IBM Sales and Distribution
White Paper

Retail

The challenge of digital security

What will it take for retailers to protect themselves?

With disastrous data breaches too often in the headlines, retail executives need to re-think the dangers of today's digital environment. What are the best ways to protect the business in the face of fast-evolving threats?

Keeping one step ahead of attackers will require a combination of measures, including robust system defenses, analytics to spot intruders fast, and the ability to react quickly whenever an intrusion occurs.

In the last year, some of the world's most prominent retailers have suffered the most devastating data security failures ever. The fallout from these episodes has been enormously damaging, both in direct financial costs as well as in terms of customer trust and goodwill: one major retailer hit by an attack saw a 46% reduction in its profits during the quarter following its breach.[1]

The perpetrators of such attacks are becoming more and more sophisticated, and the scale and destructiveness of their intrusions is growing dramatically. It's no exaggeration to say that the damage that can now be inflicted by a major security failure can approach the financial and reputational damage an airline might suffer from a serious accident. It's quite possible that we will see a retailer go out of business someday due to an attack that causes a disastrous breach.

In the face of such a dangerous landscape, many retailers are now taking additional steps to address the issue of security: implementing stronger defenses, rethinking process controls, and working with law enforcement to investigate intrusion attempts. But are these efforts enough? What are the best ways to safeguard against digital security failures? How can management be confident that the choices it is making in this regard are as effective – and cost-efficient – as they can be?

At IBM, we're convinced that the retail industry should address the challenge of digital security in a long-term, strategic way, using a multi-layered approach:

- *Anticipate security threats that are likely to manifest in the future, and put in place defenses in depth, to minimize the likelihood of a successful attack.*
- *Use advanced, automated detection mechanisms to detect patterns and catch incipient intrusions before they get far.*
- *Establish a culture of informed vigilance with regard to security, and be prepared to react swiftly and effectively to arrest attacks.*

In this white paper, we describe the long-term nature of the digital security challenge, the array of defenses and practices that are likely to be most effective in protecting a retailer from attack, and how retailers should approach this area of concern within the context of the many other business priorities that vie for executive attention.

A fast-moving target: the evolving nature of digital security threats

The realm of digital security is, by its nature, something of an open-ended arms race between system and data defenses on the one hand and creative, highly persistent attackers on the other. There will likely never be any point at which one side "wins" conclusively – each successful defense strategy or attack plan simply changes the game to a degree and raises the bar for the next round of attack-and-defend.

And let's be clear: *security* is not the same as *compliance*. Simply being compliant with protocols like PCI-DSS doesn't remotely assure that an enterprise is, in fact, well-defended against attack.

It's a safe assumption that, at any given moment, numerous intrusion attempts are underway against every major retailer. This is a demonstrated fact: retail is one of the top five most-targeted industries in terms of the volume of attacks and attempted intrusions.[2] All retailers should assume that they are continuously subject to hacking attempts, and that these efforts are becoming more frequent and more sophisticated over time.

For criminals, retailers can be quite a low-risk and high-profit target. Many of these intruders are located in countries and jurisdictions that have minimal law enforcement with regard to cybercrime, making attackers largely immune to arrest and punishment. And in the case of one of the most commonly sought targets for theft – consumer credit card data – there is a well-established global black market where such data is bought and sold on hundreds of websites, allowing successful perpetrators to profit instantly from their attacks.

Pervasive connectivity opens many new avenues of attack

The retail industry's inherent exposure to security risk is increasing steadily, for many reasons. Most obvious is the vastly increased pervasiveness of network connectivity, as more and more sensitive information is held on networked and distributed systems that are accessible to a widening array of entry points. The broad adoption of mobile applications by retailers adds many other new points of vulnerability. Enterprise applications and data must, in some cases, be made accessible to employee-owned mobile devices. Then add today's complex supply chains, where more access and data is given to vendors and external partners, and where global expansion may require retailers to expand distribution of their own information around the world.

