VANGUARD
Integrity Professionals
Information Security Experts

“Top Ten” Critical Assessment Findings in IBM® z/OS® (RACF®) Environment

Philip Emrich
Senior Professional Services Consultant
pemrich@go2vanguard.com

Anaheim, CA
9 – 14 March 2014
SHARE 122 – Session 14965

Legal Notice

Copyright

Trademarks

IBM, RACF, OS/390, System z, and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. UNIX is a registered trademark of The Open Group in the United States and other countries. Linux is a registered trademark of the Linux Mark Institute in the United States and other countries. Vanguard Administrator, Vanguard Advisor, Vanguard Analyzer, and Vanguard Configuration Manager are trademarks of Vanguard Integrity Professionals – Nevada.

Agenda

VANGUARD
Integrity Professionals
Information Security Experts

The Need for "Best Practices" for z/OS Security

1

This part introduces the need to assess z/OS systems for vulnerabilities and the reasons for doing regular vulnerability assessments.

Vanguard's most Frequently Encountered Significant Exposures

2

This part covers the "Top Ten" most frequently encountered Severe or High risk exposures encountered in assessment of z/OS systems Vanguard has conducted for our clients.

Assessment and Remediation

3

This part discusses the overall assessment process and remediation of exposures identified.

THE NEED FOR “BEST PRACTICES FOR Z/OS SECURITY

“The” Critical System in your Network.

System z® workloads are going UP in terms of data stored and transactions processed, NOT down.

This is the opposite of the public or common perception.

If you have a z/OS system in your network, that is the “bank vault” – everything else is just an “ATM”.

The Invisible Mainframe

- – Hundreds of Windows, Linux™ and UNIX® Servers.
- – One, Two, Three, four? z/OS servers

World wide, z/OS servers are far less than 1% of servers.

2,400 Enterprises with one or more z/OS systems.

The Answer…

“Western civilization runs on IBM mainframes.”

Tom Rosimilla, IBM Systems Group

65% of the world’s mission critical data resides on IBM mainframes.

CA Technologies

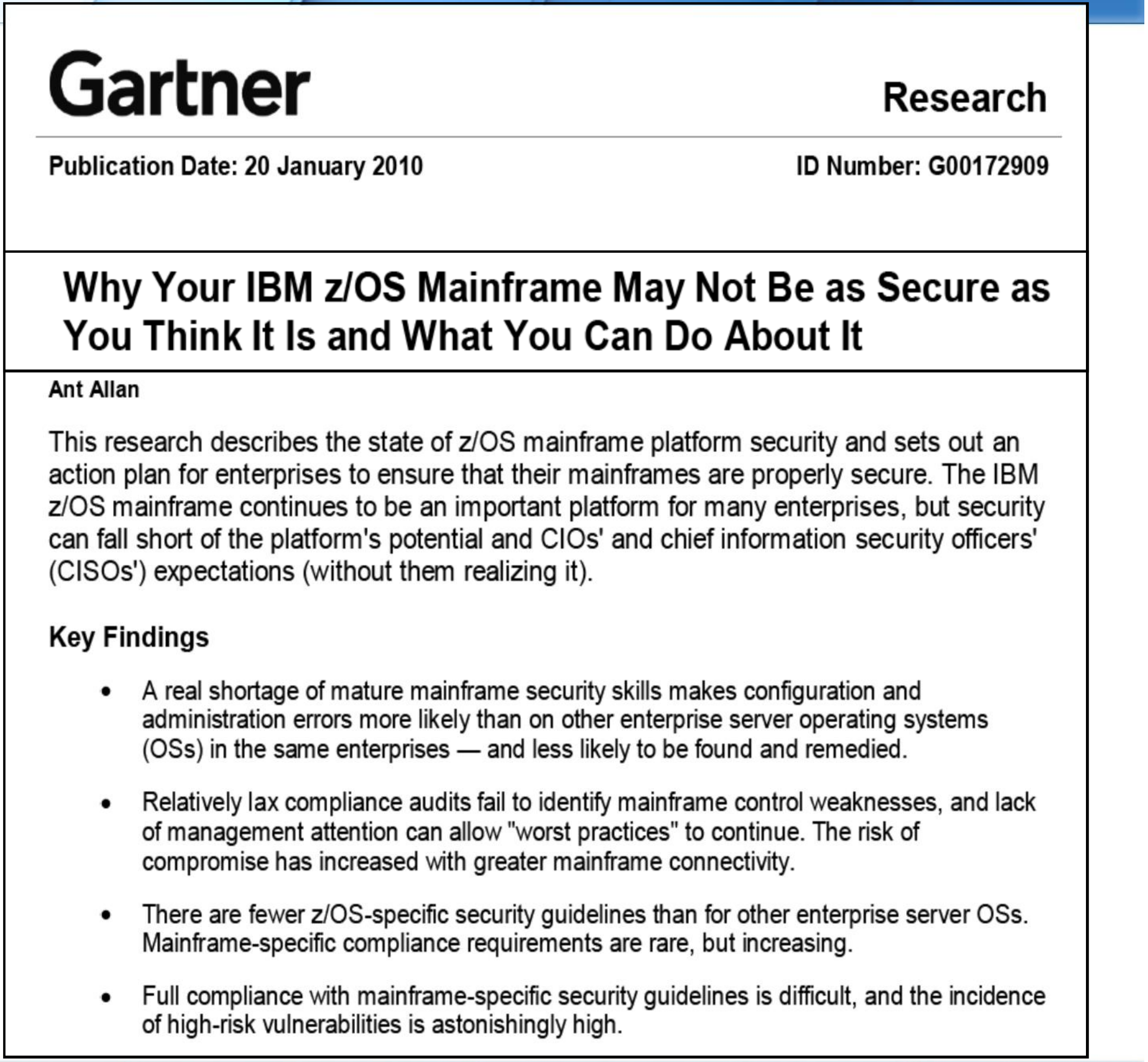
If an enterprise has IBM z/OS systems, 85 % of their critical data is processed or stored on the IBM z/OS system.

