SHARE
in Orlando 2015
SHARE
Educate · Network · Influence

The Future of Mainframe Security – A Personal Perspective

Mark Wilson
Technical Director
RSM Partners

#SHAREorg

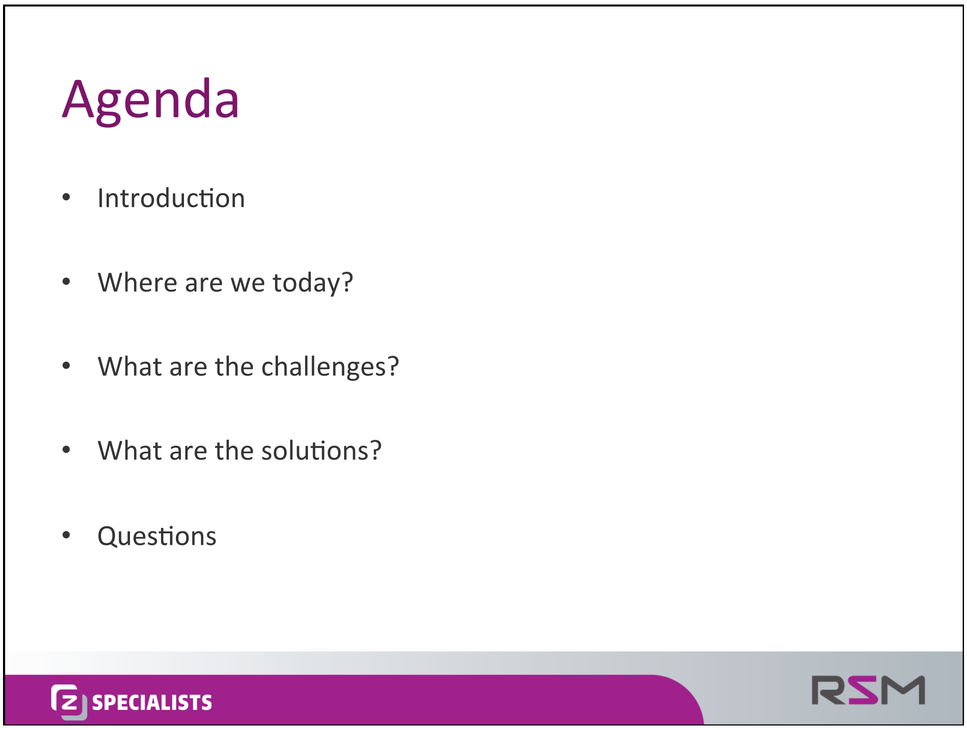
CELEBRATING
60 YEARS OF SHARE
Influencing IT Since 1955

SHARE is an independent volunteer-run information technology association that provides education, professional networking and industry influence.

RSM
PARTNERS

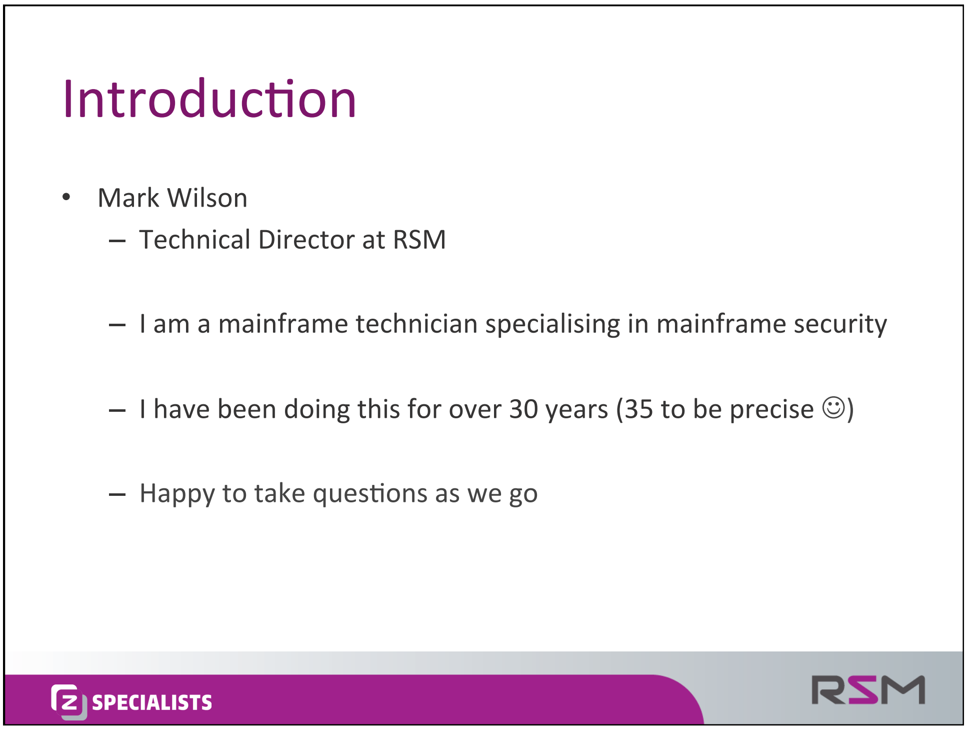
The future of mainframe security – A Personal perspective

World Class, Full Spectrum, z Services



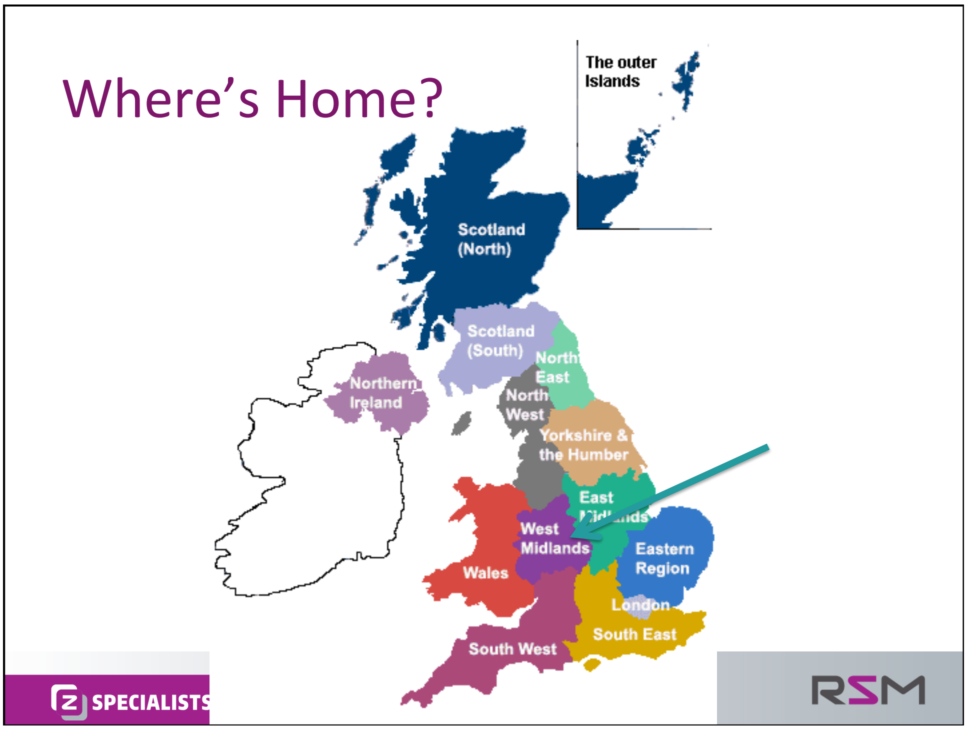
Agenda

- Introduction
- Where are we today?
- What are the challenges?
- What are the solutions?
- Questions



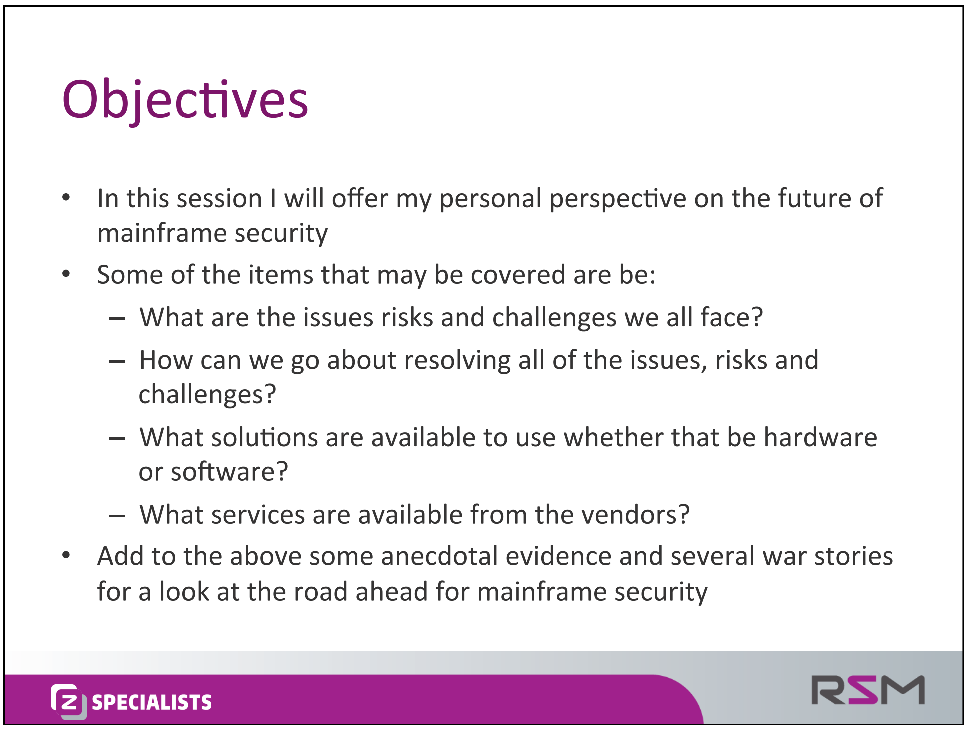
Introduction

- Mark Wilson
  - Technical Director at RSM
  - I am a mainframe technician specialising in mainframe security
  - I have been doing this for over 30 years (35 to be precise ☺)
  - Happy to take questions as we go



Where's Home?

This is where Mark works supposedly!



