The Myth of Mainframe Security
Session: 14812

Mark Wilson
RSM Partners
Markw@rsmpartners.com
Mobile +44 (0) 7768 617006
www.rsmpartners.com

Glinda Cummings
IBM
glinda@us.ibm.com

Agenda

- Objectives
- Introduction
- Where did it all start?
- Aren’t Mainframes dead?
- Where are we today?
- What do we need to do?
- Summary
- Questions

Objectives

- There are many who hold the belief that a mainframe z/OS system is inherently secure
- However, more recently, we hear the pundits changing the tune saying that it is the "most securable" platform
- This discussion will focus on the “Myth of Mainframe Security” and the speakers will debate that in the majority of organizations the mainframe is not as secure as we would like!
- We will give you plenty of food for thought and also some hints and tips for what you should be doing to protect yourselves

Introduction

Introduction

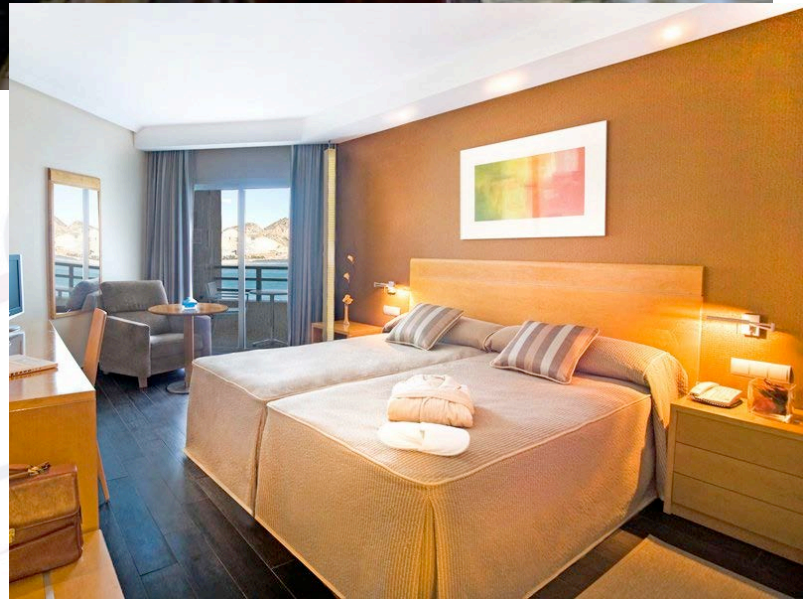
- It’s a double act:
  - Mark Wilson
    - I am a mainframe technician with some knowledge of Mainframe Security
    - I have been doing this for over 30 years
  - Glinda Cummings
    - IBM Security Worldwide Sr. Product Manager
    - 34 years in Mainframe Security
- Happy to take questions as we go

This is where Mark Lives!

Bromsgrove – Sales Kidderminster - Back Office High Wycombe - RSMT

Where he occasionally sits and dreams about

But in fact spends most of his time in



This is where Glinda Lives!

Where she occasionally sits and dreams about

But in fact spends most of her time in

Where did it all start?

Where did it all start?

- Well that depends
  - Was it the start of the Share project looking at data security which started way back in 1972
  - Was it when IBM gave us the The IBM Statement of Integrity
    - In 1973, IBM announced its Statement of Integrity for its new Operating System, OS/VS2. OS/VS2 was the predecessor to MVS and z/OS. In its current form, the IBM Statement of Integrity states…..

IBM Statement of Integrity

- IBM's commitment includes design and development practices intended to prevent unauthorized application programs, subsystems, and users from bypassing z/OS security – that is, to prevent them from gaining access, circumventing, disabling, altering, or obtaining control of key z/OS system processes and resources unless allowed by the installation. Specifically, z/OS "System Integrity" is defined as the inability of any program not authorized by a mechanism under the installation's control to circumvent or disable store or fetch protection, access a resource protected by the z/OS Security Server (RACF®), or obtain control in an authorized state; that is, in supervisor state, with a protection key less than eight (8), or Authorized Program Facility (APF) authorized. In the event that an IBM System Integrity problem is reported, IBM will always take action to resolve it.