Ant Allan, V.P. Gartner

The Situation

Ant Allan
Research VP

- The Mainframe is still an important platform
- Security can fall short
  - Creating high-risk vulnerabilities
- Lack of formal programs



Gartner **Research**

Publication Date: 20 January 2010 **ID Number: G00172909**

Why Your IBM z/OS Mainframe May Not Be as Secure as You Think It Is and What You Can Do About It

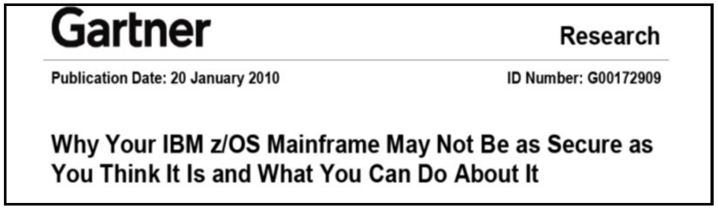
Ant Allan

This research describes the state of z/OS mainframe platform security and sets out an action plan for enterprises to ensure that their mainframes are properly secure. The IBM z/OS mainframe continues to be an important platform for many enterprises, but security can fall short of the platform's potential and CIOs' and chief information security officers' (CISOs') expectations (without them realizing it).

Key Findings

- A real shortage of mature mainframe security skills makes configuration and administration errors more likely than on other enterprise server operating systems (OSs) in the same enterprises — and less likely to be found and remedied.
- Relatively lax compliance audits fail to identify mainframe control weaknesses, and lack of management attention can allow "worst practices" to continue. The risk of compromise has increased with greater mainframe connectivity.
- There are fewer z/OS-specific security guidelines than for other enterprise server OSs. Mainframe-specific compliance requirements are rare, but increasing.
- Full compliance with mainframe-specific security guidelines is difficult, and the incidence of high-risk vulnerabilities is astonishingly high.

Top Reasons for Security Vulnerabilities



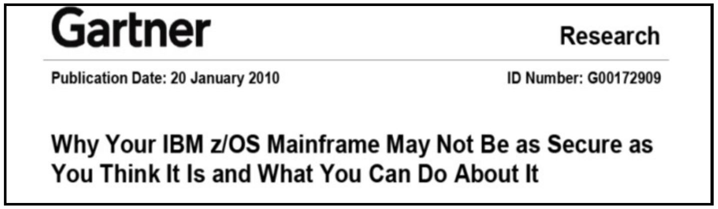
Gartner Research

Publication Date: 20 January 2010 ID Number: G00172909

Why Your IBM z/OS Mainframe May Not Be as Secure as You Think It Is and What You Can Do About It

- Retirement of skilled professionals – makes it difficult to assess your own security
- Lax in audits due to insufficient skill sets – not communicated to management
- Few documented guidelines available
- Full compliance with standards and regulations is difficult

Gartner Recommendations



Gartner Research

Publication Date: 20 January 2010 ID Number: G00172909

Why Your IBM z/OS Mainframe May Not Be as Secure as You Think It Is and What You Can Do About It

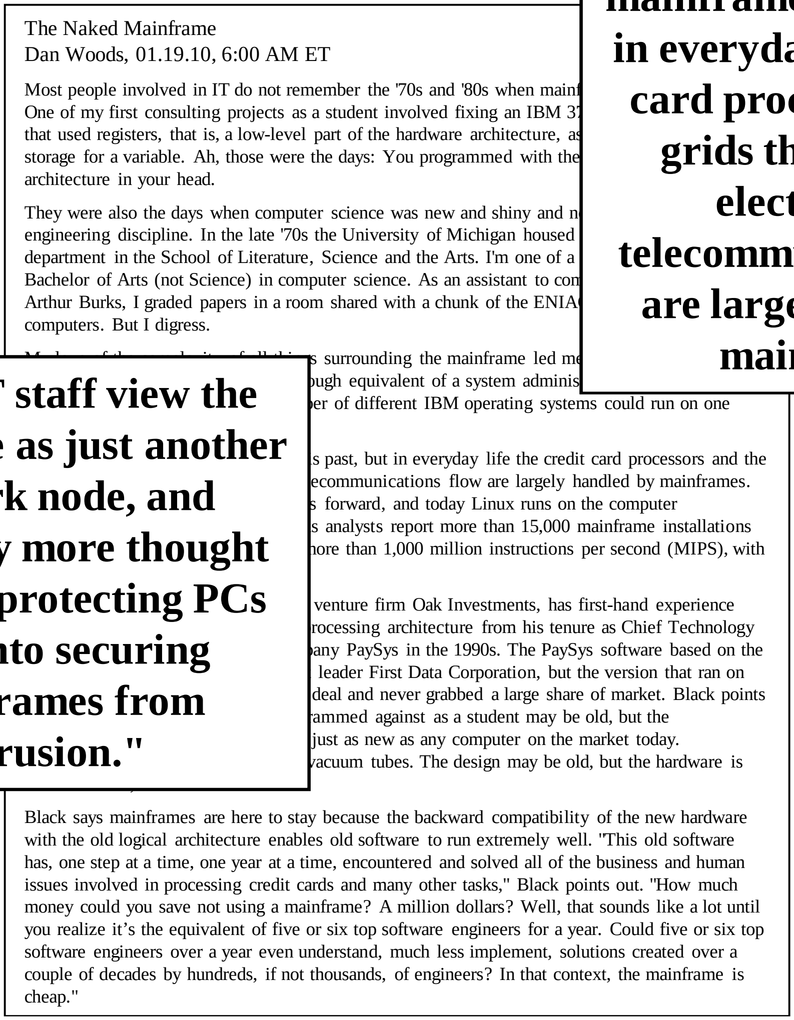
- Develop and update your policies
- Audit your mainframe, remediate vulnerabilities
- Ensure your security and risk management policies are enforced
- Invest in training and education
- Evaluate intelligent administration and auditing tools
- Execute all of the above

