Security
Thought Leadership White Paper

Four steps to smarter mainframe data security

Protect the "crown jewels" of your enterprise data with IBM Security solutions

IBM

Introduction

The value of data has skyrocketed—and with it, threats to data security. As the repository of everything from a company's intellectual property to employee and customer financial information, data is no longer of interest solely to its owners. Now, it also has significant allure for criminals who would capture and sell it. Consider: A large insurance provider loses to theft the personal information, including health records, for 80 million customers.[1] A major retailer loses credit card information on 56 million customers.[2] An international entertainment company loses 100 TB of data ranging from confidential emails to financial information on nearly 10,000 employees.[3]

But while the frequency and scope of these events make data breaches common knowledge, the conditions that make them possible are not as widely understood. Neither are the steps an organization should take to protect itself. The fact is, even the best-protected organizations need to enhance their protection against attacks.

Organizations that deploy highly-securable IBM® z Systems™ mainframes have protection built in—including security in the processor, operating system, storage and applications. They can address security requirements such as identity and access management, hardware and software encryption, and event logging and reporting. These capabilities have made IBM mainframes the platforms of choice for high-target industries. Ninety-six of the top 100 worldwide banks, 23 of the top 25 US retailers and 9 of the top 10 global life/health insurance providers run IBM mainframes.[4]

But even mainframe environments need protection against growing threats and their new levels of sophistication. They need to meet an increasing number of regulations from industry and government as well as addressing concerns from the public about whether data is sufficiently protected. And they must continue to support not only the database operations they have traditionally run, but also evolving technologies such as mobile, cloud, big-data analytic computing and a growing variety of different data sources outside of the database.

This white paper examines the security impact today's changing computing landscape has on mainframe environments, introduces the steps organizations must take to achieve the security they need, and provides an overview of IBM solutions that help provide protection.

Today's mainframe world is not what it used to be

Mainframes have achieved enormous acceptance in enterprise environments. Today, 80 percent of the world's corporate data originated on or currently resides on the mainframe platform.[5] Some 65 percent of business transactions for US retail banks are conducted on mainframes.[5]

Deployed in their traditional manner, mainframes achieved security in part by functioning in relative isolation. In such deployments, mainframes carry out operations on structured data in a tightly controlled data center. But these back-office production deployments are no longer the rule. In a world of exploding data volumes, where information originates from and resides in a wide variety of platforms, the mainframe no longer works alone. It shares more information and makes more connections with distributed environments and the Internet than ever before. Today's mainframe is considered a big-data integration hub.

In addition to databases, mainframes host mission-critical information such as financial data, business plans, product designs and source code for business applications. They host data that arrives non-stop via mobile devices. Data that is accessible worldwide via the cloud. And data that is constantly changing—and changeable by virtually anyone—via social media. Mainframes host an ever-widening variety of applications.

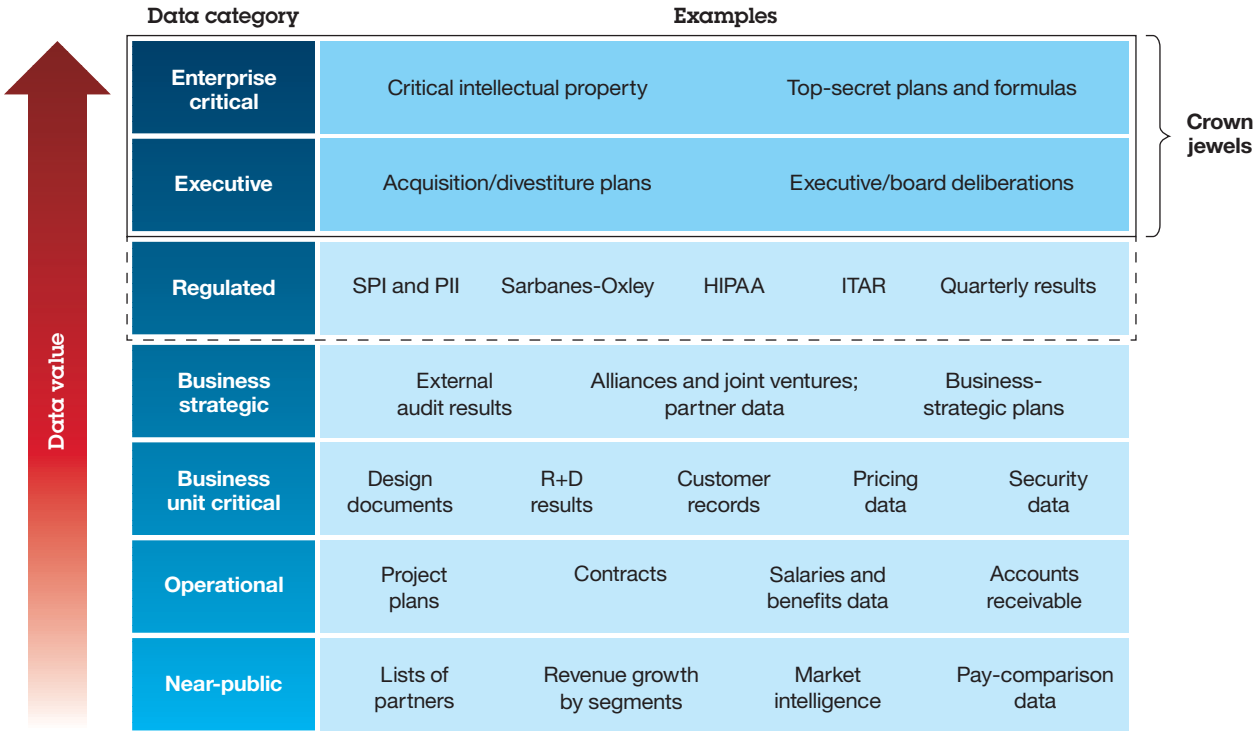
In virtualized environments, they reach across the enterprise, pooling resources with other systems, including those inside and outside of the enterprise network.

