

ANALYSIS:

Store Systems Security Preparing for the Paradigm Shift

Analysts

Jerry Sheldon, Greg Buzek

Publication Date: August 26, 2013



Sponsored By:



HARD DATA, SMART DECISIONS

Phone +1 615-591-2955 • www.ihlservices.com

IHL Group License and Fair Use Agreement

All of IHL Group's generally available research products and databases are electronic licenses and can be shared freely within the purchasing organization and wholly owned subsidiaries. We only ask that this information not be shared with partners or others outside the purchasing company without authorization from IHL Group. The license does not extend to joint ventures or other partnerships. If the relationship is not a wholly owned subsidiary, then both parties would need a license.

Practically, this implies the following:

1. The purchasing company can use the reports worldwide internally as long as the international organizations are wholly owned subsidiaries of the purchasing company.
2. The research reports and databases cannot be distributed in whole or in part to partners or customers without express written approval from IHL Group.
3. The purchasing company may quote components of the data (limited use) in presentations to customers such as specific charts. This is limited to percentage components, not individual unit information. Unit data cannot be shared externally without express written approval from IHL Group. All references to the data in presentations should include credit to IHL Group for the data.
4. The purchasing company can reference qualitative quotes in printed material with written approval from IHL Group.
5. All requests requiring written approval should be submitted to ihl@ihlservices.com and will be reviewed within one business day.

For any questions regarding this policy, please contact us at 615-591-2955 or email us at ihl@ihlservices.com

About IHL Group

Who We Are

IHL Group is a global research and advisory firm specializing in technologies for the retail and hospitality industries. The company, based in Franklin, Tenn., generates timely data reports, offers advisory services and serves as the leading retail technology spokesperson for industry and vendor events.

What We Do

IHL provides customized business intelligence for retailers and retail technology vendors, with particular expertise in supply chain and store level systems. Our customers are retailers and retail technology providers who want to better understand what is going on in the overall technology market, or wish to identify specific equipment needs for the retail market.

When We Started

Greg Buzek served as Product Development Manager for two Fortune 500 retail technology suppliers for 6 years. Faced with making recommendations to senior management with spotty reports stuffed with technical jargon and unsubstantiated data, in 1996 he left to form IHL Group as an arms length consulting firm that delivers exacting research to corporate managers.

How We Work

Reliable market analysis is essential for corporations to accelerate revenue and expand their market share. Most research providers do not disclose data sources or statistically defend the validity of their assumptions. We do. We disclose in precise detail exactly how and why we reached our conclusions so that our customers can be comfortable with the data they are using.

What We Know

Our associates and advisors have over 100 years combined years of retail technology experience. Our associates have worked as product managers, sales representatives and executives in the retail market. We have the relationships, tools, and experience to meet your research and consulting needs.

List of Figures

Figure 1 - How many of each of the following devices, on average per store by revenue.	7
Figure 2 - Level of concern by potential threat categories.....	9
Figure 3 - Level of influence by functional responsibility, on security and buying decisions for in-store systems.	10
Figure 4 - Level of influence by functional responsibility, on security and buying decisions for in-store systems, for those companies where the CIO provides only some, not significant input.....	11
Figure 5 - Security position on core POS (HW + O/S) by segments.....	12
Figure 6 - Security position on core POS (HW + O/S) by revenue.	12
Figure 7 - Security position on core POS SW by revenue.	14
Figure 8 - Internal processes & effectiveness in managing security & compliance on POS systems (managing patch/security updates).....	15
Figure 9 - Estimate of the total (HW+SW) yearly investment in POS security as a percent of what you pay for ongoing POS hardware and software license maintenance.....	16
Figure 10 - Estimate the total (HW+SW) yearly investment in POS security as a percent of what you pay for ongoing POS hardware and software license maintenance by revenue.....	17
Figure 11 - Respondents by Segment.....	18
Figure 12 - Respondents by Revenue.....	18
Figure 13 - Respondents by Executive Responsibility.....	19

Executive Summary:

In early 2013, IHL Group and McAfee conducted an anonymous survey of senior retail and hospitality executives within the North American marketplace. The Survey specifically targeted executives with an understanding and oversight into their respective company's security strategy as well as the approaches used to secure key store transactional systems. We've consolidated the results, highlighted some important observations, and pointed out several helpful takeaways.