The Situation

The Naked Mainframe

Dan Woods, 01.19.2010

Chief Technologist Officer & Editor
Evolved Technologist



The Naked Mainframe
Dan Woods, 01.19.10, 6:00 AM ET

Most people involved in IT do not remember the '70s and '80s when mainf
One of my first consulting projects as a student involved fixing an IBM 37
that used registers, that is, a low-level part of the hardware architecture, as
storage for a variable. Ah, those were the days: You programmed with the
architecture in your head.

They were also the days when computer science was new and shiny and n
engineering discipline. In the late '70s the University of Michigan housed
department in the School of Literature, Science and the Arts. I'm one of a
Bachelor of Arts (not Science) in computer science. As an assistant to com
Arthur Burks, I graded papers in a room shared with a chunk of the ENIA
computers. But I digress.

s surrounding the mainframe led me
ough equivalent of a system adminis
er of different IBM operating systems could run on one

s past, but in everyday life the credit card processors and the
ecommunications flow are largely handled by mainframes.
s forward, and today Linux runs on the computer
s analysts report more than 15,000 mainframe installations
ore than 1,000 million instructions per second (MIPS), with

venture firm Oak Investments, has first-hand experience
rocessing architecture from his tenure as Chief Technology
any PaySys in the 1990s. The PaySys software based on the
leader First Data Corporation, but the version that ran on
deal and never grabbed a large share of market. Black points
rammed against as a student may be old, but the
just as new as any computer on the market today.
vacuum tubes. The design may be old, but the hardware is

Black says mainframes are here to stay because the backward compatibility of the new hardware with the old logical architecture enables old software to run extremely well. "This old software has, one step at a time, one year at a time, encountered and solved all of the business and human issues involved in processing credit cards and many other tasks," Black points out. "How much money could you save not using a mainframe? A million dollars? Well, that sounds like a lot until you realize it’s the equivalent of five or six top software engineers for a year. Could five or six top software engineers over a year even understand, much less implement, solutions created over a couple of decades by hundreds, if not thousands, of engineers? In that context, the mainframe is cheap."

"Most people think the mainframe era is past, but in everyday life the credit card processors and the grids through which electricity and telecommunications flow are largely handled by mainframes."

"Most IT staff view the mainframe as just another network node, and frequently more thought goes into protecting PCs than into securing mainframes from intrusion."

Business Realities

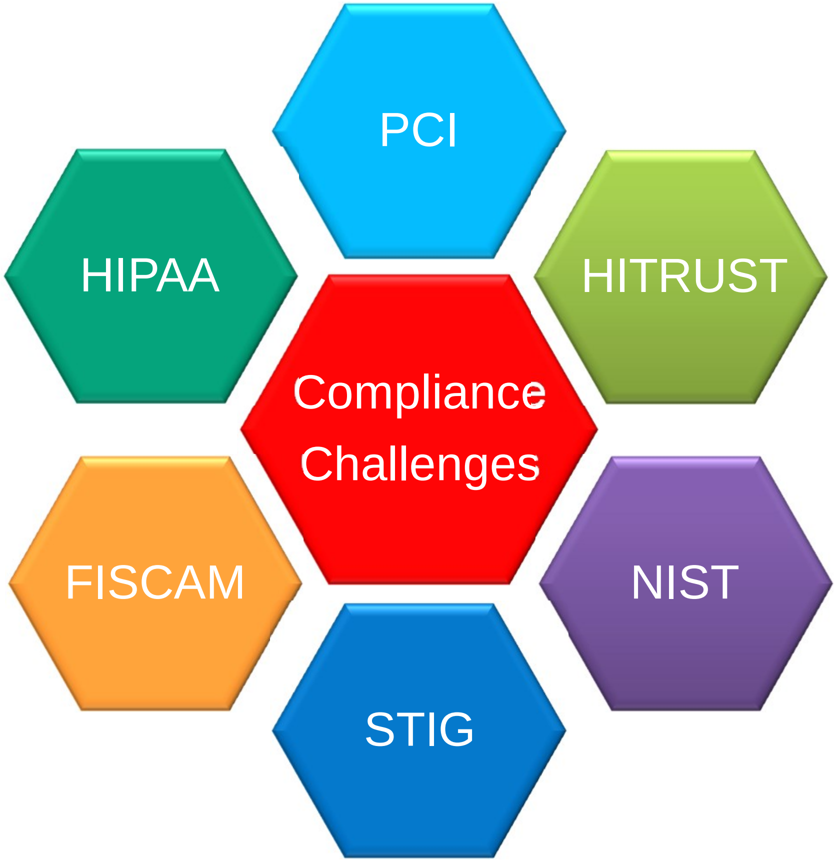
The Need to Implement Security "Best Practices"

