IBM Security

Thought Leadership White Paper

April 2015

Maximize mainframe security to reduce risk with 10 best practices

Reducing the security risk to business "crown jewels" on your IBM z Systems mainframe

Introduction

Many organizations continue to be served by IBM® z Systems™ mainframes, often regarded as the workhorse of the enterprise hosting the "crown jewels"—the critical data that is vital to business survival and success. You may not realize it, but 80 percent of the world's corporate data either resides on or originates from the mainframe.[1] Not only is the platform critical to the continuity of the business it serves, but from an individual's perspective, your personal data also probably resides on a mainframe. To support these needs, the modern mainframe has evolved to meet modern business requirements—and that includes security. Today's mainframe is the only platform with EAL5+ certification.

In many environments, however, complacency and lapses in security practices mean that even on this highly available platform, assets aren't necessarily as secure as they can—or should—be. IBM security specialists regularly encounter organizations that rate themselves high on scales of enterprise security, though when assessed against industry-standard controls, their actual level of maturity is much lower.

This white paper will discuss some of the reasons why organizations often fall short of achieving the security they expect from their mainframe environments, present best practices that organizations can employ to improve their mainframe security and provide an overview of IBM solutions that can help in implementing those best practices.

Do your practices match your mainframe's high levels of security?

When it comes to getting the strong levels of security you expect from your z Systems mainframes, trust in the highly secure platform is not enough—you cannot assume that because your data resides on the mainframe it is secure. Strong and sustainable controls are highly dependent on the enterprise adopting best practices, ranging from understanding how cybercriminals think, to controlling how you grant—and revoke—access permissions to your user population. However, while many practices, such as providing ongoing training for security teams, are relatively easy to achieve, organizations often neglect even the most basic practices. As a result, in some organizations mainframe systems can be less securely managed than distributed systems.

Why is this? In some instances, it's because of the wide-ranging and often complex nature of data access. Resources residing on mainframes are typically accessed and shared by applications and business processes both local and remote to the system. Other times, shortcomings arise because security teams don't have knowledge in specific mainframe components, such as z/OS UNIX. As a result, they hand off tasks to system programmers, who may not share a focus on security; their areas of expertise and responsibilities typically favor performance and availability—not a good scenario for building strong controls. Other security lapses come from controls that were designed for an earlier era—often the 1990s—but these controls have not evolved with the threat landscape of today. You could call this "static security"—which is not sufficient for modern mainframes that have become a popular platform for big data, Internet operations, mobile and cloud computing. All of these uses are more vulnerable to cyber-attack than traditionally isolated mainframe uses, and all increase the complexity and load for security management tasks.

Meanwhile, evolving technologies such as the increased use of shared and virtualized resources, additional requirements to meet standards and comply with regulations, and lapses such as enabling users to easily bypass access controls make security management a greater challenge than ever.

Adopting a best-practices approach to managing mainframe security can help address the full range of challenges organizations face. It is essential for security teams to have visibility of their security implementation in order to help understand where there are gaps that open the door to security breaches, whether malicious or accidental. This visibility provides a foundation for prioritizing risks and security initiatives. Importantly, best practices play a major role in reducing risk to help avoid the high cost of a security breach in the future. Outdated approaches designed for an earlier era can result in poor controls for protecting the organization's crown jewels. The net effect can place unacceptable levels of risk to the business.

Management best practices can strengthen your mainframe security posture

The wide-ranging nature of threats—and the resulting importance of comprehensive security—require wide-ranging and comprehensive security best practices. These can involve everything from technologies to processes to shifts in attitudes. At their core, however, they typically share a common characteristic—they are practices that many organizations are not always following, but should.

Best practices can address poor controls that are often the root cause of security breaches, which can be a combination of malicious and accidental. Remember, prevention is typically less expensive than the cure. You can use the following 10 best practices as a guide in helping your organization to improve controls in your mainframe environment.

1. Analyze, understand and report your risks
2. Change from a reactive to a proactive view of security
3. Take a big-picture, long-term iterative view
4. Design security into practices and applications
5. Regularly clean up your system security
6. Simplify and streamline security controls
7. Review technology to deliver state-of-the-art security
8. Test and simulate changes and controls
9. Move from point-in-time to real-time insight
10. Think outside the big box to make security pervasive

Best practice 1: Analyze, understand and report your risks

How much risk is your organization willing to take? What will the impact be if the worst happens? These are just two of the questions you and your management need to understand as you analyze and report on the effectiveness of controls.