Key Findings:

- Without adequate controls to manage store system variability or a solid plan to address security at the store level taking into consideration overall device management as an ecosystem—retailers can expect security cost to continue to increase rapidly. While IT is constantly evolving, security must evolve, and often times much more rapidly than the devices they are tasked with protecting. The ability to tightly manage the enterprise is a big driver in managing security and controlling costs.
- Security confidence can be closely tied to the device variability within the store. As we see an increase in type of devices, even within the POS device category, increasing the number of devices is a key driver around introducing significant complication around the ability to secure the store environment.
- In Tier I, we see an equal percentage of retailers using a whitelisting approach as compared to antivirus. In those with over \$5 billion in revenue, the difference between the two approaches widens significantly, with more choosing a whitelist strategy compared to the antivirus strategy. This data clearly suggests an ongoing strategy change around securing POS systems. When we consider the drivers section and Figure 2, we see a strong correlation between security concerns and strategies for addressing those concerns.

Our survey results found that PCI compliance was the first concern with respect to POS systems and potential vulnerabilities. The second concern was the category “undefined”, meaning, retailers are unsure of what concerns them, only that they know they should be concerned about something. Beyond these results, we will further examine the following questions around store systems security:

- Are today's POS systems achieving their desired security level?
- What are the key drivers and concern that drive overall security strategy?
- How are retailers marrying the security approach for POS software and hardware to create overall system security?
- What is the current level of satisfaction with POS store systems providers?
- What are retailers spending on securing POS systems and what is the rate of change in recent years?
- How do security approaches vary by size and type of retailer?
- Who are the key organizational influencers with regard to security strategy and where do Qualified Security Assessors (QSAs) fit?

Introduction:

Much has been chronicled regarding the recent changes to the retail environment. All you have to do is step into a store today and, without a doubt, things are vastly different than just a few years ago. The proliferation of devices in the store continues at an astounding pace, primarily driven by the mobile revolution. While those in the industry may refer to multi-channel or omni-channel as the more popular terms for this new shopping paradigm, to the consumer, the discussion of channels is mostly a foreign concept.

Consumers are only looking for one thing—a consistent shopping experience. This could be from a variety of devices or from a range of locations. The consumer just wants to be able to buy anywhere, fulfill anywhere, and return anywhere. On the surface, the concept of a uniform shopping experience may seem fairly simple and straightforward, but the underlying IT systems that must function together and share information results in mindboggling complexity. The complexity is exacerbated by the age and interconnectivity of the IT systems that must function together along with the data that they share. The vast majority of this complexity converges and is focused on what is happening in the store, and the underlying systems that must work correctly both within the store and within the supply chain to result in a seamless shopping experience for the consumer.

Securing those systems within the store has always been a challenge, with store data breaches long preceding the mobile revolution. With the introduction of mobile devices within the store, two significant events have been thrust to the forefront: The increased sharing of information among more and more types of devices (with either LAN or wireless connections), and the need to be able to share information wirelessly within the store. Plus, there's the sophistication of the criminal element looking to compromise systems, along with ever evolving PCI compliance requirements. All this combined is a headache for anyone looking to support the customer while at the same time maintaining the security of the enterprise. These headaches are quantifiable as well, as the increase in devices, and the bolstering or addition of wireless infrastructure adds specific requirement to secure those devices. And as requirements increase, costs are sure to follow.

This study seeks to examine the current state of store security, how the store and the store's transactional IT systems are secured, the key challenges faced, along with providing some recommendations for best practices for our readers that share these challenges. We will look at how the increasing effort to provide security and compliance of older systems decreases previously derived and expected device life spans.

So, just how varied are the store environments today? Within the scope of our survey, we chose to look at some of the key store systems, both established and emerging technologies.

	Self-Checkout	Mobile POS	Digital Signage	Information Kiosk	Transactional Kiosk	POS	Total Devices
Over \$25 Billion	2.19	0.94	0.75	1.56	0.56	13.06	19.06
\$10-25 Billion	1.83	2.08	2.67	2.67	2.25	9.42	20.92
\$5-10 Billion	0.83	0.17	2.08	1.83	3.33	7.42	15.66
\$1-5 Billion	0.65	0.73	0.62	0.62	0.73	5.92	9.27
\$500 Million – 1 Billion	0.00	0.18	0.18	0.32	0.09	4.09	4.86
\$250-500 Million	0.00	0.07	1.37	0.07	1.37	3.07	5.95
Under \$250 Million	0.00	0.42	1.67	0.33	0.33	5.33	8.08
Average	0.64	0.55	1.14	0.82	1.08	6.24	10.47

Figure 1 - How many of each of the following devices, on average per store by revenue.

In Figure 1, we see a clear trend with an increasing the number of average devices per store as the chain revenue increases, while in the same noting there are 2-3x more devices represented in the store for those chains above \$5 billion in revenue. Not only do these chains use the largest number and the most diverse technology, but because of their size, they also tend to drive technology trends.