These connections bring new capabilities to mainframe environments. But they also bring the potential for additional cyber threats and data breaches. Because now, mainframes are connecting with systems, devices and applications—with entire environments—that often are not assumed to be secure.

Criminals don't attack randomly. They target your "crown jewels."

Organizations that deploy highly securable mainframes face challenges today from the world outside the data center. And it's a world that isn't deterred by the platform where data resides. Users of mobile and social media don't care whether the data they create goes to a mainframe or distributed servers—they just want to make a connection. Regulators want to know that data is managed to uphold privacy and compliance, regardless of the platform where it resides. As for cybercriminals, all they're concerned about is finding where they can extract the most value. Today's attackers aim for an organization's crown jewels—business-critical data of high commercial value.

Enterprise data "crown jewels" are the prize that today's attacks target



Attackers have learned, in fact, that the most valuable data typically represents a very small percentage of most organization's data holdings. They know that once they find a way into the environment and locate their target, the data's relatively small size makes it possible—even easy—to exfiltrate. And they have discovered that today's interconnected enterprise environments provide multiple paths for theft. Then, once they've successfully stolen from one organization, they frequently turn on others in the same industry. That's because these companies' asset types, storage and management technologies, application programs, communication protocols, and security strengths and weaknesses tend to be similar.

Across organizations, for example, cloud computing provides a direct pipeline for information entering and leaving the data center. This data is typically stored on shared or pooled devices, and is often hosted and managed by third-party providers, where security may be lax, as well as extremely complicated.

Mobile computing generates data explosively anywhere and everywhere, and it does so around the clock. Important for users—and for criminals—this data is always accessible via private devices, not devices controlled by the organization.

Big data is the high-volume, structured or unstructured product of mobile, cloud, distributed and mainframe platforms. This data can yield business insight that is not only valuable to its owners, but a lucrative target for thieves and competitors.

With today's multiple perimeters, where do you put protection?

Significantly, the data breaches that occur via cloud, mobile and big-data computing are not specific to mainframes. They are the result of today's highly interconnected and increasingly complex distributed environments. But mainframes are a part of those environments, too. Applications on other platforms rely on mainframe-based data to get their jobs done. As a result, breaches on one of these platforms can affect the data that resides on the mainframe. A disgruntled employee may abuse access privileges to pass intellectual property to a competitor. A malware "bot" may lie hidden in the distributed infrastructure, waiting for the right opportunity to capture and exfiltrate data as it crosses the network on its way into or out of the secure mainframe. Contractors and operations staff may be granted special access that bypasses normal security protocols. And weak password values, especially for privileged users, can be compromised.

In these scenarios—and especially in mobile and cloud computing—the defensible perimeter of the computing environment shifted some time ago. Firewalls are no longer sufficient to guard against advanced attacks. Today, protection cannot simply form a ring around the data center; it has to secure every device. This can be a difficult task, as widespread devices can create hundreds of thousands of potential points of entry into a large enterprise. But business today demands openness. Customers, contractors, employees, partners and suppliers all need access to an organization's infrastructure and data resources to conduct transactions.

