SHARE
Educate · Network · Influence

Security Now!!!!

What 10 Themes You Need to Discuss with Your Director or CIO to Secure Your Communications on the Mainframe

STG LAB Services Thomas Cosenza
tcosenza@us.ibm.com

CELEBRATING 60 YEARS OF SHARE
Influencing IT Since 1955

#SHAREorg

SHARE in Seattle 2015

Trademarks and Notices

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries or both:

- Advanced Peer-to-Peer Networking®
- AIX®
- alphaWorks®
- AnyNet®
- AS/400®
- BladeCenter®
- Candle®
- CICS®
- DataPower®
- DB2 Connect
- DB2®
- DRDA®
- e-business on demand®
- e-business (logo)
- e business(logo)®
- ESCON®
- FICON®
- GDDM®
- GDPS®
- Geographically Dispersed Parallel Sysplex
- HiperSockets
- HPR Channel Connectivity
- HyperSwap
- i5/OS (logo)
- i5/OS®
- IBM eServer
- IBM (logo)®
- IBM®
- IBM zEnterprise ™ System
- IMS
- InfiniBand ®
- IP PrintWay
- IPDS
- iSeries
- LANDP®
- Language Environment ®
- MQSeries®
- MVS
- NetView®
- OMEGAMON ®
- Open Power
- OpenPower
- Operating System/2 ®
- Operating System/400 ®
- OS/2®
- OS/390®
- OS/400®
- Parallel Sysplex®
- POWER ®
- POWER7 ®
- PowerVM
- PR/SM
- pSeries®
- RACF®
- Rational Suite ®
- Rational®
- Redbooks
- Redbooks (logo)
- Sysplex Timer®
- System i5
- System p5
- System x®
- System z®
- System z9®
- System z10
- Tivoli (logo)®
- Tivoli®
- VTAM®
- WebSphere®
- xSeries®
- z9®
- z10 BC
- z10 EC
- zEnterprise
- zSeries®
- z/Architecture
- z/OS®
- z/VM®
- z/VSE

* All other products may be trademarks or registered trademarks of their respective companies.

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries or both:

- Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license there from.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- InfiniBand is a trademark and service mark of the InfiniBand Trade Association.
- Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
- IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

Notes:

- Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
- IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
- All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
- This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
- All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
- Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
- Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Refer to www.ibm.com/legal/us for further legal information.

Introduction

- Work for IBM for 17 years
- IBM Consultant for 11 years
- Working with customers in different business meeting their Network and Security needs

2014 was ……..

The Year of the HACK

2014 a Scary Look Back

- Hacking has gone into overdrive
- 2014 have seen an increase in every type of hacking
  - Denial of Service
  - Criminal
  - Hacktivism
  - Terrorism
  - State Sponsored Attacks

Some Highlights

- Major US Retail Outlets
  - Point of Sales terminals Targeted
- US Banks
  - State Sponsored
  - 76 Million US Households effected
- SONY hack
  - Possibly State Sponsored
  - Hackers had months in their network
  - Demands shut down of a movie
    - So not all bad, I mean did you see it

Some you may not have hear of

- Foreign Nuclear Plant
  - Server administrator discovers access to servers on the site
- Government
  - Homeland Security
    - Web Portal Breach exposes US contractors
  - Immigration Services
    - POS terminals have been breached
  - Justices Services
    - DDOS attacks
- MANY MANY MORE
  - http://hackmageddon.com/2014-cyber-attacks-timeline-master-index/

Clarion Call

- The US Government is spending more on Cybersecurity then many small governments (> 100 Billion)
- However more is needed
- We are the ones that stand between these hackers and our customers

