

# *Legacy Security is Just Not Enough!*

Paul R. Robichaux  
NewEra Software, Inc.  
pr@newera.com

Monday, March 10, 2014 - 4:30PM  
Platinum Ballroom Salon 1  
Anaheim Marriott Hotel

Session Number - 14797



# Abstract and Speaker



- Information System Security, the freedom from loss and/or misuse of data and/or information services, and the System Professionals charged with protecting the zEnterprise are consistently under attack from an ever evolving set of persistent external and internal threats and the often unintended consequences of threats that emerge from regulatory and/or technological changes.
- More likely than not, the tools and methods used to detect and defend against these mutating threats are inadequate, often out-of-date. Accepted reasons for this “*Risky State of Affairs*” supports only the status quo; none should be considered reasonable or acceptable.
- Failure to evolve our defenses and responses at a pace as fast or faster than the threats they defend against is increasingly difficult and places the integrity of the zEnterprise in an unacceptable state of risk.
- This presentation will provide insight into:
  - First, A Review of the “Bottom-Line” Goals of IT Security - Identify and Protect “Corporate Value”.
  - Second, Recent revelations of Corporate Spying by Nation States - Work to defeat these Goals.
  - Third, Tools from IBM, Xbridge and Vanguard and Others - Assist with Close-In Security Operations.
  - Fourth, A perspective on the future of IT Security - Returning the Advantage to the “Good Guys”.
- Paul R. Robichaux is CEO of NewEra Software, Inc. He served as the Chief Financial Officer of Boole and Babbage for the ten years immediately preceding his co-founding of NewEra in 1990. He holds a BS in Accounting and a Masters in Business Administration from a Louisiana State University and is a Certified Public Accountant.
- The corporate mission of NewEra Software is to provide software solutions that help users avoid non-compliance, make corrections as needed and in doing so, continuously improve z/OS integrity.



# Legacy Security is Just Not Enough!



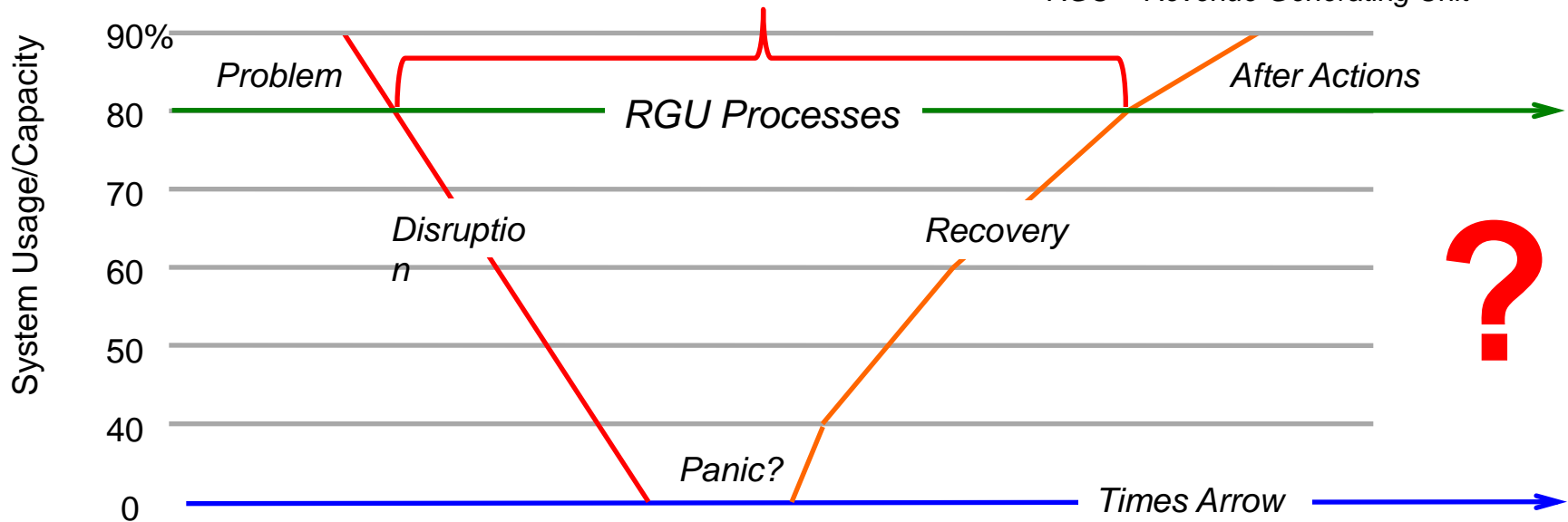
Part 2: Security - What's New in V2R1 - Thursday, March 13, 2014 - 8:00AM

This is all about RAS - Reliability, Availability and Securability



The Bottom !

RGU = Revenue Generating Unit



“...tracking and installing security and system integrity fixes will help to mitigate risk in the System z Environment. Recommended Service Upgrades (RSUs) help to minimize your exposure to security threats and system integrity issues.” What level are you at?

RGU = Revenue Generating Unit



# Legacy Security is Just Not Enough!

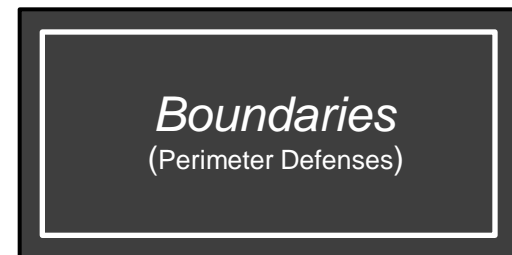
*Information System Security Exists to Protect:*