Objectives

- In this session I will offer my personal perspective on the future of mainframe security
- Some of the items that may be covered are be:
  - What are the issues risks and challenges we all face?
  - How can we go about resolving all of the issues, risks and challenges?
  - What solutions are available to use whether that be hardware or software?
  - What services are available from the vendors?
- Add to the above some anecdotal evidence and several war stories for a look at the road ahead for mainframe security

SPECIALISTS

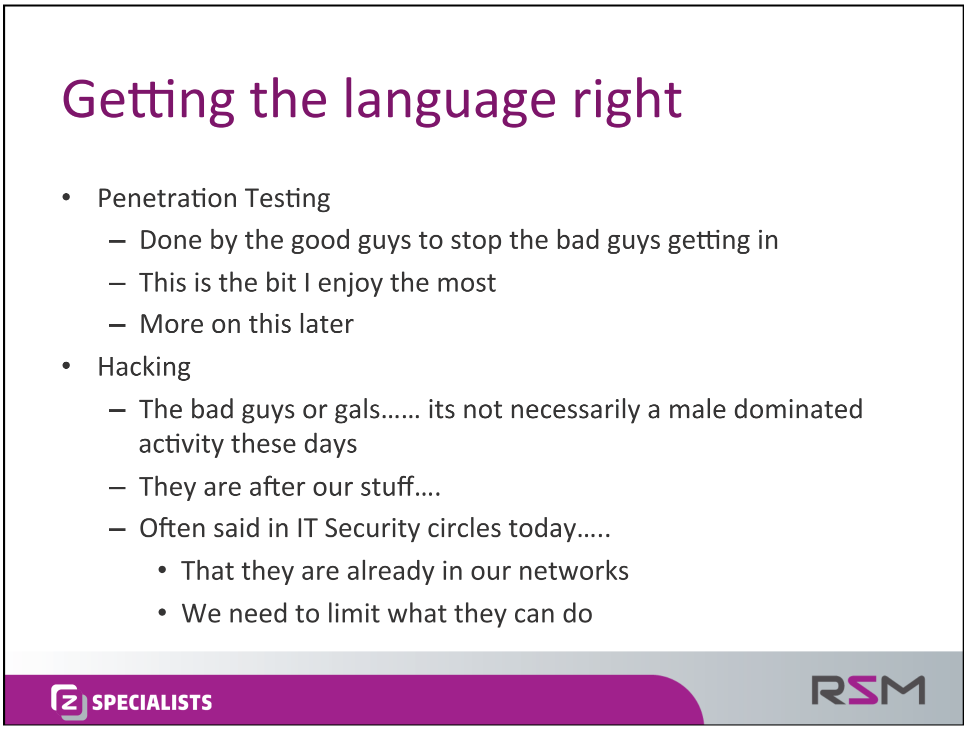
RSM

Getting the language right!

Session !!!!!

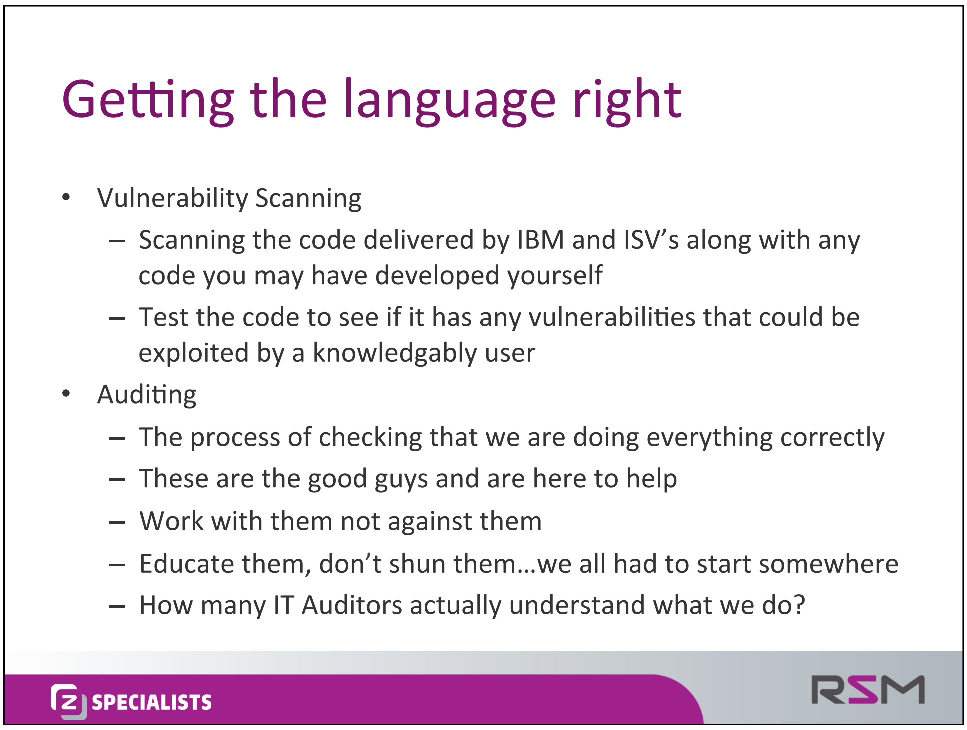
SPECIALISTS

RSM



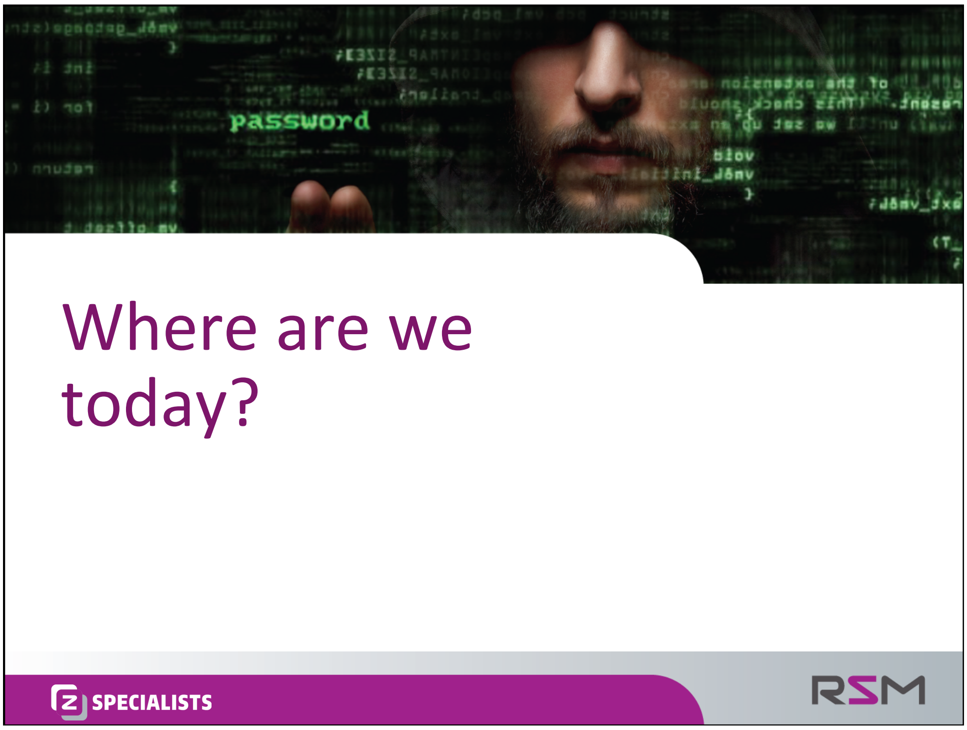
Getting the language right

- Penetration Testing
  - Done by the good guys to stop the bad guys getting in
  - This is the bit I enjoy the most
  - More on this later
- Hacking
  - The bad guys or gals…… its not necessarily a male dominated activity these days
  - They are after our stuff….
  - Often said in IT Security circles today…..
    - That they are already in our networks
    - We need to limit what they can do



Getting the language right

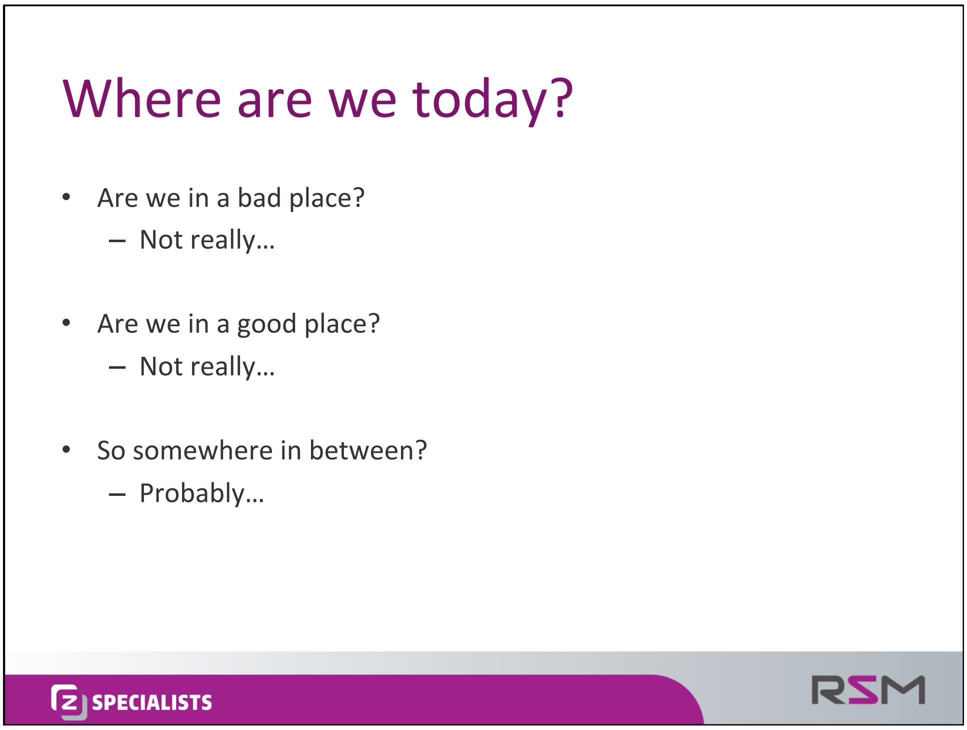
- Vulnerability Scanning
  - Scanning the code delivered by IBM and ISV's along with any code you may have developed yourself
  - Test the code to see if it has any vulnerabilities that could be exploited by a knowledgably user
- Auditing
  - The process of checking that we are doing everything correctly
  - These are the good guys and are here to help
  - Work with them not against them
  - Educate them, don't shun them…we all had to start somewhere
  - How many IT Auditors actually understand what we do?



Where are we today?

SPECIALISTS

RSM

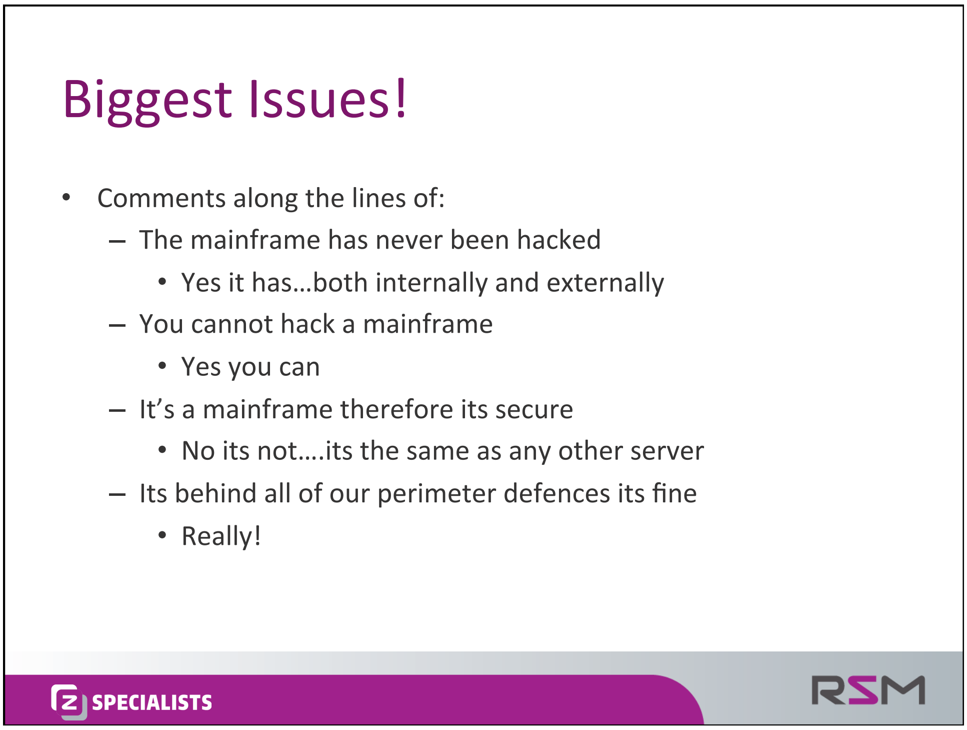


Where are we today?