Mainframes play a role in this new openness. They connect to distributed, mobile and cloud-based devices. They store and process the big data that flows into and out of the enterprise via these many conduits. And mainframes, with their highly securable, highly manageable architecture, can also play a role in protecting against threats. When it comes to security, the primary need of an enterprise is to protect its crown jewels data. And whether operating in a traditionally cloistered, database-centric data center or today's newly open environments, mainframes are designed precisely for this purpose. They provide intrinsic protection that is not available on other platforms. They deliver a set of data management and security tools that can enhance protection across the enterprise.

Even mainframes are subject to security challenges

Compared with other platforms, mainframes are better suited to protecting critical information, but they are not without challenges. As mainframes increasingly share information with cloud, mobile and distributed environments, security teams must put more and more preventive, proactive methods in place, such as sustainable access controls, real-time alerting and reporting of suspicious/abnormal behaviors. They must deploy scalable, integrated solutions that meet the expanded demands of platforms and big data. They must avoid any negative performance impact that security solutions might have on the rest of the environment. They must continue to comply with privacy and security regulations to support best practices.

So if the advantages and requirements of mainframe security are known, what's standing in the way?

For many organizations, mainframe management comes up against perceived difficulties that are external to the system—but that can be effectively resolved with the right solution. Costs are rising due to the shortage of skilled administrators—but can be controlled with automated administrative tools and processes. Compliance can be hard to maintain—but can be monitored with automated verification and real-time alerts. Stopping threats can be complex and critical—but can be made more effective with state-of-the-art security intelligence. Visibility can be opaque—but can be clarified by breaking down the silos separating processes, procedures and reports from the rest of the organization.

And while mainframes themselves provide highly securable environments, standard mainframe management practices can also be enhanced. Increasing the granularity of access controls can help prevent vulnerabilities that result when users are granted greater data privileges than their jobs warrant. Giving the security team easy-to-use tools can eliminate the common tendency to delegate security management tasks to system programmers who can handle complex technologies but who lack a security mindset and who have performance and availability as their core objectives instead. Technologies such as data masking and encryption can help reduce risk when organizations share disks among development, test and production environments. Comprehensive monitoring, alerting, analysis and reporting tools can help ensure the security team doesn't miss intelligence about vulnerabilities in their defense and the strength of attacks.

And on top of it all, there's a critical factor that organizations cannot ignore—the need to act quickly to proactively protect data. A cybercriminal has no boundaries and is lying in wait. In fact, to defend against today's sophisticated attacks, the enterprise must assume that it is continuously under attack. This is especially true for the cloud, mobile and distributed platforms that connect with mainframes. An attacker's attempt at a data breach may take only seconds or minutes to occur, but malware that enables data theft is likely to operate undetected for days, weeks or even months, compromising systems and extracting valuable information. In the interim, the rewards for a cybercriminal can be massive.

Security professionals, on the other hand, know that preventive measures will always be more effective than other controls, making prevention the best form of defense. The key is to think like a hacker—then your first instinct will be to ask: "How can I prevent this?"

Now the focus of protection moves from infrastructure to data

The shift from firewalls surrounding the data center to protection for users' devices has been critical to ensuring security in distributed and mobile environments. But recently, another significant shift has been gaining ground. Increasingly, the emphasis is on protecting not only the device but the business data on the device. Because data is where value resides.

Properly managed, the highly securable architecture of the mainframe can be instrumental to avoiding data theft or compromise. With its increasing connections to distributed, mobile, cloud and big-data environments, the mainframe can also be the ideal platform for helping secure data throughout the enterprise.

To realize the benefits a mainframe can provide, organizations need to enhance their information governance capabilities. By orchestrating people, processes and technology, information governance can improve management of information quality, the information lifecycle, and information security and privacy. Ultimately, organizations need information governance capabilities that can enhance data quality to help improve customer satisfaction, meet the demands of regulators and auditors, lower business risk, and drive new business opportunities.

In fact, working together with day-to-day mainframe management, governance becomes a critical part of protection in the new data-security model. Deploying the right hardware and software technologies is not enough. Standards for system security as well as processes and controls that oversee functions and people are both critical. Even in a secure mainframe, the security team must detect, track, observe and report on what's happening with data—not only because breaches can go undetected if actions are not monitored, but also because people inside and outside the organization alike can wreak malicious or careless havoc. Their actions can have devastating effects on the integrity and availability of data, ultimately impacting the ability to operate the business and meet core objectives.

