White Paper:

Retail Security for the Digital Age: Preventing a Data Breach in Your Store

As customer-facing businesses, retail brands have to work hard to uphold their reputations, and information security is a vital component of this effort. Retailers have to accept that today every business — big or small — can be a target, and they must do all they can to minimize the risk. As the retail industry makes the shift to digital platforms and mobile devices proliferate, the security of both the physical and digital environments of retail stores is more important than ever.

Chapter One: New Technology, New Risks

Protecting their assets has always been a crucial challenge for retailers, thanks largely to their vulnerability as publicly accessible businesses. But where security issues once threatened only the physical store, today they also include cyberthreats such as data breaches, and they're keeping security managers up at night.

The explosion of e-commerce and the growing use of mobile in stores, both as a direct selling tool and for assisted selling, has opened up new opportunities for retailers. Traditional brick-and-mortar businesses are going digital, while top retailers are embracing innovation to steal a lead on rivals and disrupt the market. The rise of omnichannel digital platforms is dramatically enhancing customer engagement and increasing employee efficiency. But as a market becomes more attractive for business, it also becomes a more appealing target. Therefore, in order to reap the full benefits of digital innovation, it's crucial for retailers to prioritize the security of customer data.

The Cost of Data Breaches

Website hacking and malware attacks are big businesses, especially when attackers are breaking into networks to steal customers' credit card numbers and personal details. This means that retailers in the e-commerce and m-commerce age are natural targets. According to Verizon's 2016 Data Breach Investigations Report, 89 percent of breaches had a financial or espionage motive last year.[1] The 2016 Cost of Data Breach Study: Global Analysis from IBM and the Ponemon Institute reports that the average total cost of a data breach in the U.S. rose 7 percent in the last year, from $6.53 million to $7.01 million.[2]

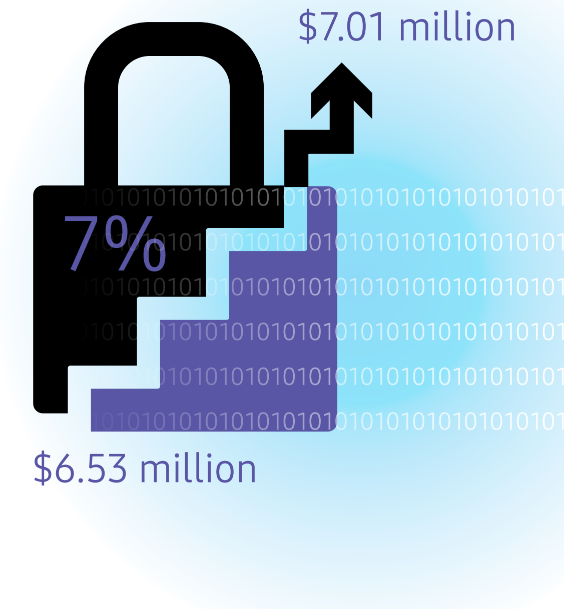
For large retailers hit by the most public of breaches, the cost has run into the tens and even hundreds of millions, as they face multiple losses from such breaches. It's big bucks for the criminals attacking retailers, too. The average cost of a record containing sensitive and confidential information rose globally from $105 in 2014 to $165 in 2015.[3] For the U.S. specifically, that equated to a 2 percent increase in the cost per lost or stolen record, up from $217 to $221.[4] These costs include both the turnover or churn of customers and the direct costs incurred to resolve such breaches, such as investments in technologies or legal fees.

But the financial cost of the breach itself is just part of the total cost. It makes huge headlines when large, well-known businesses are targeted and customer details are compromised, creating a huge impact on customer confidence and churn. This means the biggest financial implications for retailers can actually be the lost business caused by customers losing trust in their brand.

Attacks Happen Fast, But Detection Can Be Slow

Cybercriminals aren't fussy about who they target — they'll simply focus on the weakest link, whether that's the retailer or a third-party supplier. The threat applies to retailers large and small, and can be so sophisticated that businesses often don't realize they've been attacked, particularly if they have a low level of security awareness.

