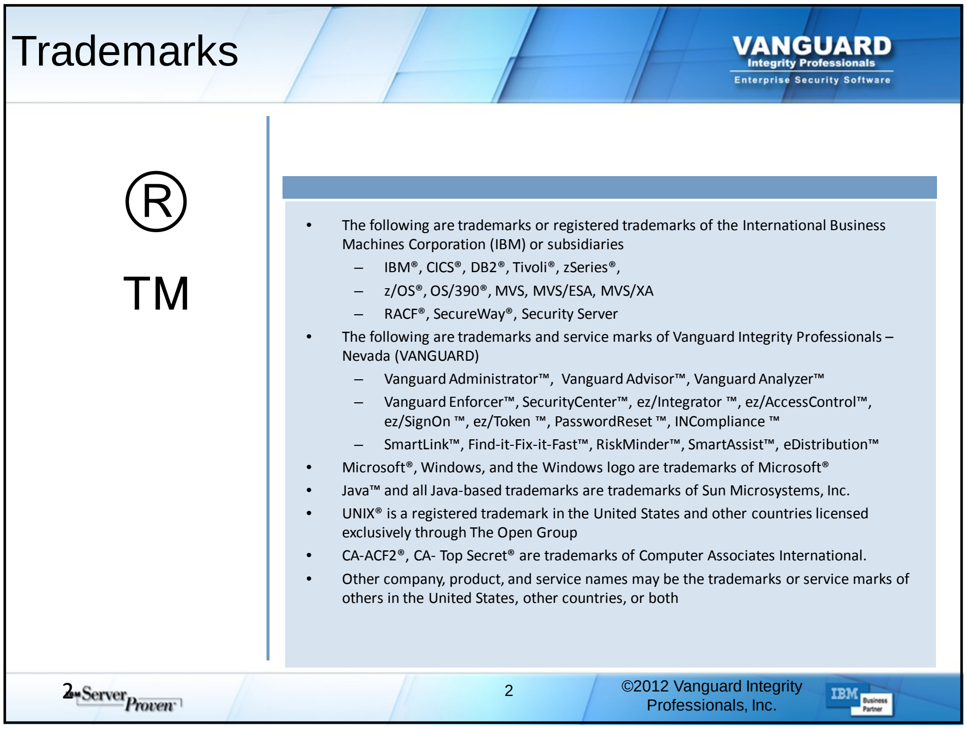
VANGUARD
Integrity Professionals
Enterprise Security Software

"Top Ten" z/OS (RACF) Security Assessment Findings

Philip Emrich
Senior Professional Services Consultant
pemrich@go2vanguard.com

Anaheim, CA
5 – 10 August 2010
SHARE 119 – Session 11676

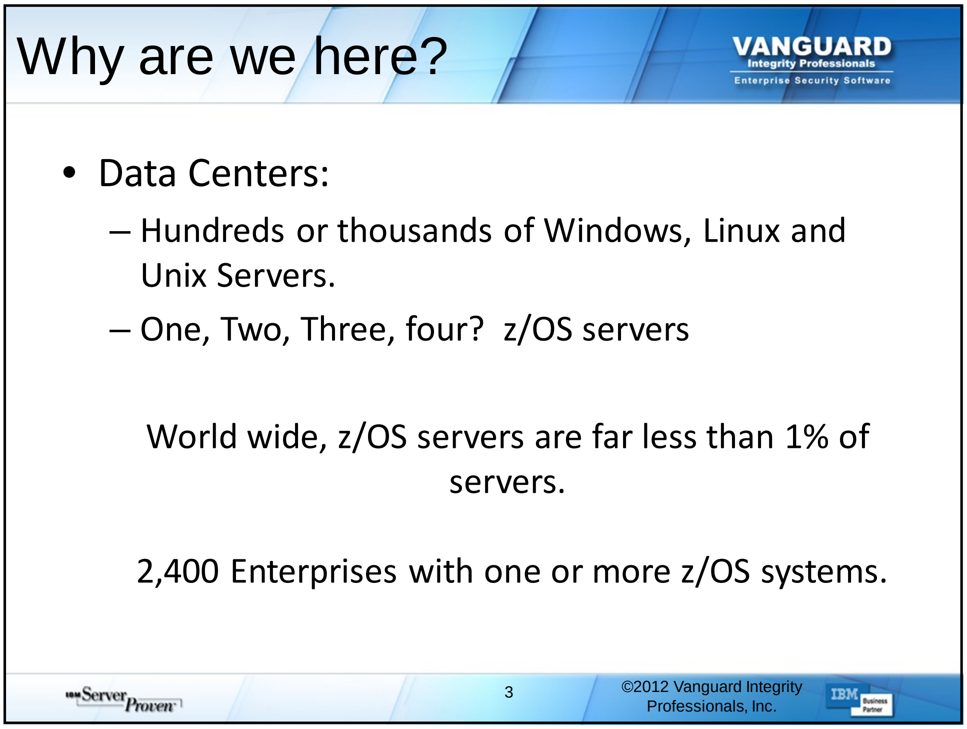


Trademarks

®

TM

- The following are trademarks or registered trademarks of the International Business Machines Corporation (IBM) or subsidiaries
  - IBM®, CICS®, DB2®, Tivoli®, zSeries®,
  - z/OS®, OS/390®, MVS, MVS/ESA, MVS/XA
  - RACF®, SecureWay®, Security Server
- The following are trademarks and service marks of Vanguard Integrity Professionals – Nevada (VANGUARD)
  - Vanguard Administrator™, Vanguard Advisor™, Vanguard Analyzer™
  - Vanguard Enforcer™, SecurityCenter™, ez/Integrator ™, ez/AccessControl™, ez/SignOn ™, ez/Token ™, PasswordReset ™, INCompliance ™
  - SmartLink™, Find-it-Fix-it-Fast™, RiskMinder™, SmartAssist™, eDistribution™
- Microsoft®, Windows, and the Windows logo are trademarks of Microsoft®
- Java™ and all Java-based trademarks are trademarks of Sun Microsystems, Inc.
- UNIX® is a registered trademark in the United States and other countries licensed exclusively through The Open Group
- CA-ACF2®, CA- Top Secret® are trademarks of Computer Associates International.
- Other company, product, and service names may be the trademarks or service marks of others in the United States, other countries, or both



Why are we here?

