of Operations				
			functionality. **Indicators of achievement** Offline capabilities are deployed and well documented.	**Indicators of achievement** Process for fallback to a selected level of security when offline are documented and implemented.
Device Scope Considerations				

Table 3-18: Remediation, Recovery and Continuity of Operations

Annex A ACRONYMS

CAPEC	Common Attack Pattern Enumeration and Classification
IIC	Industrial Internet Consortium
IIRA	Industrial Internet Reference Architecture
IISF	Industrial Internet Security Framework
IoT	Internet of Things
IT	Information Technology
OT	Operational Technology
OWASP	Open Web Application Security Project

Annex B DEFINITIONS

The following terms, specific to the context of the SMM, are defined here:

Security Level: Security Level is a measure of confidence that the system is free of vulnerabilities and functions in an intended manner.

Security Maturity: Security Maturity is a measure of an understanding of the current Security Level, its necessity, benefits, and cost of its support.

Domain: Domains are the strategic level priorities for security maturity. In the SMM, there are three domains: Governance, Enablement, and Hardening.

Sub Domain: Sub Domains refer to the basic means to address a domain at the planning level. Each domain currently defines three sub domains.

Security Practice: Practices are the typical activities performed for a given sub domain; they provide the deeper detail necessary for planning. Each sub domain has a set of practices.

Comprehensiveness: The model defines comprehensiveness levels as a measure of the Comprehensiveness, consistent, and highly assured implementation of measures supporting the security maturity domain, sub domain or practice.

Scope: The model defines scope as a measure for the customized, technically appropriate approach to the implementation of measures supporting the security maturity domain, sub domain or practice, and fitting the needs and constraints of IoT sector or system.

Security Maturity Target: The Security Maturity Target is the desired "end state" Security Maturity for an organization or system. The Security Maturity Target can apply to a new system under development or an existing brownfield system. The Security Maturity Target is determined based upon the business objectives of the organization or group.

Industrial Internet Consortium: (IIC) an open membership, international not-for-profit consortium that is setting the architectural framework and direction for the Industrial Internet. Founded by AT&T, Cisco, GE, IBM and Intel in March 2014, the consortium's mission is to coordinate vast ecosystem initiatives to connect and integrate objects with people, processes and data using common architectures, interoperability and open standards.

Annex C REFERENCES

[ARTS-CYBERP2015] ARTS Cybersecurity Primer, December 2015, retrieved 2020-02-25
https://www.omg.org/cgi-bin/doc?retail/2019-02-06

[ARTS-DATAP2015] ARTS Data Privacy Primer, December 2015, retrieved 2020-02-25
https://www.omg.org/cgi-bin/doc?retail/2019-02-07

[ARTS-DATA2017] ARTS Privacy and Security Data, January 2017, retrieved 2020-02-25
https://www.omg.org/cgi-bin/doc?retail/2019-02-08

[IEC-62443-33] IEC 62443-3-3:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels, 2013
https://webstore.iec.ch/publication/7033

[IIC-IIRA2019] **Industrial Internet Consortium**: The Industrial Internet, Volume G1: Reference Architecture Technical Report, version 1.9, 2019-06-19, retrieved 2020-04-29
https://www.iiconsortium.org/IIRA.htm

[IIC-IIV2019] **Industrial Internet Consortium**: The Industrial Internet, Volume G8: Vocabulary Technical Report, version 2.2, 2019-11-06, retrieved 2020-01-24
https://www.iiconsortium.org/vocab/index.htm

[IIC-IISF2016] **Industrial Internet Consortium**: The Industrial Internet of Things Volume G4: Security Framework Version 1.0, 2016-September-26
http://www.iiconsortium.org/IISF.htm

[IIC-SMMD2020] **Industrial Internet Consortium**: IoT Security Maturity Model: Description and Intended Use, version 1.2, 2020-05-05, retrieved 2020-05-05
https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_V1.2.pdf

[IIC-SMMP2020] **Industrial Internet Consortium**: IoT Security Maturity Model: Practitioner's Guide, Version 1.2, 2020-05-05, retrieved 202-05-05
https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf

[PCI-DSS] Payment Card Industry Security Standards Council. (2018). Payment Card Industry Data Security Standard. Version 3.2.1. Retrieved from
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

[PCI-PADSS] Payment Card Industry Security Standards Council. (2018). Payment Card Industry Payment Application Data Security Standard. Version 3.0. November 2013. Retrieved 19 May 2020 from
https://www.pcisecuritystandards.org/minisite/en/docs/PA-DSS_v3.pdf

[PCI-PTS] Payment Card Industry Security Standards Council. (2018). Payment Card Industry PIN Transaction Security (PTS) Point of Interaction (POI). Version 4.0. June 2013. Retrieved 19 May 2020 from
https://www.pcisecuritystandards.org/documents/PCI_PTS_POI_SRs_v4_Final.pdf

[PCI-MON] Information Supplement: Effective Daily Log Monitoring, May 2016. PCI Security Standards Council.
https://www.pcisecuritystandards.org/documents/Effective-Daily-Log-Monitoring-Guidance.pdf

[RFC 2119] S. Bradner. IETF. "Key Words for Use in RFCs To Indicate Requirement Levels." March 1997. Best Current Practice. *https://ietf.org/rfc/rfc2119.txt*

Annex D AUTHORS AND LEGAL NOTICE

This document is a joint work product of the OMG Retail Task group chaired by Andy Mattice (Lexmark), Leonid Rubhakin (Aptos) and the Industrial Internet Consortium Security Applicability Task Group, co-chaired by Ron Zahavi (Microsoft) and Jim Clardy (NetFoundry).

Authors: The following persons contributed substantial written content to this document: Frederick Hirsch (Upham Security), Andy Mattice (Lexmark), Bart McGlothin (Cisco), Leonid Rubhakin (Aptos), Ekaterina Rudina (Kaspersky), and Ron Zahavi (Microsoft).

Technical Editor: Stephen Mellor (IIC staff) oversaw the process of organizing the contributions of the above Authors and Contributors into an integrated document.