The Problem though

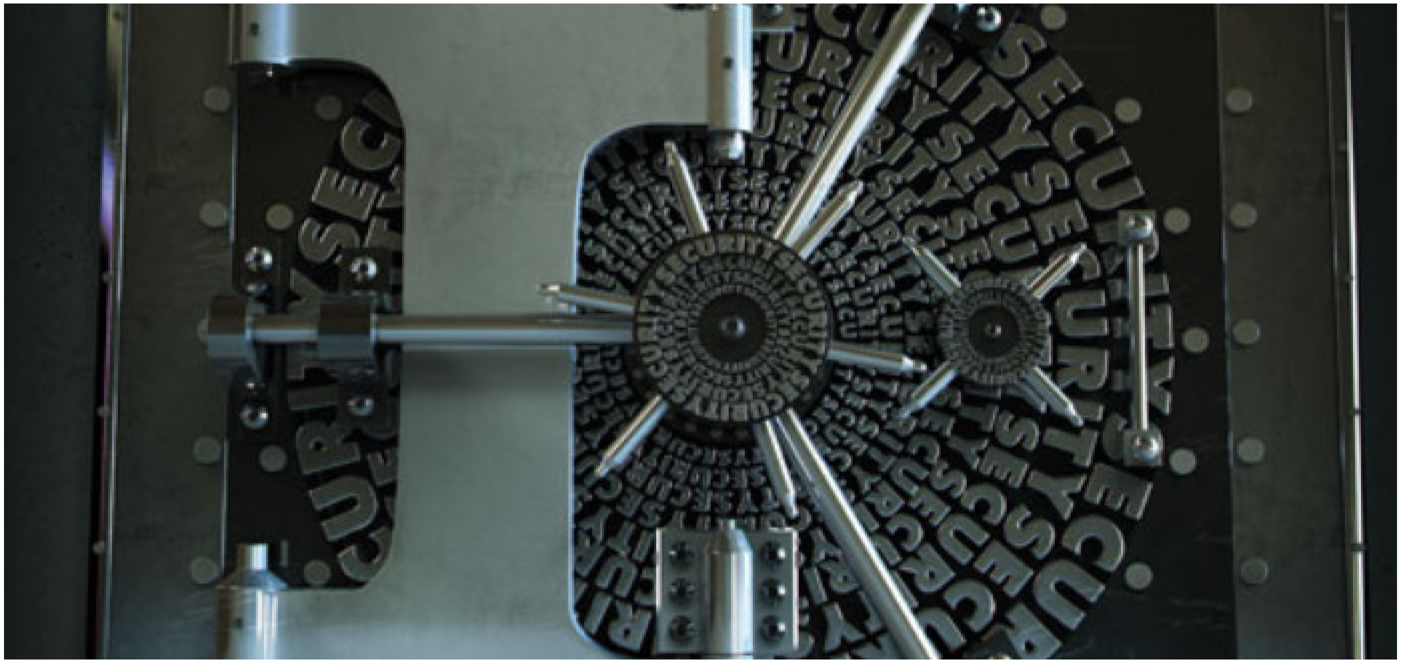
- Your CIO does not take this seriously
- Missing the forest for the trees
- Does not see the mainframe as a priority
- Sounds familiar?

The Reason Why You came here

- I am going to giving you the top 10 reasons I have heard from directors why security is not an issue
- And what I have told them to change their stance and join the fight

Excuse 1

- The Mainframe is already the most secure piece of the environment



So the Truth

- The Mainframe is the most secur**able** piece of environment
- There is a big difference between secure and securable
- While z/OS meets the highest standards in security if you do not enable those securities it does not do you any good.
  - The equivalent of locking your door but leaving all your windows open with only the screen to protect it

Excuse 2

- Security is handled by
  - The security team
  - By our Third Party Vendor

So the Truth

- First lets take the Third Party part of this first.
  - Lawsuit involving Target Breach
    - For a long time there has been a legal question of Liability where it comes to these types of breaches
    - Target attempted to get the lawsuit thrown out against them since Target's lawyer claimed that a third-party firm handles all credit and debit card payments and therefore the company had no obligation to the banks.
    - The judge threw out that argument stating that Target had enough warnings which warrant the case to continue
      - "Plaintiffs have plausibly alleged that Target's actions and inactions - disabling certain security features and failing to heed the warning signs as the hackers' attack began - caused foreseeable harm to plaintiffs," Magnuson wrote in his order.
    - Even if Target is not held liable, this was a land mark decision in addressing companies responsibility

So the Truth

- This leads me into my next point about internal teams
- Security is spread across the entire z/OS product
  - RACF
  - Communication Server
  - Subsystems: DB2, IMS, CICS, WMQ
  - ETC
- Impossible for any one group to know
- Security now more then ever is:

EVERYONES REPONSIBILTY

Excuse 3

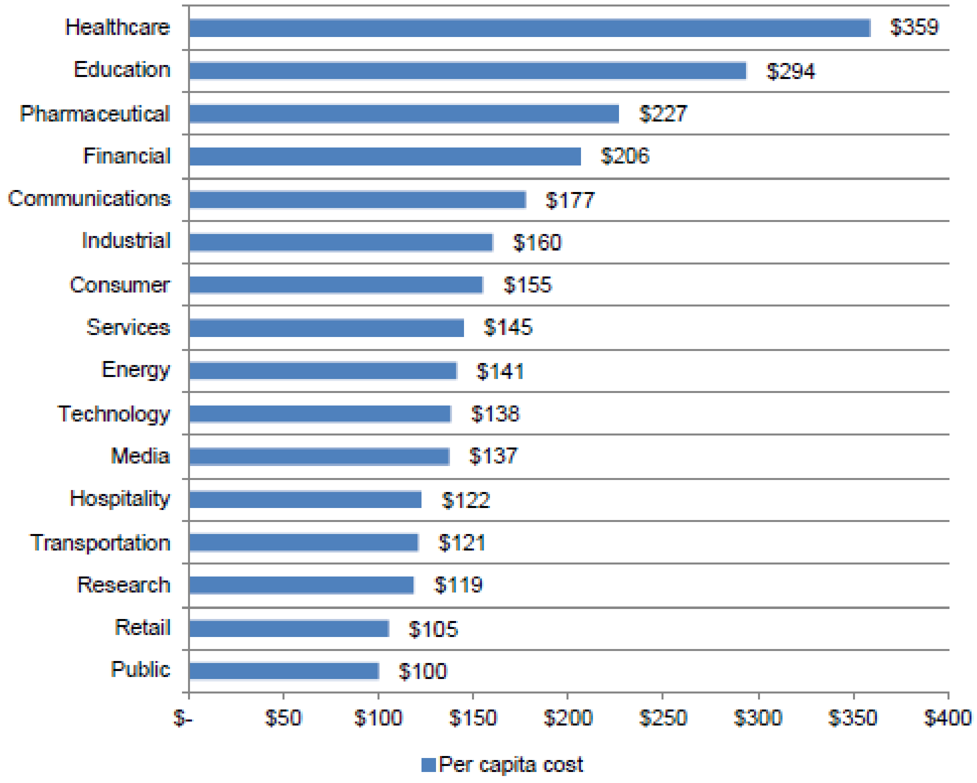
- Security Costs Money

So the truth

- The costs of not securing your business are so much bigger.
  - These costs are rising exponentially
  - Legal liability expanding (see excuse 2)
  - Regulations are starting to catch up with what is going on

So the truth

- Costs per Industry
  - http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/



Excuse 4

- We don’t have the time to do security

So The Truth

- We are all driven by deadlines granted, but if you put something out that lacks security you will be hacked
- Nothing is worse then putting a product or website up and have it full of Security Issues from a visibility standard
  - This can lead in a lack of trust
  - Can also lead to falling stock prices
  - Regulations violations can be a massive liability

Excuse 5

- Everyone on the team can be trusted

So The Truth

- The first rule of security
  - Don’t Trust Anyone
- Criminal enterprises have been known to infiltrate technical teams
- Anyone can be compromised
- Even if you trust everyone now situations changes
  - Disgruntled employees
  - Layoffs occur
  - Healthcare Bills
  - etc

Excuse 6

- Who would want to attack us??

So The Truth

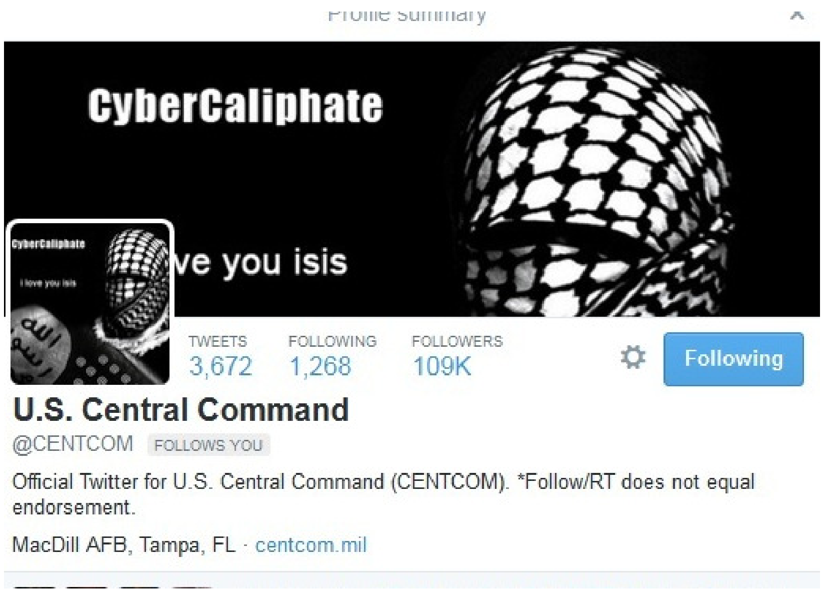
- If you have anything of value you will be attacked
- Everyone has value even if its only storage space
- Hacktivists look to create Anarchy
  - Denial of Service attacks
  - Attempt to breakdown civil services
  - Take down social media services
- US Weather Systems were hacked into

Excuse 7

- Hackers are nothing but those snot nosed little millennials in their parents basement.