Paramount among new technology is mobile POS (herein we define mobile POS as a transactional based device capable of completing a purchase transaction that is wirelessly connected, that may or may not have all of the functionality of the base POS system). As you will note from the Figure 1, use of mobile POS is found primarily in those retailers above \$1 billion in revenue. But for retailers not currently using it, a great many in Tier II and below are currently running active pilots. The use of mobility is worth noting in that it is one of the most disruptive technologies that we have seen in the last five-plus years. It is disruptive not only for the impact it has on the store shopping environment, but also for the impact it has on the store infrastructure to back office systems and essentially every point in between. Additionally, from a security standpoint, it is significantly impacting the store. Previously, critical data flowed between wired systems. Now we have both greater interconnectivity required between store and back office systems driven by mobility, but also sensitive data is being shared wirelessly. This creates new opportunities and entry points for nefarious activities and an additional burden for security coverage.

Every change in these complex environments brings with it the very real chance for the introduction of unintentional vulnerabilities and possibility for rogue access or code to infiltrate and obtain critical data. The nuts and bolts that go into protecting the enterprise make not only for a challenging task, but also interesting and relevant subject matter that today's retailers seek to understand better. This is obvious from the respondents at the largest retailers who indicated that they are now using whitelisting as a key strategy for securing their POS systems. We will investigate this, along with other key insights as we explore this subject.

Survey Respondents:

In February of 2013, IHL Group surveyed a group of 66 respondents from a broad range of retail and hospitality executives in North America. Loosely speaking, respondents fell into three macro-groupings: Hospitality, General Retail, and Fast Moving Commodities. The concentration of our survey respondents maps pretty closely to the numbers provided by the commerce departments of the US¹ and Canada²: Hospitality (24%), General Retail (36%), and Fast Moving Commodities (40%). Based on these demographics, we think the survey results closely represent the overall retail and hospitality community footprint within North America. More detail about survey respondents can be found near the end of this report.

Security Drivers:

Before looking at what retailers are doing to secure their enterprises, it is first important to look at what they are protecting against. These will act to frame the context of our discussion around protection strategies. Loosely speaking, the key drivers fall into one of these broad categories:

- Compliance
- Security Approaches
- Tampering
- Unidentified concerns

Compliance can mean anything from internal security procedures, requirements at a municipality, city, state or even country level up to PCI compliance. Compliance covers many different facets as well. While we often think of compliance within the realm of protecting credit card data, within retail, we see it extend to personal information as well such as health care data. The penalty for breach of any of these areas can come at an extensive financial cost to a retailer. But more importantly, it can mean loss of trust and brand reputation.

Being able to keep up with operating system patching for vulnerabilities, keep relevant malware protection, and adherence to the best practices for file integrity monitoring and the process for authorizing application and system changes is a necessity for PCI-DSS. But we wanted to see how these components ranked individually as a concern/effort for retailers.

Tampering can take a variety of forms as shown in Figure 2 from employee, the customer, to third-party maintenance providers.

The final category we include is “Unidentified Concern.” This goes far beyond a security catch-all option or “Others” category often included as part of the survey process. Our survey results validate this concern as well as “Unidentified Concern” ranked second, only to PCI compliance, as the second highest concern that our

¹ US Economic Census, <http://www.census.gov/econ/census/>

² Statistics Canada, <http://www.statcan.gc.ca/start-debut-eng.html>

respondents identified with respect to their POS systems. Year after year in surveys done by IHL Group³, we find PCI compliance to be a foremost concern in the eyes of retailers with regard to their key store challenges.

Curiously enough, as we surveyed respondents on the age of POS systems, we thought there might be an interrelationship between the age of the systems and evolving concerns on securing the POS. There was no such relationship. As a group, we follow the POS industry closely and see the constantly evolving nature of development in hardware, operating systems, and software. Since there was no difference by age, we were lead to conclude that while there are advancements, system developers continue to be challenged in making significant headway against their criminal adversaries.

While we will speak on this further in the section covering security approaches, it should be noted here that there are two key software approaches for securing POS systems: Antivirus (essentially blacklisting) and whitelisting software. While initial approaches to securing computer systems focused on the common antivirus approach, as we will cover later, whitelisting is an increasingly more effective approach against the key concerns noted in these results, especially when considering the five most highly rated concerns shown in Figure 2.