- ✓ *Individual Identity*
- ✓ *Financial Values*
- ✓ *Intellectual Property*



*The Level of Protection Afforded is Determined by:*

- ✓ *Best Practices*
- ✓ *Industry Standards*
- ✓ *Legislated Requirements*



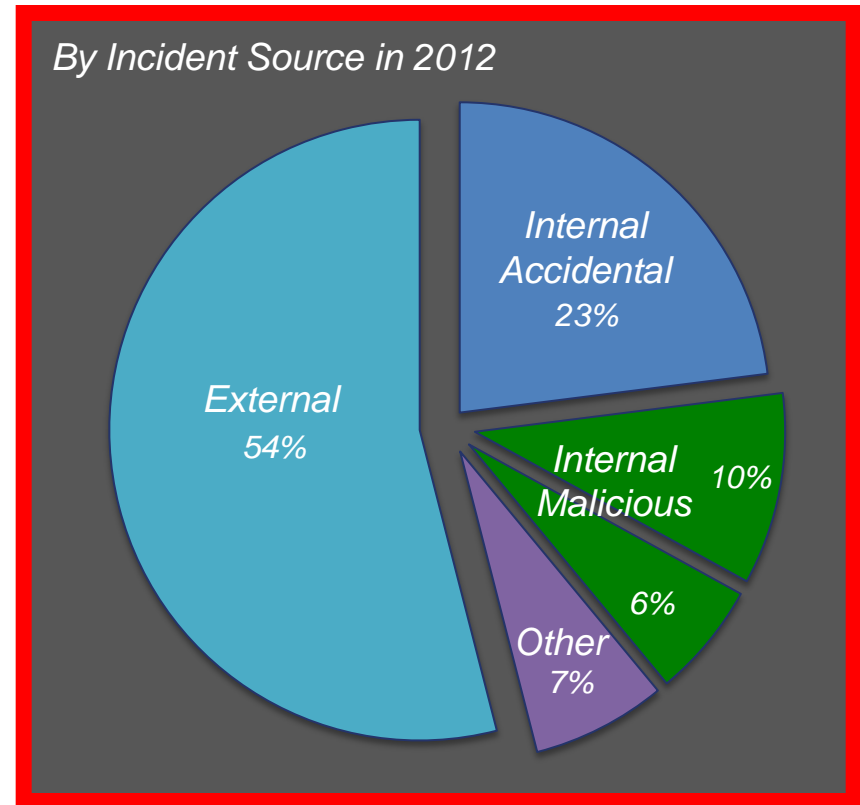
Sources: *The Father of IT Security, Founder of SHARE Security Project - Barry Schrager President, Xbridge*

# Legacy Security is Just Not Enough!

<http://www.redbooks.ibm.com/abstracts/redp4944.html?Open>

## Threats to IT Security Exist at Three Different Levels

- ✓ **External** - include denial of service (DoS), web vandalism and propaganda, botnets, and equipment disruption including attacks on power grids and fuel, communication, and transportation systems.
- ✓ **Internal** - include insider malicious attempts and unintentional attempts to breach security with malware, data leaks, or stealing valuable data, breaking through vulnerable points in the system.
- ✓ **Other** - include SQL injection, phishing, and Advanced Persistent Threats. APT is the most severe attack on business assets because of staged progression over time.



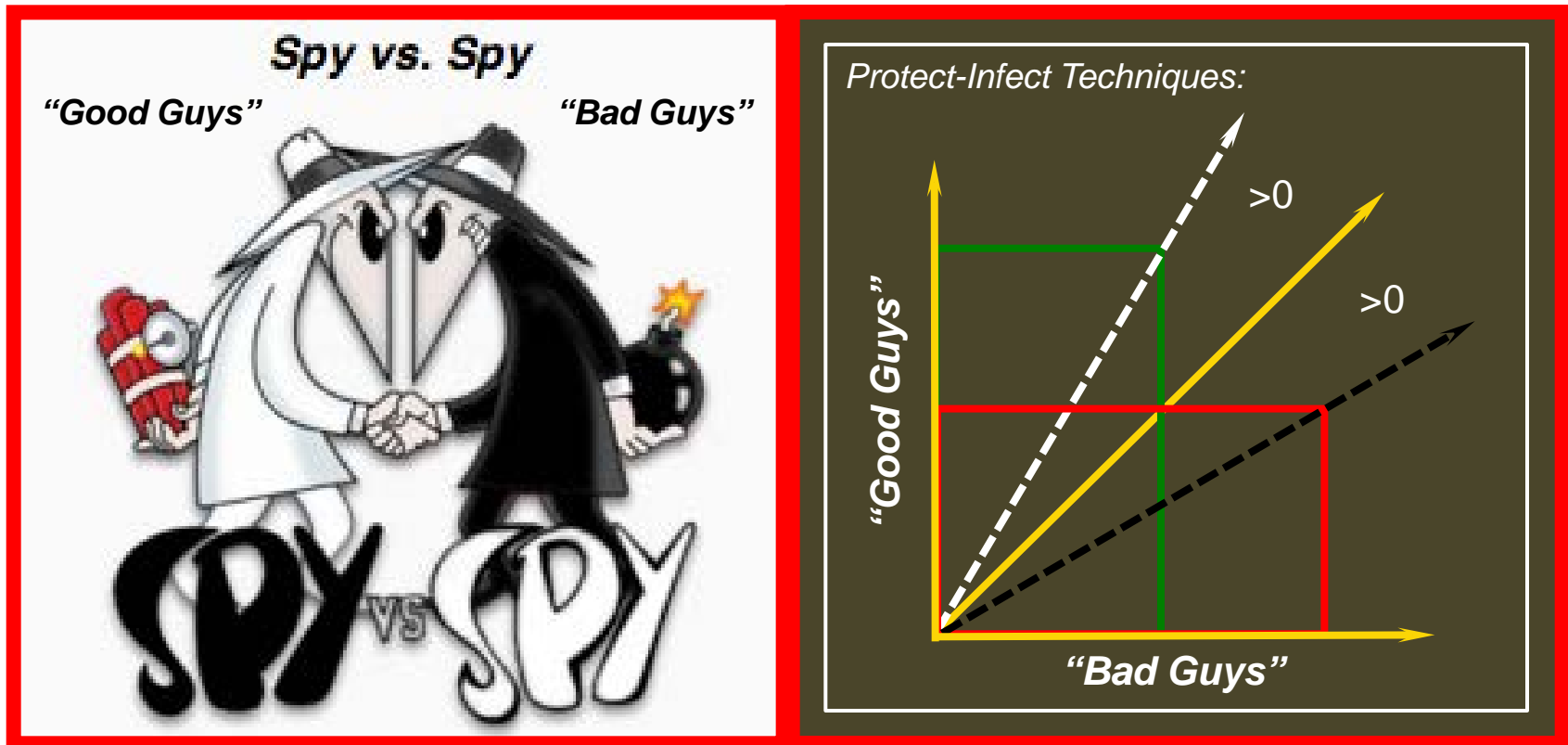
Source: Chung-Sheng Li, Ph. D., Director IBM Research, Katsumi Ohnishi, IBM Executive Architect, and Josuyla R. Rao, Director IBM Research