The average cost of a data breach continues to rise



Cybercriminals aren’t fussy about who they target — they’ll simply focus in on the weakest link, whether that’s the retailer themselves or a third-party supplier.

Early detection is vital. The longer a data breach remains undetected and the malware collects data, the greater the damage, and the longer a company takes to discover a breach, the greater the negative impact will be on its reputation. Yet detection isn’t happening quickly enough: It takes an average of 229 days to identify a data breach incident caused by malicious or criminal attacks.[5]

Similar findings are evident in the 2016 Data Breach Investigations Report from Verizon,[6] which shows that attackers work quickly, with systems compromised within hours or less in 99 percent of cases. In 44 percent of cases, systems were compromised within hours. Yet in more than 70 percent of cases, it took retailers weeks or more to discover that a breach had occurred. In effect, this means hackers are able to continue to mine confidential systems for an extended period before the loophole is closed.

Even when customer financial or personal data isn’t exposed, any type of service interruption means lost revenue for retailers and potential damage to their brand and to customer relationships. Deloitte reports that 73 percent[7] of consumers said they’d reconsider using a company if it failed to keep their data safe, and a third would subsequently close their online accounts following a breach or stop dealing with the affected business. Eighty-five percent said that it’s the responsibility of the companies that collect or process personal details or financial transaction data online to keep it secure from criminals.

For millennial customers, who are more concerned than any other generation about doing business with a company they trust, data security is even more important and therefore vital for businesses to get right.

The Move to Mobile In-store Brings Additional Threats

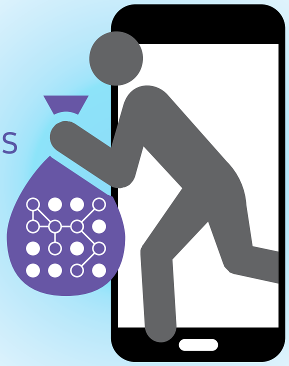
Mobile is changing the way customers work, shop and pay, revolutionizing the selling experience and allowing retailers to provide an enhanced customer experience through mobile payments and assisted selling on tablets and mobile devices. But the increase in mobile experiences brings with it an increase in the flow of data. A recent report from Gartner[8] suggests that by 2018, a quarter of corporate data traffic will flow directly from mobile devices to the cloud, bypassing enterprise security controls. New technologies such as the Internet of Things offer opportunities to personalize the retail experience, but it also increases the number of endpoints that must be secure.

The increasing use of mobile point-of-sale (mPOS) could also present a risk if devices aren’t effectively secured and managed. According to Juniper Research, by 2021, more than one in three POS terminals will be mobile, handling 20 percent of all retail transaction value — up from an expected 4 percent this year — as retailers are increasingly using the technology to keep checkout lines to a minimum.[9]

But retailers are introducing other uses for mobile, too — from more sophisticated mobile apps that tie in with loyalty programs to apps that enable customers to scan in-store products for additional information — all of which increases risk. As mobile usage proliferates in-store, retailers must tackle the threat apps pose. Although malware on mobile devices is currently limited, it will grow — rapidly. Research from NowSecure revealed that 25 percent of mobile apps include at least one high-risk security flaw.[10] In 2014, Gartner predicted smartphones and tablets would be the primary focus of endpoint breaches by 2017.[11]

Chapter 2: Types of Security Breaches and Risks

Mobile is changing the way customers work, shop and pay, but retailers aren't necessarily keeping up with the data breach risks this can cause.



Samsung's Knox Platform

Samsung Knox, a security platform built into the latest Galaxy smartphones and tablets, is a case-in-point for the value of multilayered security, making it an excellent fit for retail use cases. Knox protects the integrity of the entire device, from the hardware to the application layer. This multilevel approach to security includes tamper-evident fuses built into the device from the factory, combined with Trusted Boot, TrustZone-based Integrity Measurement Architecture (TIMA) and Security Enhancements for Android, providing real-time protections throughout the entire device life cycle. Knox received the most "strong" ratings of any mobile security platform in the Gartner report "Mobile Device Security: A Comparison of Platforms."

To find out more, visit samsung.com/knox.