- Are we in a bad place?
  - Not really…
- Are we in a good place?
  - Not really…
- So somewhere in between?
  - Probably…

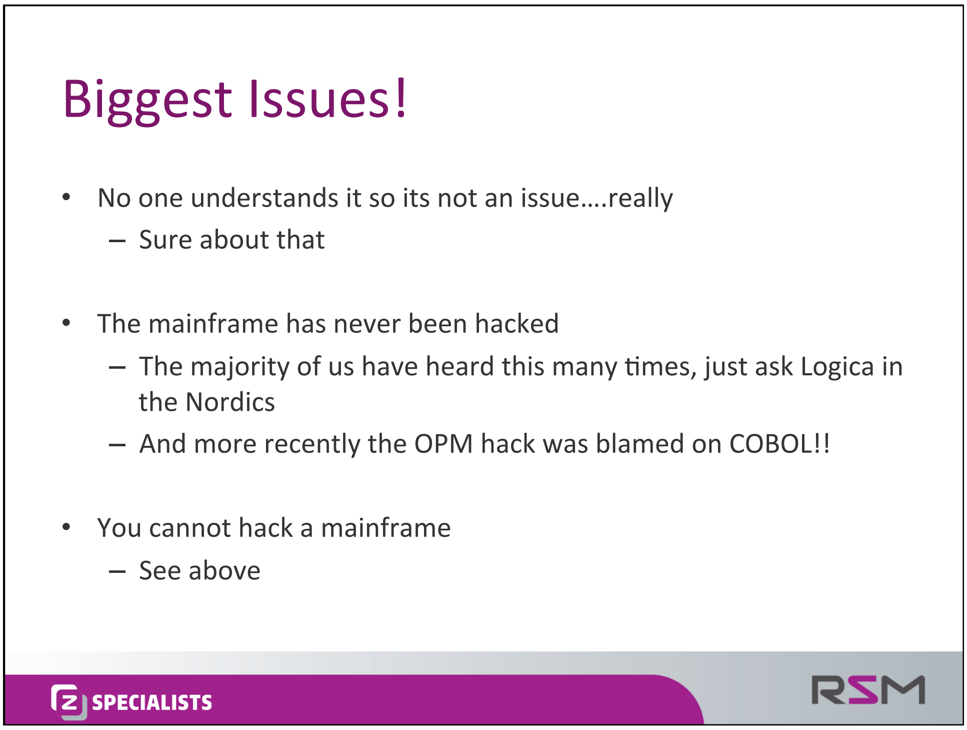
SPECIALISTS

RSM



Biggest Issues!

- Comments along the lines of:
  - The mainframe has never been hacked
    - Yes it has…both internally and externally
  - You cannot hack a mainframe
    - Yes you can
  - It's a mainframe therefore its secure
    - No its not….its the same as any other server
  - Its behind all of our perimeter defences its fine
    - Really!

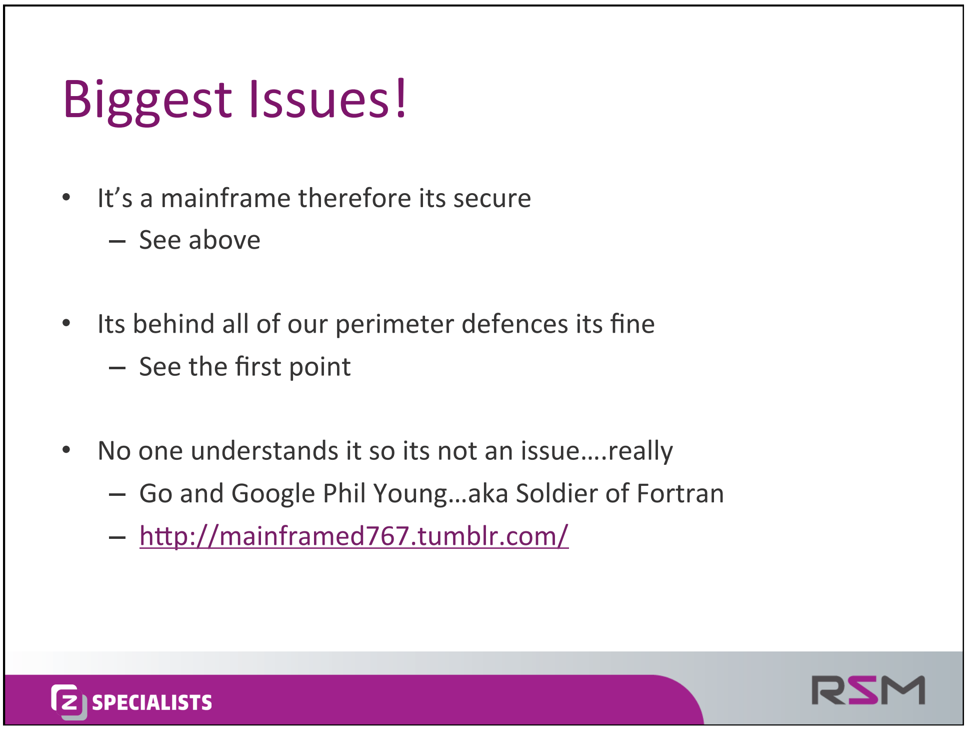


Biggest Issues!

- No one understands it so its not an issue….really
  - Sure about that

- The mainframe has never been hacked
  - The majority of us have heard this many times, just ask Logica in the Nordics
  - And more recently the OPM hack was blamed on COBOL!!

- You cannot hack a mainframe
  - See above

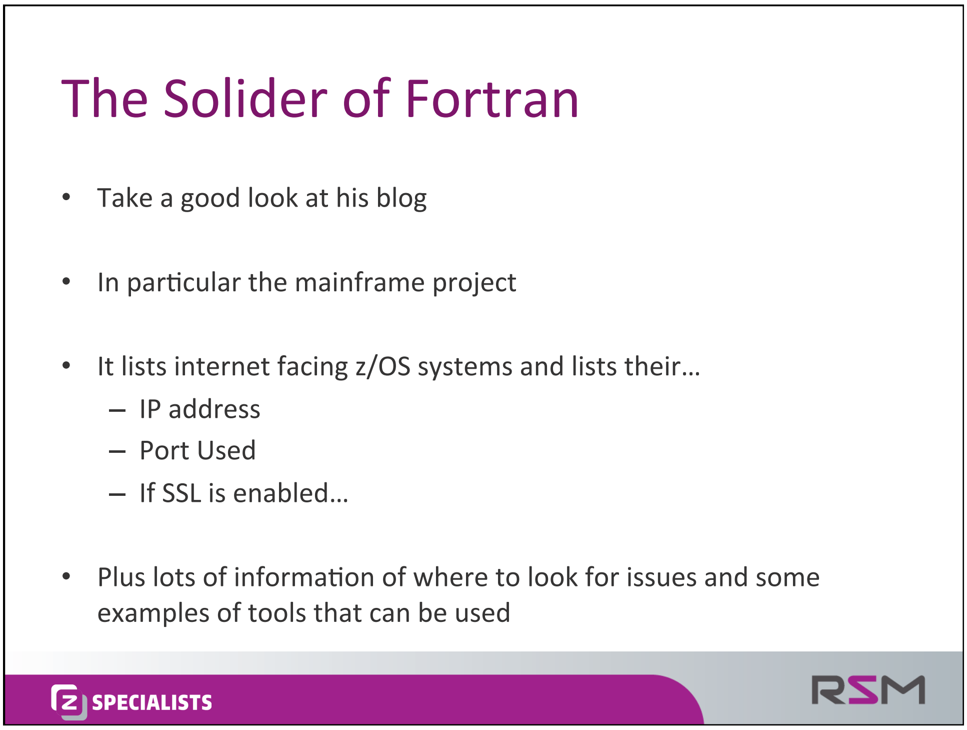


Biggest Issues!

- It's a mainframe therefore its secure
  - See above
- Its behind all of our perimeter defences its fine
  - See the first point
- No one understands it so its not an issue….really
  - Go and Google Phil Young…aka Soldier of Fortran
  - http://mainframed767.tumblr.com/

SPECIALISTS

RSM



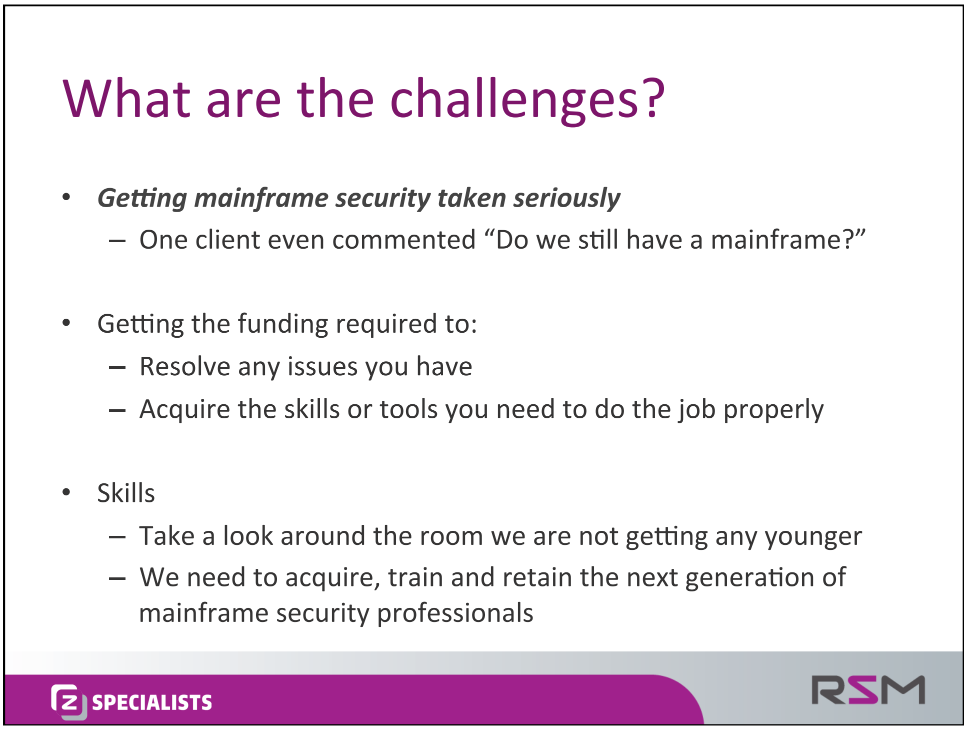
The Solider of Fortran

- Take a good look at his blog
- In particular the mainframe project
- It lists internet facing z/OS systems and lists their…
  - IP address
  - Port Used
  - If SSL is enabled…
- Plus lots of information of where to look for issues and some examples of tools that can be used

SPECIALISTS

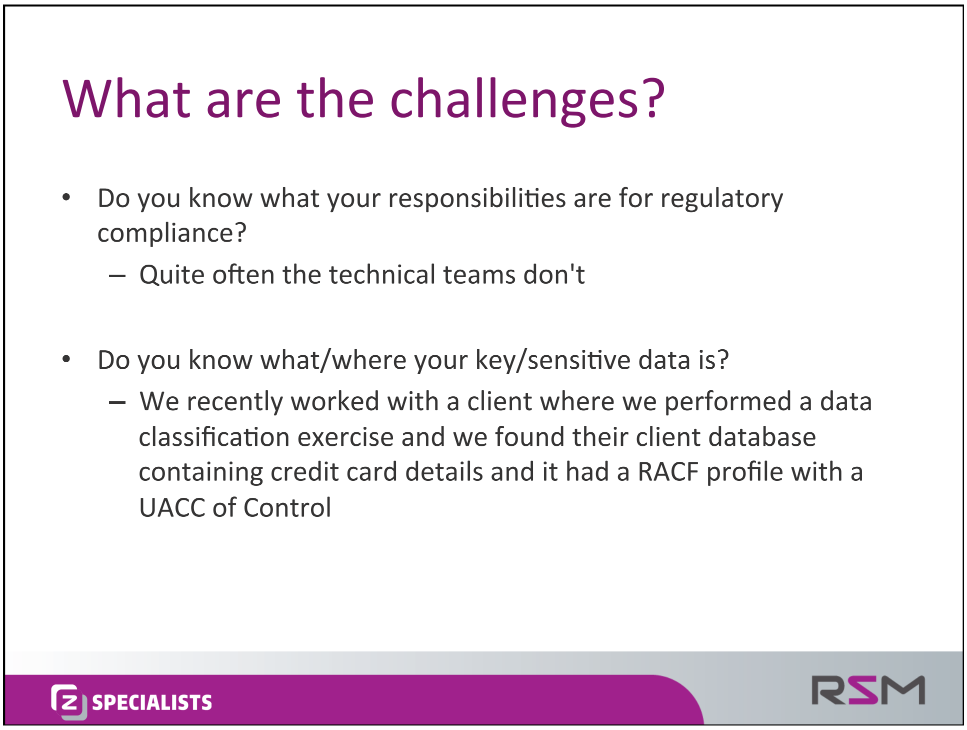
RSM

What are the challenges?