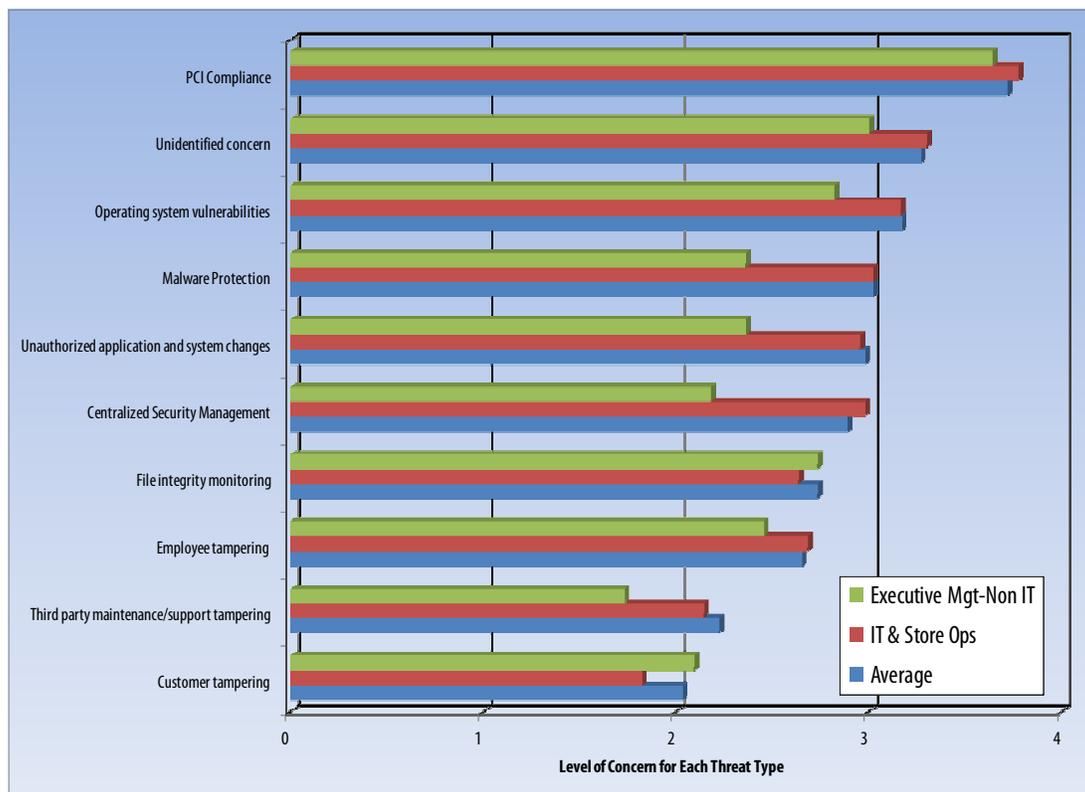


Figure 2 - Level of concern by potential threat categories.

³ 10th Annual Store Systems Study - Mobility Meets Retail's Big Data, http://www.ihlservices.com/ihl/product_detail.cfm?page=Store%20Automation&ProductID=79

In dissecting the results of this survey, we thought it would be insightful to consider the differing respondent populations and the overall security concerns at the POS from those in Non-IT Executive management and those in IT and Store Operations responsibilities. Almost universally, we see that in every category of concern, IT has a higher degree of concern than non-IT. We see the biggest differences in Centralized Security Management (37%), Malware Protection (28%), and Unauthorized application and system changes (25%).

While non-IT management no doubt has a great appreciation for security, those on the front line of defense and who on a daily basis address these concerns, have a heightened awareness that somehow has not been communicated to the broader executive management ranks. By contrast, the difference between the two groups around awareness of PCI compliance is essentially nothing—an area that has gotten a great deal of publicity and attention. Here we offer that the data suggests an increased opportunity, even need, for better communication and dialogue around security approaches and their effectiveness in these complex environments.

Organization Influencers:

As we look further into organizational structure, we now turn our attention to those in the organization that influence and impact security decisions. In our survey we asked the following question: “Each of the following can influence security & buying decisions for in-store systems. Please rate the influence of each within your organization?” Results are presented in Figure 3.

	None	Some	Significant
CISO (Chief Information Security Officer)	22%	37%	41%
Loss Prevention	20%	66%	14%
CIO/CTO	0%	25%	75%
Store Operations	16%	47%	37%
QSA (Qualified Security Assessors)	37%	41%	22%
3 rd Party Integrators	50%	50%	0%
Compliance officer	31%	49%	20%

Figure 3 - Level of influence by functional responsibility, on security and buying decisions for in-store systems.

As one might imagine, the actual influencers are quite varied, with many functional areas providing feedback. The overwhelming functional area with significant influence is that of the CIO/CTO. We found that in 75% of all companies the CIO/CTO provides significant input.

In the 25% of those companies that noted the CIO/CTO only provided some input, we thought it would be insightful to see how responsibility shifted. These results are shown in Figure 4. Those with the most significant input were the CISO (40%) and QSA (43%). Interestingly, the CISO input stays about the same as shown in Figure 3, but the QSA’s role in providing significant input almost doubles from 22% to 43%. In the

same scenario, significant Store Operations input decreases from 37% to 27%. The net impact is a greater propensity of many influencers providing some input.