Information Security Compliance is a top organizational initiative

- Laws, Regulations, and Standards require validation of proper implementation of IT internal controls.
- IT Internal Control failures threaten the organization's image and can carry heavy fines and even executive management imprisonment.
- Cyber-crime activities are a serious threat and companies are expected to implement all reasonable measures to prevent successful attacks.
- Outside auditors can and are issuing sanctions that restrict core business activities based on IT security risks identified in their audits.

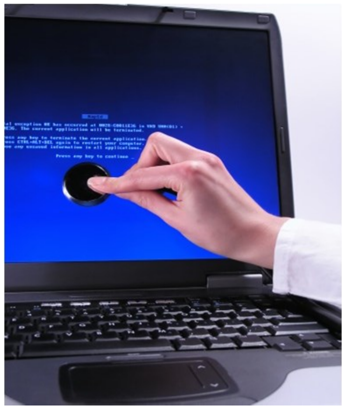
Bottom Line: The Information Security organization must be proactive in their efforts to implement and maintain Security "Best Practices" in their enterprises.

Regulatory Compliance



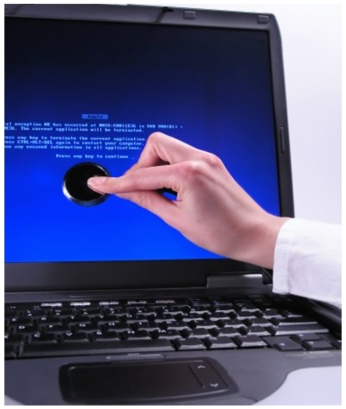
The identified Security Issues present risk to regulatory / industry compliance standards depending on the data present within the assessed system.

z/OS and RACF "Best Practices"



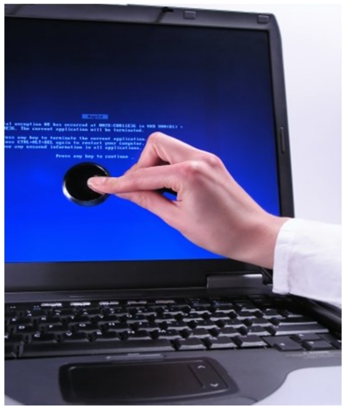
- Where do "Best Practices" come from?
  - Subjective Sources:
    - Vanguard Integrity Professionals Professional Services Consultants with an average of 30+ years experience
    - Based on a technical understanding of z/OS and key Subsystem software
    - Related to risks and exposures identified in 100s of Security Assessments conducted over more than 20 years

z/OS and RACF “Best Practices”



- Where do “Best Practices” come from?
  - Objective Sources:
    - HIPAA (1996)
      - HITECH Act 2009
    - Gramm-Leach-Bliley Act – 1999 (GLBA)
      - Financial Privacy Rule
      - Safeguards Rule
    - Sarbanes-Oxley Act of 2002 (SOX)
      - Section 404: Assessment of internal control
    - PCI-DSS (Data Security Standard)

z/OS and RACF “Best Practices”



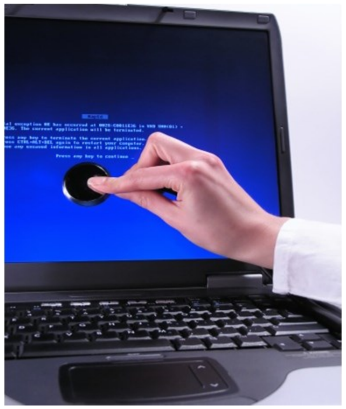
- Where do “Best Practices” come from?
  - Objective Sources:
    - DOD DISA STIGs (Security Technical Implementation Guides)
      - z/OS STIG adopted by Centers for Medicare & Medicaid Services (CMS)
    - NIST: Security Configuration Controls
    - NIST: Co-hosts with DHS security configuration checklists on the National Vulnerability Database

http://web.nvd.nist.gov/view/ncp/repository

Target Product: IBM OS/390®

VANGUARD'S MOST FREQUENTLY ENCOUNTERED SIGNIFICANT EXPOSURES

Vanguard's "Best Practices"



Vanguard Professional Services consultants with an average of 30+ years experience

Based on our technical understanding of z/OS and key Subsystem software

Related to risks and exposures identified in hundreds of Security Assessments conducted over more than 20 years