Management support is critical for security to succeed, so you need to be prepared to take the "so what" test from a skeptical audience. You must come armed with insight into specific security issues, and you must report those insights in a business-focused manner. The bottom line is: What is the risk to the business? Quantifying risk is important—and being able to articulate to management the potential loss to the organization will help gain the support you need. In approaching management, be sure to involve your audit and risk management team; they have the focus and methodologies for assessing risk in business terms.

Security standards are critical—they define expectations for the level of controls, which are based on your corporate security policies and industry regulations. Measure your controls against these standards to verify their effectiveness. Lack of standards results in poor security.

Data classification is a must. If you don't understand the value of your data, you cannot determine if an asset is at risk, and you cannot implement the necessary controls to mitigate the risk. Your organization's various lines of business must discover their sensitive information, classify it and adequately protect it. To align assets and controls properly, it is essential to have governance tools that bring together the languages of IT and business personnel to establish optimal access permissions.

A deep-dive audit can reveal security issues in systems and provide the most effective way to help you understand if the business is exposed. To aid the audit, you need to know what data you have, where it resides and how you can address vulnerability issues. Many organizations take excessive risks by having a less-than-precise understanding of their assets and deploying outdated or inadequate technology and controls. They gamble that they will not need protection from events that are unlikely to happen. But when events happen, the results can severely damage business operations, ruin reputations and cause financial loss. For too long, organizations have ignored audit concerns that carry a high-impact, low-probability risk—but that can damage your enterprise.

Best practice 2: Change from a reactive to a proactive view of security

Hackers and cybercriminals are constantly changing their method of attack. So if your security team simply follows processes and procedures it put into place some time ago, it will have limited success in keeping pace with the threat landscape. Pre-existing techniques were created, after all, to combat known attack vectors—but the criminals have long ago moved on.

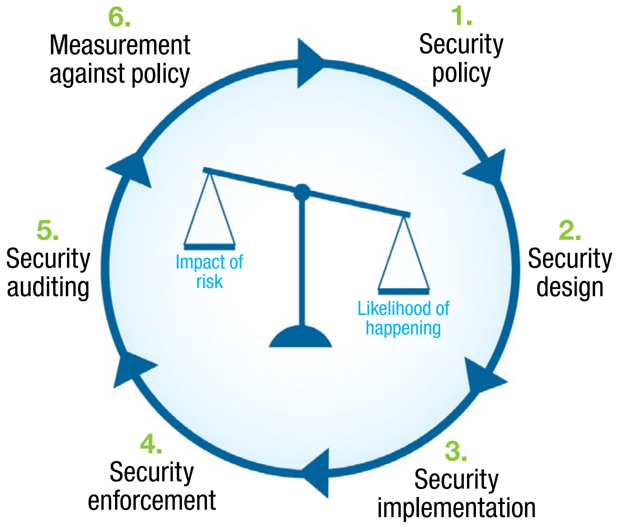
Instead of thinking like a follower of processes, you need to think like the cybercriminals you're combating. When you are protecting an asset, think of different ways in which an intruder can bypass controls. Always ask the question, "Where are the loopholes?" Identify methods by which an intruder can achieve the desired outcome, and discover the access paths into your valuable resources.

Analyzing, understanding and reporting risks helps you implement strong and sustainable controls. Knowing the criminal's mindset can help give your security efforts a proactive business focus—protecting areas that are most important to your organization's goals and supporting an understanding that security is a concern for the entire business, not just IT.

Best practice 3: Take a big-picture, long-term, iterative view

Effective security and risk management are not capabilities an organization can achieve in a day; it can take years to build a mature practice. Even the most thorough approach to remediating vulnerabilities and erecting defenses begins to deteriorate rapidly if the security team does not exercise continuous improvement. What the organization needs instead is an iterative approach to security, a journey more than a destination. It needs to add improvements through a step-by-step series of processes affecting policy, design, implementation, enforcement, auditing and measurement—and then build on these improvements by repeating the processes in a continuous loop.

Take an iterative approach as you assess risk



Within this iterative cycle, individual security programs can be complex undertakings that require years to complete. So in addition to an ongoing approach, a long-term view also is important. Security is a key component of reliable mainframe operations and successful business processes—and as such, security demands ongoing care in its planning, implementation and management. At the end of the day, the threat landscape is constantly changing, so your job is never done.