Data breaches make big headlines, largely because of the sheer numbers that are usually involved, but also because many retailers suffering breaches are household names. A number of recent, high-profile cases have illustrated just how big the losses can be in terms of customer or card details compromised and the damaging PR and financial impacts on a business as a result.

Threats can come from a number of sources. In nearly half of cases (48 percent), hackers and criminal insiders are responsible. However, system glitches and human error or negligence can also be to blame, and can be nearly as costly: The average cost per record to resolve a malicious or criminal attack is $170, compared to $138 per record for system glitches and $133 for human error or negligence.[12]

As well as harming relationships with customers, data breaches can also seriously harm relationships with suppliers if a breach occurs due to the security vulnerabilities of a third-party partner. This has already happened in a number of high-profile cases, proving that retailers can't assume that they're 100 percent secure against attacks. Determined hackers will find a way in by looking for the path of least resistance, making suppliers an obvious next target.

Areas attackers may target include:

Wireless connections and servers

Wireless technologies are a major risk for retailers because they open up new routes for determined attackers to get in — with some hackers going so far as launching an attack from the store parking lot. Access via wireless is being blamed for many recent retail data breaches, with several big-name retailers being hit. As such, retailers must ensure they aren't leaving their wireless and back-end systems open to attack. Encryption can help, and while large retailers typically use encryption, small and mid-size retailers sometimes overlook such protective measures.

In-store, the retail industry is increasingly adopting free Wi-Fi for customer use. While it is a big draw for customers, if retailers fail to secure Wi-Fi networks, or isolate them from their back-office systems, then they're opening a gateway for attack. Hackers are also setting up rogue Wi-Fi networks — particularly in markets such as Asia. To protect themselves, retailers should use a QIR-certified VAR or SI when choosing their hardware.

The POS system

Financial transactions pose one of the biggest areas of risk for retailers, and cybercriminals have much to gain from accessing the financial data transmitted through POS devices. According to the 2016 Data Breach Investigations Report from Verizon, 64 percent of breaches with confirmed data disclosures involved POS intrusions.[13]

Attacks can be made through a number of routes, from phishing to credential theft to skimming. Although phishing is an older approach, it's still surprisingly effective. The use of stolen third-party credentials to access POS systems, install malware and collect customer data has been documented in a number of recent cases, illustrating both the importance of employee and third-party education and the need for revision of cybersecurity procedures. Skimming, in which a third-party device is installed over a legitimate POS device to capture credit and debit card information, is also a huge threat, especially since skimming devices can be indistinguishable from the real thing. The rise of self-checkout in retail stores makes this an increasing threat.

In the U.S., the retail market is particularly at risk as it continues to move toward chip and PIN or the EMV (EuroPay, MasterCard and Visa) standard. In these payment methods, sensitive card data is stored on an encrypted computer microchip on the card instead of on the magnetic stripe, and the card is authenticated only by PIN rather than signature. Implemented in October 2015, the EMV liability shift means that retailers that haven't installed new chip-enabled card reader equipment must now foot the bill for any fraudulent activity. The estimated to cost each retailer to pay for new card readers is around $2,000, according to the National Retail Federation.[14]

Some retailers have been slow to adopt the new card readers, citing delays from credit card companies. Customers have also been slow to adopt. According to a 2015 survey by the National Retail Federation, among consumers who have a credit card, 71 percent have at least one chip-enabled credit card in their wallets, but only 47 percent have used it in a chip reader.[15]

Although EMV is a long-established technology in much of the rest of the world, hesitation from U.S. consumers could mean a boost for mobile payments. This, coupled with the increasing popularity of mobile POS, offers U.S. retailers the opportunity to leapfrog chip and PIN with a potentially safer, more effective payment solution. Mobile wallets such as Samsung Pay, for example, offer a tokenized method of storing credit and debit card information, meaning that the card number is never transferred between shopper and retailer or stored on the customer's phone, so card details can't be stolen even if the hardware is attacked.

Customer information and personalization

Although transactions are an obvious and established target for data breaches, another vulnerability lies in the data that retailers collect from their customers to improve personalization and the customer experience.