# Legacy Security is Just Not Enough!

[http://en.wikipedia.org/wiki/Advantage\\_\(cryptography\)](http://en.wikipedia.org/wiki/Advantage_(cryptography))

<http://www.zdnet.com/mega-to-fill-secure-email-gap-left-by-lavabit-7000019232/>

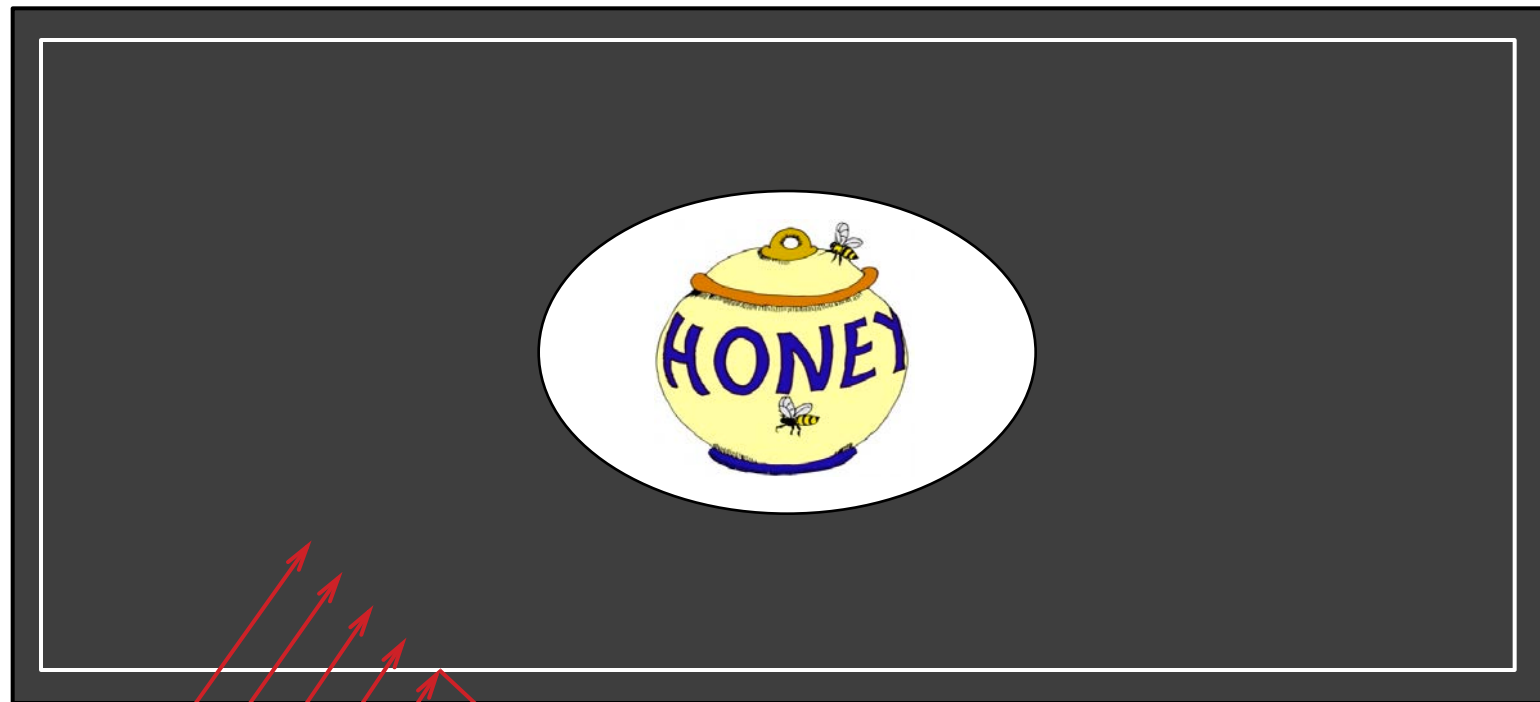
*The Goal is to Reduce an Adversary's Advantage to "Zero"!*



*A System is Considered Secure when “Bad Guys” have a Negligible Advantage over “Good Guys”.*