In short, everything is becoming more connected, and the Internet is becoming ever more vital to the functioning of global society and the global economy. With this comes untold benefits and efficiencies, but also some insidious risks and dangers. The recent *Heartbleed* incident has drawn attention to our heavy reliance on – and the vulnerability of – some of the basic building blocks of the Internet. *Heartbleed* worked by compromising OpenSSL, which is used to secure sensitive pages and transactions by over half of the world's websites.

The nature of today's cyber attackers

"Inside jobs" are always a concern, but the sheer number of external attackers is larger (see Fig. 1). And as mentioned, many of these groups and individuals are located in jurisdictions where they may be virtually immune to prosecution or punishment.

Security threats: Types of attackers

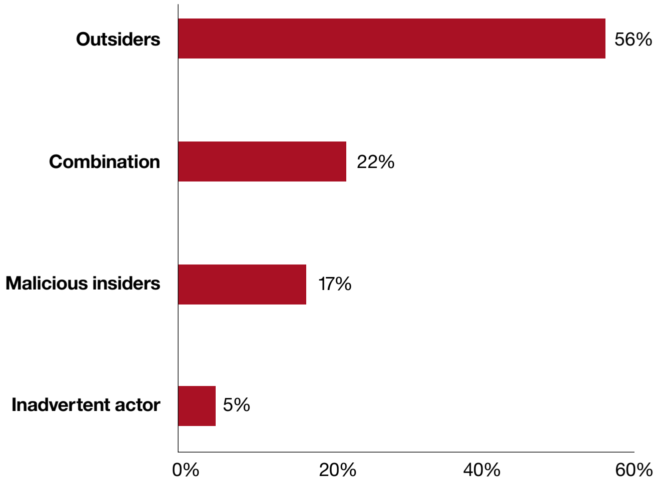

Figure 1: The majority of attacks originate outside the enterprise.
Source: IBM Security Services Cyber Security Intelligence Index. IBM Corporation. July, 2013.

Many intrusion attempts are executed by attackers who are operating opportunistically, to exploit "doors left unlocked." These are still remarkably common and they can make life easy for criminals: they include basic security lapses caused by lack of discipline and poor adherence to process controls, as well as system misconfigurations that can remain unrecognized and uncorrected for an extended time (see Fig. 2).

A smaller but still substantial number of intrusion attempts are the result of sustained, concentrated efforts to gain knowledge of a company's systems and controls, so that the perpetrators can employ an informed approach – using malware or another method – to thwart these controls. Their objective may be to gain access, steal data, or sometimes go even further, such as taking clandestine control of specific systems (see Fig. 3).

First things first: addressing the most common vulnerabilities

Let's first take a look at the most common failure points that let intruders gain easy entry. Attackers prefer to hit wherever security is weakest and where it will take the least effort to steal something valuable.

According to the IBM Cyber Security Intelligence Index, these are the five most common vulnerabilities that attackers exploit. A retailer that takes steps to address these weak spots will close the door on a wide range of intrusions that would otherwise likely be successful:

1. End user didn't think before clicking to open an email or website

This is still painfully common, and needs to be addressed primarily by effective process controls and an informed culture of vigilance.