	None	Some	Significant
CISO (Chief Information Security Officer)	7%	53%	40%
Loss Prevention	7%	71%	21%
Store Operations	13%	60%	27%
QSA (Qualified Security Assessors)	14%	43%	43%
3 rd Party Integrators	43%	57%	0%
Compliance officer	13%	60%	27%

Figure 4 - Level of influence by functional responsibility, on security and buying decisions for in-store systems, for those companies where the CIO provides only some, not significant input.

Looking at the overall results (Figure 3) we see that beyond the CIO/CTO providing significant input, CISO (41%) and Store Operations (37%) do in many cases as well. Ultimate security responsibility happens at the highest level of the organization and these results reflect that is the way today's retailers are managed. Of course, there's also a healthy amount of input from Store Operations. This group is on the front lines, and in many cases, most intimately understands store architecture concerns. Within the context of our earlier discussion around the differences in concern by responsibility, Store Operations reported a heightened vulnerability concern overall, yet they are not as influential with regards to the ultimate security decisions taking place in the store.

As we look at the data by tier, we see that the CISO's input becomes more significant the smaller the retailer, while the CIO/CTO's influence was found to be significant across the board. Similarly to the CISO, we found that Store Operations input is most significant (52% reporting such) among Tier III/IV retailers compared to less than 30% for Tier I and II. Trends for QSA, 3rd Party Integrators and Compliance officers were inconclusive by tier, but generally speaking, the variability was within sampling error with no trends identified. The results suggest that decision making in the largest retailers is fairly centralized and that major input is minimal and concentrated at the highest levels within the organization with the goal of achieving uniformity throughout the enterprise. As the organization gets smaller, the decision can be a bit more decentralized with those closer to the store, having more influence on the final decision.

Current Store Systems Security Approaches:

We wanted to find out what tools and techniques today's retailers employ in their efforts to maintain their key transactional systems. To measure this, we first asked regarding core POS systems the following question: "With regards to your POS core components (hardware & operating system), which statement best describes your security position?" Similarly for software, we asked: "With regards to your POS software, which statement best describes your security position?" These questions help us to understand the security evolution retailers are making as they move from the initial purchase to actual in-store operation.

Overall results for the core POS (Hardware and Operating System) are shown in Figure 5. The most predominant approach for retailers is that 66% of them choose to manage core POS security themselves. We didn't investigate what specific steps this entails, but we imagine that within the realm of PCI compliance, internal procedures, and store operations requirements, a framework exists for the management of the POS core. There are a wide array of variables that bring differentiation among manufacturers around the core POS, especially around the operating system chosen. We know retailers are significantly absorbing the burden and responsibility of managing core POS security.

	We trust the manufacturer to provide security	We manage the POS core component security ourselves	We use a third party to manage the security
Restaurant/Hospitality	30%	40%	30%
Food/Drug/Conv/Gas	16%	64%	20%
GMS-Dept, Soft, Hard	24%	76%	0%
Average	22%	66%	13%

Figure 5 - Security position on core POS (HW + O/S) by segments.

As we look at the revenue range in Figure 6, clear trends emerge. Larger companies are increasingly more reliant on providing the internal controls for their core POS systems. This is similar to Figure 7. Regardless of verticals or size of company, the majority are burdened in providing security for systems.

	We trust the manufacturer to provide security	We manage the POS core component security ourselves	We use a third party to manage the security
Tier I	16%	78%	6%
Tier II	18%	73%	9%
Tier III-IV	33%	43%	24%
Average	22%	66%	13%

Figure 6 - Security position on core POS (HW + O/S) by revenue.

As we turn our attention to POS software, those results are presented in Figure 7. Two predominant approaches emerge: Those that choose antivirus/anti-malware software as their primary line of defense (47%) and those that take a whitelist approach allowing only pre-authorized programs to load and run (31%).

Here it is worth defining the two key software approaches for securing POS systems: Antivirus (essentially blacklisting) and whitelisting software. In its most simplistic form, antivirus works by detecting either suspicious or known signature-based malware and identifying its presence and scanning to remove it from the system utilizing .dat updates to continually keep on top of the newly identified malicious programs. Whitelisting takes a different approach in that a systems executable (applications and operating system) is explicitly allowed and authorized to run, with no need for a continued .dat update. Any unauthorized executable that is introduced to the system will be blocked. The system will be protected from executables that could be introduced through the exploit of a currently running application, operating system vulnerability or even new malware. While initial approaches to securing computer systems focused on the common anti-virus approach whitelisting is as an increasingly more effective approach against the key concerns noted in these results, especially when considering the five most highly rated concerns shown in Figure 2.