# Legacy Security is Just Not Enough!

*We Identify the Value and Erect Boundaries to Protect it!*



*Intrusion Attempts*  
*Advanced Persistent Threat (APT)*

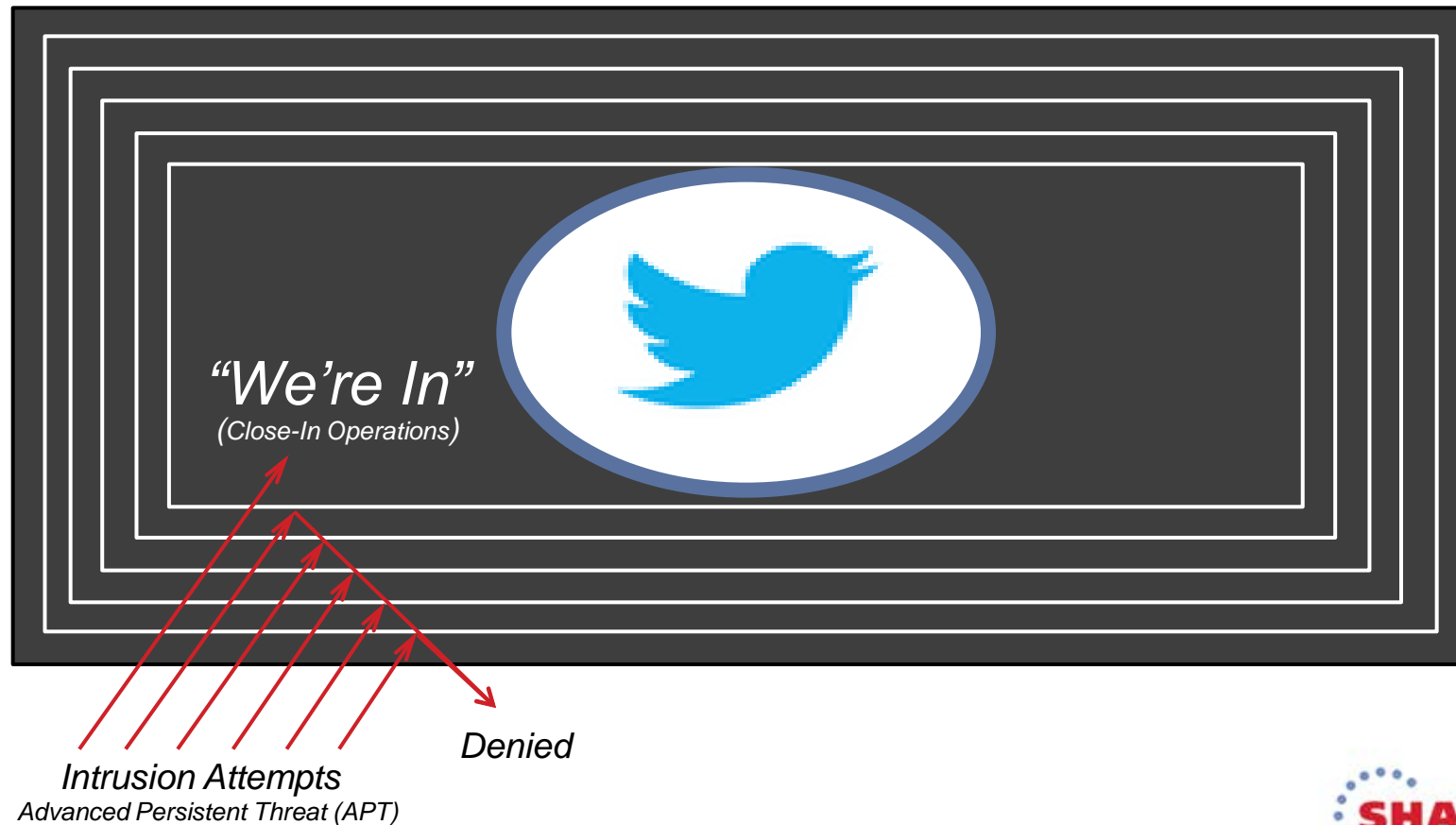
*Denied*

# Legacy Security is Just Not Enough!

<http://www.youtube.com/watch?v=zis5w3SiQbg>

<http://business.time.com/2014/01/20/russian-teen-suspected-as-author-of-target-hacking-code/>

*We Identify the Value and Erect Boundaries to Protect it!*





# Legacy Security is Just Not Enough!

*All Control Boundaries Degrade with the Passage of Time!*

- ✓ As with all things, time ages even the best concepts and designs. With this inevitability in mind, today's Security Professionals are facing threats that require agility in the application of security that cannot be easily implemented with Legacy Security.
- ✓ The application of Legacy Security within the broader base of users, applications and data resources is adequate and will continue, as is, into the foreseeable future.
- ✓ When the security needed to protect zEnterprise System configurations and resources is considered, it becomes clear that we are rapidly approaching a state of non-compliance.



# Legacy Security is Just Not Enough!

## Business Enterprises are Under Attack from All Sides!

*“...Microsoft EVP labels the US Government an Advanced Persistent Threat in plan to cutoff NSA.”*

*Source: The Washington Post - December 5, 2013*



*“Shareholder Lawsuit accuses IBM of hiding China risks amid NSA spy scandal”*

*Source: Reuters - December 12, 2013*



*“In 2014 major brands - Snapchat, Target, Skype, and Yahoo! - have fallen victim to hackers.”*

*Source: HUFF POST - January 8, 2014*



*“...of the 3,236 US Businesses asked, 43% reported data lost in a Public or Private Cloud.”*

*Source: San Jose Mercury - Symantec Corp. - March, 2013*



*“...In 2012 Security Breaches Cost US Companies an Estimated \$US175 Billion.”*

*Source: The Ponemon Institute – www.ponemon.org - 2012*



# Legacy Security is Just Not Enough!



## Factors that Tend to Diminish the Integrity of IT Security!

### ☑ *Explosion in External Threats*

Commodity Threats - Kiddy Hackers  
Advanced Persistent Threats - NSA  
Coordinated Actors/Actions/Activities

### ☑ *Graying of Security Assets*

Resulting from Retirements, Reductions in  
Workforce and a Misguided Emphasis on  
Non-Mainframe platforms.

### ☑ *The Flood of System Events*

Driven primarily by advances in Hardware,  
they are now generated at a rate 1200 X  
faster than 15 years ago.

### ☑ *Reliance on Consultants/Outsourcers*

Often seen as a strategy for reducing cost,  
these dependencies move Security control into  
the hands of others - Cloud Providers.