Best practice 4: Design security into practices and applications

Your organization must assume that its systems will always be subject to criminal attacks, privileged insider abuse and accidental errors. So don't let security slip from your attention. Focus on security regardless of which phase of the systems development lifecycle you're in.

Discovering late in a project that security has not been incorporated can bring operations to a halt. Practices without security built in can violate the organization's security policies, or fail to meet industry or government regulations, running the risk of fines or sanctions but almost definitely incurring delays and cost overruns for retrofitting. Worse still, deploying applications or practices with security vulnerabilities can be an invitation to criminals to break into the resources you thought were safe.

The key is to build in controls that align with business objectives—but you can't do that if your security team has not been engaged. Given the applications and data running on the mainframe and the business needs for security, you need to know early on in the systems development lifecycle what standards and controls are necessary, and then ensure that they are in place before going live. Failure to do so can result in your business operating with unacceptable levels of risk.

Best practice 5: Regularly clean up your system security

IBM introduced the mainframe more than 50 years ago—and many organizations have been using the platform ever since for business-critical data and applications. Longevity is one of the system's greatest benefits. But as the years pass, organizations add more data and applications to their systems, customize settings, add security controls and alter the mainframe's configurations. As a result, mainframe administrators can encounter outdated controls that add layers of unnecessary complexity and cost.

The first step is to collect information about security decisions that are made by your security system. For example, collect usage data for access permissions, profile definitions and group membership. This is where the Access Monitor feature in IBM Security zSecure™ Admin can help. Based on this intelligence, you can make informed decisions on removing some of those definitions.

The next step is to keep your security database from becoming polluted again. When the mainframe's security systems are cleaned up, it becomes critical to put both preventive and corrective controls into place to maintain a clean and stable security environment. It is important to note that clean-up is not a one-time effort; it is a continuous process that must be embedded into a business as usual practice. If you stop, controls will rapidly erode, paving the way for costly audit remediation in the future.

Best practice 6: Simplify and streamline security controls

One way to reduce the complexity and increase the effectiveness of your security systems is to take firm control of users' access to systems, applications and data. Designing and implementing role-based access controls can help ensure that only those people whose jobs require access actually have it—and that privileges are removed from those who don't. Always grant the least possible privilege necessary to do the job. A smaller number of authorized people with a recognized "need to know" can reduce the risk of insiders who may steal or corrupt information for gain, make mistakes, or who simply view it out of inappropriate curiosity.

If you are conducting a system clean-up using the Access Monitor feature in IBM Security zSecure Admin, you're already collecting information about security decisions that are made by your security system. This gives you a major advantage in the business analysis stage of a role-based access controls project. Too often, security teams approach business units with complex access lists, expecting the units to make decisions about access requirements. Instead, the key step to simplifying access is to provide intelligence about what access is being used, and more importantly, what is not. You'll likely find that users are less inclined to retain all of their access when they understand the security issues involved. In this way, you can remove enormous amounts of excessive access for a more streamlined security environment.

Best practice 7: Review technology to deliver state-of-the-art security

Hackers and cybercriminals exploit technology to its fullest in their attacks on your systems. You should do no less in your defense.

Begin with the security technologies you have. This can be a significant investment, so you want to get the most out of it. But do you? Many organizations use only a small fraction of the capabilities they have in place. You may have deployed your defenses for a particular purpose, but is that what you need today? A gap analysis that examines threats, vulnerabilities and software capabilities can quickly show new opportunities for safeguarding resources with your existing systems—without the need to invest in additional infrastructure. In the same way, it is also important to keep pace with software upgrades and fixes to help improve your security implementation.

If new security features and functions have been introduced since you deployed your defenses, an analysis of new products, together with your existing capabilities and criminals' attack methods, can tell whether or not you should take steps to improve your controls. Consult with your security software vendor about additional capabilities that integrate with your deployment. Building a defense on integrated solutions rather than siloed point products can provide a more comprehensive defense against attack, simplify management and reduce infrastructure cost.

Best practice 8: Test and simulate changes and controls

Business requirements change. So do attack vectors and defense mechanisms. But as you're evolving your security systems to meet those challenges, keep a close eye on what you're doing. Many exposures to attack come from security administration errors.

To help avoid errors, it's important to test systems and simulate effects whenever you make a change. Historically, this hasn't always been possible—mainframe security teams have often lacked the ability to test and simulate change in a production-like environment before the change goes live. Capabilities, such as the IBM Remote Access Control Facility (RACF®)-Offline and the Access Monitor feature in zSecure Admin make it possible to perform comprehensive testing.