VANGUARD Integrity Professionals Enterprise Security Software

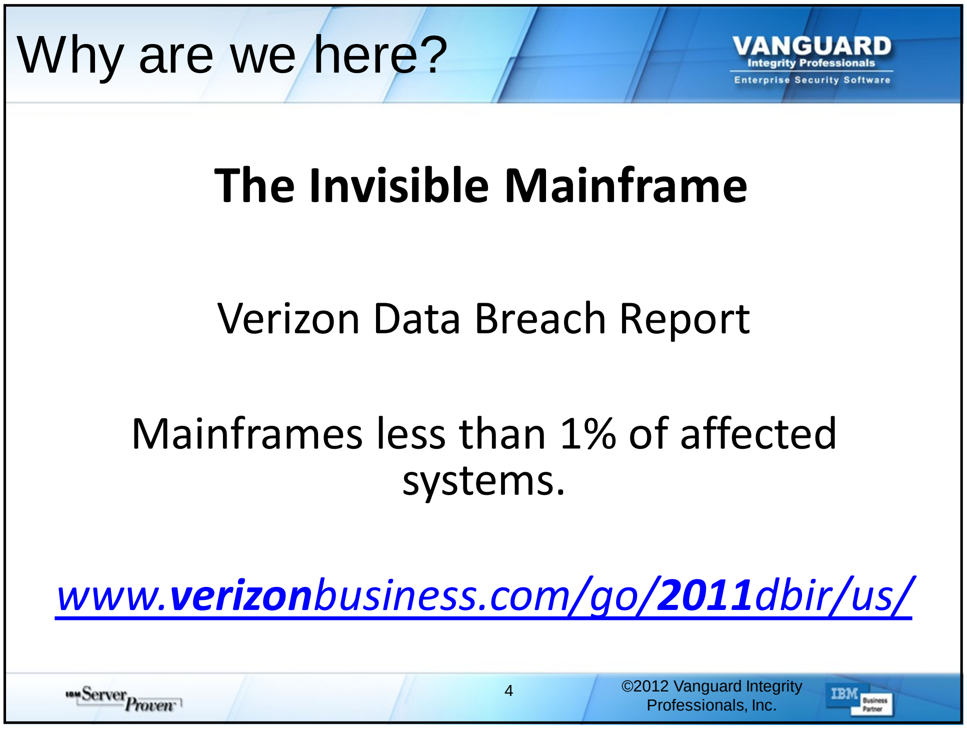
- Data Centers:
  - Hundreds or thousands of Windows, Linux and Unix Servers.
  - One, Two, Three, four? z/OS servers

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

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

IBM ServerProven

IBM Business Partner



Why are we here?

VANGUARD Integrity Professionals Enterprise Security Software

The Invisible Mainframe

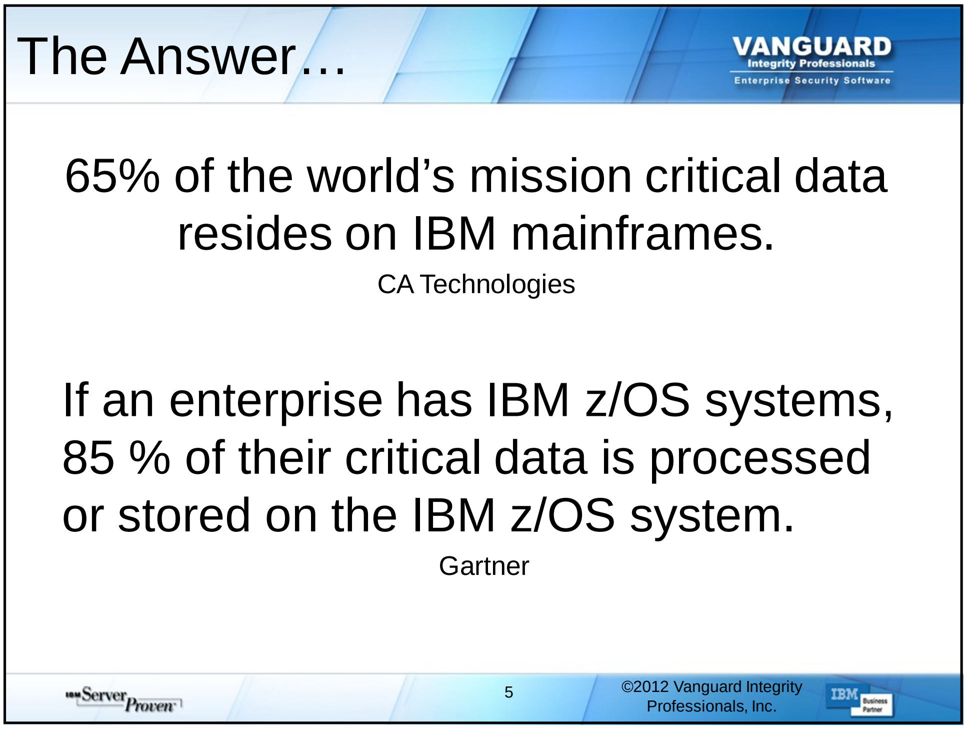
Verizon Data Breach Report

Mainframes less than 1% of affected systems.

*www.**verizon**business.com/go/**2011**dbir/us/*

IBM ServerProven

IBM Business Partner



The Answer…

VANGUARD Integrity Professionals Enterprise Security Software

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

CA Technologies

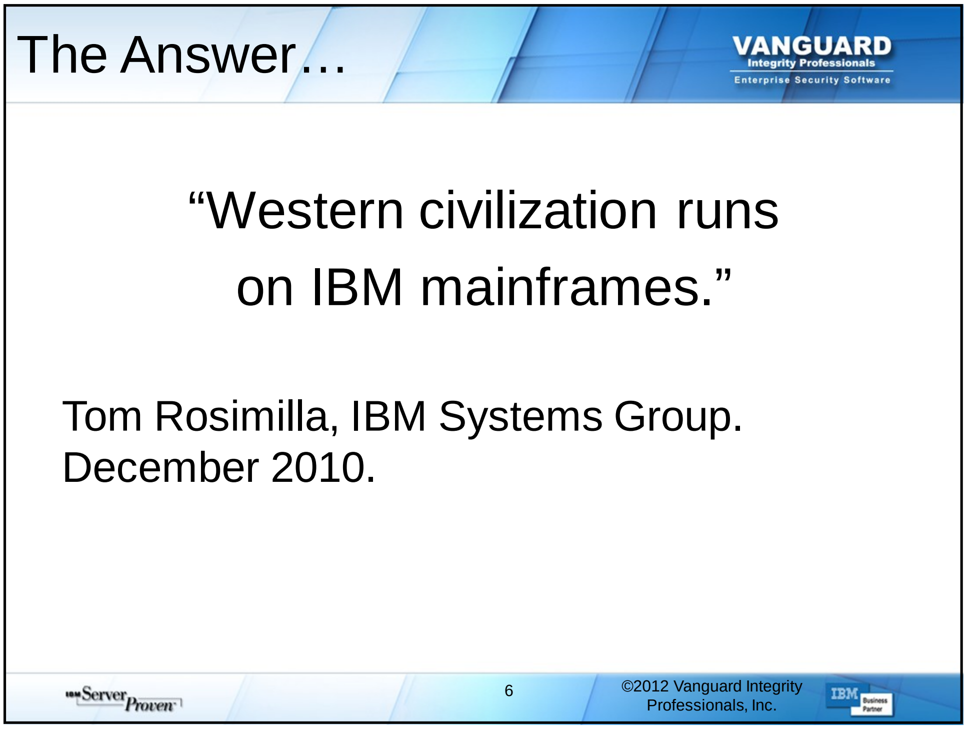
If an enterprise has IBM z/OS systems, 85 % of their critical data is processed or stored on the IBM z/OS system.