Data residing on a mainframe can represent a high-value target

The shift to protecting data recognizes the importance of enterprise data. This includes financial and personally identifiable information that cybercriminals can use to commit fraud—and that usually get the attention in a major data breach. But crown jewels also include intellectual property and trade secrets that form the heart of an organization's identity and mission. Information such as new product designs, formulas and features; research and development findings; and IT system architecture designs, source code and algorithms can all carry tremendous value. So can information that in the past was not considered useful at all—but that is now made valuable with its ability to yield business insights via analytics.

With their built-in security capabilities, mainframes are often the repository for this most valuable data. And information in databases, which often reside on a mainframe, represents precisely the high-value targets that cybercriminals seek. Mainframes may be secure—one recent study found that only six percent of successful breaches involved databases. But among the breaches that are successful, the study found that high-value records from databases represent 96 percent of the information stolen.[6] It is true that less secure mobile, cloud, distributed and big-data platforms also contain valuable data that needs protecting. This is the case considering today's increasing data sharing and systems connectivity. But clearly, the data on a mainframe is what cybercriminals are ultimately after.

What steps can you take to enhance mainframe security?

The primary goal of security is to reduce an organization's exposure to threats and risk. And to achieve that, there are well-defined steps for the organization to follow—from defining what the crown jewels are, to implementing security processes and controls, to monitoring ongoing security-related events. The security team needs to examine data at rest, data in motion and system configurations. It needs to ask where sensitive data is located, who should own it, who should have access, how the team can prevent unauthorized access, and more.

Steps to effective information governance

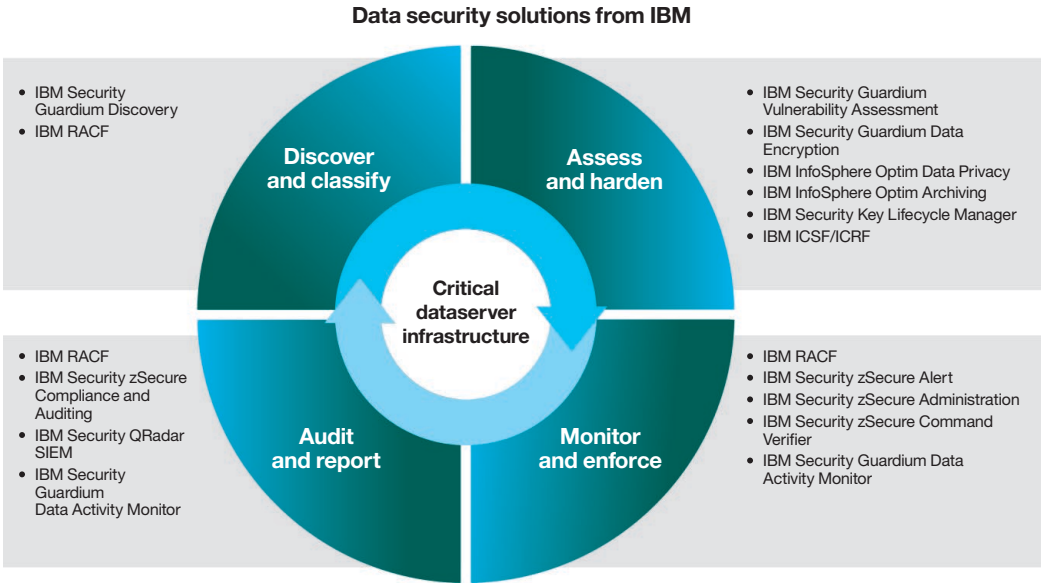
As a foundation for providing security, the organization needs to ensure there are no vulnerabilities in the dataserver hardware or system software infrastructure. If vulnerabilities exist—in system configurations or authorized program libraries, for example—cybercriminals can often find a "back door" that gives them access by circumventing the system's security management and governance controls. This can be true even for the highly securable mainframe platform, especially when the mainframe is connected via the network to less secure platforms such as mobile, social media, distributed and big-data environments. This vulnerability requires an in-depth approach to defense.

With the infrastructure made secure, the process for establishing effective information governance then proceeds with discovering what data the organization has and where it is stored, then classifying the information to reflect its sensitivity. The organization next assesses vulnerability (For example: Have all recent patches been applied?) and takes steps to make it secure. The organization monitors ongoing actions (Who is accessing data? When are they accessing it?). It enforces policies against actions that threaten data security. It audits and reports on the results to identify additional vulnerabilities and help ensure security in the future. And this process is repeated continuously throughout the data security lifecycle.