Whitelisting also has a negligible impact on performance because its primary task is to control the loading of software code – there are no malware signature files to download and run. This is in contrast to traditional anti-virus (AV) security that blocks, and often eradicates, malicious code or data containing a known or suspicious character string documented in a regularly updated malware signature file. The approach with whitelisting relieves this burden, making it easier to manage the integrity of these retail systems with less overhead.

As a company with a strong focus on POS systems as well as the market concentration of those systems, we would also be remiss to not mention that whitelisting, from some vendors, provides the additional benefit of being able to secure operating systems that are no longer supported by the manufacturer. Salient to our discussion, support for Windows XP will end in less than a year⁴. In our analysis of North American POS systems, we estimate that by the end of 2012 approximately 31% of the current installed base will comprise of DOS and Legacy Windows applications running at the POS. When we consider this is over 2 million units⁵, it's not a trivial benefit.

Again as we refer to Figure 7, we see a definite trend by retailer size in the approach to software security. Tier I retailers (those with more than \$1 billion in revenue) tend to be among the most progressive with regards to technology innovation and incorporation. It appears that following the technology decisions made by the largest of retailers provides a good perspective into the future direction of any given technology. This can be seen in the move toward the whitelisting approach and away from an antivirus approach. In Tier I, we see an equal percentage of retailers (38%) using a whitelisting approach as compared to antivirus. When we look further into those over \$5 billion in revenue, the difference between the two approaches widens significantly

⁴ <http://www.microsoft.com/en-us/windows/endofsupport.aspx>

⁵ 2013 North American Retail POS Terminal Market Study by IHL Group, February 26, 2013

with 47% choosing a whitelist strategy compared to 26% selecting the antivirus strategy, a difference approaching 2x. This data clearly suggests an ongoing strategy change around securing POS systems.

When we consider the drivers section and Figure 2, and then consider the key benefits of whitelisting, we see a strong correlation between security concerns and strategies for addressing those concerns. No survey respondents below \$250 million in revenue noted the use of whitelisting, though two-thirds utilized antivirus/anti-malware software to secure their POS systems.

We should also note that with regard to the use of third-party companies and those that rely on POS component vendors to provide integrated security, we did not investigate the specific techniques employed by those supporting organizations. Those two approaches combined are used by around 20% of the respondents.

	We install and manage anti-virus/anti-malware software	We use security software to manage and allow only pre-authorized programs to load and run	We use a third party (VAR, System Integrator, etc.) to manage the software security	We rely on the POS component vendor to provide integrated security	We rely on the POS component vendor to provide remote security management
Over \$5 Billion	26%	47%	11%	16%	0%
Tier I	38%	38%	9%	13%	3%
Tier II	55%	36%	9%	0%	0%
Tier III-IV	57%	19%	10%	14%	0%
Average	47%	31%	9%	11%	2%

Figure 7 - Security position on core POS SW by revenue.

A Self-Assessment of Internal Security Compliance:

Given the techniques that were established in the previous section, we wanted to get a better feel for the internal effectiveness for those policies and procedures. To do that we asked the following question: “With regards to maintaining the security and compliance on your POS systems, which best describes your internal processes and effectiveness in managing patch and security updates (where 1 – Significant improvement needed; 5 – We do an excellent job)?”

The results by retail vertical are shown in Figure 8. We’ve also included information on POS systems, other surveyed devices, and a total device summation. The overall result is slightly above average at 3.56, meaning our survey respondents felt they did an above-average job on security compliance and effectiveness. But when we overlay the device metrics trends, a clearer picture develops. We believe this speaks to the overall macro trends around device proliferation and what that means from a practical sense. If you look by segment

at the reported increase in security effectiveness, it correlates to both a decrease in the total number of POS systems as well as the total devices per location. This reinforces our point regarding the impact on security confidence as we see an increase in devices. Increasing the number of devices is a key driver around introducing significant complication around the ability to secure the store environment. The only exception to this trend is Restaurant/Hospitality which is worth noting.

	Average	Below Average (1 or 2)	3	Above Average (4 or 5)	POS Per Location	Other Devices Per Location	Total Per Location
Convenience/Gas	3.83	8%	25%	67%	2.58	2.29	4.87
Specialty Soft Goods	3.56	0%	44%	56%	3.05	2.91	5.96
Specialty Hard Goods	3.43	14%	43%	43%	5.50	6.71	12.21
Food/Grocery	3.33	22%	22%	55%	9.61	4.94	14.55
Restaurant/Hospitality	3.30	30%	20%	50%	4.85	0.95	5.80
Average	3.56	13%	33%	54%	6.24	4.23	10.47

Figure 8 - Internal processes & effectiveness in managing security & compliance on POS systems (managing patch/security updates).