The IBM MVS Authorized Assembler Services Guide

- goes on to say that…

- "… to ensure that system integrity is effective and to avoid compromising any integrity controls provided in the system, the installation must assume responsibility … that its own modifications and additions to the system do not introduce any integrity exposures. That is, all installation-written authorized code (for example, an installation SVC) must perform the same or equivalent type of validity checking and control that the system uses to maintain its integrity."

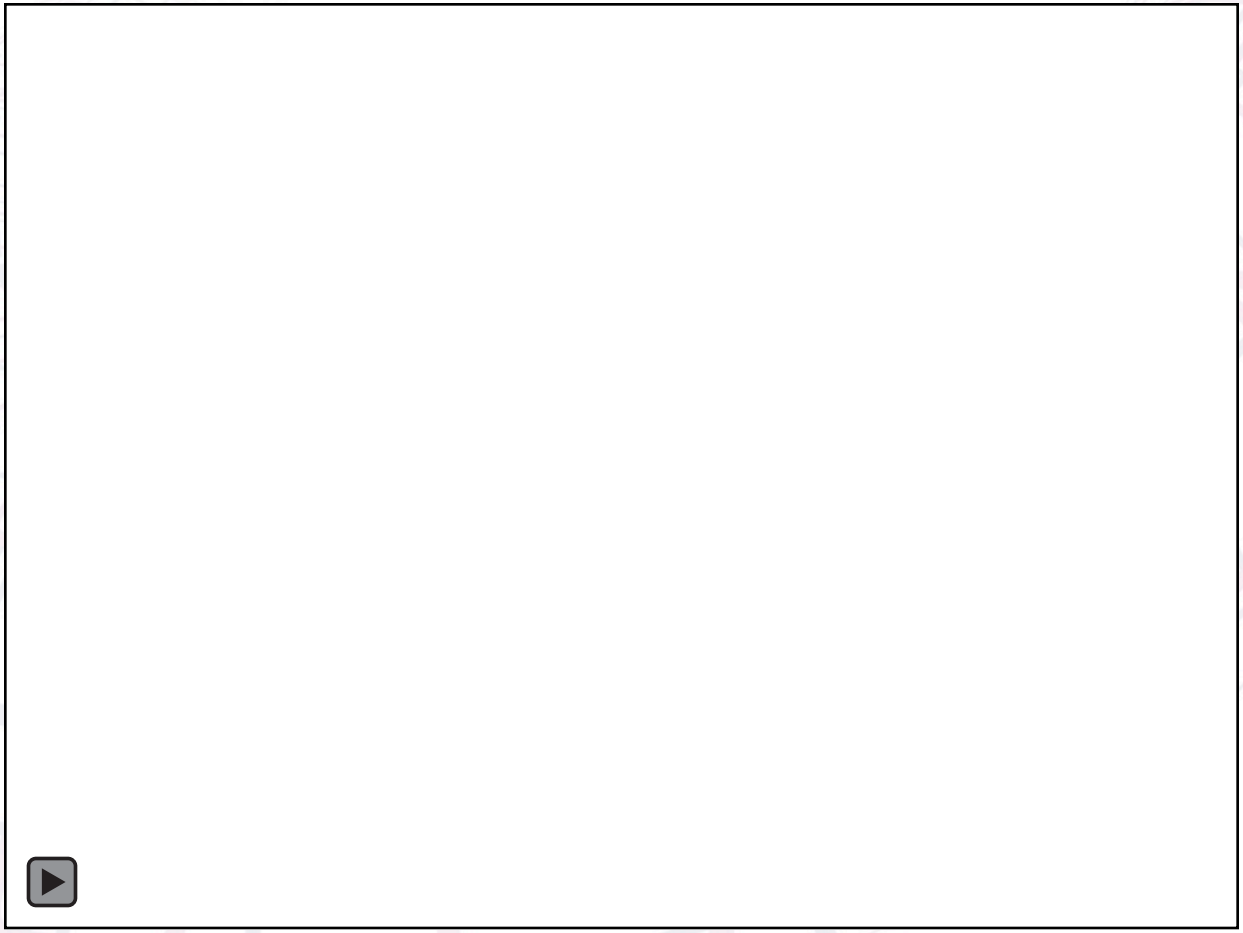
IBM Statement of Integrity

- It is important to note in the first statement that IBM does not state that z/OS will have no system integrity problems, but rather that if one is reported, they will always take action to resolve it. And, the second reference clearly states that it is the installation's responsibility that any authorized code they add, and this would include products from Independent Software Vendors and any installation developed code, also performs the same validity checking that z/OS uses to maintain its integrity

- http://www-03.ibm.com/systems/z/os/zos/features/racf/zos_integrity_statement.html

- z/OS MVS Programming: Authorized Assembler Services Guide – SA22-7608-15, page 423

So……Where did it all start….Well a long time ago..



Aren't mainframes dead?

Aren't mainframes dead?

- OK, some twenty plus years after InfoWorld editor Stewart Alsop announced the death of the mainframe, it's time to put the poor thing out of its misery. I declare the mainframe finally.... DEAD……. RIP……..really ☺

- Of course, if you want a server that is highly available (well, one where 5 minutes downtime a year, including "planned downtime", is worrying); one which can handle multi-tenanting with no possibility of one tenant affecting another's service; which can run several programs at the same time with no risk of something low priority stopping something higher priority working; and one that is capable of running, say, an ATM business for the whole of Europe or North America; then you might still get a zEnterprise as an alternative to other technologies

Aren't mainframes dead?

- But stories of the mainframes demise have led to poor investment in system z infrastructure and security tools and processes