Gartner

IBM Server Proven

5

IBM Business Partner



The Answer…

VANGUARD Integrity Professionals Enterprise Security Software

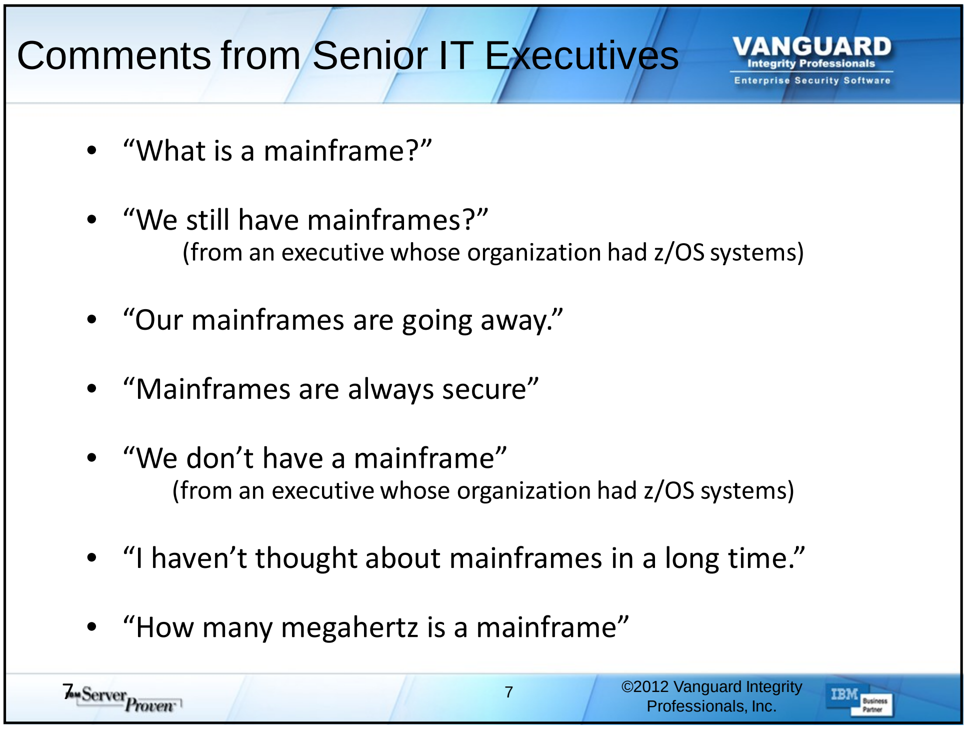
“Western civilization runs on IBM mainframes.”

Tom Rosimilla, IBM Systems Group.
December 2010.

IBM Server Proven

6

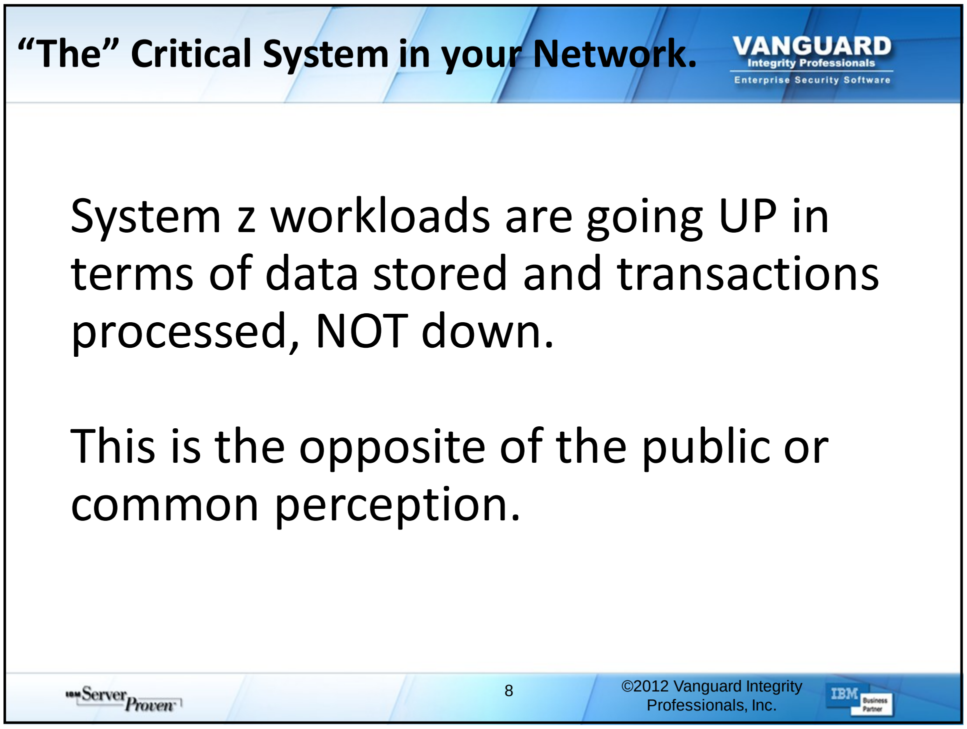
IBM Business Partner



Comments from Senior IT Executives

- “What is a mainframe?”
- “We still have mainframes?”
  (from an executive whose organization had z/OS systems)
- “Our mainframes are going away.”
- “Mainframes are always secure”
- “We don’t have a mainframe”
  (from an executive whose organization had z/OS systems)
- “I haven’t thought about mainframes in a long time.”
- “How many megahertz is a mainframe”