Similarly, it's important to benchmark and test your controls against external standards developed by organizations such as the National Institute for Standards and Technology (NIST) and the Defense Information Systems Agency (DISA). You can have stronger controls when you test them against the newest cyber-security standards.

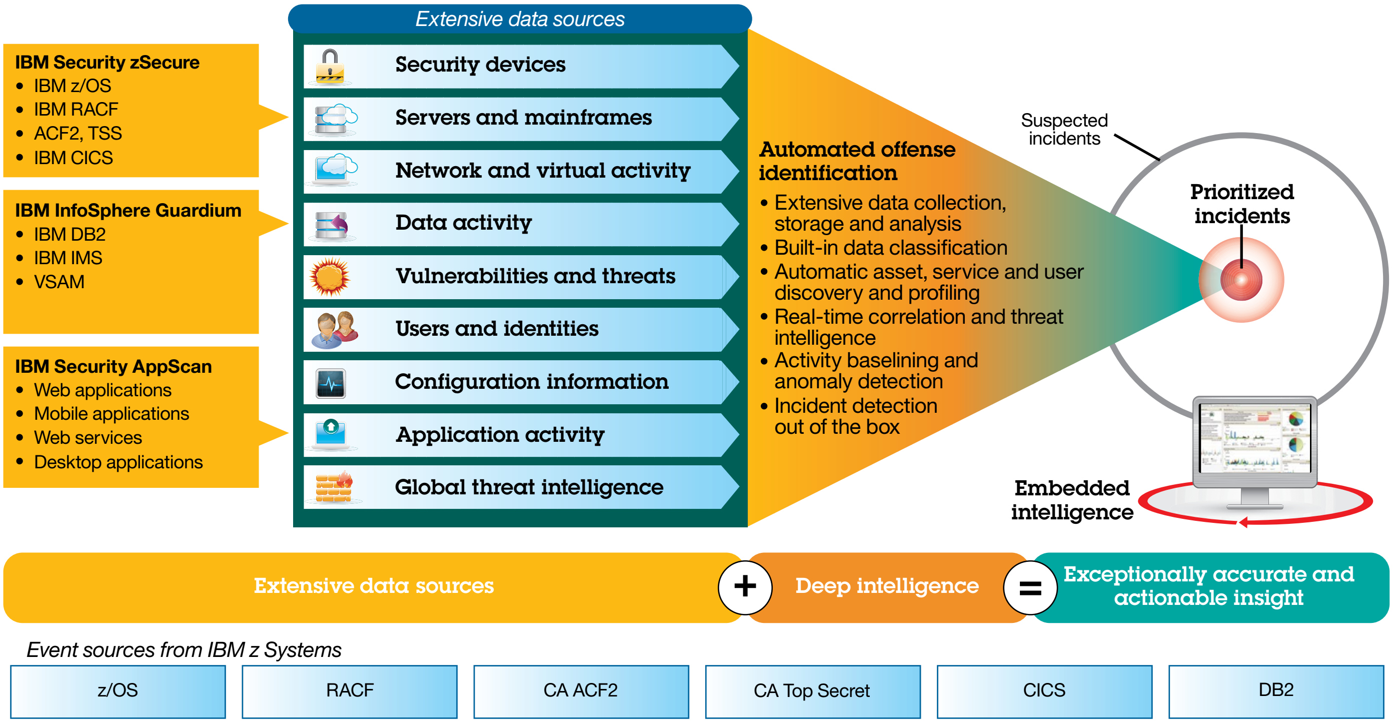
Best practice 9: Move from point-in-time to real-time insight

Knowing what happened after an attack occurs can provide some defensive help—but it's not the best approach. That's because while you can use information from yesterday's attack to be more secure tomorrow, hackers and cybercriminals can do a lot of damage when there's a time lag between their entry, your discovery and the ultimate remediation of the problem. Looking at individual points in time may tell you what happened then, but it doesn't necessarily tell you what's happening now—and that's when you need insight.

A better approach is to take a real-time view that examines the ongoing status of your mainframes, security systems, subsystems and data. For the big picture, integrate your security monitoring with your enterprise infrastructure monitoring systems. For pinpointing true threats among millions of events and network flows, deploy security information and event management (SIEM) solutions that are proactive and can detect threats and vulnerabilities.