Customer data breaches are particularly concerning when the data is stored on mobile devices or other endpoints such as kiosks, which can be accessed in stores by staff and customers alike. With retailers using such devices to offer endless shopping options, the ability to control access and prevent attacks on this technology is key. Such mobile devices need to be secured at the enterprise level, with features locked down to prevent unauthorized access. In addition to protecting against potential data breaches, this also helps retailers supervise their employees, making sure they're not playing Angry Birds when they should be concentrating on customer service and selling.

Mobile device management should also focus on how to prevent attacks if devices are stolen, since their use in-store once again encompasses the physical risk of theft that retailers have always faced. The right mobile device management will ensure that retailers' security teams are still able to manage security and wipe the data on a device even if it's physically stolen, lost or otherwise compromised.

Locking Down Mobile Endpoints

Samsung's Knox Customization solution provides an effective approach to securing mobile devices deployed in retail environments, whether with sales associates or in customer-facing kiosks. Retailers can use the toolkit to customize mobile devices for a specific use case, tailoring the user experience and taking advantage of advanced device configuration capabilities. By creating a customized point-of-sale mode, for example, Knox Customization prevents associates from connecting the device to unsecured networks or accessing unsafe websites or applications.

To find out more, visit samsung.com/knox.

Chapter 3: Bolstering Security

Retailers must be prepared not only for the “if” of a cyber breach but also the “when.” What can they do to prepare?

1. Ensure all technology is protected

To protect their core retail systems from possible attack, retailers must assess their infrastructure and tools to determine if there are any weaknesses. Firewalls, network segmentation and compliance with the Payment Card Industry Data Security Standard (PCI DSS) will all help improve the safety of data, while two-factor authentication makes it harder for intruders to access a network.

Retailers also need to review infrastructure such as free in-store Wi-Fi to ensure that it isn’t susceptible to attack. Such networks need to be isolated or hosted on a standalone network that isn’t connected to systems that hold sensitive data. If they are, then such data needs to at least be secure and protected by a firewall.

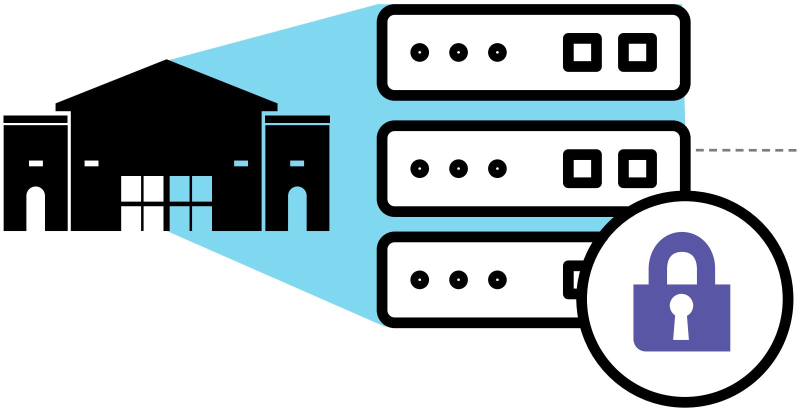
That said, retailers can’t assume that because they have the necessary controls in place, they’ll be immune from attack. Months after its data breach in 2014, Target’s executive vice president and chief financial officer John Mulligan highlighted how even the most prepared can be hit by a breach. “We had in place multiple layers of protection, including firewalls, malware detection software, intrusion detection and prevention capabilities, and data loss prevention tools. We perform internal and external validation and benchmarking assessments. And, as recently as September 2013, our systems were certified as compliant with the PCI Data Security Standards. But, the unfortunate reality is we suffered a breach…” he said.[16]

Attackers are turning to the mobile environment to exploit new weaknesses and new opportunities — and assessments of risks and prevention of breaches must be taken. Retailers must securely encrypt their data to protect everything from their mobile devices and the applications that run on them, to the data centers that the mobile devices connect to.

“Retailers have a number of challenges,” says Christopher Campbell, director of product marketing for VMWare AirWatch. “They have to secure any type of mobile device being brought into the company and also have point-of-sale devices that they need to secure, too,” he says.