- Mainframes are very-much-alive and as Mark Twain famously commented that reports of his death were greatly exaggerated
- Recent Share News Flash: The Mainframe (Still) Isn't Dead
  - http://www.share.org/p/bl/et/blogaid=256

Where are we today?

Where are we today?

- Some may say Old Dog, New Tricks…..Just look at the uptake of Linux on system z on a worldwide basis
- The mainframe is still one of the IT industry's most enduring inventions
- Growing sales abroad have allowed IBM to invest heavily in the new mainframe, dubbed zEnterprise EC12
- The mainframe has stayed relevant by adapting, whereas the PC, its supposed slayer, has stayed pretty much the same and is now being pushed aside
- A recent quote stated: "PCs are considered a mature platform"
- A don't forget the mainframe is 50 years old on the 7th April 2014!
- But….so are many of the security professionals looking after them!

Where are we today….

- We are faced with ever increasing compliance challenges at the Enterprise Level
- Auditors are becoming increasingly Knowledgeable about Mainframes, zOS, RACF, ACF2 & TSS

- The biggest threat is still the Insider one
- There have been several recent breaches at organisations such as Barclays & Nordea Bank….BUT these are only the ones that get found out or reported…

- Don’t ever forget the Mainframe IS the most secur**able** server on the planet……*BUT* …

Where are we today….

- Security Wise?
  - Well its not all doom and gloom
  - There are solutions to the issues we face…but…..
  - We are faced with serious security issues on the mainframe and an ever growing list of compliance and audit issues

Gartner Comment

- *"The IBM z/OS mainframe continues to be an important platform for many enterprises, hosting about 90% of their mission critical applications.* ***Enterprises may not take the same steps*** *to address configuration errors and poor identity and entitlements administration on the mainframe as they do on other OS's.*

- *Thus,* ***the incidence of high-risk vulnerabilities is astonishingly high****, and enterprises often lack formal programs to identify and remediate these."*

- Gartner Research Note G00172909

Ok, great job folks .. so all of our sensitive data is now identified and protected .....