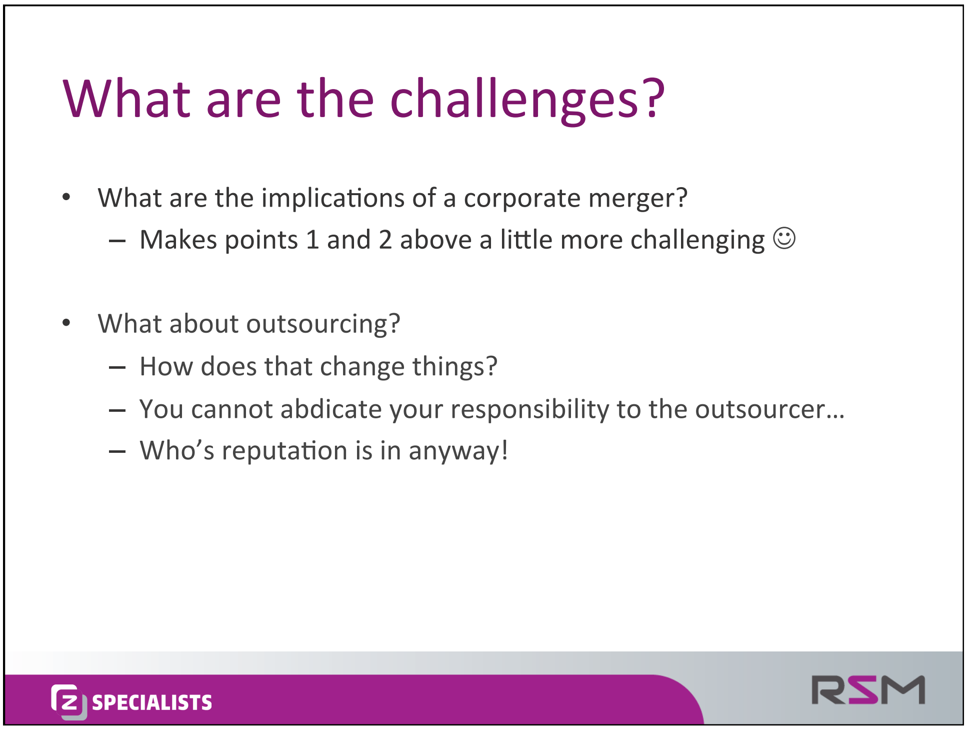
What are the challenges?

- ***Getting mainframe security taken seriously***
  - One client even commented “Do we still have a mainframe?”
- Getting the funding required to:
  - Resolve any issues you have
  - Acquire the skills or tools you need to do the job properly
- Skills
  - Take a look around the room we are not getting any younger
  - We need to acquire, train and retain the next generation of mainframe security professionals



What are the challenges?

- Do you know what your responsibilities are for regulatory compliance?
  - Quite often the technical teams don't
- Do you know what/where your key/sensitive data is?
  - We recently worked with a client where we performed a data classification exercise and we found their client database containing credit card details and it had a RACF profile with a UACC of Control



What are the challenges?

- What are the implications of a corporate merger?
  - Makes points 1 and 2 above a little more challenging ☺
- What about outsourcing?
  - How does that change things?
  - You cannot abdicate your responsibility to the outsourcer…
  - Who’s reputation is in anyway!

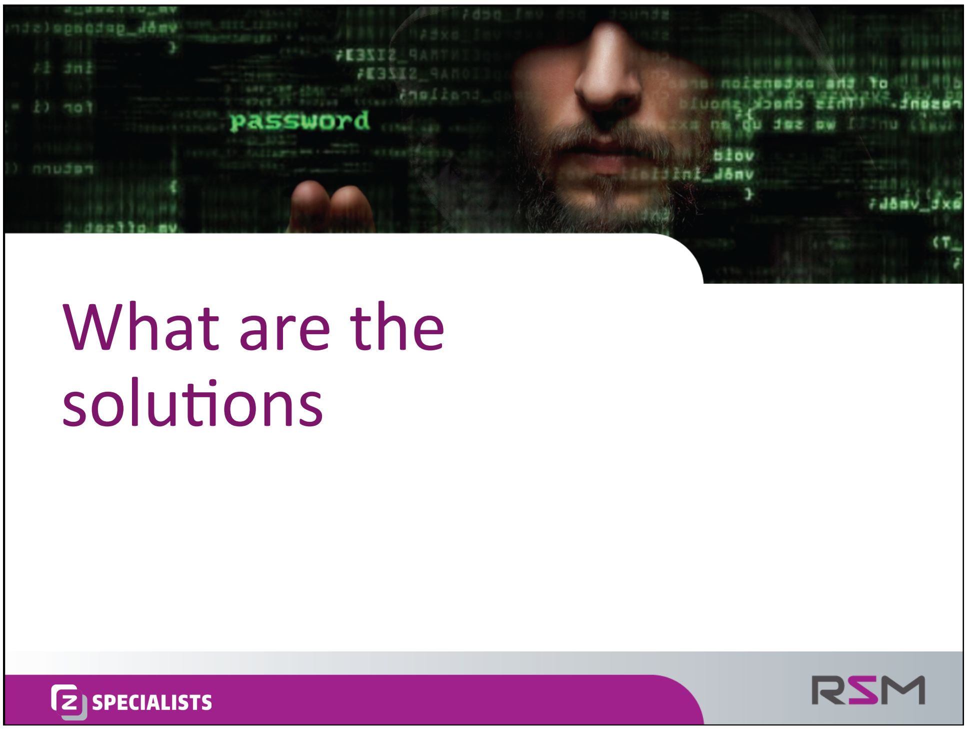
Gartner Comment

"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.

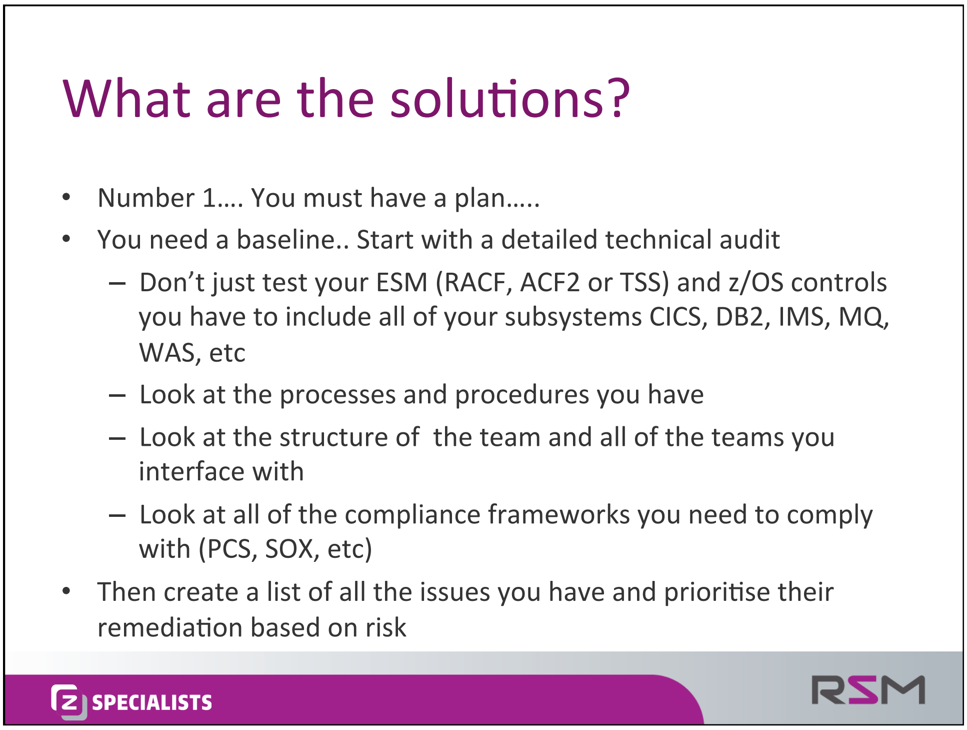
Thus, the incidence of high-risk vulnerabilities is astonishingly high, and enterprises often lack formal programs to identify and remediate these."

– Gartner Research Note G00172909

Ok, great job folks .. so all of our critical systems are protected??? .....
MAINFRAME
Data & Access
By the way what's with the elephant?