“One of the unique challenges is that there is a lot of unknown traffic that walks into the retail environment, so you need to lock down mobile devices so that they are communicating over the right networks,” adds John Britton, director of product security at VMWare AirWatch.

In-store apps also need to be isolated to protect the rest of the business from attack. Campbell suggests segmenting the data from other information in the data center, treating the app as if it’s on its own network. “We had a retailer recently approach us who had the challenge of needing to roll out an app, but was concerned about security,” Campbell says. “We were able to segment security policies for that app and treat it as though it was in its own secure environment.”



Another challenge, according to Britton, is understanding users. Devices must be properly configured so they are connected only to the store-wide network and so they run only approved apps.

It's also about controlling access to mobile devices for both current and former employees, reminds Campbell, especially due to the often more transient nature of the retail workforce. Current and former employees, he says, are responsible for many cyber breaches in retail.

"You have to put up real fences at each different area," says Britton, "If a mobile device does get comprised, how do you prevent a larger problem and someone getting access from a mobile device into the back office and then moving from server to server in the back office? You need to be able to prevent that device communicating with the server and lock it down."

2. Lead from the top to change security attitudes

Despite the headlines, some retailers still think a breach won't happen to them.

Leading from the top is vital, according to Ted Brodheim, vice president of vertical business at Samsung Electronics America. "Leaders need to recognize that the threat is very real and make an active decision regarding their risk tolerance," says Brodheim. "The benefits gained for retailers adopting new digital platforms and mobile workflows are significant, but brands must also be prepared to invest in securing these platforms and their customers' information."

Sadly, this doesn't always happen. The U.K. Cyber Security Breaches Survey 2016[17] showed that a quarter (26 percent) of senior managers were never updated on actions taken in relation to cybersecurity. Many in the survey identified the lack of knowledge of the board as one of their main barriers in getting management to engage with cybersecurity, caused simply by their failure to understand it technically.

3. Make cybersecurity a company-wide priority

Although nearly half of all data breaches are the result of malicious or criminal attacks, a quarter are due to negligent employees or contractors, meaning that a cybersecurity-focused attitude has to run throughout the business and be constantly reinforced.

The Ponemon Institute study highlighted that 27 percent of data breaches are the result of system glitches that include both IT and business process failures.[18] As 60 percent of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk,[19] a strong focus on cybersecurity is even more important.

"It's critical there is a strong awareness of the risks and a clear, well communicated protocol in place," says Brodheim. "Awareness isn't something that happens once — it's understanding what the threat is and then helping staff understand the process for reporting potential issues."

60 percent of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk.

Fraudsters now perceive mobile payment channels to be particularly vulnerable, as many organizations have yet to apply the same levels of protection to mobile as they have to desktop transactions.

In addition to virtual threats, retailers need to educate staff to look out for physical threats, too, such as skimming devices attached to payment devices in stores, particularly at self-checkout lanes where such devices aren't as closely monitored.

In the U.K. Government's Cyber Security Breaches Survey 2016, 69 percent of businesses said cybersecurity was a high priority for senior managers, and yet only 51 percent had taken recommended action to identify cyber risk. Only 29 percent had formal, written cybersecurity policies, and a mere 17 percent of businesses had provided cybersecurity training in the previous 12 months.[20]

These figures demonstrate the importance of proper staff training, especially given that data breaches can often be caused by factors as simple as users choosing default configurations and settings rather than setting their own strong passwords or using two-factor authentication. The 2016 Cost of Data Breach Study says that nearly two-thirds of confirmed breaches last year involved the use of weak, default or stolen passwords.[21]

4. Validate third-party suppliers

Once overlooked, the possibility of a breach via a third-party supplier has become all too real, with a number of the highest-profile retail data breaches in recent years caused by an attacker gaining credentials through a weak-link supplier that allows them in to do damage.

Data breaches caused by the poor security of third-party suppliers not only harm the affected businesses from a PR perspective but also tend to cost more — up to $172 per record, according to the 2016 Cost of Data Breach Study.[22]

The damage to supplier and retailer relationships can be severe, since it's the retailer's name that will be cited most. Businesses lack focus in this aspect as well, with only 13 percent of all businesses setting cybersecurity standards for their suppliers, although this number increases to 34 percent for large firms.[23]

Many of those hit by breaches, especially where supplier access was the cause, have reviewed their use of vendor permissions as a result, or have disabled components like multiple vendor accounts. Retailers should consider additional steps such as creating third-party assessment models and asking suppliers about their security models.