7

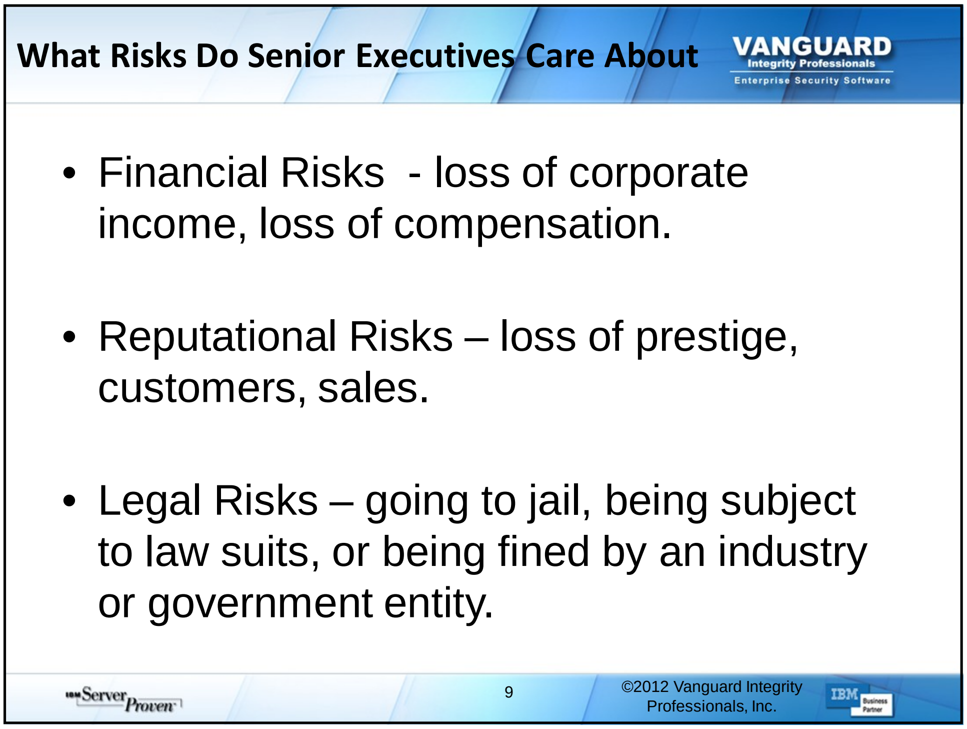


“The” Critical System in your Network.

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.

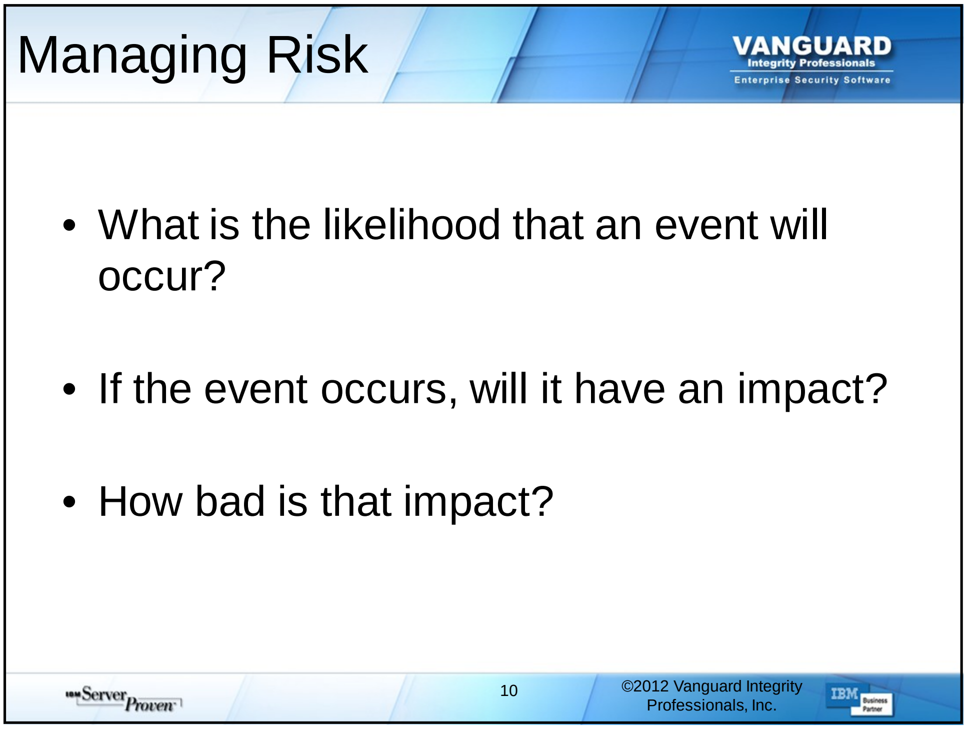
8



What Risks Do Senior Executives Care About

VANGUARD Integrity Professionals Enterprise Security Software

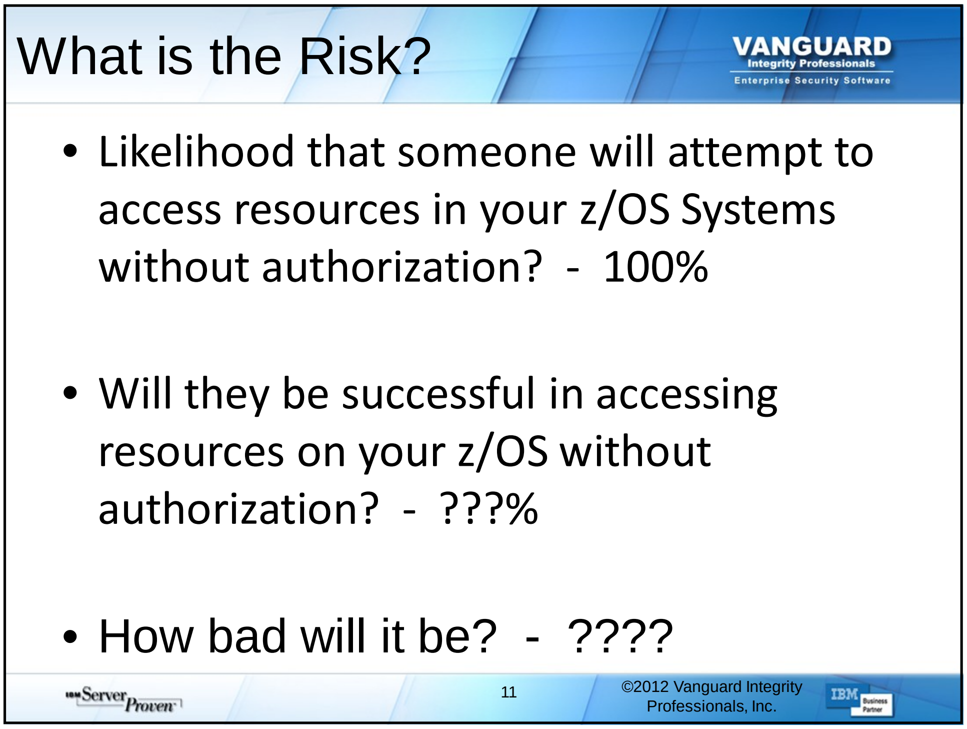
- Financial Risks - loss of corporate income, loss of compensation.
- Reputational Risks – loss of prestige, customers, sales.
- Legal Risks – going to jail, being subject to law suits, or being fined by an industry or government entity.



Managing Risk

VANGUARD Integrity Professionals Enterprise Security Software

- What is the likelihood that an event will occur?
- If the event occurs, will it have an impact?
- How bad is that impact?