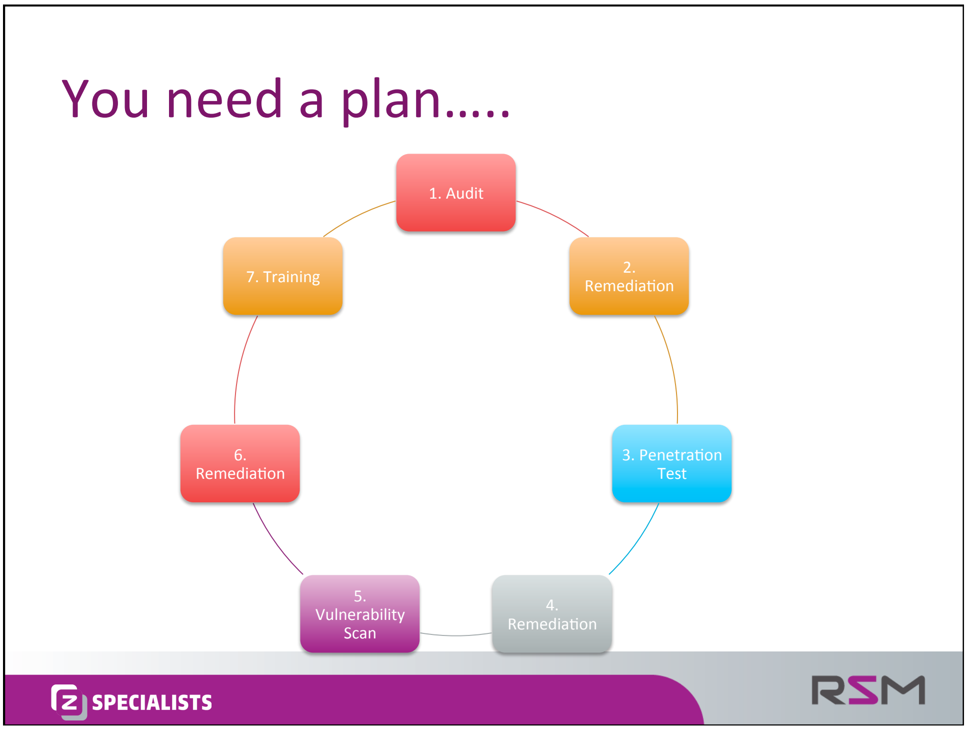


What are the solutions

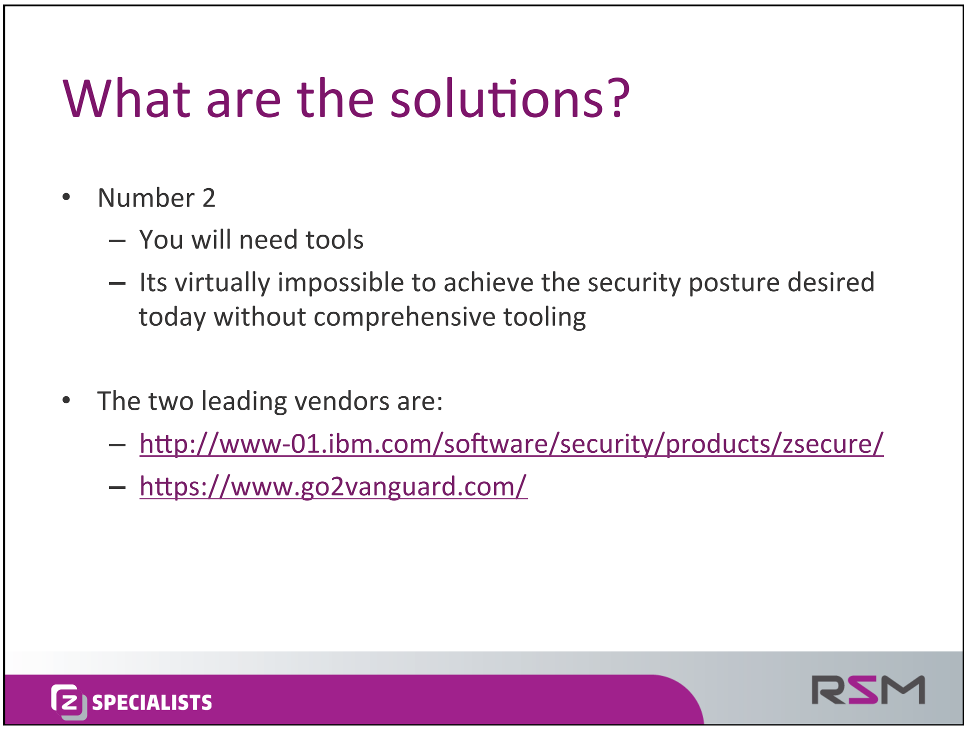


What are the solutions?

- Number 1…. You must have a plan…..
- You need a baseline.. Start with a detailed technical audit
  - Don’t just test your ESM (RACF, ACF2 or TSS) and z/OS controls you have to include all of your subsystems CICS, DB2, IMS, MQ, WAS, etc
  - Look at the processes and procedures you have
  - Look at the structure of the team and all of the teams you interface with
  - Look at all of the compliance frameworks you need to comply with (PCS, SOX, etc)
- Then create a list of all the issues you have and prioritise their remediation based on risk



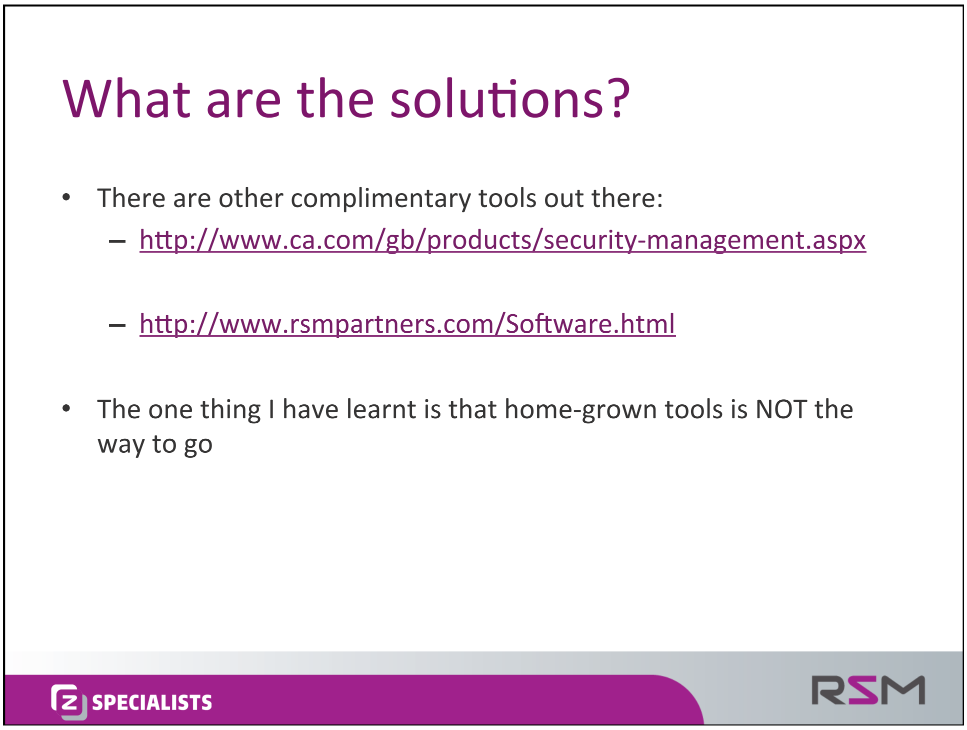
You need a plan…..



What are the solutions?

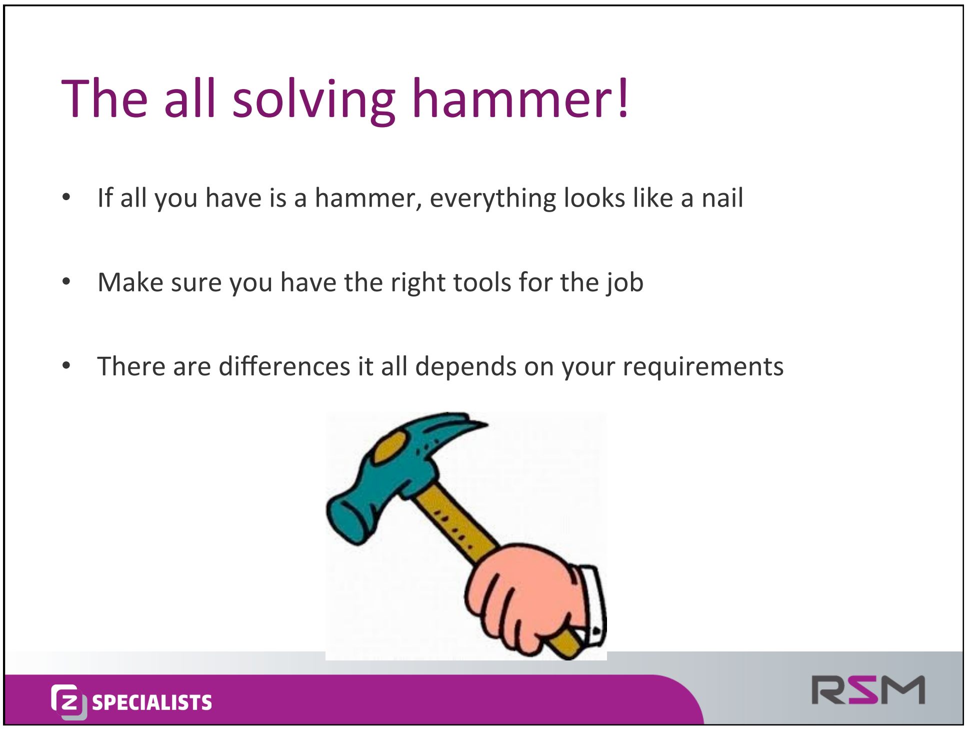
- Number 2
  - You will need tools
  - Its virtually impossible to achieve the security posture desired today without comprehensive tooling

- The two leading vendors are:
  - http://www-01.ibm.com/software/security/products/zsecure/
  - https://www.go2vanguard.com/



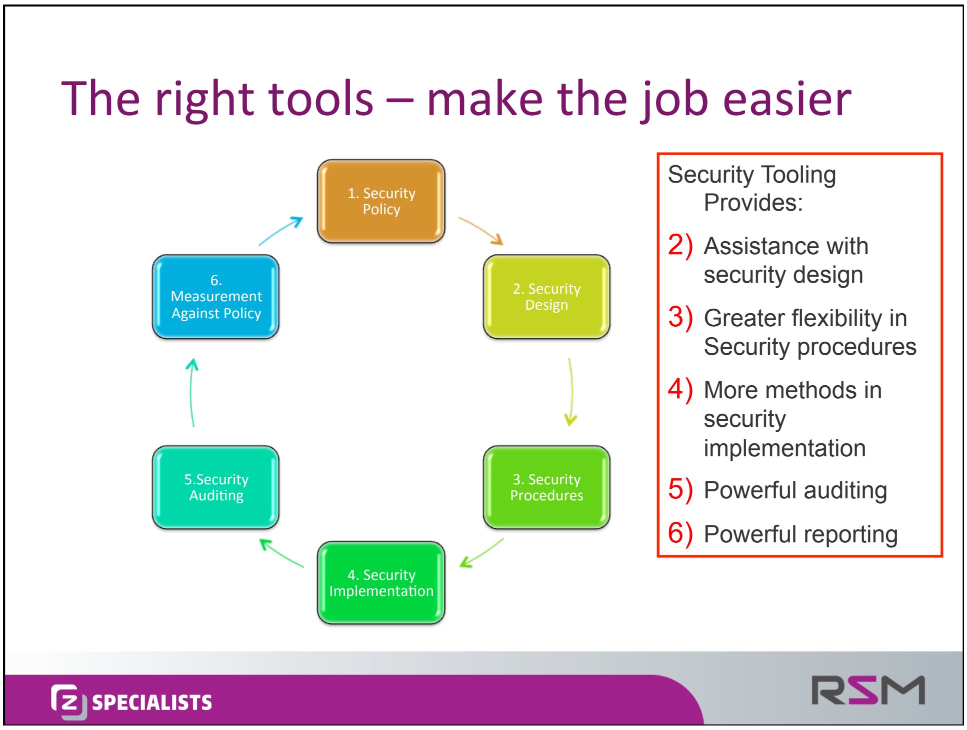
What are the solutions?

- There are other complimentary tools out there:
  - http://www.ca.com/gb/products/security-management.aspx
  - http://www.rsmpartners.com/Software.html
- The one thing I have learnt is that home-grown tools is NOT the way to go



The all solving hammer!