At first glance, Restaurant/Hospitality would seem to buck the trend. But as we understand this sector a bit better, their response is actually in line with the results. While we have mentioned that with both Convenience/Gas and Restaurant/Hospitality there is a high degree of franchises as a percent of the overall market. The key difference is that with Convenience/Gas there is a much less diversity in the POS hardware and software allowed by the parent company. The uniformity is driven by two key areas: Interfacing with pump-control software and hardware; and the ability to interface with fuel-card authorization devices. Typically in a Convenience/Gas environment you have two or three allowed POS hardware offerings and two to three software packages approved by corporate. In other words, across the enterprise, there may be four to six total POS system configuration combinations that have to be secured and managed.

When we look at the Restaurant/Hospitality space, the environment is not the same. Though this is starting to change somewhat as parent companies limit selection, historically, the hospitality sector has allowed much greater franchisee flexibility with regard to POS hardware and software selection. We are even familiar with instances where larger franchisees are using no approved software and hardware. In reality, there can be both four to six approved software packages and hardware offerings, meaning that within a global chain you can easily have 30 different POS system combinations that need to be addressed from a security perspective. So while Hospitality may not have as many total devices within a store, it's easily more complex managing images due to the diversity of POS system combinations allowed. In such diverse environments, a solution that allows top-level security of devices in the store across the enterprise instead of the approach of individually securing point solutions would be a real advantage. Our data suggests the greater variability is currently leading to decreased procedural effectiveness.

The Cost of Security:

How much should retailers spend on security? While we did not ask that question, we can tell you approximately how much retailers are currently spending. To get a feel for exactly how much, we asked the following question: “What would you estimate the total (including money spent on both hardware and software) yearly investment in POS security as a percentage of what you pay for ongoing POS hardware and software license maintenance?” Survey results are shown in Figure 9 by segment.

Using these results by vertical and applying metrics from our 2013 North American POS Report, we find that \$212.7 million is being spent on hardware and software by North American retailers yearly just to secure their POS systems. Within context, this represents about 24% of what will be spent on retail Business Intelligence software in all its forms this year in North America⁶, and around 50% of what will be spent for all forms of mobile-based hardware and software technologies in the store and throughout the enterprise in 2013⁷.

	Average	Estimated Yearly Security Expenditure
Restaurant/Hospitality	8.33%	\$105,258,769
Food/Drug/Conv/Gas	6.82%	\$36,446,211
GMS-Dept, Soft, Hard	5.92%	\$70,976,722
Average/Total	6.56%	\$212,681,753

Figure 9 - Estimate of the total (HW+SW) yearly investment in POS security as a percent of what you pay for ongoing POS hardware and software license maintenance.

As we have looked by retail vertical at some of the differences in expenditure in Figure 9, we also wanted to look at the data by size of company. These results are shown in Figure 10. Probably not a surprise, but we see larger companies spend more. As we have previously noted, most Tier II retailers aspire to grow into the Tier I ranks. As we have historically tracked IT spend, our data shows that Tier II retailers spend more as a percentage on IT than their Tier I counterparts. Again, while there are many reasons for this, one of the greatest drivers is the belief that technology can be a significant enabler within the engine that drives growth.

⁶ 2013 Retail Worldview IT Spend Model from IHL Group

⁷ 2013 Retail Worldview IT Spend Model from IHL Group

Revenue Range	Average
Tier I	7.38%
Tier II	7.67%
Tier III-IV	4.50%
Average	6.56%

Figure 10 - Estimate the total (HW+SW) yearly investment in POS security as a percent of what you pay for ongoing POS hardware and software license maintenance by revenue.

Looking at the overall trends from small to larger retailers, the biggest difference is most likely due to compliance drivers. While we will avoid a review of PCI standards, a quick look at merchant tier levels⁸ (based upon card transactional volume, not overall revenue) that defines the varying security requirements, shows increasing and more stringent activities are mandated as transactional volume increases. To no one's surprise, these result in higher costs that retailers must bear.

Furthermore as we see from Figure 1, these retailers tend to have a lot more devices in the store that need to be secured, again driving up costs. The data as a whole continues to emphasize that more complexity, more devices, and more transactional volume yields more costly security. This, in turn, drives up security management costs as a whole. Why do we find security spend by Tier III/IV retailers to be relatively so low? There can be many reasons for this, but most probable as the leading reason is lack of budget. Furthermore, as we return to the PCI compliance discussion, there are literally fewer requirements. And while a Qualified Security Assessor (QSA) is a definite requirement for a large company, smaller companies may be able to internally self-assess reducing this cost.

To get a directional feel for how these costs had changed over the previous years we queried our audience. We posed the following question: "Now considering your overall yearly spending levels on POS security, how would you describe that trend?" In every vertical grouping, the most predominant response was that the overall cost of security was increasing on a yearly basis.