Vanguard's Assessment Process

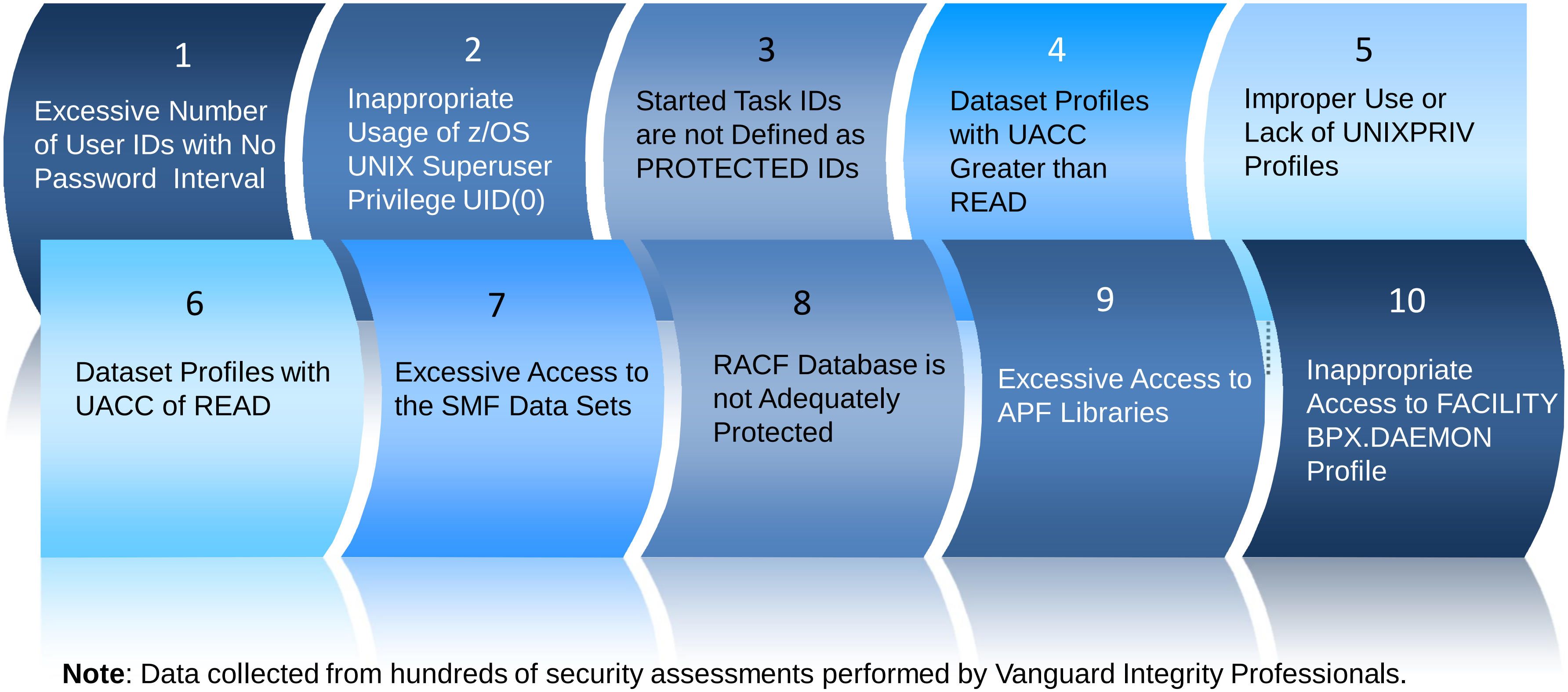
- Analysis of over Hundreds of Assessments
  - Private firms across numerous industries
  - Various governmental agencies:
    - Federal
    - State
    - Local
  - Totaling over 1800 Individual Findings
  - Over 300 unique Findings
  - Correlated to regulations or compliance requirements
  - Categorized by Severity and Remediation effort

Vanguard's Exposure Severity Rating

- SEVERE (needs immediate remediation)
  - Immediate unauthorized access into a system
  - Elevated authorities or attributes
  - Cause system wide outages
  - the ability to violate IBM's Integrity Statement
- HIGH (needs remediation in the near future)
  - Vulnerabilities that provide a high potential of disclosing sensitive or confidential data
  - cause a major sub-system outage
  - assignment of excessive access to resources
- MEDIUM(needs a plan for remediation within a reasonable period)
  - Vulnerabilities that provide information and/or access that could potentially lead to compromise
  - the inability to produce necessary audit trails
- LOW (should be remediated when time and resources permit)
  - Implementation or configuration issues that have the possibility of degrading performance and/or security administration

Vulnerability Assessment Findings

Scope: Vanguard Top 10 z/OS Risks Identified in Client Security Assessments



1 Excessive Number of User IDs with No Password Interval

2 Inappropriate Usage of z/OS UNIX Superuser Privilege UID(0)

3 Started Task IDs are not Defined as PROTECTED IDs

4 Dataset Profiles with UACC Greater than READ

5 Improper Use or Lack of UNIXPRIV Profiles

6 Dataset Profiles with UACC of READ

7 Excessive Access to the SMF Data Sets

8 RACF Database is not Adequately Protected

9 Excessive Access to APF Libraries

10 Inappropriate Access to FACILITY BPX.DAEMON Profile

Note: Data collected from hundreds of security assessments performed by Vanguard Integrity Professionals.

“Top Ten” Assessment Finding #1

Finding

Excessive Number of User IDs with No Password Interval

Explanation

User IDs with no password Interval are not required to change their passwords

Risk

Since passwords do not need to be changed periodically, people who knew a password for an ID could still access that ID even if they are no longer authorized users.

Remediation

Review each of the personal user profiles to determine why they require NOINTERVAL. Their passwords should adhere to the company policy regarding password changes. If the user ID is being used for started tasks or surrogate, it should be reviewed and changed to PROTECTED.