- If all you have is a hammer, everything looks like a nail
- Make sure you have the right tools for the job
- There are differences it all depends on your requirements



The right tools – make the job easier

1. Security Policy

2. Security Design

3. Security Procedures

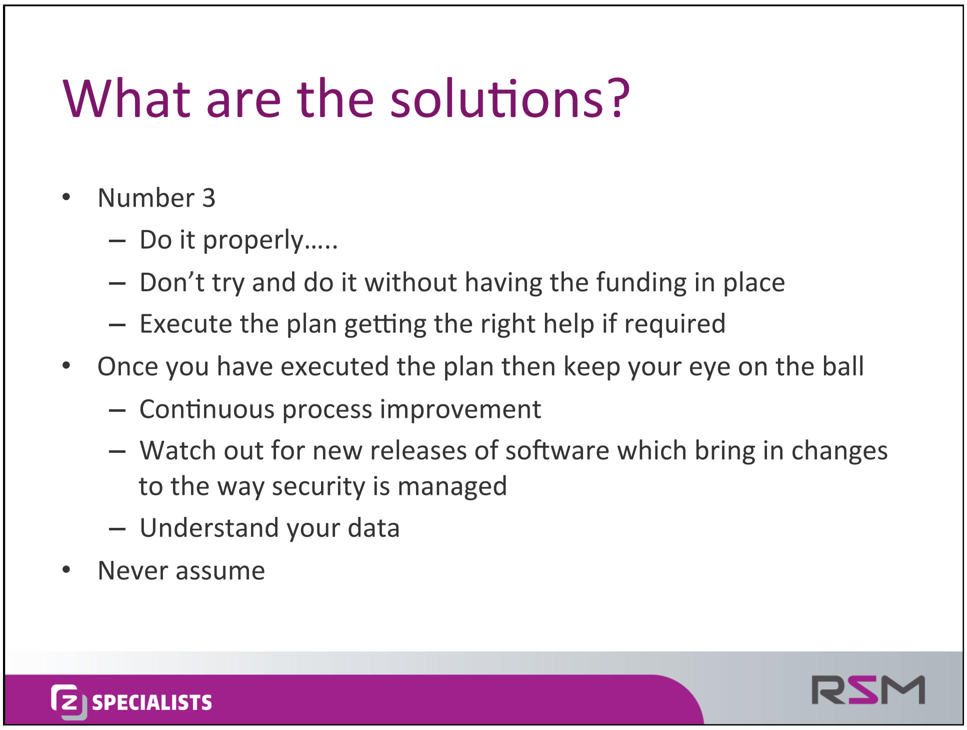
4. Security Implementation

5.Security Auditing

6. Measurement Against Policy

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



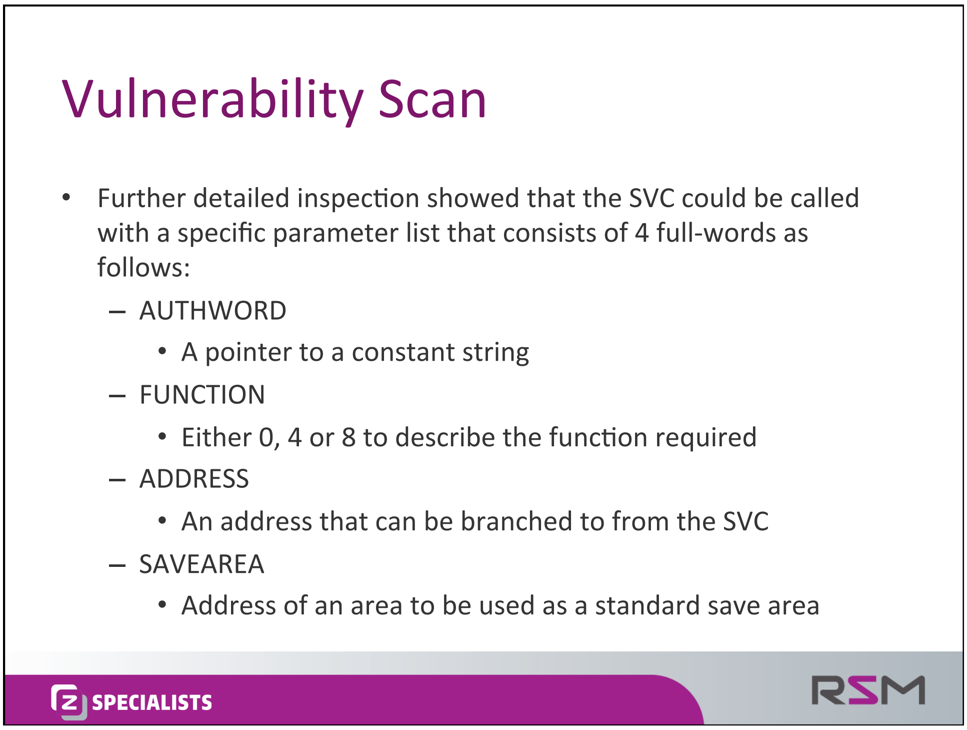
What are the solutions?

- Number 3
  - Do it properly…..
  - Don't try and do it without having the funding in place
  - Execute the plan getting the right help if required
- Once you have executed the plan then keep your eye on the ball
  - Continuous process improvement
  - Watch out for new releases of software which bring in changes to the way security is managed
  - Understand your data
- Never assume

Vulnerability Scan

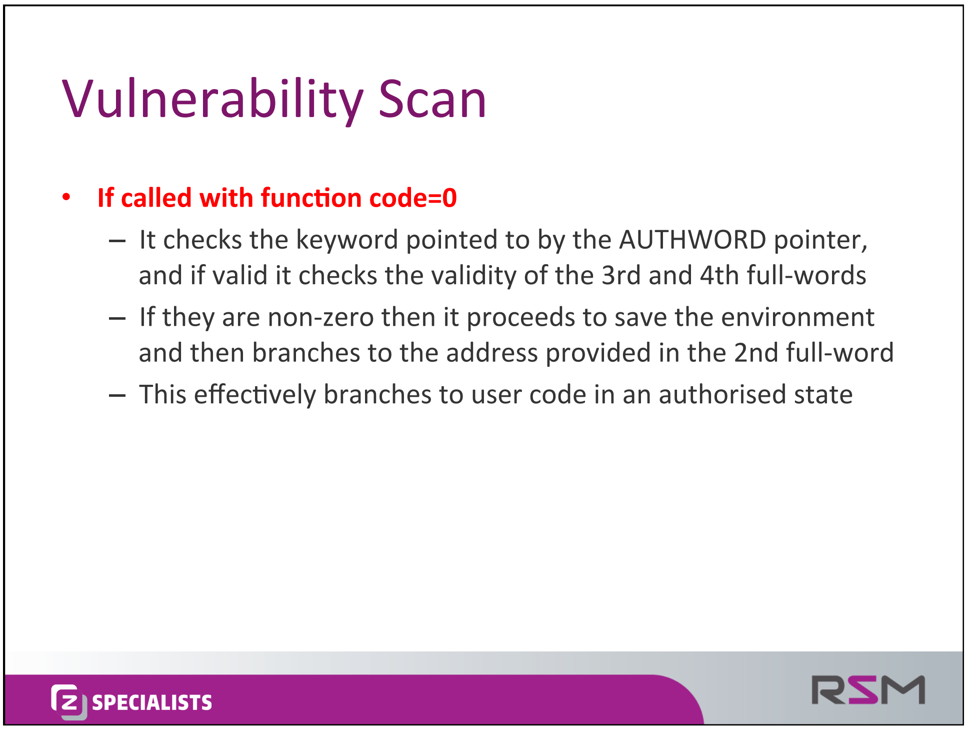
Vulnerability Scan

- Recent scan for a North American client revealed an ISV product with an exploitable SVC
- The SVC is installed as a type 3 ESR (Extended SVC Routing) SVC 109 with routing code 201 as module IGX00201
- A visual inspection of the binary code showed that there was an instruction that modified the TCBJSCB field of the TCB by switching on the JSCBAUTH bit, there was also an instruction to switch it off again



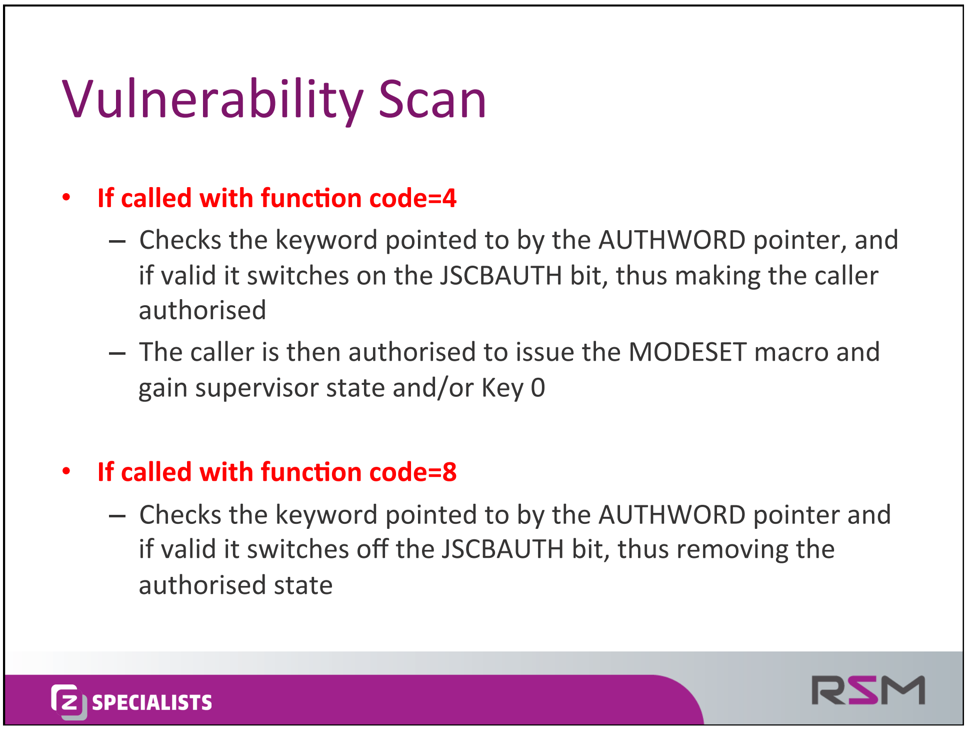
Vulnerability Scan

- Further detailed inspection showed that the SVC could be called with a specific parameter list that consists of 4 full-words as follows:
  - AUTHWORD
    - A pointer to a constant string
  - FUNCTION
    - Either 0, 4 or 8 to describe the function required
  - ADDRESS
    - An address that can be branched to from the SVC
  - SAVEAREA
    - Address of an area to be used as a standard save area