### ☑ *Drive Towards Globalization*

Different cultures will view security in  
ways that conform to their view of best  
practices - Deployment of State Trojans.

### ☑ *“Starving the Beast”*

A myopic focus on the Total Cost of Ownership  
will result in a diminished view of the value of  
information security towards the Bottom Line.

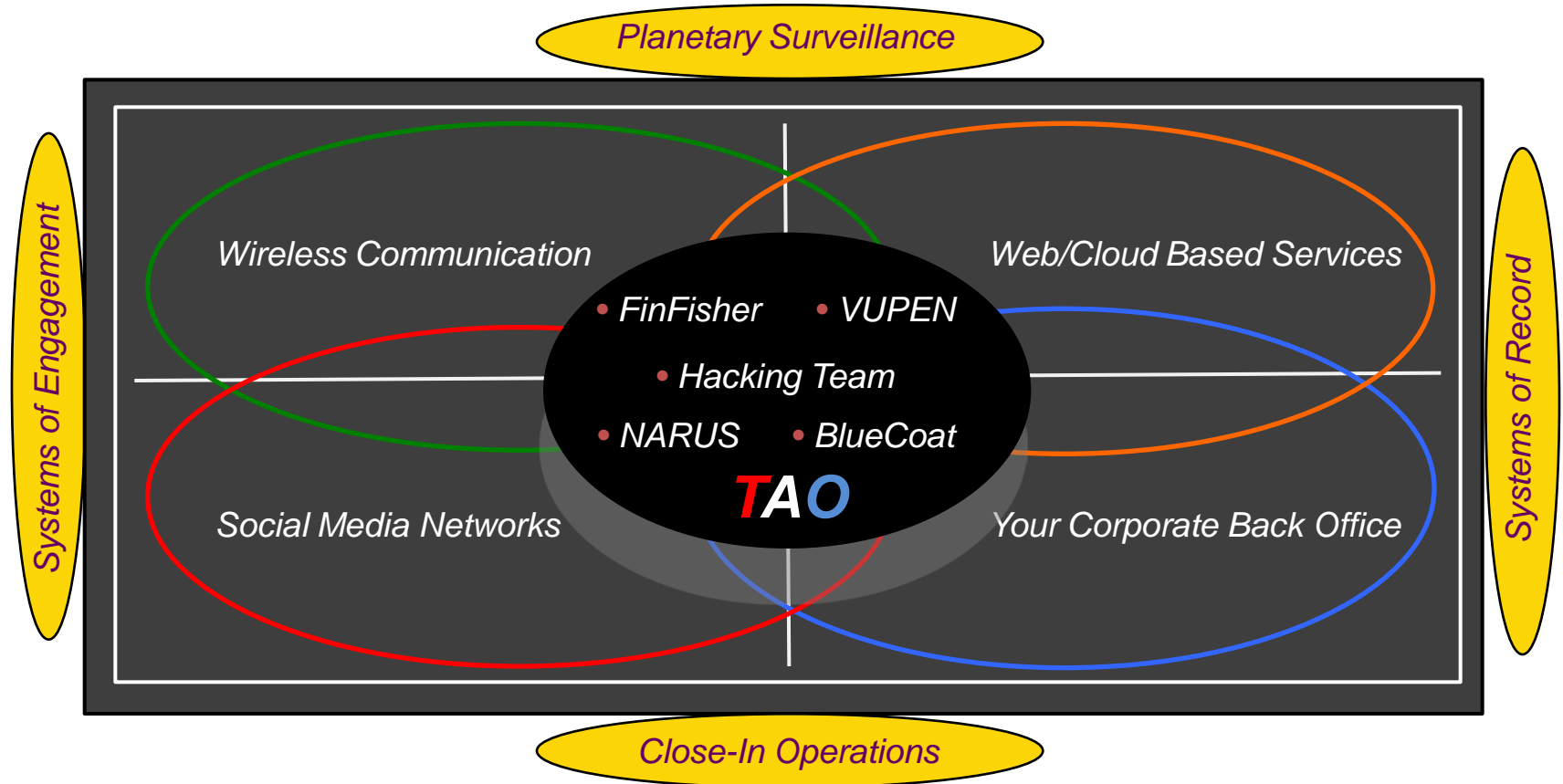


# Legacy Security is Just Not Enough!

<https://www.youtube.com/watch?v=b0w36GAyZIA>

<http://www.cruxialcio.com/nsa-special-ops-team-reportedly-hacked-everything-3200>

## Mapping Service Domains with Potential Intrusions Threat:



Sources: Chaos Communication Congress - To Protect and Infect -12/30/2013 - Jacob Applebaum

# Legacy Security is Just Not Enough!

<http://cryptome.org/2013/12/nsa-catalog-appelbaum.pdf>

Hacking Team Home Video - <http://vimeo.com/36090385>

Mapping Service Domains with Potential Intrusions Threat:

Planetary Surveillance

→ (Low end) corporate spying

- Commercial hardware solutions are rather boring
- Forensics hardware like the "Mouse Jiggler"
  - Now disabled in systemd (!)
- Power insertion attacks
  - Hotplug seizures
- Keystroke recorders
  - largely lame
- FinFisher, HackingTeam, VUPEN

FinFisher is a trojan spyware kit developed and marketed by the UK/German company Gamma Group. It is used by many governments around the world for surveillance purposes.