5. Devise a plan and put incident response teams in place

Once a retailer has reviewed their technology and corporate, employee and third-party security stances, much of their preventative work is done — which means moving to ensure that they're prepared if a data breach does occur.

"Every organization should have a clear protocol in place that addresses as many scenarios as possible," says Brodheim. "If you have a breach, you have to know who needs to be involved internally and have representation from IT, legal, communications, HR and other relevant teams." This should involve having immediate access to third-party partners who specialize in dealing with such issues.

Despite the importance of having a plan in place, this aspect is often overlooked. According to the U.K. Government's Cyber Security Breaches Survey 2016, only 10 percent of businesses had a formal incident plan in place.[24] Having an incident response team in place also helps reduce costs, which fell from $158 to $142 per record.[25]

Once a response plan and templates for dealing with a breach are in place, they must be reviewed regularly as infrastructure, processes and threats evolve.

6. Test attack scenarios rather than just writing them down

In March, the Cyber Storm Exercise, a U.S. event focused on helping retailers run through their responses to a simulated cyberattack, tested the reaction of their IT security teams and the robustness of their incident response plans with the aim of improving cyber defenses across the retail industry. Conducting test runs through simulated attacks is crucial because when an incident occurs, if a retailer reacts by looking up what they should be doing instead of actually responding, they might as well have no plan at all.

Brodheim points out that retailers must run through all eventualities and do the necessary prep work to effectively deal with a breach. This could be, for example, having a press release on file and ready to go, or knowing which law enforcement organizations need to be notified. "It's damage control. Having well constructed responses that can be used quickly will minimize the brand, financial and legal impact," he says.

7. Trust systems and alerts with incident response procedures

With plans in place and technology and processes reviewed, retailers now need to make sure they're ready to react to any system alerts. They need to encourage trust in such systems and empower their staff to react to and deal with any alerts that may come up — rather than simply dismissing them as an anomaly or allowing them to disable or ignore alert functions. According to Brodheim, this should include both formal escalations when a breach has clearly occurred, as well as informal communication when there is an unexplained anomaly or someone has a "gut feeling" that something may have occurred. "The reality is, for many large retailers, attempted breaches are occurring almost constantly," says Brodheim. "When systems appear to be secure, the risk is that people often become complacent."

8. If the worst happens, regain trust quickly

After Target's breach, the company worked fast to assure its customers that they would endure no liability for the cost of any fraudulent charges, and also offered free credit monitoring and identity theft protection to its shoppers to help calm worries. The company's chairman, president and CEO Gregg Steinhafel used a number of communications strategies to reach customers, including a letter admitting that the company had failed.[26] At the time, Steinhafel noted, "Target will not be defined by the breach, but how we handle it."[27] This type of accountability should be the aim of any retailer that suffers a data breach.

As previously noted, retailer incident response plans should be in place and tested. "It's about being able to demonstrate and communicate clearly to the public that you had a plan in place, you worked quickly to address the problem, and you've done everything you can to protect your customers," says Brodheim. "If you don't and you are scrambling, then your credibility starts to drop off, and you start losing customers and getting more intrusive questions from authorities," he says.

Once a response plan and templates for dealing with a breach are in place, they must be reviewed regularly as infrastructure, processes and threats evolve.