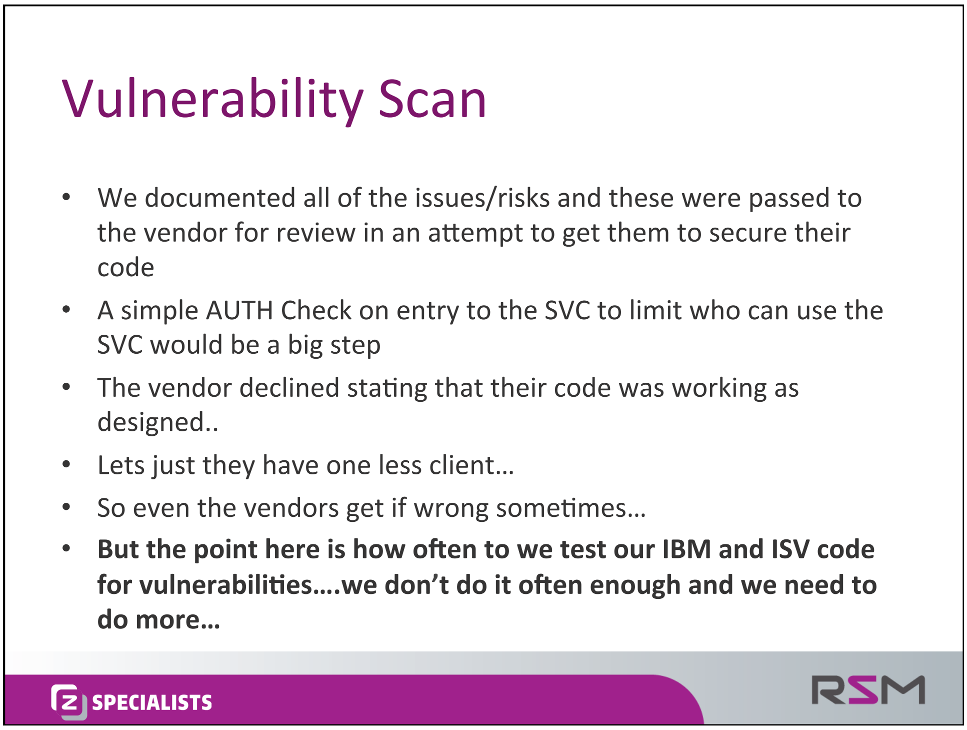
Vulnerability Scan

- **If called with function code=0**
  - It checks the keyword pointed to by the AUTHWORD pointer, and if valid it checks the validity of the 3rd and 4th full-words
  - If they are non-zero then it proceeds to save the environment and then branches to the address provided in the 2nd full-word
  - This effectively branches to user code in an authorised state



Vulnerability Scan

- **If called with function code=4**
  - Checks the keyword pointed to by the AUTHWORD pointer, and if valid it switches on the JSCBAUTH bit, thus making the caller authorised
  - The caller is then authorised to issue the MODESET macro and gain supervisor state and/or Key 0
- **If called with function code=8**
  - Checks the keyword pointed to by the AUTHWORD pointer and if valid it switches off the JSCBAUTH bit, thus removing the authorised state



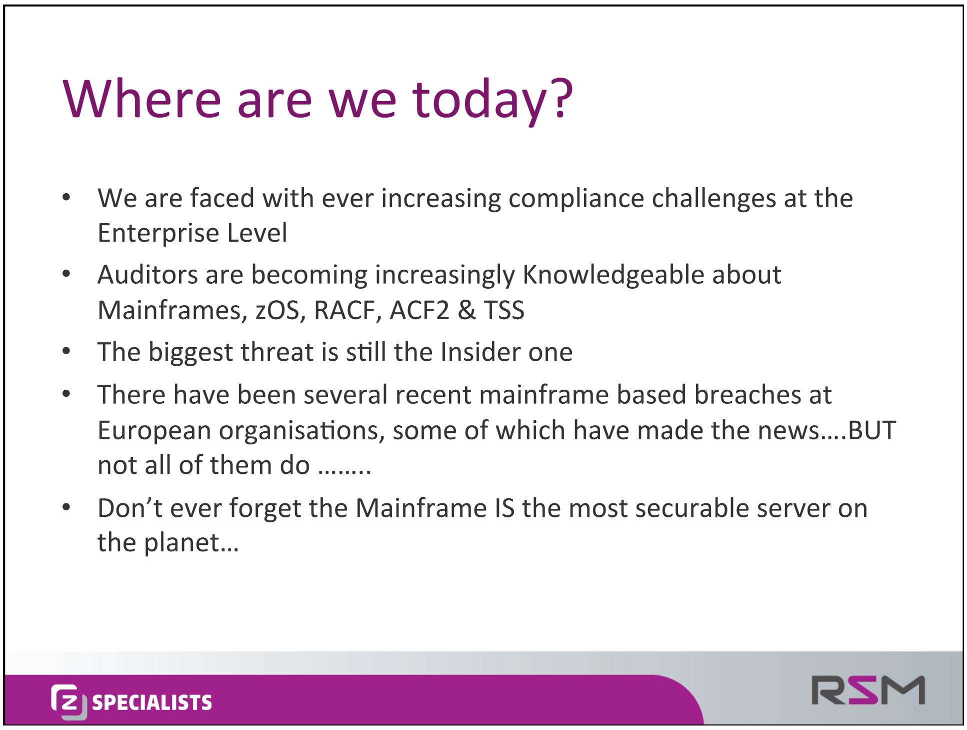
Vulnerability Scan

- We documented all of the issues/risks and these were passed to the vendor for review in an attempt to get them to secure their code
- A simple AUTH Check on entry to the SVC to limit who can use the SVC would be a big step
- The vendor declined stating that their code was working as designed..
- Lets just they have one less client…
- So even the vendors get if wrong sometimes…
- **But the point here is how often to we test our IBM and ISV code for vulnerabilities….we don't do it often enough and we need to do more…**

Where are we today?

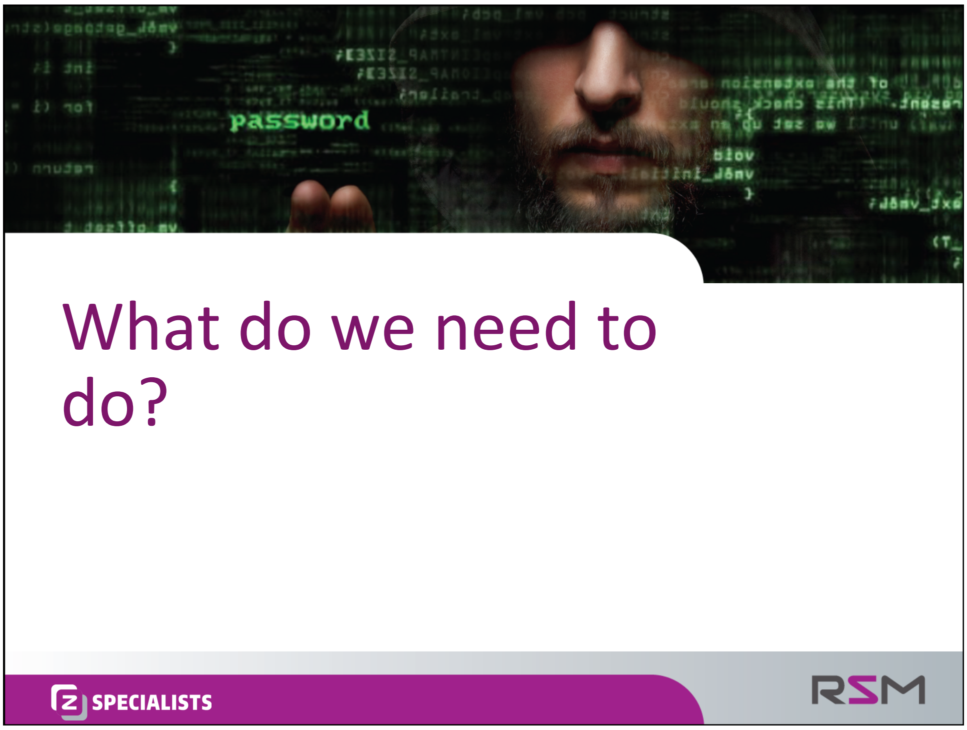
Where are we today?

- The mainframe is still one of the IT industry’s most enduring inventions and I don’t believe they will be going away anytime soon
- IBM have recently announced the zEC13 and still invest heavily in the platform
- A recent quote stated: “PCs are considered a mature platform”
- A don’t forget the mainframe was 50 years old on the 7th April 2014!
- But….so are many of the security professionals looking after them!

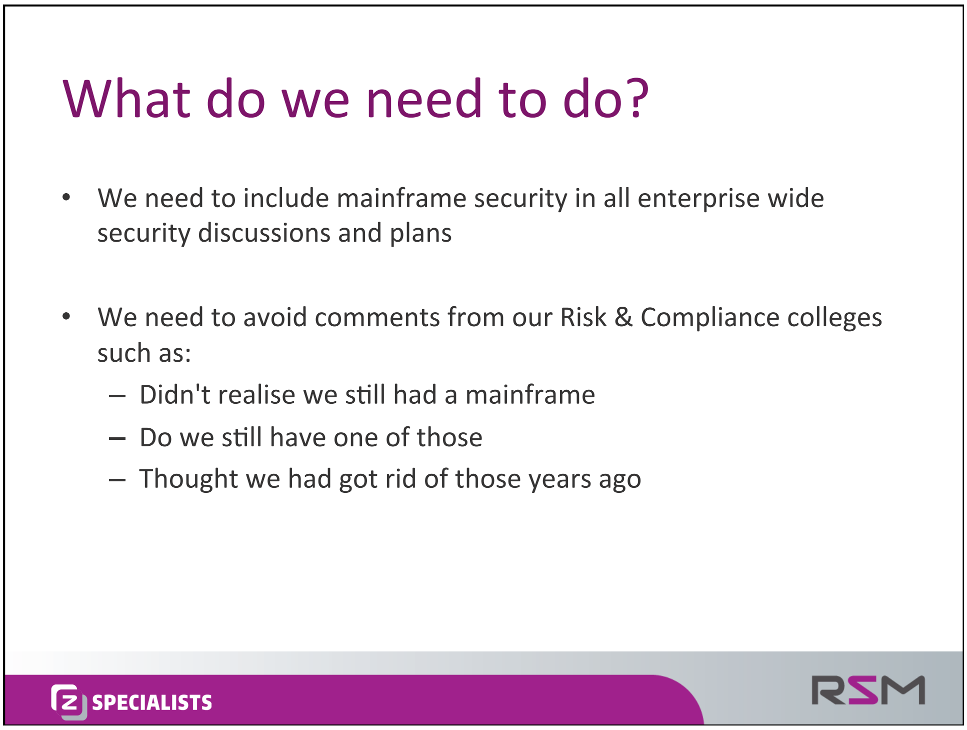


Where are we today?

- 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 mainframe based breaches at European organisations, some of which have made the news….BUT not all of them do ……..
- Don't ever forget the Mainframe IS the most securable server on the planet…



What do we need to do?

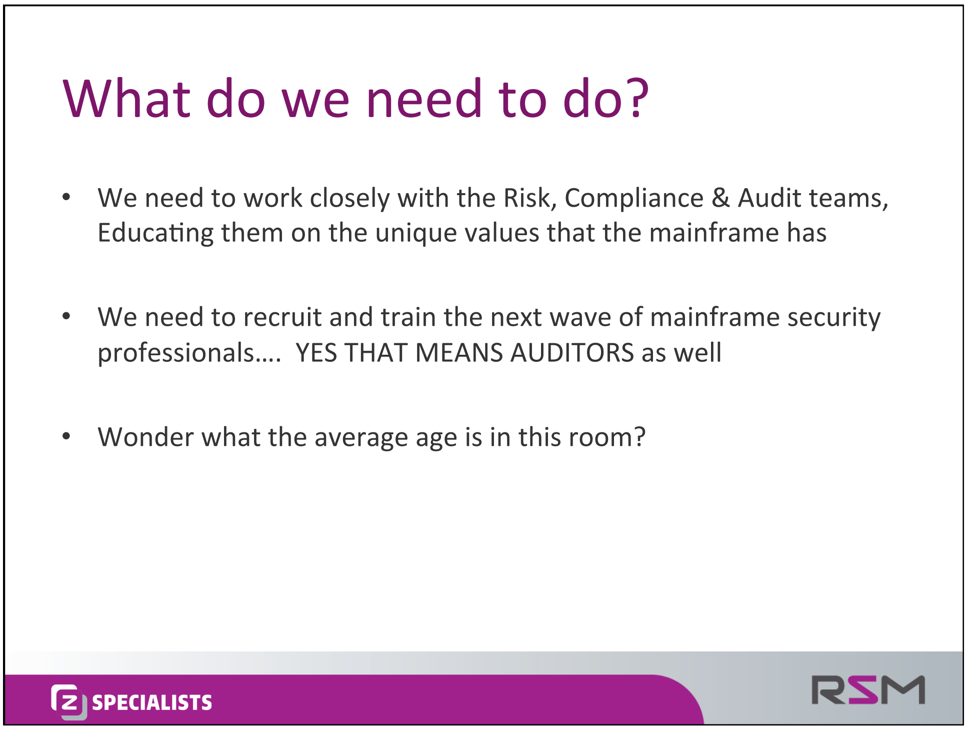


What do we need to do?