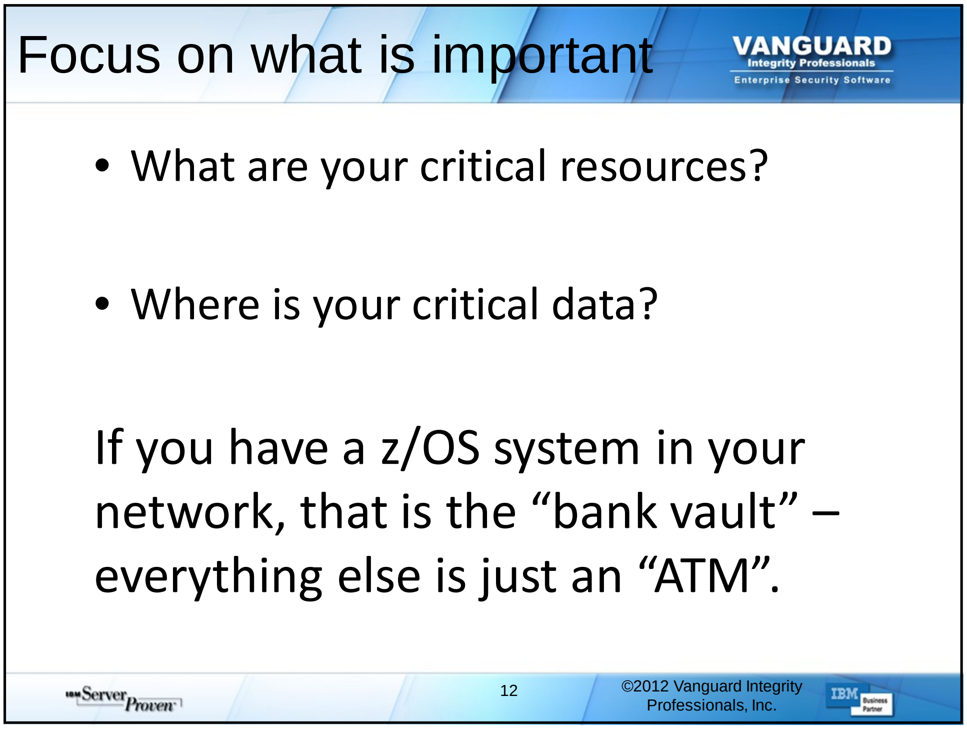


What is the Risk?

- Likelihood that someone will attempt to access resources in your z/OS Systems without authorization? - 100%
- Will they be successful in accessing resources on your z/OS without authorization? - ???%
- How bad will it be? - ????

11

©2012 Vanguard Integrity Professionals, Inc.



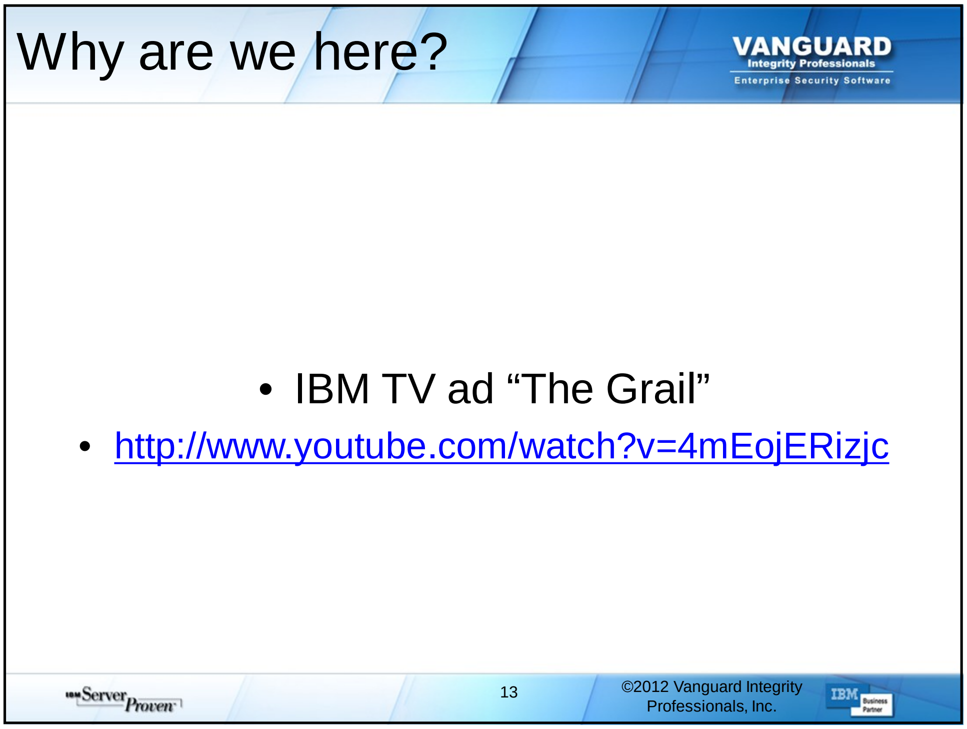
Focus on what is important

- What are your critical resources?
- Where is your critical data?

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

12

©2012 Vanguard Integrity Professionals, Inc.



Why are we here?

VANGUARD Integrity Professionals Enterprise Security Software

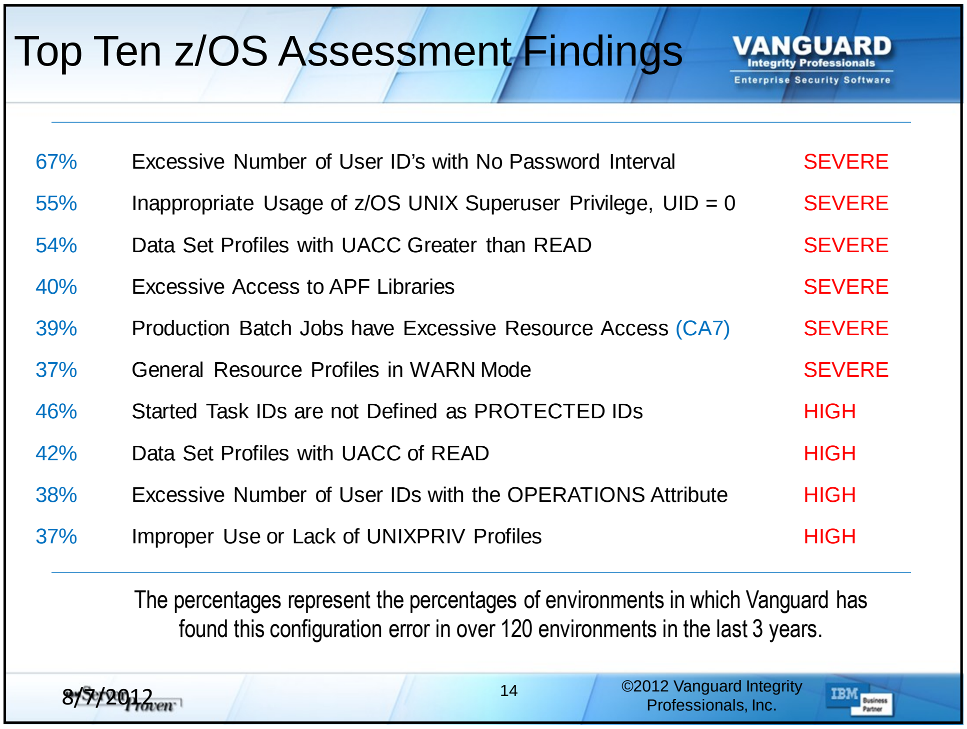
- IBM TV ad “The Grail”
- http://www.youtube.com/watch?v=4mEojERizjc

IBM Server Proven

13

©2012 Vanguard Integrity Professionals, Inc.