Each phase involves key capabilities, including:

- **Step 1: Discover and classify—**The security team scans the network to develop an inventory of data sources—and schedules regular scans for the future to discover new instances that it must protect. Because sensitive data is not revealed in a simple scan, organizations can undertake custom discovery processes that include descriptions and examples, scans for matching columns, searches for sensitive data in free text columns, and searches for sensitive data that is partial or hidden.
- **Step 2: Assess and harden—**Mainframes have built-in security features such as automated data encryption. This protects data at multiple points, including in processing, during transmission and communication, and at rest. To supplement the mainframe's capabilities, however, the team needs to assess the entire infrastructure for vulnerabilities such as unpatched and misconfigured systems, or inappropriate privileges granted to users. It must mask data used for testing during development processes while retaining any behavioral characteristics. It must ensure scalability of encryption and performance across multiple, diverse devices.
- **Step 3: Monitor and enforce—**To keep up with the speed and force of threats, security teams need to employ continuous, policy-based and real-time monitoring of all data—including big-data traffic and actions by privileged users, as well as data indicating suspicious behavior that must be blocked. To help prevent compromise by insiders as well as attacks by cybercriminals, the organization can create custom policies and processes by specifying combinations of workflow steps, and separation of duties, actions and users. To ensure compliance and reduce operational costs, it can automate oversight processes.
- **Step 4: Audit and report—**Ensuring security is a continuous process. It doesn't stop with deploying applications—or even a high-security mainframe. Security teams can't let up on their efforts to gather information and gain insights into threats and potential breaches. The ability to monitor access to sensitive data—including access by specific users—is critical. Custom and pre-built compliance reports can help. So can the ability to easily create custom reports with an easy-to-use, point-and-click interface. The ability to integrate the report information across an enterprise with security information and event management (SIEM) solutions helps identify large-scale attacks.

These steps to information governance support enterprise-wide protection across databases, platforms and data streams—for a preventive and proactive approach that is far less expensive than trying to clean up the years of financial impact the business can suffer as the result of a data breach. The process dovetails smoothly with leading solutions from IBM designed to help reduce exposure to risk and provide fast response in today's rapidly changing threat landscape.

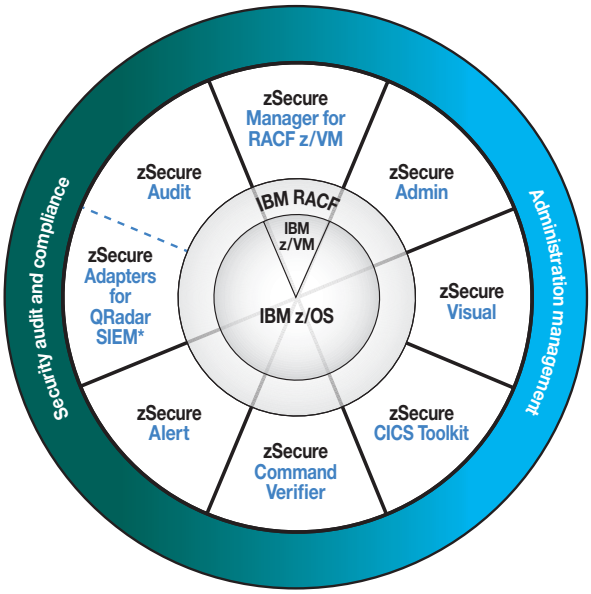


What solutions should you deploy to provide mainframe security?

The new openness in enterprise computing environments has created new opportunities for data breaches. IBM X-Force® has found, for example, that 33 percent of all disclosed vulnerabilities are web application vulnerabilities.[7] And the impact can be huge. The average cost of a corporate data breach is now set at USD6.5 million.[8]

IBM can help protect against these threats with best-of breed security solutions. Capabilities build on a 50-year tradition of features such as encryption that are inherent to z Systems mainframes. Additional capabilities are provided by a portfolio of integrated industry-leading IBM Security software offerings that are kept constantly up-to-date to meet today's changing threats. Integrated mainframe software offerings help provide security with measures such as real-time monitoring, alerting, behavior blocking, vulnerability identification, and security intelligence reporting. With IBM solutions, organizations can help reduce their risk exposure and better protect data while complying with regulations.