- 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

SPECIALISTS

RSM

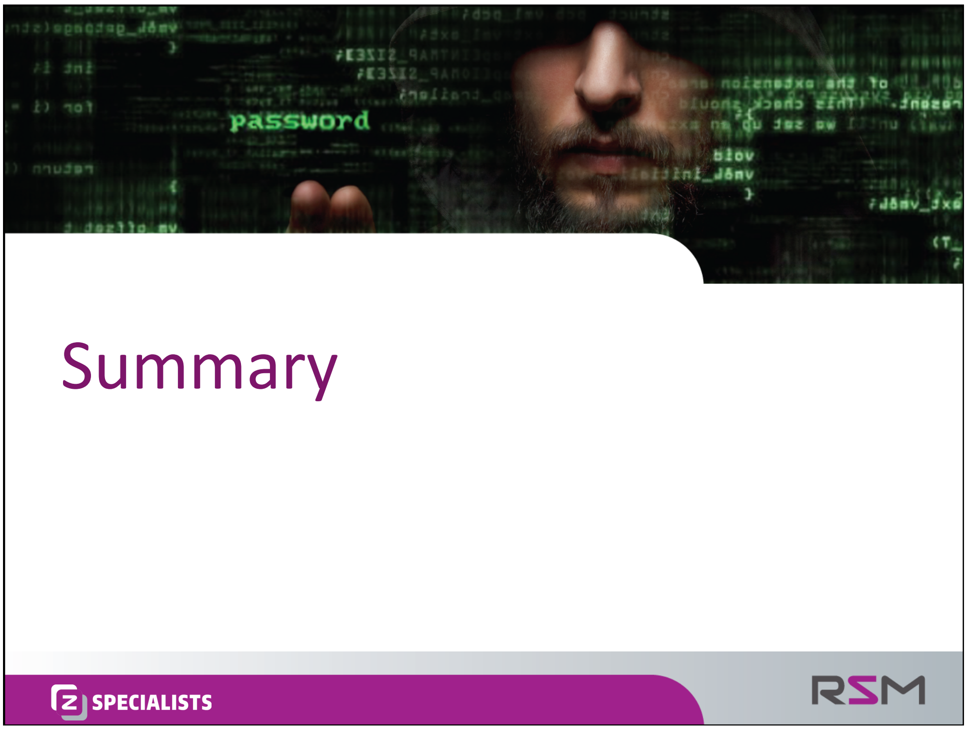


What do we need to do?

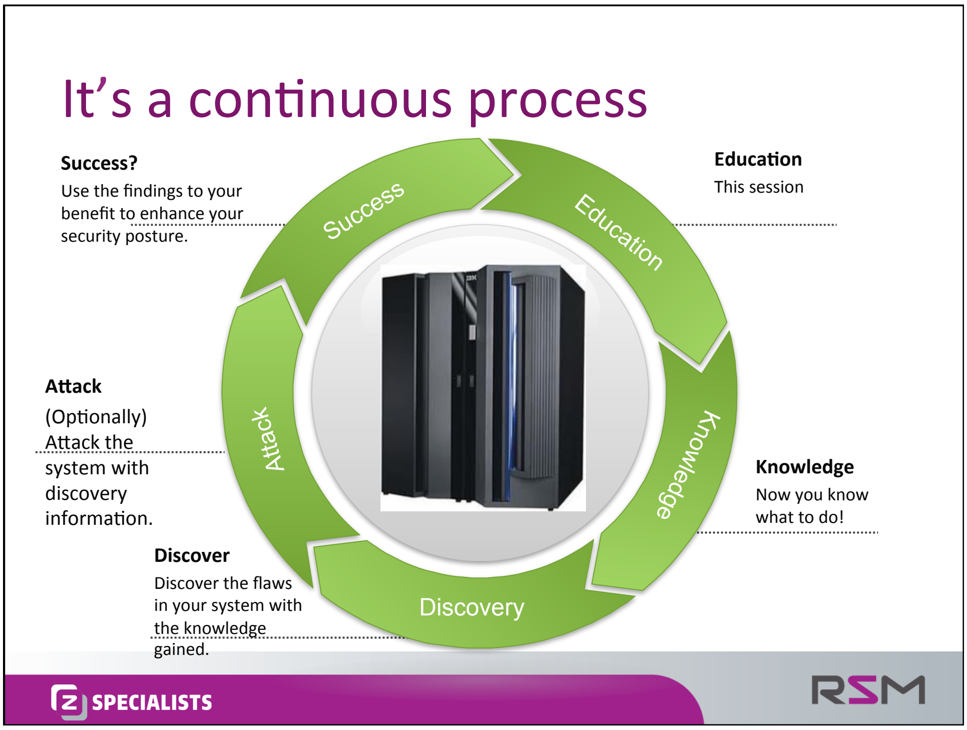
- We need to work closely with the Risk, Compliance & Audit teams, Educating them on the unique values that the mainframe has
- We need to recruit and train the next wave of mainframe security professionals.... YES THAT MEANS AUDITORS as well
- Wonder what the average age is in this room?

SPECIALISTS

RSM



Summary



It’s a continuous process

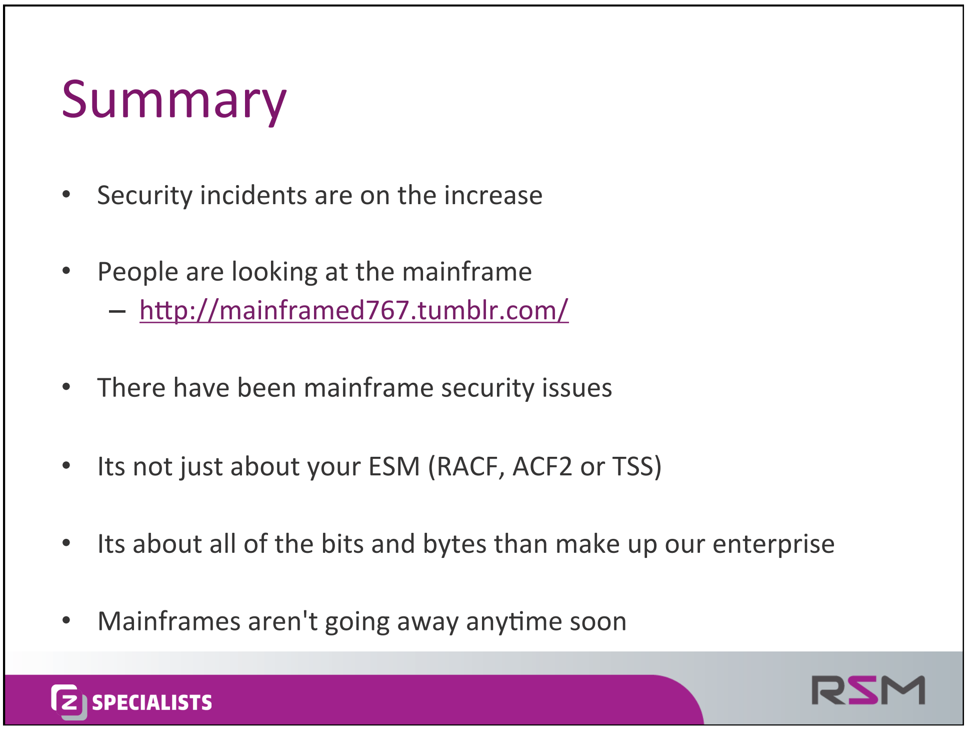
Success?
Use the findings to your benefit to enhance your security posture.

Education
This session

Attack
(Optionally) Attack the system with discovery information.

Knowledge
Now you know what to do!

Discover
Discover the flaws in your system with the knowledge gained.



Summary

- Security incidents are on the increase
- People are looking at the mainframe
  - http://mainframed767.tumblr.com/
- There have been mainframe security issues
- Its not just about your ESM (RACF, ACF2 or TSS)
- Its about all of the bits and bytes than make up our enterprise
- Mainframes aren't going away anytime soon

1.1 MILLION
CICS Transactions.
Every Second.
Every Day.

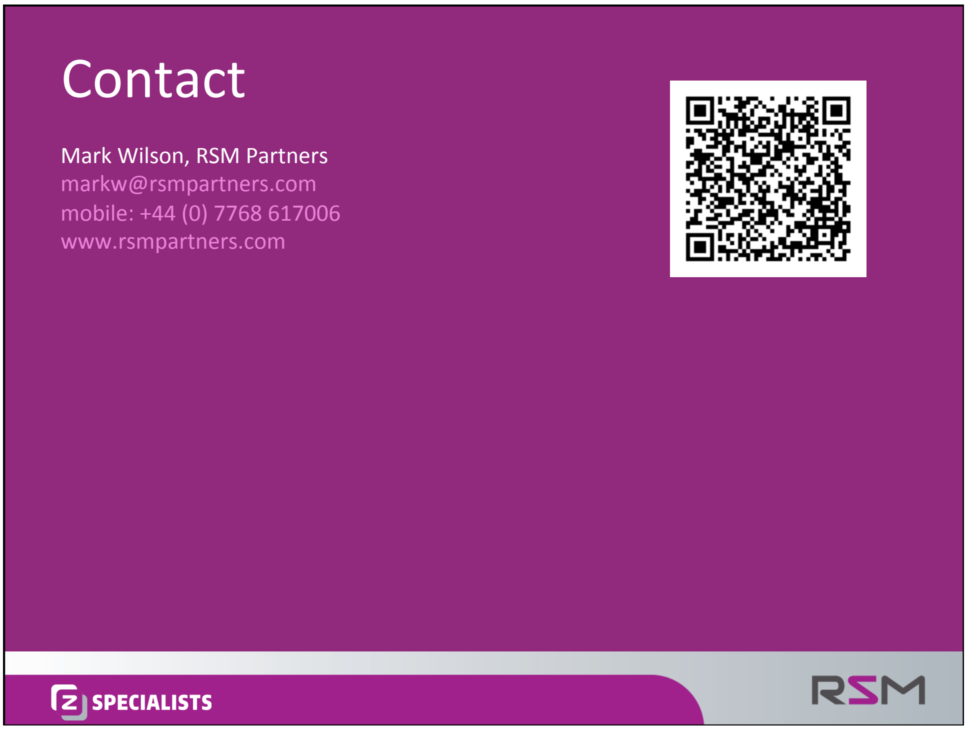
In comparison,
there are only 59,421
Google searches
every second globally.

→ **IBM.com/Mainframe50**

Summary

- The myth that mainframes are secure …is just that, a myth….
- Mainframes are securABLE
- The correct tooling makes life significantly easier
- If you want to really protect your enterprise you need to go on the offensive
- You need to start thinking like the bad guys
- But with the right tools, skills and sheer bloody mindedness then you can defend yourself

Questions



Contact

Mark Wilson, RSM Partners
markw@rsmpartners.com
mobile: +44 (0) 7768 617006
www.rsmpartners.com

SPECIALISTS
RSM