IBM Business Partner



Top Ten z/OS Assessment Findings

VANGUARD Integrity Professionals Enterprise Security Software

67%	Excessive Number of User ID’s with No Password Interval	SEVERE
55%	Inappropriate Usage of z/OS UNIX Superuser Privilege, UID = 0	SEVERE
54%	Data Set Profiles with UACC Greater than READ	SEVERE
40%	Excessive Access to APF Libraries	SEVERE
39%	Production Batch Jobs have Excessive Resource Access (CA7)	SEVERE
37%	General Resource Profiles in WARN Mode	SEVERE
46%	Started Task IDs are not Defined as PROTECTED IDs	HIGH
42%	Data Set Profiles with UACC of READ	HIGH
38%	Excessive Number of User IDs with the OPERATIONS Attribute	HIGH
37%	Improper Use or Lack of UNIXPRIV Profiles	HIGH

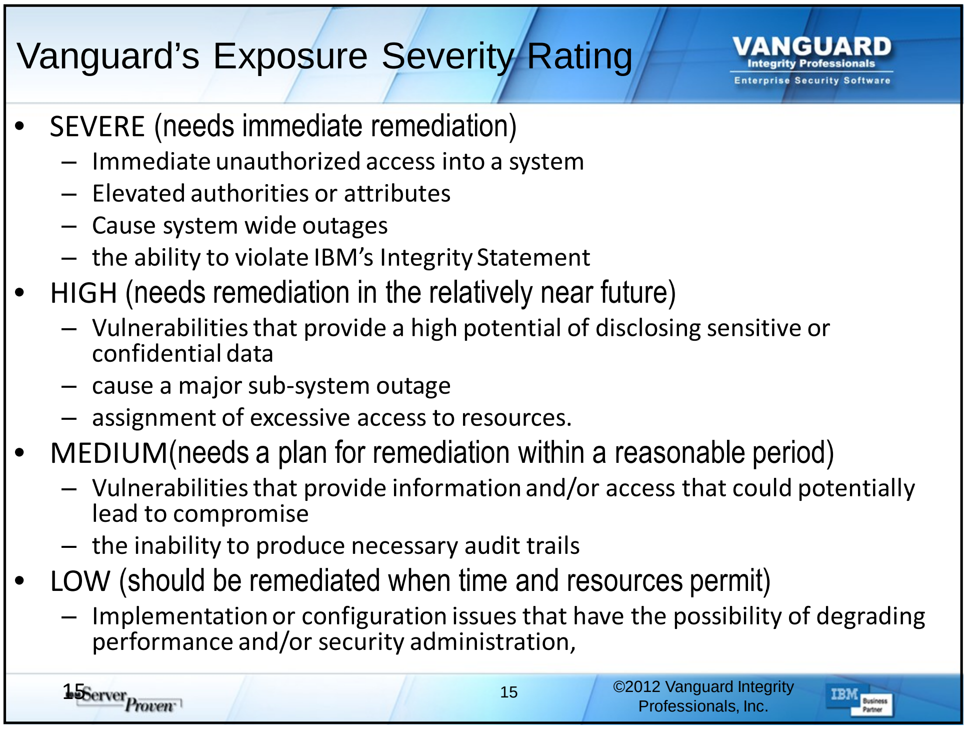
The percentages represent the percentages of environments in which Vanguard has found this configuration error in over 120 environments in the last 3 years.

8/7/2012 IBM Server Proven

14

©2012 Vanguard Integrity Professionals, Inc.

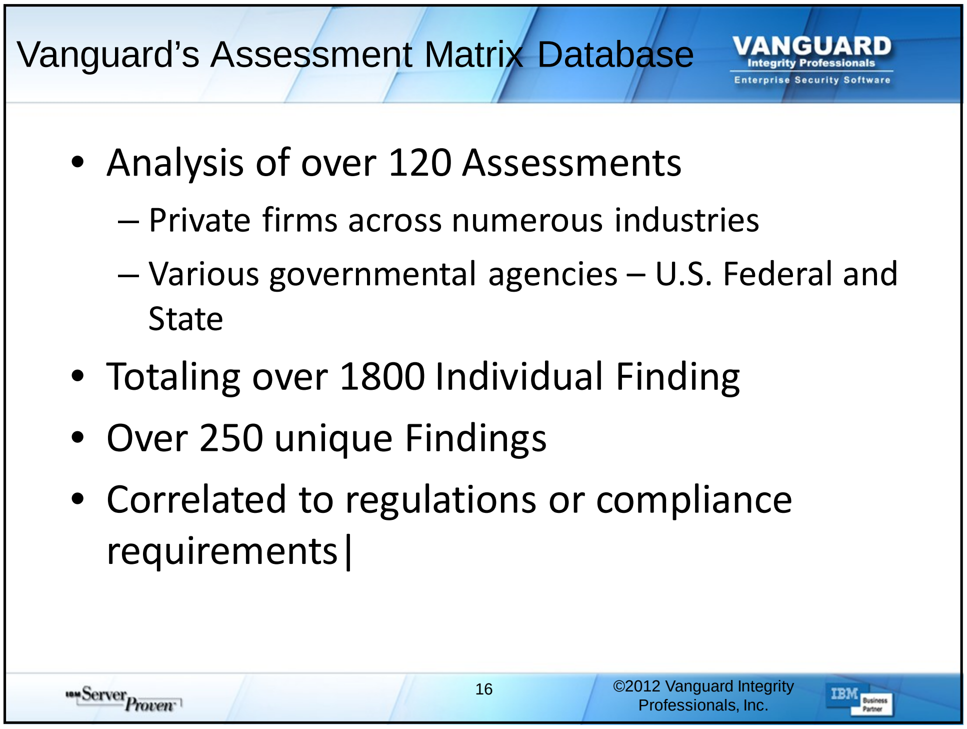
IBM Business Partner



Vanguard's Exposure Severity Rating

VANGUARD Integrity Professionals Enterprise Security Software

- 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 relatively 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,



Vanguard's Assessment Matrix Database

VANGUARD Integrity Professionals Enterprise Security Software

- Analysis of over 120 Assessments
  - Private firms across numerous industries
  - Various governmental agencies – U.S. Federal and State
- Totaling over 1800 Individual Finding
- Over 250 unique Findings
- Correlated to regulations or compliance requirements|

The Situation

VANGUARD Integrity Professionals
Enterprise Security Software

Forbes.com

The Naked Mainframe
Dan Woods, 01.19.2010

Chief Technologist Officer & Editor
Evolved Technologist

JargonSpy

“MF’s are wrongly considered invulnerable from a security standpoint. And that most IT staff view the MF as just another Network node, and frequently more thought goes into protecting PC’s - than into securing mainframes from intrusion”.