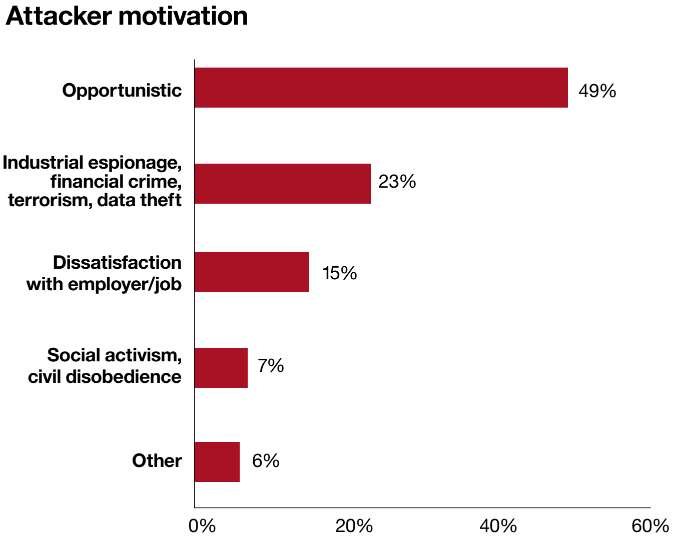

Figure 2: Opportunistic hacking still accounts for about half of all intrusion attempts
Source: IBM Security Services Cyber Security Intelligence Index. IBM Corporation. July, 2013.

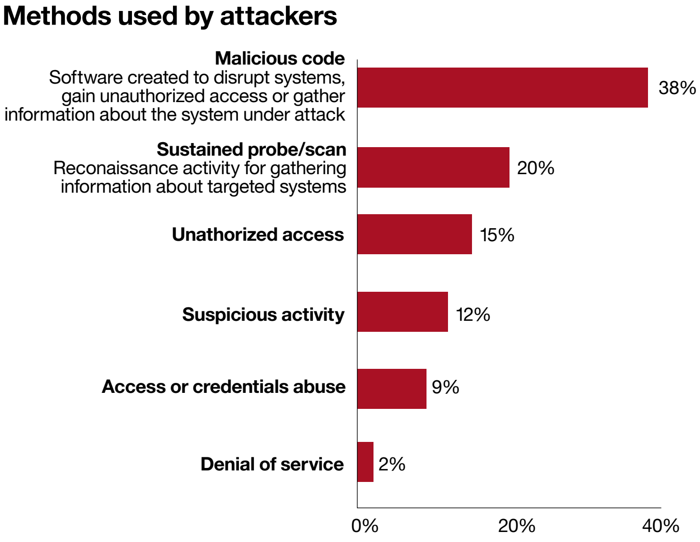

Figure 3: Malware and sustained system probes are the tactics used most often by attackers
Source: IBM Security Services Cyber Security Intelligence Index. IBM Corporation. July, 2013.

2. Weak or default passwords in use

Again, processes and internal controls are central here, and can be reinforced by advanced system security to consistently enforce password standards.

3. Insecure configurations

Attackers are always probing to discover misconfigurations that have inadvertently created open-ended security holes. This issue must be addressed through a combination of greater vigilance in process controls and improved testing during the process of system configuration, as well as by the use of analytics to detect and report irregular activity that could indicate an intrusion that is taking advantage of a system misconfiguration.

4. Use of legacy or unpatched hardware or software

As with #3 above, attackers are always probing to find lapses of this kind. This issue has to be addressed in a similar manner, through improved process controls and through analytics to detect irregular activity.

5. Lack of basic network security protection and segmentation

Too often, existing controls and defined safe practices are simply ignored or disregarded, as security takes a back seat to other priorities. Retailers need to institutionalize critical practices around network protection and data-access security, and take proactive steps to monitor and ensure adherence.

Beyond the basics: crafting a retail security strategy in depth

Given the ongoing evolution of the tactics used in intrusion attempts, it's important for retailers to keep in mind not just the methods that have been used in the recent past, but also the patterns that suggest the shape that defenses will need to take in the future.

IBM's recommended enterprise security strategy relies on three key elements. Each must be robustly implemented to establish effective defenses in depth:

- *Advanced system security*, to provide defense at every network access point, with intelligent security fences to impede breaches and isolate threats, supplemented by defenses to protect each type of sensitive data.
- *The use of advanced analytics as a weapon*, to continuously scan for and detect patterns that may indicate an intrusion, so these can be brought to management's attention and contained before they do serious harm.
- *Effective process controls and rapid response mechanisms*, to enforce good habits regarding digital security, to establish a culture of informed vigilance, and to enable quick action when a breach does occur.