Conclusion

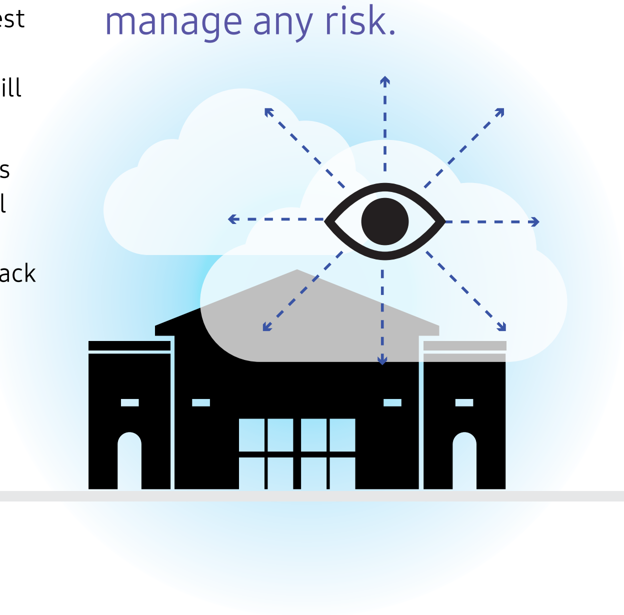
Even the most prepared retailers are at risk. It's a question of not "if" but "when" your organization will suffer a breach.

Retailers have to come to grips with what's going on within their businesses to ensure they can best manage any risk — be it a lax attitude among staff, lack of security controls by vendors or weaknesses in their infrastructure. When it comes to mobile, however, they must look again at the role of mobility in their organizations and how best to enable it without posing a risk to the rest of the business. Mobile is a growing trend both for retailers and customers, and in addition to offering one of the biggest opportunities for retailers to grow their businesses, it also opens up a whole new avenue of risk when it comes to the possibility of a data breach, which attackers will increasingly focus on.

The risk of a data breach won't go away, as the technology used to get into systems evolves as fast as the technology that keeps attackers out. However, with a careful review of current systems and processes in place, a revisiting of employee and employer attitudes toward cybersecurity and an appreciation of new potential attack avenues, such as in-store mobile usage, the risk of a data breach in your business can — and should be — dramatically lessened.

To learn more about how Samsung helps retail businesses prevent data breaches and protect their customers, click here: samsung.com/retail

Retailers have to come to grips with what's going on within their businesses to ensure they can best manage any risk.



Sources:

1 2016 Data Breach Investigations Report. Verizon Enterprise. 2016.

2 2016 Cost of Data Breach Study: Global Analysis. IBM and Ponemon Institute. 2016.

3 2016 Cost of Data Breach Study: United States. IBM and Ponemon Institute. 2016.

4 2016 Cost of Data Breach Study. IBM and Ponemon Institute. 2016.

5 2016 Cost of Data Breach Study: United States. IBM and Ponemon Institute. 2016.

6 2016 Cost of Data Breach Study. IBM and Ponemon Institute. 2016.

7 2016 Data Breach Investigations Report. Verizon Enterprise. 2016.

8 2015 Deloitte Consumer review. Deloitte UK. 2015.

9 Cyber Security at the Speed of Digital Business. Gartner. 2016.

10 Worldwide mPOS Markets: Devices, Technologies and Growth Opportunities 2016-21. Juniper Research. 2016.

11 Press release. Gartner. 2014.

12 2016 Cost of Data Breach Study. IBM and Ponemon Institute. 2016.

13 2016 Data Breach Investigations report – Retail. Verizon Enterprise. 2016.

14 Press Release. National Retail Federation. 2015.

15 Ibid.

16 Corporate statement. Target. 2014.

17 Cyber Security Breaches 2016. UK Government. 2016.

18 2016 Cost of Data Breach Study. IBM and Ponemon Institute. 2016.

19 Press release. Gartner. 2016.

20 Cyber Security Breaches 2016. UK Government. 2016.

21 2016 Cost of Data Breach Study. IBM and Ponemon Institute. 2016.

22 Ibid.

23 Cyber Security Breaches 2016. UK Government. 2016.

24 Ibid.

25 2016 Cost of Data Breach Study. IBM and Ponemon Institute. 2016.

26 Corporate letter to customers. Target. 2014.

27 Transparency, Timeliness, and Putting Principles First. Target. 2014.

Learn more: samsung.com/retail | insights.samsung.com | 1-866-SAM4BIZ
Follow us: youtube.com/samsungbizusa | @SamsungBizUSA

SAMSUNG

This white paper is for informational purposes only. Samsung makes no warranties, express or implied, in this white paper.