70s and '80s when mainframes ruled the world.
volved fixing an IBM 370 Assembler program
ardware architecture, as a convenient form of
u programmed with the details of computer

as new and shiny and not categorized only as an
ity of Michigan housed the Computer Science
d the Arts. I'm one of a few people with a
e. As an assistant to computer science pioneer
th a chunk of the ENIAC, one of the first digital

g the mainframe led me to my first job as an
ent of a system administrator. Back then,
nt IBM operating systems could run on one

everyday life the credit card processors and the
tions flow are largely handled by mainframes.
nd today Linux runs on the computer
port more than 15,000 mainframe installations
00 million instructions per second (MIPS), with

Oak Investments, has first-hand experience
chitecture from his tenure as Chief Technology
in the 1990s. The PaySys software based on the
Data Corporation, but the version that ran on
er grabbed a large share of market. Black points
inst as a student may be old, but the
as any computer on the market today.

"Mainframes are not implemented in vacuum tubes. The design may be old, but the hardware is state of the art," said Black.

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."

IBM Business Partner

The Situation

VANGUARD Integrity Professionals
Enterprise Security Software

Ant Allan
Research VP

Gartner Research

Publication Date: 20 January 2010 ID Number: G00172909

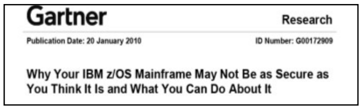
Why Your IBM z/OS Mainframe May Not Be as Secure as You Think It Is and What You Can Do About It

Ant Allan

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

IBM Business Partner

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 audit security
- Lax audits due to insufficient skill sets – not communicated to management
- Few documented guidelines available
- Full compliance with standards is difficult

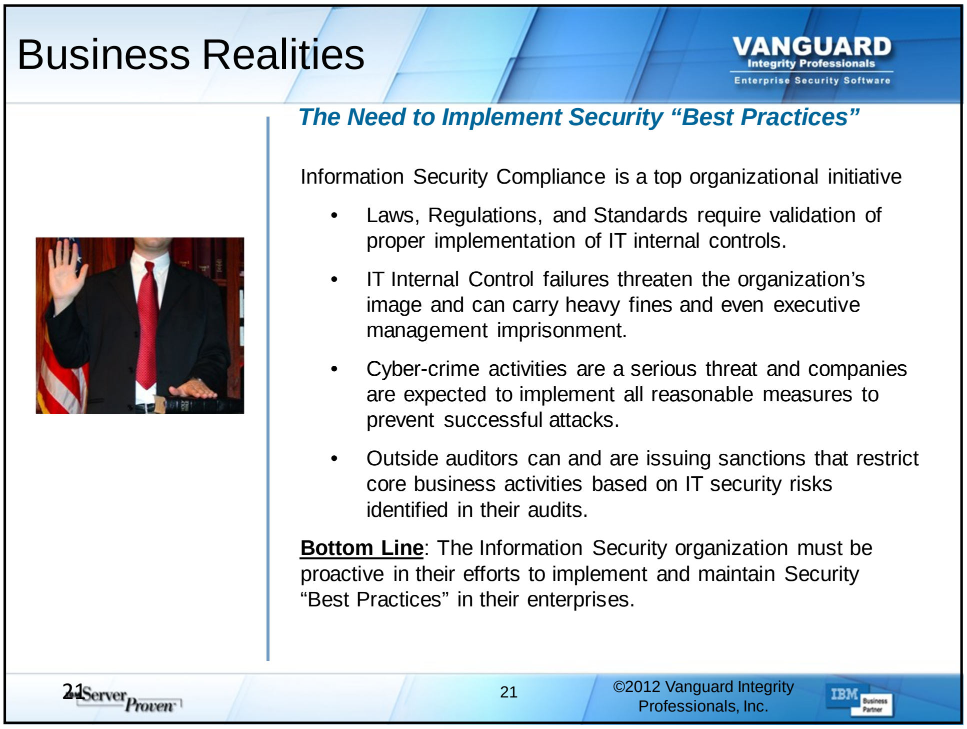
Top Gartner Recommendations

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



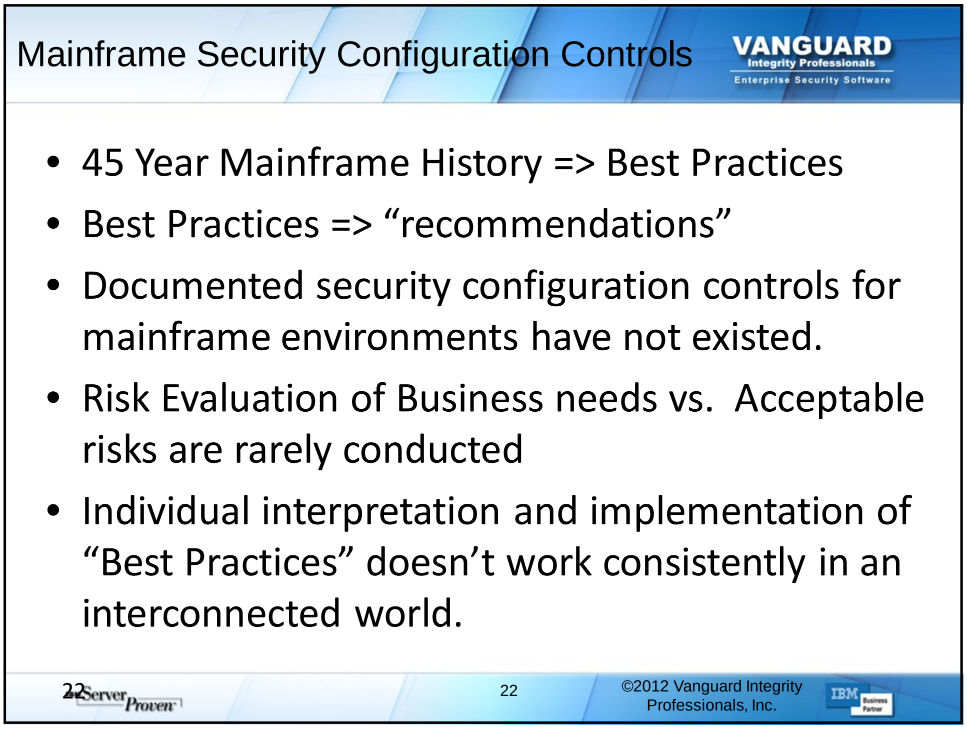
Business Realities

The Need to Implement Security "Best Practices"