So the Truth

- Hackers today are way more sophisticated then what their public persona shows
  - State Sponsored Hackers
  - Criminal Organizations
  - Hactivist Organizations
  - Terrorists
- These groups have real financing and are putting it all into getting through networks like the one you have



TWEETS 3,672 FOLLOWING 1,268 FOLLOWERS 109K

U.S. Central Command

@CENTCOM FOLLOWS YOU

Official Twitter for U.S. Central Command (CENTCOM). *Follow/RT does not equal endorsement.

MacDill AFB, Tampa, FL · centcom.mil

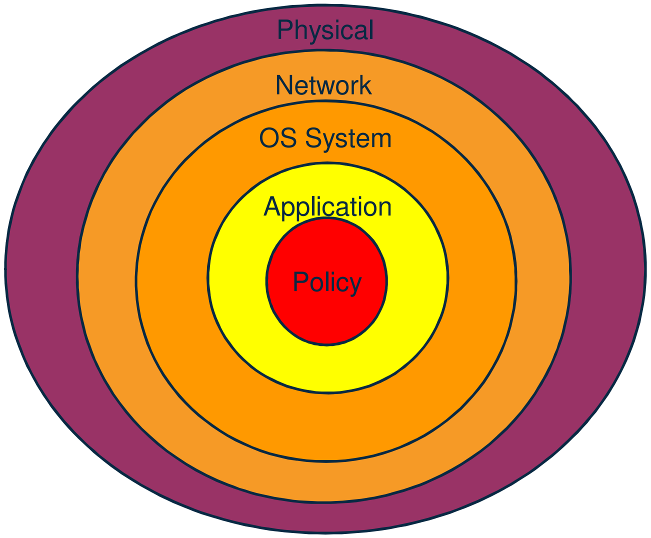
Excuse 8

- We never worried about designing security in the past

IBM
DS43
UNIVERSITY OF BRITISH COLUMBIA COMPUTING CENTRE - DEVICE: DS43 TASK: 245
MTS
WHEN PEOPLE ARE WAITING PLEASE KEEP SESSIONS AS SHORT AS POSSIBLE.
714

So the Truth

- The world has changed
- 40 years ago we could depend on physical security however now more needs to be done.



Excuse 9

- We don't need to encrypt data internally

So the Truth

- 70% of all breaches have an internal component
- Things being transferred in the clear across your networks can see everything
  - User ID
  - Passwords
  - PI info
- Example Sony Hack
  - While there was an external component there are too many systems affected that point to some type of insider

Excuse 10

- WHATEVER ELSE HE/SHE MIGHT COME UP WITH

So the Truth

- We are under siege!!!!

The Security Perimeter is now at the End Point

So What Should be Done

- Once you have convinced your boss of the need here are some of the things you can do
  - Review Your RACF Profiles
  - Go through your Subsystems
  - Look at your network setup
  - z/OS Health Checker
  - Is your organization registered with the Security Portal
    - http://www-03.ibm.com/systems/z/solutions/security_subintegrity.html

What can be done to help

- Get a manager for your RACF database
  - zSecure
  - Other Third party products
- Bring in qualified external resources to review
  - RACF Database
  - z/OS UNIX
  - Storage
  - Network Security Design
  - Subsystem Setup
  - etc
- Make sure they review any necessary regulations that pertain to your industry

For more information

URL	Content
http://www.twitter.com/IBM_Commserver	**IBM Communications Server Twitter Feed**
http://www.facebook.com/IBMCommserver	**IBM Communications Server Facebook Fan Page**
http://www.ibm.com/systems/z/	**IBM System z in general**
http://www.ibm.com/systems/z/hardware/networking/	**IBM Mainframe System z networking**
http://www.ibm.com/software/network/commserver/	**IBM Software Communications Server products**
http://www.ibm.com/software/network/commserver/zos/	**IBM z/OS Communications Server**
http://www.ibm.com/software/network/commserver/z_lin/	**IBM Communications Server for Linux on System z**
http://www.ibm.com/software/network/ccl/	**IBM Communication Controller for Linux on System z**
http://www.ibm.com/software/network/commserver/library/	**IBM Communications Server library**
http://www.redbooks.ibm.com	**ITSO Redbooks**
http://www.ibm.com/software/network/commserver/zos/support/	**IBM z/OS Communications Server technical Support – including TechNotes from service**
http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs	**Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)**
http://www.rfc-editor.org/rfcsearch.html	**Request For Comments (RFC)**
http://www.ibm.com/systems/z/os/zos/bkserv/	**IBM z/OS Internet library – PDF files of all z/OS manuals including Communications Server**

Don’t forget your evals

Complete your session evaluations online at www.SHARE.org/Seattle-Eval