These three layers of protection can be consistently effective in frustrating intruders and mitigating attacks. When employed in a thorough and consistent manner, they can help to address future security issues through early detection, removal and remedy.

Advanced system security: defending at every network access point

Barriers at access points are designed to keep intruders off the network. These are the first line of defense against external attack.

We choose to use the term *network access point defense* here, rather than *perimeter defense*, because "perimeter" may suggest a single boundary line that one might intuitively equate with the boundaries of the enterprise. But in today's interconnected environment, a retailer's secured network can extend far beyond this to include elements that are the responsibility of suppliers, contractors, business partners, employees and others. For this reason, in order to effectively secure the network, attention must be paid to each of these access points and each must be secured by an appropriate defense.

The widening array of network access points

To give a sense for the range of access points a retailer must identify and secure, at a minimum these will likely include:

- Point-of-sale (POS) terminals in stores
- Mobile POS access points
- Customer-facing e-commerce websites
- Links with each third-party vendor, supply-chain vendor, ecosystem partner and contractor
- Employee-facing access points — including those that may utilize employee-owned mobile devices — and the social workplace
- Links to connected data centers via the cloud
- Links to financial institutions and payment processors
- Links to managed service providers
- Links to delivery services
- Links to all other contractors who are provided with network access
- B2B, intranet and extranet portals
- In-store wireless routers, kiosks and networks
- The expanding "Internet of Things": IP-based printers, IP-linked surveillance cameras and similar devices

Accounting for every network access point is becoming more challenging as the shape and interconnectedness of the digital world gets more complex. To cite an example of a relatively recent development that can have an impact here: connected applications may extend to mobile platforms, hybrid clouds, and into arenas like Infrastructure-as-a-Service (IaaS) and virtual data centers. When combined with the emerging "Internet of Things"–the widening range of network-connected devices–this represents more avenues for intrusion and attack. Since connected apps are frequently updated and repaired via automatic patches that might contain a virus or other malware, this represents another source of danger.

Attackers who find their way onto any given component on a network can conceivably find a way to get to seemingly unrelated components–even the "crown jewels" of the enterprise. The 2013 breach at Target highlights how important it is to secure every access point–even those outside the enterprise itself. In this incident, the attackers were apparently able to use the stolen credentials of one of Target's heating/air-conditioning contractors to work their way onto the retailer's store network, eventually succeeding in stealing a huge quantity of customer credit card data from their POS systems.[3]

News accounts indicate that the initial intrusion happened several months before the mass theft of data was executed. The intruders were apparently confident enough that they chose to lie in wait for several months, until the massive burst of shopping activity over the U.S. Thanksgiving Day weekend gave them the opening to steal a vastly larger trove of sensitive customer financial data. The thieves were able to maneuver across Target's systems until they were in position to use malware now known as KAPTOXA/BlackPOS to pull decrypted credit card data from Target's store POS systems.[4]

The bottom line here is that retailers need to take careful inventory of all their network access points and assess the risk posed by each. Then, the appropriate defenses and controls must be implemented and enforced. At the same time, a process must be put in place to review this inventory of access points on a regular basis, to identify changes and additions.

Data security: protecting valuables inside the enterprise

If effectively implemented and maintained, network access point defenses will keep most intruders from penetrating a retailer's systems. But there will be intrusion attempts that make their way past these defenses. The second line of access defense, therefore, is specific protection for each form of sensitive data.

Although customer credit card data has been the target of many of the most damaging recent intrusions, retailers need to consider the entire range of data they hold that merits protection (see Fig. 4).

The process that must be followed here requires identifying every kind of data that needs protection and then every instance of such data that must be secured. These protections might take the form of access and port restrictions, strengthened encryption methods, tokenized data vaults, selective network segregation, identity management and other barriers. The goal must be to maintain the access that is required to conduct business smoothly, while frustrating unauthorized or suspicious access attempts.