“Top Ten” Assessment Finding #2

Finding

Inappropriate Usage of z/OS UNIX Superuser Privilege UID(0)

Explanation

User IDs with z/OS UNIX superuser authority, UID(0), have full access to all UNIX directories and files and full authority to administer z/OS UNIX.

Risk

Since the UNIX environment is the z/OS portal for critical applications such as file transfers, Web applications, and TCPIP connectivity to the network in general, the ability of these superusers to accidentally or maliciously affect these operations is a serious threat. No personal user IDs should be defined with an OMVS segment specifying UID(0).

Remediation

The assignment of UID(0) authority should be minimized by managing superuser privileges by granting access to one or more of the ‘BPX.qualifier’ profiles in the FACILITY class and/or access to one or more profiles in the UNIXPRIV class.

“Top Ten” Assessment Finding #3

Finding

Started Task IDs are not Defined as PROTECTED IDs

Explanation

User IDs associated with started tasks should be defined as PROTECTED which will exempt them from revocation due to inactivity or excessive invalid password attempts, as well as being used to sign on to an application.

Risk

RACF will allow the user ID to be used for the started task even if it has become revoked, but some started tasks may either submit jobs to the internal reader that will fail or may issue a RACROUTE REQUEST=VERIFY macro for the user ID that will also fail.

Remediation

Review all started task user IDs that are not protected. Determine if the user IDs are used for any other function that might require a password. Define the started task user IDs as PROTECTED for those tasks that do not require a password.

"Top Ten" Assessment Finding #4

Finding

Dataset Profiles with UACC Greater than READ

Explanation

The UACC value for a dataset profile defines the default level of access to which any user whose user ID or a group to which it has been connected does not appear in the access list.

Risk

Data sets that are protected by a RACF profile with a UACC greater than READ allow most users with system access to read or modify these data sets. In addition, users may be able to delete any data set covered by the dataset profiles that have a UACC of ALTER.

Remediation

Review each of these profiles and determine whether the UACC is appropriate. For those profiles where the UACC is excessive, you will have to determine who really needs access before changing the UACC. To find out who is accessing these data sets, review SMF data to determine who is accessing the data sets with greater than READ access.

“Top Ten” Assessment Finding #5

Finding

Improper Use or Lack of UNIXPRIV Profiles

Explanation

The UNIXPRIV class resource rules are designed to give a limited subset of the superuser UID (0) capability. When implemented properly, UNIXPRIV profiles can significantly reduce the unnecessary requests for assignment of UID (0) to user IDs.

Risk

The lack of UNIXPRIV profiles or excessive to these profiles represents an exposure to the integrity of UNIX file systems.

Remediation

Review the users’ activity that are currently defined as SUPERUSERs to determine if more granular profiles may be defined in the UNIXPRIV class that will authorize their activity. Refine the access list and define more granular profiles based upon the superuser functions that the users with UID(0) need.

“Top Ten” Assessment Finding #6

Finding

Dataset Profiles with UACC of READ

Explanation

The UACC value for a dataset profile defines the default level of access to which any user whose user ID or a group to which it has been connected does not appear in the access list.

Risk

Data sets that are protected by a RACF profile with a UACC of READ will allow most users with system access to read or copy sensitive and critical data residing in these data sets.

Remediation

Review each of these profiles and determine whether the UACC is appropriate. For those profiles where the UACC is excessive, you will have to determine who really needs access before changing the UACC. To find out who is accessing these data sets, review SMF data to determine who is accessing the data sets with READ access.

“Top Ten” Assessment Finding #7

VANGUARD
Integrity Professionals
Information Security Experts

Finding

Excessive Access to the SMF Data Sets

Explanation

SMF data collection is the system activity journaling facility of the z/OS system. With the proper parameter designations, it serves as the basis to ensure individual user accountability.

Risk

The ability to READ SMF data enables someone to identify potential opportunities to breach your security. If UPDATE or higher access is granted, a risk of audit log corruption exists. Access control for the unloaded data is critical to ensure a valid chain of custody.

Remediation

Review the RACF profiles protecting the active and dumped SMF data to ensure that access authority to SMF collection files is limited to only systems programming staff and and/or batch jobs that perform SMF dump processing and ensure the UPDATE and higher accesses are being logged.

IBM Server Proven

Business Partner IBM

“Top Ten” Assessment Finding #8

Finding

RACF Database is not Adequately Protected

Explanation

The RACF database contains extremely sensitive security information. No access to the RACF database is required for normal administration activities using either RACF commands or the RACF provided ISPF panels.

Risk

Any user who has read access to the RACF database or any backup copy could make a copy and then use a cracker program to find passwords for user IDs and could obtain a list of user IDs and resources.

Remediation

Review the protection for the RACF database and any backup copies and remove any access list entries granting access higher than NONE, other than to senior RACF administrators and system staff tasked to run RACF database utilities.

“Top Ten” Assessment Finding #9

VANGUARD
Integrity Professionals
Information Security Experts

Finding	Excessive Access to APF Libraries
Explanation	Authorized Program Facility (APF) libraries are in integral part of the z/OS architecture to enable maintenance of the integrity of the z/OS operating system environment. Libraries designated as APF allow programs to execute with the authority of z/OS itself, so the ability to modify these libraries must be strictly controlled.
Risk	UPDATE or higher access to an APF library can allow an individual to create an authorized program which can bypass security controls and execute privileged instructions. UPDATE or higher access should be limited to senior systems support staff.
Remediation	Review the protection of all APF libraries and remove or change inappropriate access list entries and ensure that all IUPDATE activity is logged to SMF.