Systems of Engagement

Systems of Record

Close-In Operations

The Era of the Digital Mercenaries - <http://surveillance.rsf.org/en/>



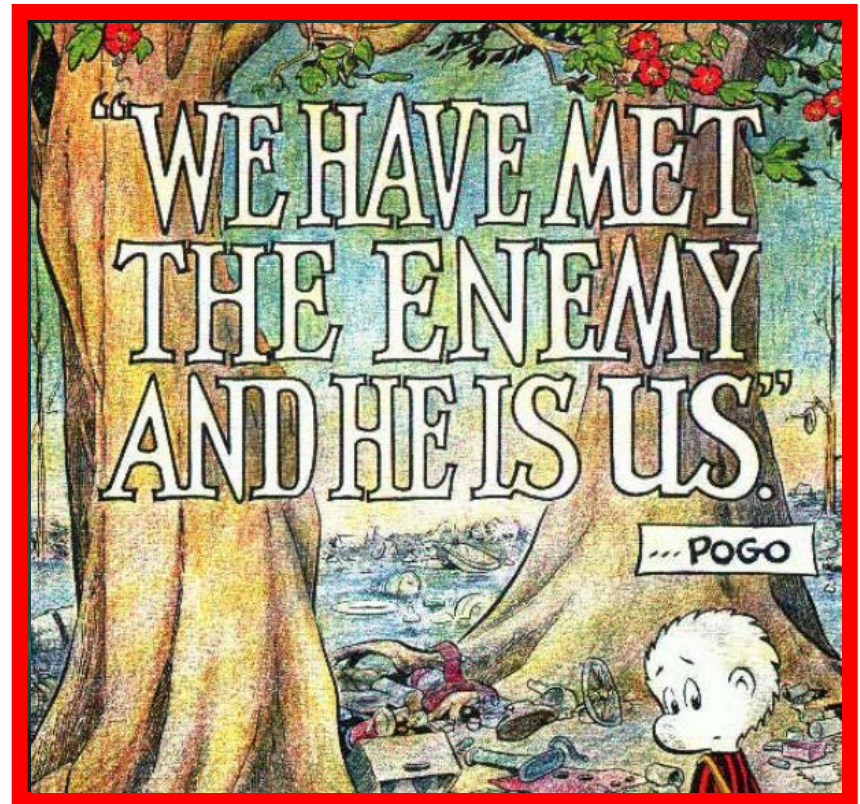
# Legacy Security is Just Not Enough!

<http://www.cruxialcio.com/nsa-special-ops-team-reportedly-hacked-everything-3200>

*Spies seem to be Popping-up Everywhere!*

- ✓ *“...Der Spiegel has uncovered NSA documents that reveal details on the NSA's abilities to implant backdoors in computer systems, infiltrate Internet service providers and telecom networks and tap into international fiber-optic cables...”*
- ✓ *“...The Office of Tailored Access Operations, or TAO, does most of the NSA's hacking work, according to the magazine. TAO workers have exploited Microsoft software and Internet service providers, such as Facebook, Yahoo, Twitter and YouTube; and have developed backdoors for systems developed by Juniper Networks, Cisco, Huawei and Dell...”*

Source: Business Korea - January 9, 2014



# Legacy Security is Just Not Enough!

<http://www.techtimes.com/articles/2364/20131231/nsa-hackers-ate-iphone-breakfast-silicon-valley-giants-lunch.htm>

*Report says - NSA can Eat Apples for Lunch!*

- ✓ *“...NSA get full access to smart-phones, especially iPhones, with a program called "DROPOUT JEEP." In fact, the intelligence agency says it has 100% success rate installing malware in iPhones...”*
- ✓ *“...Der Spiegel report indicates NSA used Microsoft Windows crash reports to spy on targets. Also says Microsoft Internet Explorer was also very popular amongst NSA hackers...”*
- ✓ *“...Secret servers and privileged position on the internet's backbone helps identify users and attack target computers...”*

Source: Sumit Passary - Tech Times - 12/31/13



# Legacy Security is Just Not Enough!

<http://www.techweekeurope.co.uk/news/huawei-ceo-china-cyber-attack-us-115784>

*Exploits are Everywhere; some are Embedded into your Hardware!*

## ✓ Direct Memory Access (DMA) Attacks

- A type of side channel attack where the corruption of basic OS security mechanisms is conducted by an attacker with direct access to a physical memory address space.
- Systems are vulnerable to a DMA attack by external device if port like PCI and PCI-Express are hooked directly to a physical address space. Security concerns argue against PCIe as a host-to-host interconnect.

## ✓ HUAWEI CEO Responds

- “Huawei equipment is almost non-existent in networks currently running in the US. We have never sold any key equipment to major US carriers, nor have we sold any equipment to any US government agency,”





# Legacy Security is Just Not Enough!



Slipping down this **Rabbit Hole** Results in:

*All of these “Anecdotal Findings”, can be viewed as good news for people who like bad news.*



*Today there are more threats than there are qualified people or capable tools to identify and resolve them.”*



*This may be good for those individuals wanting to pursue a career in Information System Security.*



*This is clearly bad for business integrity and consumer confidence in Systems of Engagement.*



# Legacy Security is Just Not Enough!

<http://bigstory.ap.org/article/cybercrime-disclosures-scarce-despite-new-sec-rule>

*No Matter how you “Slice-and-Dice” these are Criminal Acts!*

✓ *Following these Tips and Best Practices can help you to avoid entanglements:*

*1. With Respect to Employees*

1. Educate
2. Equip
3. Empower

*1. With Respect to Stakeholders, Disclose*

1. Material Attacks
2. Potential Damages
3. Damage Mitigation
4. Corrective Actions

*1. With Respect to Law Enforcement*

1. Report, Cooperate
2. Prosecute Offenders



# Legacy Security is Just Not Enough!

<https://www.youtube.com/watch?v=d-diB65scQU>

## *The Biggest Threats to IT Security - What, me worry?*

*“There are two things that IT Security people worry about these days:*

*1<sup>st</sup> , That things will never get back to normal.*

*2<sup>nd</sup> , That they already have!”*



*“One slip, and down the hole we fall. It seems to take no time at all.”*



*”Don’t worry, be Happy! When you’re not, your troubles will double.”*



Sources: Google - alfred e neuman quotes, Anderson Layman, Pink Floyd, Bobby McFerrin