By the way Glinda…
what's with the elephant?

What do we need to do?

What do we need to do?

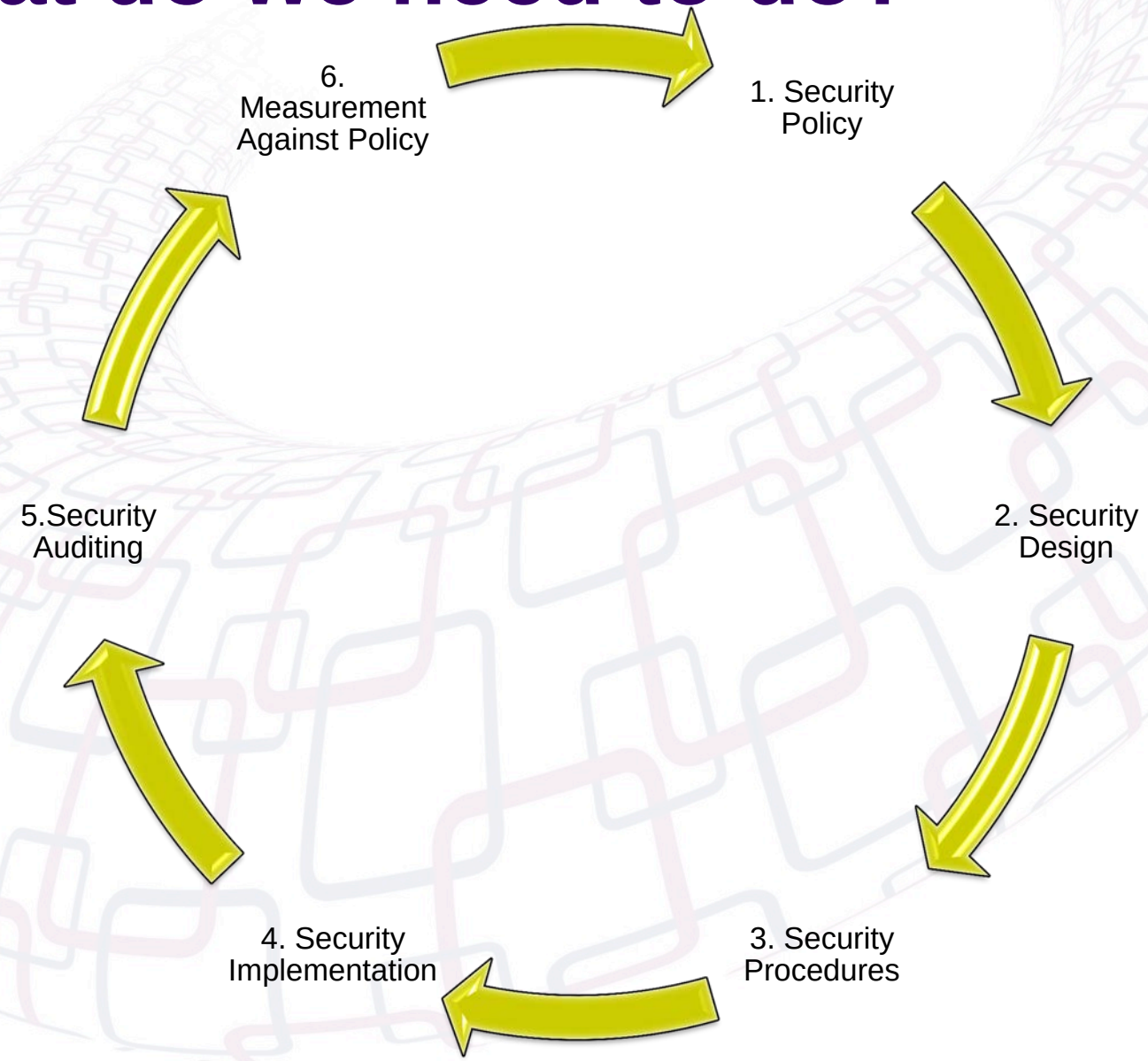
- We need to include mainframe security in all enterprise wide security discussions and plans
- We need to avoid comments from our Risk & Compliance colleges such as:
  - Didn't realise we still had a mainframe
  - Do we still have one of those
  - Thought we had got rid of those years ago
- We need to work closely with the Risk, Compliance & Audit teams, Educating them on the unique values that the mainframe has
- We need to recruit and train the next wave of mainframe security professionals…. YES THAT MEANS AUDITORS as well
- Wonder what the average age is in this room?