“Top Ten” Assessment Finding #10

Finding	Inappropriate Access to FACILITY Class BPX.DAEMON Profile
Explanation	Daemons are processes that perform services for other users. In order to do this, a daemon must be able to change its identity temporarily to the identity of the user it will perform work for. The RACF FACILITY class profile called BPX.DAEMON can be used to control the use of the daemon functions.
Risk	The ability to assume the identity of another UNIX user must be limited to the user IDs that are actual UNIX Daemons.
Remediation	Review the access list of the BPX.DAEMON profile to remove any access for users that are not actual z/OS UNIX Daemons.

Performing a z/OS Vulnerability Assessment

ASSESSMENT & REMEDIATION

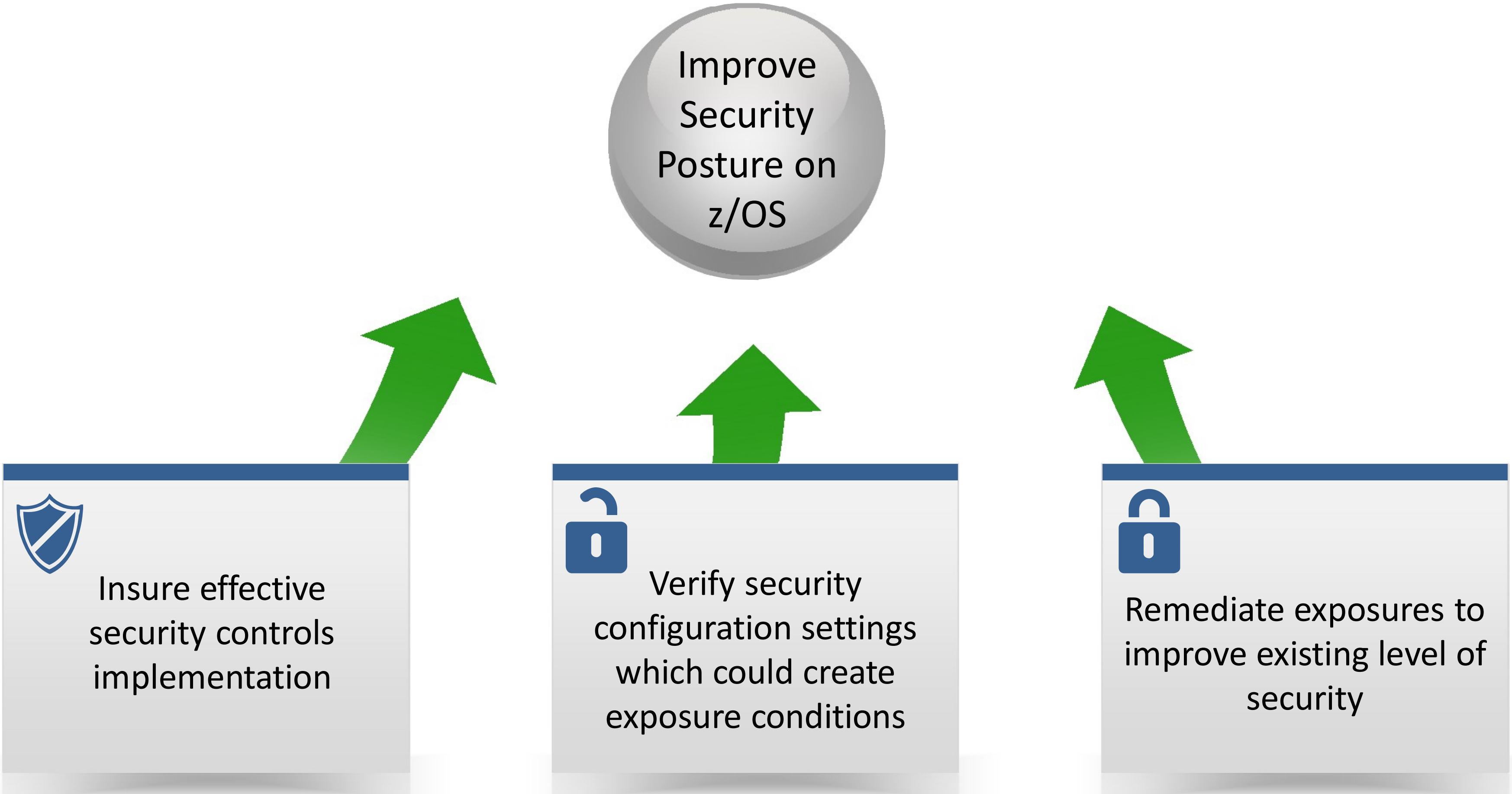
It’s All about Risk

- **What Risks Do Senior Executives Care About**
  - Financial Risks - loss of corporate income, loss of compensation.
  - Reputational Risks – loss of prestige, customers, sales.
  - Legal Risks – going to jail, being subject to law suits, or being fined by an industry or government entity.

Managing Your Risks

- What is the likelihood that an event will occur?
  - Attempt to access your system without authorization?
- If an event occurs, will it have an impact?
  - Will they be able to access resource on your system?
- How bad would that impact be?
  - ???