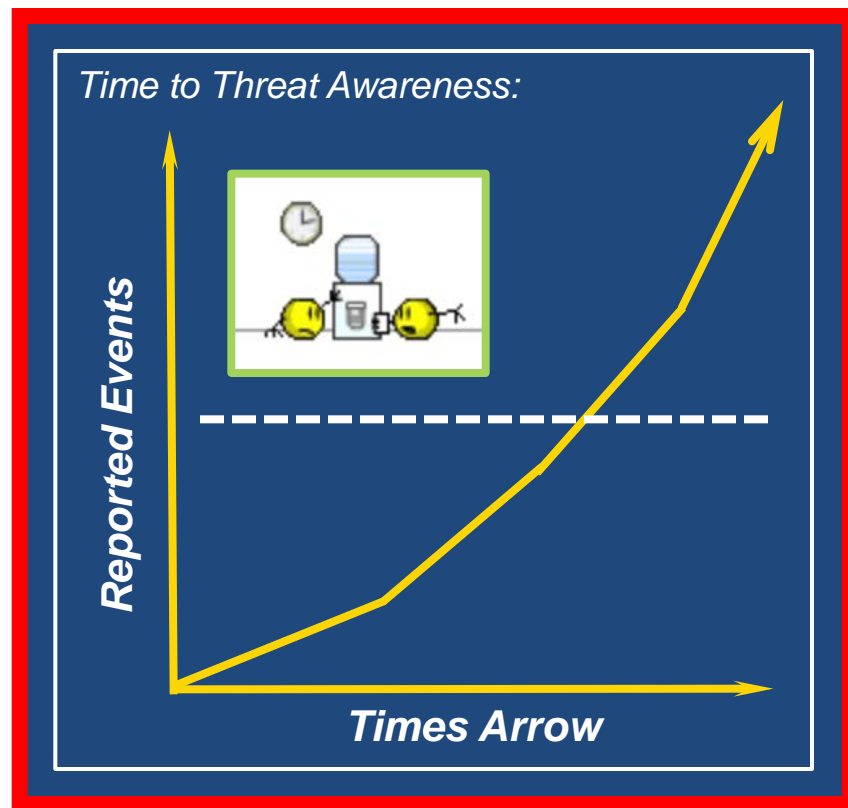
# Legacy Security is Just Not Enough!

<http://searchsecurity.techtarget.com/videos>

## *The Best Defense? A Commitment to Threat Awareness!*

✓ A zero-day attack or threat is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on "day zero" of awareness of the vulnerability. This means that the developers have had zero days to address and patch the vulnerability.

## *“Zero-Day Attack”*



Source: [http://en.wikipedia.org/wiki/Zero-day\\_attack](http://en.wikipedia.org/wiki/Zero-day_attack) - Zero-day or next-generation malware

# Legacy Security is Just Not Enough!



<http://searchsecurity.techtarget.com/videos>

## *The Best Defense? A Commitment to Threat Awareness!*

**From:** SearchSecurity.com <no\_reply@techtarget.com>  
**Subject:** Infosec 2012: How to Help Your Organisation Deal with Next-Generation  
**Date:** June 26, 2013 6:27:39 AM PDT  
**To:** Paul Robichaux

---

### Today's Top White Papers:

[Infosec 2012: How to Help Your Organisation Deal with Next-Generation Cyber-Attacks](#)  
[Compliance Frameworks Live Chat](#)  
[Why Your Security Strategy Needs Universal Log Management](#)  
[Email Security Technical Guide](#)  
[Antivirus: The Hippest New Apple Accessory](#)

### **Infosec 2012: How to Help Your Organisation Deal with Next-Generation Cyber-Attacks**

*eGuide sponsored by Hewlett-Packard Company*

This E-Guide offers expert insight on how to address next-generation cyber-attacks. View now to learn how network visibility can help you mitigate advanced threats, and much more!

**View Now**

Source: Techtarget - <http://www.techtarget.com/>





# Legacy Security is Just Not Enough!



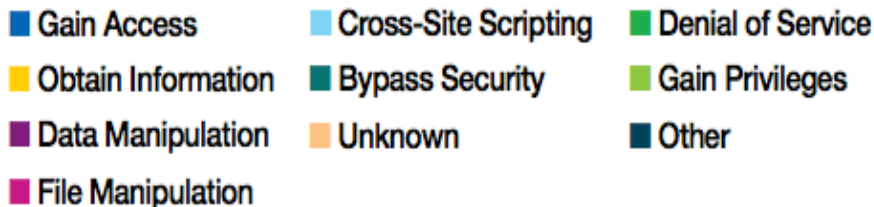
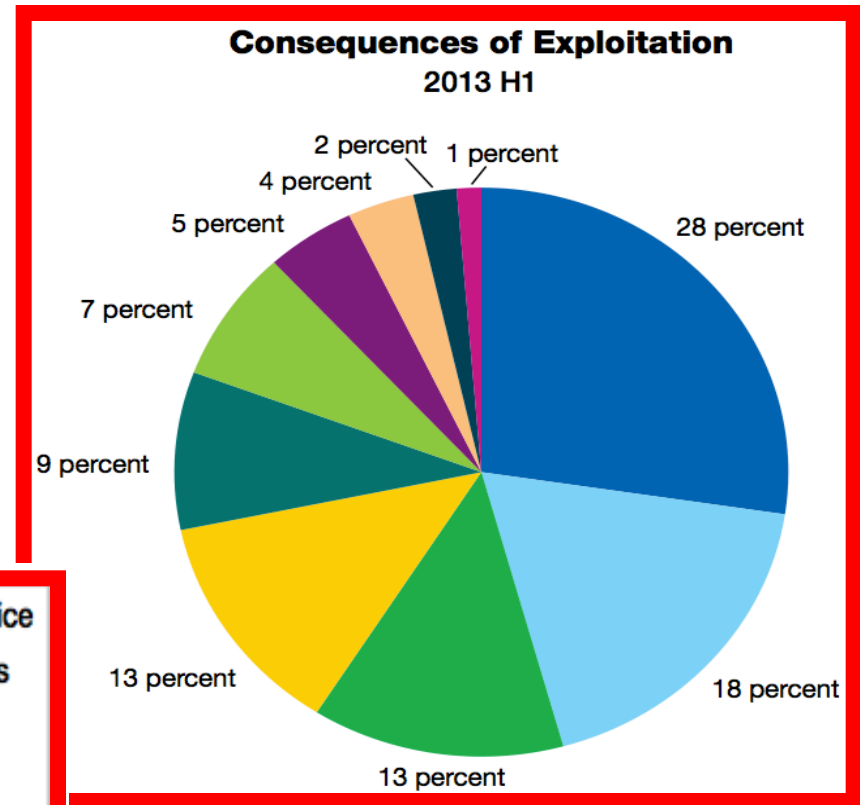
<http://www.ibm.com/developerworks/security/library/se-sweep/index.html>