Information Security Compliance is a top organizational initiative

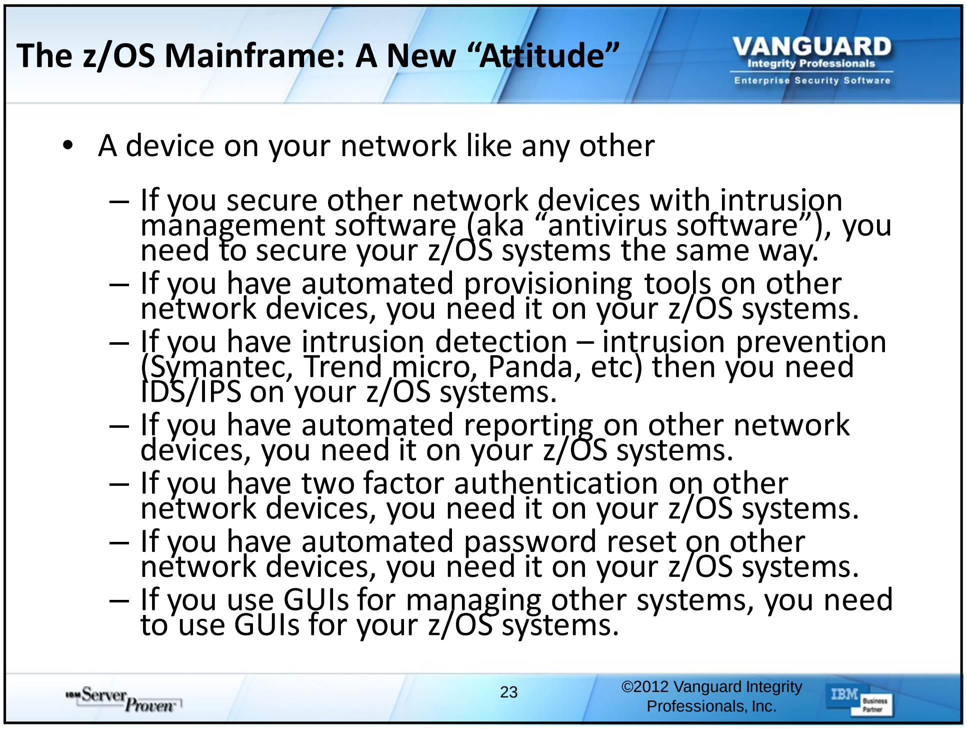
- Laws, Regulations, and Standards require validation of proper implementation of IT internal controls.
- IT Internal Control failures threaten the organization's image and can carry heavy fines and even executive management imprisonment.
- Cyber-crime activities are a serious threat and companies are 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.



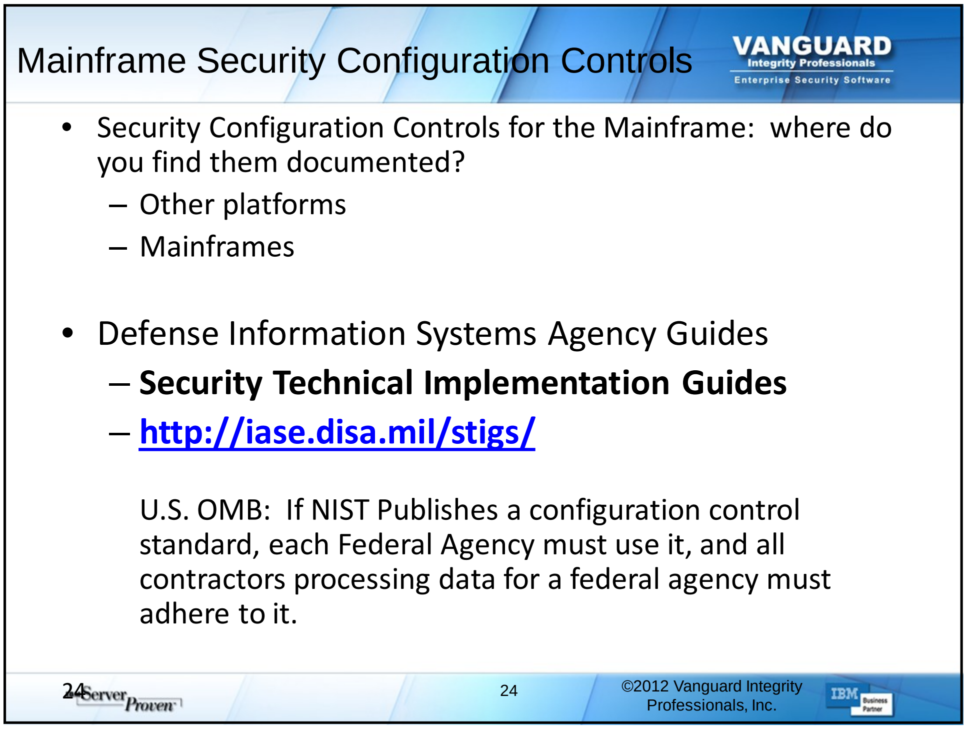
Mainframe Security Configuration Controls

- 45 Year Mainframe History => Best Practices
- Best Practices => "recommendations"
- Documented security configuration controls for mainframe environments have not existed.
- Risk Evaluation of Business needs vs. Acceptable risks are rarely conducted
- Individual interpretation and implementation of "Best Practices" doesn't work consistently in an interconnected world.



The z/OS Mainframe: A New "Attitude"

- A device on your network like any other
  - If you secure other network devices with intrusion management software (aka "antivirus software"), you need to secure your z/OS systems the same way.
  - If you have automated provisioning tools on other network devices, you need it on your z/OS systems.
  - If you have intrusion detection – intrusion prevention (Symantec, Trend micro, Panda, etc) then you need IDS/IPS on your z/OS systems.
  - If you have automated reporting on other network devices, you need it on your z/OS systems.
  - If you have two factor authentication on other network devices, you need it on your z/OS systems.
  - If you have automated password reset on other network devices, you need it on your z/OS systems.
  - If you use GUIs for managing other systems, you need to use GUIs for your z/OS systems.



Mainframe Security Configuration Controls

- Security Configuration Controls for the Mainframe: where do you find them documented?
  - Other platforms
  - Mainframes

- Defense Information Systems Agency Guides
  - **Security Technical Implementation Guides**
  - **http://iase.disa.mil/stigs/**

U.S. OMB: If NIST Publishes a configuration control standard, each Federal Agency must use it, and all contractors processing data for a federal agency must adhere to it.

Mainframe Security Configuration Controls

- NIST: Publishes 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 OS390
- Current NVD checklists for z/OS:
  - zOS RACF STIG Checklist V6,R12 (27 July 2012)
  - zOS ACF2 STIG Checklist V6,R12 (27 July 2012)
  - zOS TSS STIG Checklist V6,R12 (27 July 2012)

Conclusion

Questions??

Thank You!

VANGUARD
Integrity Professionals
Enterprise Security Software

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

27 Server Proven 27 ©2012 Vanguard Integrity Professionals, Inc.