Vulnerability Assessment Objectives



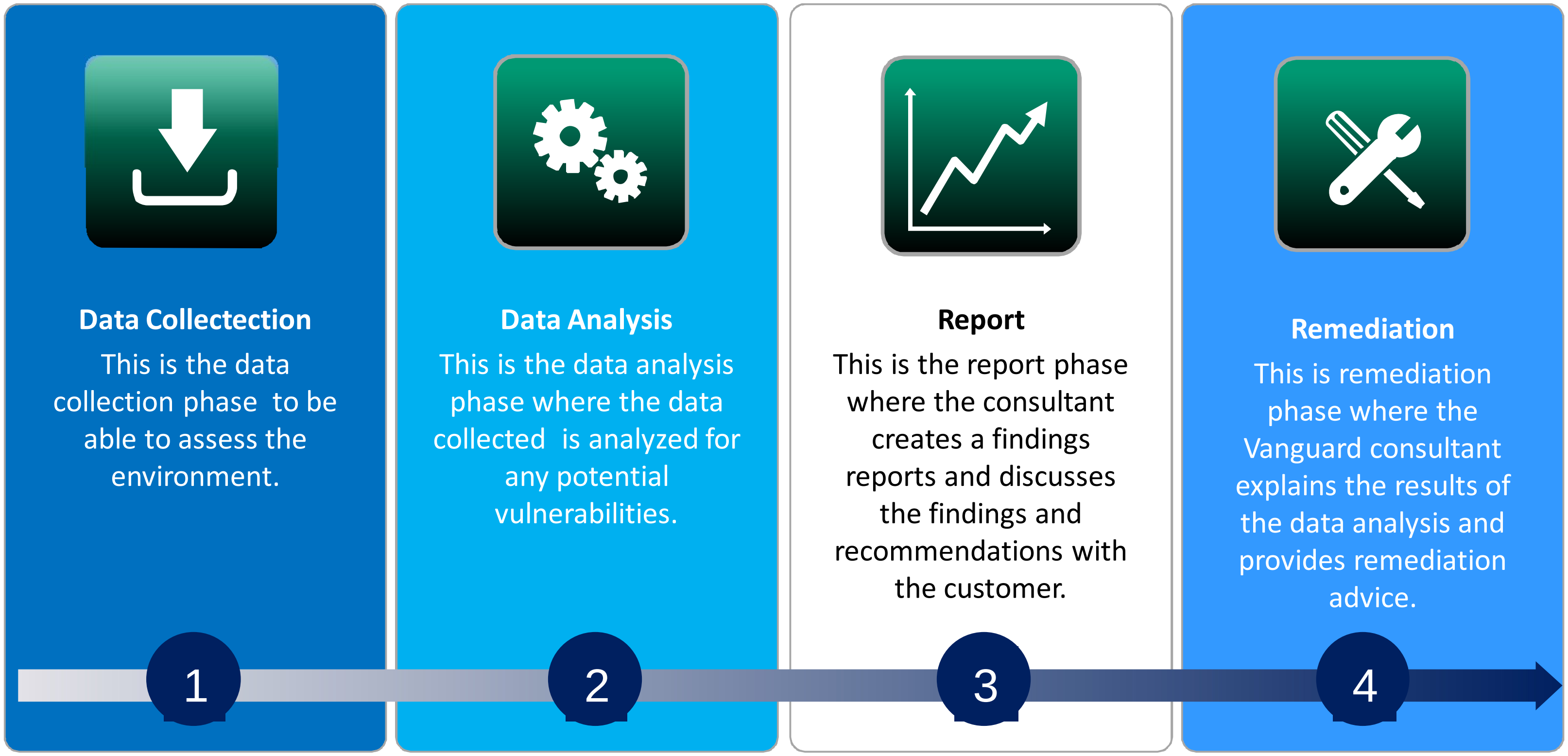
Improve Security Posture on z/OS

Insure effective security controls implementation

Verify security configuration settings which could create exposure conditions

Remediate exposures to improve existing level of security

Vulnerability Assessment Approach



Data Collectection

This is the data collection phase to be able to assess the environment.

Data Analysis

This is the data analysis phase where the data collected is analyzed for any potential vulnerabilities.

Report

This is the report phase where the consultant creates a findings reports and discusses the findings and recommendations with the customer.

Remediation

This is remediation phase where the Vanguard consultant explains the results of the data analysis and provides remediation advice.

Conclusion

Questions?

Thank You!

For more information, please visit:

http://www.go2vanguard.com

sales@go2vanguard.com

Спасибо
Russian

ขอบคุณ
Thai

شكراً
Arabic

多謝
Traditional Chinese

감사합니다
Korean

ありがとうございました
Japanese

धन्यवाद
Hindi

நன்றி
Tamil

多谢
Simplified Chinese

Danke
German

Obrigado
Brazilian Portuguese

Grazie
Italian

Merci
French

Gracias
Spanish

Thank You
English

Vanguard Assessment Tools Available

VANGUARD
Integrity Professionals
Information Security Experts

Vanguard

Provides Identity & Access Management solutions and Governance, Risk & Compliance solutions for z/OS and other enterprose platforms.

Vanguard Administrator™

Simplify and Enhance Security Management Functions on systems running IBM's Security Server™ (RACF)

Vanguard Analyzer™

Delivers expert-level Vulnerability Assessments and Audit results for System z in minutes

Vanguard Advisor™

Offers the most comprehensive Event Detection, Analysis and Reporting package for the z/OS environment

Vanguard Configuration Manager™

Provides the fastest and most accurate method to verify that mainframe security configuration controls are in compliance with the DISA STIGs