In reviewing your security monitoring efforts, be careful of falling into the common pattern by which mainframe security teams are responsible for both implementation and monitoring—in effect, self-policing. As the practice of monitoring one's own work is a sure path to weak security, take care to ensure separation of duties for security monitoring. A security team that implements a change one day and then reviews or approves that change the next day creates a weak link that can reduce the effectiveness of the entire security chain. Instead, independent monitoring by a separate team can provide the most effective approach to reducing errors and fraud in internal operations.

IBM z Systems products enable integration with IBM Security QRadar solutions


IBM Security zSecure
• IBM z/OS
• IBM RACF
• ACF2, TSS
• IBM CICS
IBM InfoSphere Guardium
• IBM DB2
• IBM IMS
• VSAM
IBM Security AppScan
• Web applications
• Mobile applications
• Web services
• Desktop applications
Extensive data sources
Security devices
Servers and mainframes
Network and virtual activity
Data activity
Vulnerabilities and threats
Users and identities
Configuration information
Application activity
Global threat intelligence
Automated offense identification
• Extensive data collection, storage and analysis
• Built-in data classification
• Automatic asset, service and user discovery and profiling
• Real-time correlation and threat intelligence
• Activity baselining and anomaly detection
• Incident detection out of the box
Suspected incidents
Prioritized incidents
Embedded intelligence
Extensive data sources
+
Deep intelligence
=
Exceptionally accurate and actionable insight
Event sources from IBM z Systems
z/OS
RACF
CA ACF2
CA Top Secret
CICS
DB2

Best practice 10: Think outside the big box to make security pervasive

Are you focusing your efforts only one place, on the security system? If so, don't forget to look beyond. There are also controls in the operating system, middleware, virtualization software and other components of your mainframe environment—each with settings that need to be activated, regularly reviewed and monitored. Business applications can have internal controls that are not connected to your security environment. Don't neglect these, or you can create security vulnerabilities.

Security doesn't happen only one time, either. Solutions designed for the threat landscape of a decade ago—and in some cases of only a year ago—are not likely up to the job of keeping your assets safe. Employ regular evaluation, periodic security health checks and ongoing improvements to proactively protect your organization.

And don't forget that, ultimately, security is about people—who has access and who has authority to grant access. The expertise of your security team is critical to the success of your security efforts. So keep your team up to date with the latest threats, trends and best practices with regular training. Conferences, webinars and courses can provide the insight into new threats and the latest security solutions that are indispensable in a changing threat landscape.

The mainframe supports the cloud, mobile computing and big-data analytic applications of your enterprise—enabling people doing their jobs—and as such it's a vital part of your operation. A comprehensive iterative approach for embracing security best practices and risk management is essential to maintaining the security your organization needs.

Take advantage of IBM Security Solutions to reduce mainframe risk

IBM provides a full range of security solutions to enable security management best practices and provide a comprehensive approach to mainframe security.

- **IBM Security zSecure** solutions simplify the administration of security when creating, provisioning and authorizing users, groups and resources. They enforce best practice security policies and help clean up security profiles. zSecure solutions automate audit reporting, monitor compliance, detect potential threats or harmful configuration changes, and provide closed loop remediation and real-time alerts. zSecure solutions help provide comprehensive, end-to-end security across z System environments, providing integration with distributed security solutions to eliminate security silos, reduce risk and enhance enterprise security intelligence.
- **IBM InfoSphere® Guardium®** helps prevent unauthorized data access, provides alerts on changes, assesses and addresses vulnerabilities to help ensure data security, automates compliance controls, and helps protect against internal and external threats. Continuous monitoring, real time blocking of suspicious behavior and real-time security policies help protect data across the enterprise without changes to databases or applications and without impact on performance.
- **IBM RACF** provides the foundation for z Systems security with identity and access controls on mainframe users and resources, along with extensive system logging of security events.
- **IBM Security QRadar®** family of solutions provides security intelligence with integrated SIEM, log management, vulnerability management, risk management, anomaly detection and incident forensics.
- **IBM Security AppScan®** helps identify and fix security vulnerabilities by scanning web and mobile applications before deployment.
- **IBM InfoSphere Optim™ Data Masking** de-identifies and masks data so it can be used in application development testing without the chance of inappropriate use if it is stolen; at the same time, it the data retains its behavioral characteristics and referential integrity.

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**/software/os/systemz/security or **ibm.com**/security

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM 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.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
April 2015

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 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.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

[1] Cliff Saran, "Can the mainframe remain relevant in the cloud and mobile era?" *Computer Weekly*, 2014. http://www.computerweekly.com/feature/Can-the-mainframe-remain-relevant-the-cloud-and-mobile-era