What do we need to do?

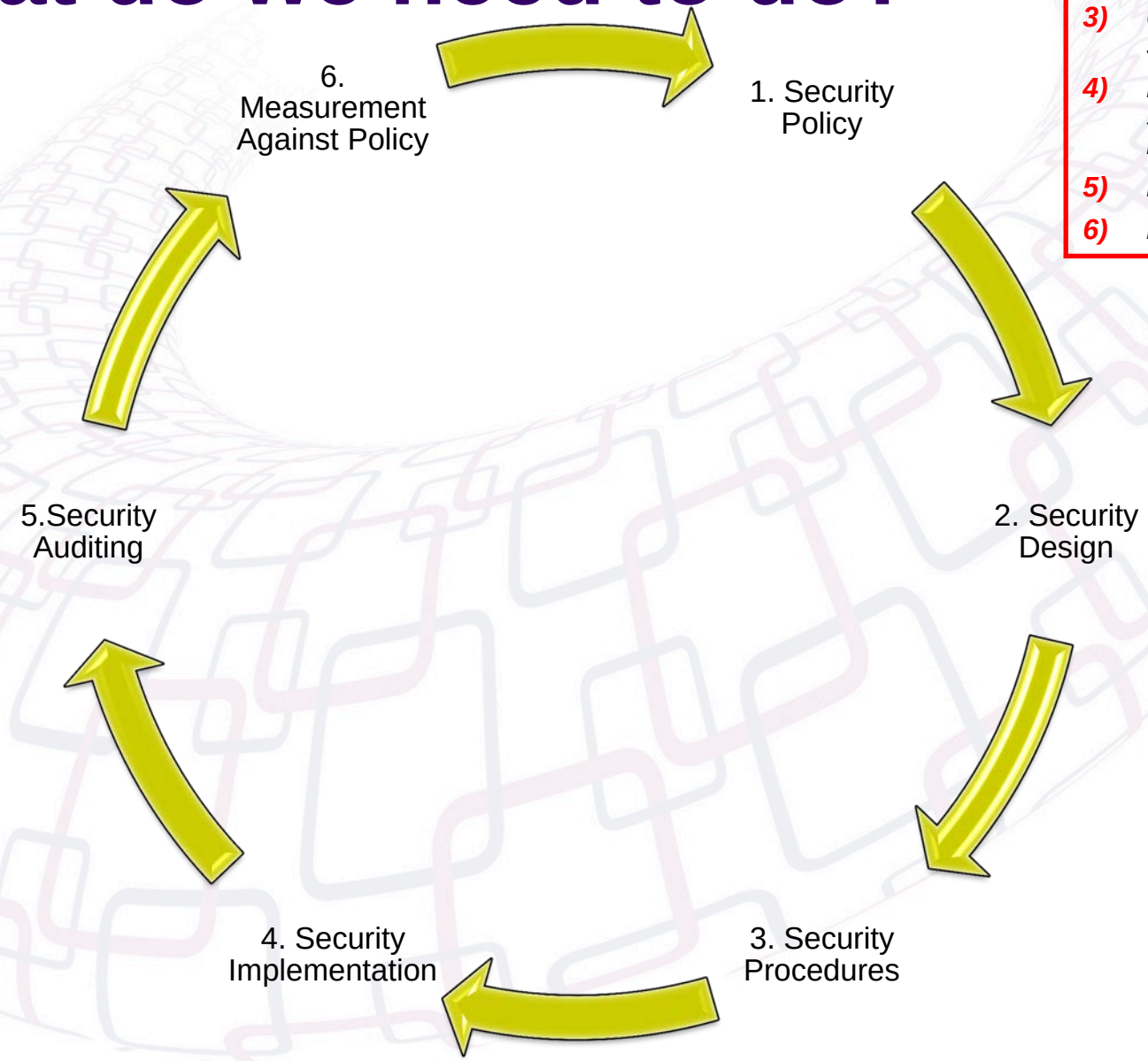
- We need more real time; proactive monitoring of our mainframe systems
- We need to equip the security teams with the correct tooling to meet the security requirements effectively