Those in the Restaurant/Hospitality sectors noted a more drastic increase in expenditure that we suggest ties to our previous discussion around POS configuration variability allowed. The Food/Drug/Convenience and GMS groups noted more modest increases. This speaks to the ever-evolving nature of threat prevention and mitigation and the need for constant attention and evolution of threat deterrent processes.

Without adequate controls to manage store system variability and without a solid plan addressing security at the enterprise level looking at overall device management as an ecosystem, you can expect cost to continue to increase rapidly. While IT is constantly evolving, security must evolve--oftentimes more rapidly than the

⁸ http://usa.visa.com/merchants/risk_management/cisp_merchants.html#anchor_4

devices they are tasked with protecting. The ability to tightly manage the enterprise is a big driver in managing security and controlling costs.

Review of Survey Respondents:

IHL Group surveyed a broad range of retail and hospitality executives in North America. The results of the 66 respondents are detailed in this report. Respondents came from a very broad range of retail segments and chain sizes. Figure 11 summarizes the respondents by vertical. Loosely speaking, these form into three macro-groupings: Hospitality, General Retail, and Fast Moving Commodities. Figure 12 shows that survey responses were somewhat skewed to larger retailers. As we noted earlier, this is beneficial in that large retailers tend to drive technology trends. By understanding their thinking, it's almost like a crystal ball into the direction that we can expect future technology trends to take.

Segment	Percent	Number
Restaurant/Hospitality	17%	11
Convenience/Gas	18%	12
Department Stores	6%	4
Drug Stores	3%	2
Food/Grocery	14%	9
Mass Merchant/Warehouse Clubs	3%	2
Specialty Hard Goods	23%	15
Specialty Soft Goods	17%	11
Food/Drug/Conv/Gas	38%	25
GMS-Dept, Soft, Hard	45%	30
Restaurant/Hospitality	17%	11
Overall	100%	66

Figure 11 - Respondents by Segment.

Revenue	Percent	Number
Tier I	51%	33
Tier II	17%	11
Tier III-IV	32%	21
Overall	100%	65

Figure 12 - Respondents by Revenue.

With respect to the individual responsibility (Figure 13) of those responding to the survey as a whole, we see that IT and Store Operations personnel made up around 69% of the respondents and non-IT executives around 17%. These are decision makers, those with budget responsibility, and those with a firsthand understanding of the technology decisions and strategy supporting security.

Executive Responsibility	Percent	Number
Executive Management: VP-Level (non IT)	9%	6
Executive Management: C-Level (non IT)	8%	5
CIO/CTO/VP of MIS	34%	22
IT Director - Manager	25%	16
Store Operations	9%	6
Merchandising/Supply Chain	5%	3
Division/Store Management	2%	1
Other (please Specify)	8%	5
Overall	100%	64

Figure 13 - Respondents by Executive Responsibility.

About IHL Group:

IHL Group is a global research and advisory firm for technologies deployed in the retail and hospitality industries. With our core research and data services we are the world leader in tracking who uses what systems in retail technology, especially those systems used within the store. We are able to help retailers and restaurants evaluate those technologies that are working and those that are not before they spend the money on costly systems. With researchers around the world, we also provide market analysis and opportunity assessment for technology vendors. Retailers use our services for solution research, contract negotiations, and competitive intelligence. Vendors use our services for market opportunity and partnerships.

About McAfee:

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe.



Other IHL Reports Available Include:

- Europe/Middle East/Africa POS Terminal Market Study - \$3,495
- Asia/Pacific POS Terminal Market Study - \$3,495
- Latin/South American POS Terminal Market Study - \$3,495
- Mobile POS: The First Real Test - \$3,500
- RIS News/IHL Store Systems Study "Mobile Meets Retail's Big Data" - \$3,500
- POS Software for Hardgoods Retailers - \$795
- POS Software for Hardgoods Retailers - \$795
- North American Self-Service Kiosk Study - \$995
- North American POS Printer Report - \$2,695
- Small/Medium POS Sizing - \$4,000



SOPHIA

From data to insight ~ WISDOM for Retail

Retail Technology Data Services Include:

Sophia is the most comprehensive review of retail technology in our industry, providing the key performance, technology, and contact information on 3,500 Retailers and 2.5 Million records. It is the only **Subscription** data service that takes an enterprise view of the technology that retailers are deploying AND the performance that they are achieving with the use of these technologies. For Details and a Free Report, visit our website at www.ihlservices.com

Prepared by:

IHL Group

For Questions or Information:

1064 Cedarview Lane * Franklin, TN 37067

Phone: +1.615.591.2955

<http://www.ihlservices.com>

ihl@ihlservices.com