A South Korean multi-channel retailer addresses endpoint security to ensure business continuity

This retailer, who markets its products through cable television, web, catalog and other channels, suffered a damaging outage that interrupted their business in 2012. An issue was their reliance on infrastructure that lacked appropriate security controls.

IBM Security Services evaluated their environment and recommended Geni Networks Genian NAC software to guard against viruses and malevolent network traffic, as well as Symantec Data Loss Prevention software to protect critical information.

By establishing more effective endpoint controls and safeguards for data, this retailer has significantly reduced the risk of business interruption, as well as the risk of a serious data breach

Categories of sensitive data requiring protection

	Potential damage from a successful breach/theft		
Type	Trust	Competitiveness	Bottom line
Customer data	High	High	High
Employee data	High	Medium	Medium
Enterprise financial data	Medium	High	High
Pricing/strategy data	Medium	High	High
Vendor data	Medium	High	High
Inventory data	Medium	High	High
Product data	Medium	High	Medium
Location data	Medium	High	Medium

Figure 4: Retailers hold a broad range of information that could be damaging if exposed.

A European retailer improves security while lowering costs with IBM solutions

This retailer sought to provide security services to their internal customers and to third parties following a transition to new ownership and a related migration to new infrastructure.

To provide management and monitoring for the new infrastructure, IBM Managed Security Services delivered a turnkey solution that included IBM firewall management, intrusion detection and prevention, SecureWeb Gateway, and X-Force® Threat Analysis, plus technology from Cisco and BlueCoat.

These services were provided under a single contract, with migration services and managed security services, which reduced transition and implementation time significantly and provided a single point of contact for all network security-related components.

Using analytics as a weapon: detecting and blocking intruders before they get far

Access-point and data-specific safeguards notwithstanding, every retailer should expect that at least a few intruders will make it past both these barriers. For that reason, analytics must be in place to watch for patterns that could indicate an intruder in the system and to issue alerts so counteractions can be taken quickly.

Analytics therefore represents the proactive counterpart to defensive access-point barriers. While many intrusion attempts will be defeated, the prudent approach is to assume that barrier walls can never be high enough. The questions then become, “How quickly can we identify and counter each successful entry?” and “Will we be able spot intruders immediately, before harm is done, or only much later, after a disastrous disruption or loss of data?”

Spotting threat patterns proactively

Security analytics tools work by scanning to identify anomalous behavior within your network: patterns that might indicate that something suspicious is taking place. Monitoring infrastructure logs, security logs, database logs, network data packets, DNS transactions, configuration changes and even social chatter, these tools look for the unusual, with specific attention paid to actions that touch upon sensitive data. Advanced analytics tools even go a step further and watch for patterns as they may manifest across signals from different sources and different kinds of activity.

When they identify an action or pattern that appears out of place, security analytics tools can alert managers, who can then take a closer look to determine whether further investigation is warranted. The best and most advanced of these tools are designed to “learn” from the evolution of network activity, so as to dynamically refine the criteria around what may constitute unusual behavior. They are also regularly updated to watch for new intrusion tactics.

An effective and well-deployed security analytics tool will be able to identify genuinely suspicious patterns of activity, while avoiding an excessive number of false alerts. It will also present to security managers the relevant information on the nature of activities in a concise and accessible way. Both of these characteristics are critical to timely and appropriate counteraction.

Effective process controls: establishing a culture of security, and reacting rapidly

Once network access defenses and analytic defenses are in place, the goal becomes to keep system security up-to-date and as advanced as possible, while maintaining and strengthening process controls. Security must also include the human element: the need to foster a culture of informed vigilance is a “softer” and more elusive part of an effective security posture, but nonetheless a vital component.