Mainframe Security Management Vision

What do we need to do?



What do we need to do?

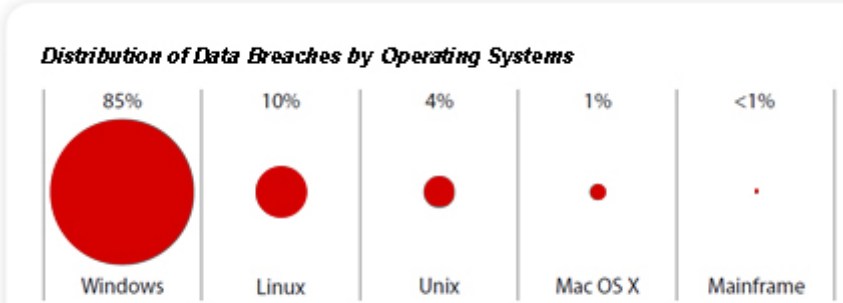


Security Tooling Provides:

2) ***Assistance with security design***
3) ***Greater flexibility in Security procedures***
4) ***More methods in security implementation***
5) ***Powerful auditing***
6) ***Powerful reporting***

Fortunately IBM's System z is Highly Secure

- Highly secure platform for virtual environments and workloads
  - **80%** of all active code runs on the Mainframe[1]
  - **80%** of enterprise business data is housed on the Mainframe[1]
  - ***This makes the Mainframe a desirable target for hackers***
- Security is built into every level of the System z structure
  - Processor
  - Hypervisor
  - Operating system
  - Communications
  - Storage
  - Applications
- System z security features address compliance
  - Identity and access management
  - Hardware and software encryption
  - Communication security capabilities
  - Extensive logging and reporting of security events
- Extensive security certifications (e.g., Common Criteria and FIPS 140) including EAL5+
- But today's mainframe must interoperate in a complex environment including cloud, mobile, big data and social networking and is susceptible to multiple vulnerabilities
  - [1]Source: 2013 IBM zEnterprise Technology Summit



Summary

- The myth that mainframes are secure has definitely been busted
- Mainframes are secur**ABLE**
- There are processes that can help
- The correct tooling makes life significantly easier
- We need to act fact as recent breaches show just how costly these issues can be

Questions?

IBM Security

Where to get more information

- Get actionable insight with Security Intelligence for mainframe environments
- Consolidating Security Management for Mainframe Clouds
- New White Paper: Creating the Ultimate Security Platform
- Video: zSecure for Superior Mainframe Security
- IBM Security zSecure Products at Allied Irish Bank (00:09:14)
- Forrester Mainframe TLP: Secure the Enterprise with Confidence

Contact Details

Mark Wilson
RSM Partners
Markw@rsmpartners.com
Mobile +44 (0) 7768 617006
www.rsmpartners.com

Glinda Cummings
IBM
glinda@us.ibm.com
925 683 9252