IBM Security zSecure suite



* Product offers a subset of the capabilities provided by zSecure Audit

- **IBM Security Guardium suite:** Helps protect many enterprise-wide data sources with continuous, policy-based, real-time monitoring of data traffic activities, including actions by privileged users. Guardium solutions provide automated blocking of data with automated workflows to support regulatory compliance and scanning to identify vulnerabilities such as missing patches and misconfigured privileges. Capabilities also include granular encryption for databases, data masking and archiving of unnecessary data.
- **IBM Security zSecure suite:** Provides automated and integrated solutions for IBM z/OS®-based systems via security analysis, threat detection, problem remediation, user provisioning, compliance auditing and enterprise-wide security intelligence. zSecure solutions provide management across strategic applications, transactions, data and applications, including cloud, mobile and big-data applications.
- **IBM QRadar Security Intelligence Platform:** Provides a unified architecture for integrating SIEM, log management, anomaly detection, incident forensics and configuration, risk management and vulnerability management. Full visibility into network, application and user activity supports regulatory compliance with collection, correlation and reporting.
- **IBM Resource Access Control Facility (RACF):** Integrates with the mainframe's built-in security features to enhance data security still further. An industry leader for almost 40 years, RACF identifies, verifies and authorizes system users; identifies and classifies system resources; logs and reports attempts at unauthorized access; and protects data resources by controlling access with integrated IBM DB2®, IBM IMS™ and IBM CICS® controls.
- **IBM InfoSphere® Optim™ Data Privacy:** De-identifies confidential data on demand throughout the enterprise including big-data platforms. It masks data statically or dynamically in applications, databases and reports across production and nonproduction environments. It comes with predefined actionable data privacy classifications and rules. While masking the true value of the source data, it retains the data's behavioral characteristics and referential integrity.
- **IBM Security Key Lifecycle Manager:** Provides a single point of control, policy management and reporting to simplify encryption key security lifecycle management. Integrating with IBM self-encrypting storage systems, it helps address regulations that call for strong protection of encryption keys.

Conclusion

The rapidly growing and constantly evolving threat of enterprise data breaches means that highly securable technologies—including mainframes—need more protection than ever before. Increasingly, mainframes connect to and share data with mobile, cloud and big-data environments. These less-secure platforms might provide cybercriminals with "back door" access to data as it passes across the network and into and out of the secure mainframe. Users who gain unauthorized access privileges or authorized users who exceed their privileges can present further risk even to a secure mainframe.

To protect the valuable crown jewels of their data, organizations need comprehensive, integrated, end-to-end data security solutions. IBM solutions enable security intelligence that supports automated threat detection and response. They provide asset protection via role-based access controls. They deliver analytics that provides insight necessary to stop threats. And they support mobile- and cloud-focused capabilities for collaboration by utilizing smarter data governance solutions to protect the crown jewels of the enterprise.

For more information

To learn more about IBM Security solutions for mainframe environments, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2015

Please Recycle

[1] Michael A. Riley and Jordan Robertson, "Chinese State-Sponsored Hackers Suspected in Anthem Attack," *Bloomberg Business*, February 5, 2015. http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack

[2] Brian Krebs, "Banks: Credit Card Breach at Home Depot," *Krebs on Security*, September 2, 2014. http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/

[3] Tom Gara and Charlie Warzel, "A Look Through The Sony Pictures Data Hack: This Is As Bad As It Gets," *BuzzFeedNews*, December 2, 2014. http://www.buzzfeed.com/tomgara/sony-hack#.dpx8dPzjW

[4] Janet Sun, "Don't believe the Myth-information about the Mainframe: Part 1," *Share*, May 7, 2013. www.share.org/p/bl/et/blogid=2&blogaid=234

[5] Mike O. Villegas, "Mainframe security best practices for compliance with PCI DSS," *TechTarget*, October 2014. http://searchsecurity.techtarget.com/tip/Mainframe-security-best-practices-for-compliance-with-PCI-DSS

[6] Verizon RISK Team, "2012 Data Breach Investigations Report," *Verizon*, April 2012. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

[7] "IBM X-Force Threat Intelligence Quarterly – 1Q 2014," *IBM Corp.*, February 2014. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGL03045USEN&attachment=WGL03045USEN.PDF

[8] "2014 Cost of Data Breach Study: Global Analysis," *Ponemon Institute, sponsored by IBM*, May 2014. http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

WGW03124-USEN-00