Looking back at the most common vulnerabilities discussed earlier, it bears mention that the top two of these indicate a deficient culture of vigilance: end users not thinking before clicking on an email or attachment, and of the use of weak or default passwords. Some of these vulnerabilities can be policed through automation, such as enforcement of strong passwords, but technology solutions can be only part of the answer. These topics must be addressed directly with employees, suppliers and others who have access to secured assets, and whose behavior has an inevitable impact on security. Management at every level of the enterprise must make it a priority to address the issue of security regularly, to make it a central feature of the life and culture of the organization.

And since an actual breach is always possible, retailers need to be ready to react decisively. The goal is to quickly contain the intrusion, assess the damage, and address the situation, in terms of rectifying the failure as well as in communicating responsibility outwardly to customers and the public in a proactive and thoroughgoing way. Doing so will limit the direct cost of the intrusion as well as the potential damage to trust and reputation.

Learning from the experience of others

It's a truism that one tends not to get rewarded for disasters that didn't happen–and the measures that have prevented disaster may erode over time, in the absence of a costly failure that would demonstrate their value and importance. This risk of complacency is one of the challenges inherent in maintaining effective security over the long term.

For this reason, when addressing security within their organizations, retail executives should certainly make reference to failures that occur at other retailers and to the intrusion attempts that are taking place everywhere, all the time, in all industries. These should serve as constant reminders of how close and immediate the threat remains.

A multinational supermarket chain implements role-based user access controls to facilitate the conduct of business while safeguarding data

This retailer wanted to increase sharing and internal communications around customer-related data, and wanted to make employee HR functions easier to access. But they were also concerned about maintaining proper controls over the distribution of these kinds of information.

Using IBM Security Identity Manager in conjunction with IBM Websphere, this client implemented user access controls for its internal employee portal to create a single sign-on, personalized work environment. Individual access rights are automatically updated as roles change and as employees are on- and off-boarded, and each person's use is recorded to ensure audit-readiness and compliance with security standards.

The retailer credits this solution with helping to facilitate and streamline the functioning of their business, while at the same time restricting access to sensitive data to those having verified and legitimate purposes.

The cat-and-mouse game will always mean that whatever security is in place can never be assumed to be provide perfect protection. This is an arena in which the weaker players can expect to be victimized more readily than the strong. Whenever a security failure is reported at another enterprise, an immediate re-evaluation to assess one's own vulnerability is warranted. This is particularly true if a failure is a result of a new form of intrusion: retailers always need to be ready to quickly take new pre-emptive steps as information about new threats emerges, to stay one step ahead of the attackers.

Next steps: re-assessing the strength of current defenses

Retailers seeking to take a fresh look at their security posture should:

- *Establish a recurrent process that comprehensively re-evaluates all security measures in place*, including network access point defenses, analytics to detect incipient intrusions, and the maintenance of a vigilant internal culture through strong process controls and habits. To be robust, such re-evaluations must be performed by someone other than those who have been responsible for defining and implementing current security defenses. This helps to ensure objectivity, and a fresh view on existing defenses, to spot vulnerabilities that the organization itself has not identified. External security specialists should be utilized to assure that the assessment will be thorough and independent.
- *Use the findings of security assessments to prioritize the next steps*, and define an action plan to bring all elements up to strength.
- *Keep an eye on the evolving nature of security threats:* Success in preventing intrusions means that the organization needs to watch how the failures of others occur and immediately take steps to pre-empt similar incursions.
- *Establish security as an ongoing theme and priority*, shared by executives at all levels and reflected in the culture as well as the engrained habits of employees, suppliers, and other relevant parties.

Certainly, there is no “magic bullet” here. Digital security will remain a primary concern into the indefinite future, and must therefore be treated as a continuing and significant risk by organizations of all kinds.

IBM offerings for retail security

At IBM, we consider it one of our foremost responsibilities to provide the most effective security support for our clients. IBM offers one of the most advanced and comprehensive portfolios of security-related services and solutions for the retail industry.

IBM service offerings

An *IBM Cybersecurity Executive Awareness Briefing* can help educate on the anatomy of current attack methods and defenses, the role of social media, and the latest advances in technological and operational defenses. This briefing can be useful in helping define key actions that can be taken to immediately bolster defenses.

The *IBM Security Maturity Benchmark Assessment* can evaluate the effectiveness of a retailer’s overall security defenses, using data to make specific comparisons with peer organizations. This assessment can therefore highlight where a retailer is strongly defended, and where it is vulnerable, providing the basis for a security enhancement plan of action.

IBM software offerings

IBM’s comprehensive range of technology solutions can establish strong defenses for network access points and for each type of data that requires protection.

IBM QRadar® Security Intelligence Platform can serve as a foundational element of retail organizations’ network defense capabilities, helping to cost-effectively guard against sophisticated attackers. QRadar encompasses advanced threat detection, intelligent vulnerability analysis, device configuration alignment, and network traffic telemetry reviews, as well as other elements. QRadar collects events and logs from a heterogenous set of sources including network infrastructure, security devices, servers, operating systems and applications. It then normalizes all events to enable out-of-the-box correlation with other events, network flows and intelligence feeds. In addition to event data, QRadar also gathers vulnerability insights within profiles built for each business asset, by passively monitoring network traffic between all IP addresses.

IBM Trusteer Apex can extend this protection to help prevent advanced malware from gaining control over user access points, and from stealing data or propagating advanced attacks. Trusteer Apex is designed to prevent exploitation of unpatched and zero-day vulnerabilities. Unlike many other solutions, Trusteer Apex does not rely on traditional malware detection processes like signatures and behavioral profiling, which can be bypassed by advanced evasion techniques. Trusteer Apex blocks application vulnerability exploitation – the primary way cyber criminals install malware on endpoint devices – even while organizations test the impact of vulnerability patches across their software suites.

IBM Security SiteProtector™ System provides virtual patching capabilities, using network intrusion prevention system signatures to block associated connections, and helping to protect against the exploitation of identified vulnerabilities.

IBM X-Force threat intelligence feed supplies up-to-date information on recommended fixes and security advice for active vulnerabilities, viruses, worms and threats

IBM Endpoint Manager streamlines remediation tasks by automatically managing patches to hundreds of thousands of endpoints, including the latest mobile devices, and provides integrated reporting for real-time monitoring of patch progress.

IBM Security AppScan® supports web application vulnerability assessments, enabling QRadar Vulnerability Manager to provide visibility and prioritization of web application vulnerabilities within its integrated dashboard.

IBM InfoSphere® Guardium Database Vulnerability Assessment supports the scanning of database infrastructure, enabling QRadar Vulnerability Manager to provide visibility and prioritization of database vulnerabilities within its integrated dashboard.

Find out more

For more information, please contact your IBM representative or visit:
ibm.com/retail

About the authors

Mark Yourek is IBM Global Solutions Lead for the Retail Industry.

Vish Ganapathy is IBM’s Global Chief Technologist for the Retail Industry.

Karl Cama is IBM’s Executive Architect for the Retail Industry.

Sources

[1] Ziobro, P. "Target Earnings Slide 46% After Data Breach." Wall Street Journal online. February 26, 2014. http://online.wsj.com/news/articles/SB10001424052702304255604579406694182132568

[2] IBM Security Services Cyber Security Intelligence Index. IBM Corporation. July, 2013.

[3] Krebs, B. "Target Hackers Broke in Via HVAC Company." Krebs on Security. February 14, 2014. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[4] Freed, A. "FBI Says Kaptoxa/BlackPOS Malware Connected to Twenty Breaches." *Tripwire News*. January 24, 2014. http://www.tripwire.com/state-of-security/top-security-stories/fbi-tells-retailers-credit-card-breaches-expected/

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2014

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Please Recycle