<http://www-935.ibm.com/services/us/iss/xforce/>

## The Best Defense? A Sweeping New Approach to Security!

### ✓ Implement security intelligence

- Allows you to shift your security paradigm from a traditional perimeter defense to a fine-grained, micro-perimeter security in an effort to address emerging threats in mobile, social, and cloud computing
- Allows you to mitigate risks from growing data volume, proliferation of clouds and mobile users, and web technologies.



Source: IBM X-Force 2013 Mid-Year Trend and Risk Report, September 2013



# Legacy Security is Just Not Enough!



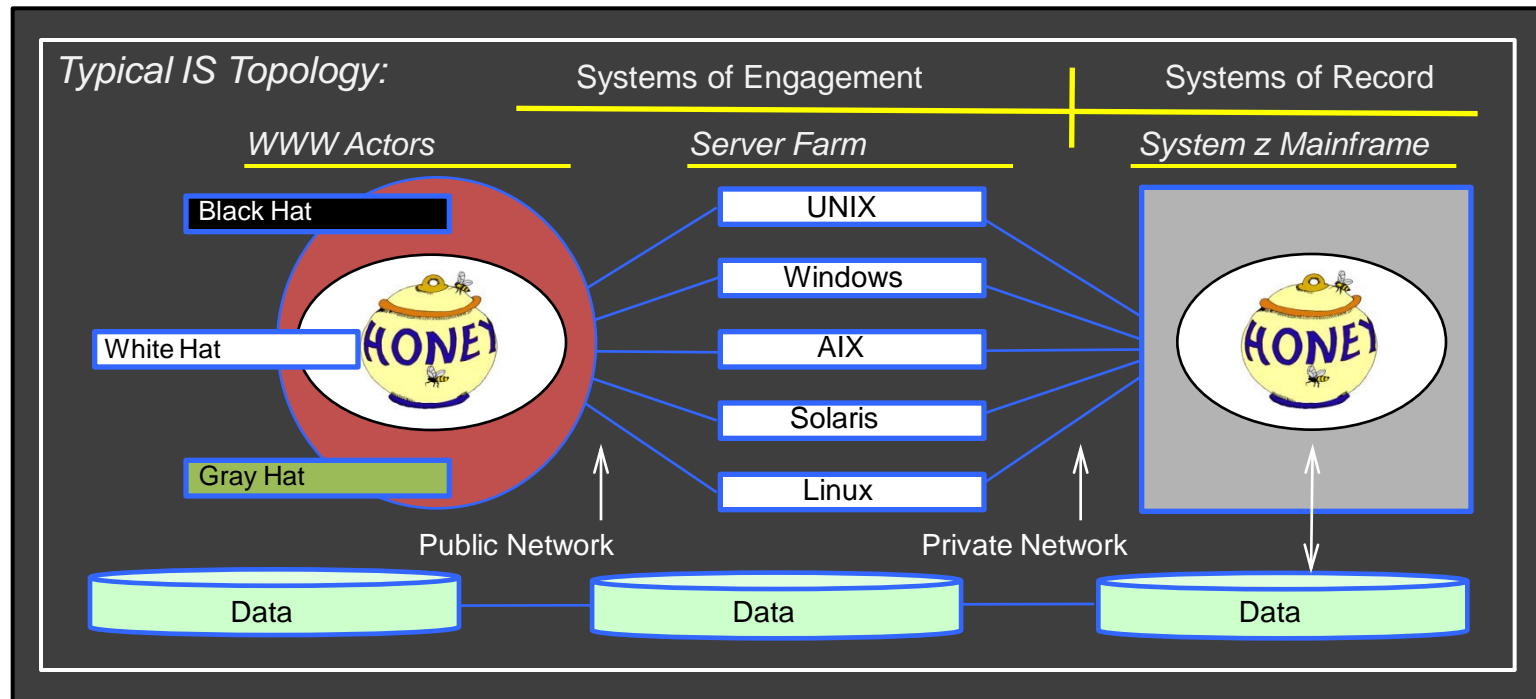
*Where do we go from here?*

- Network, Crypto and Policy Management*
- A focus on 12 specific System z Mainframe Exploits*
- Staying in Compliance: Copies of Copies, Enforcement*
- An Internal Issue: Reinforcing OS Configuration Boundaries*
- Getting z/OS Up-to-date and the System z Security Portal*
- The future of Information System Security, my Perspective*



# Legacy Security is Just Not Enough!

## Double Honey, Double the Trouble?



*Most attacks against a System z Mainframe begin with an attack on Network Assets and/or Open Ports.*



# Legacy Security is Just Not Enough!

[http://www.privacysos.org/technologies\\_of\\_control/naurus](http://www.privacysos.org/technologies_of_control/naurus)

*Your Network is a Wild-and-Wooly Place to do Business!*

✓ The goal of network security is to provide confidentiality, integrity and authenticity:

- Confidentiality

*Keeping the data secret from the unintended listeners on the network.*

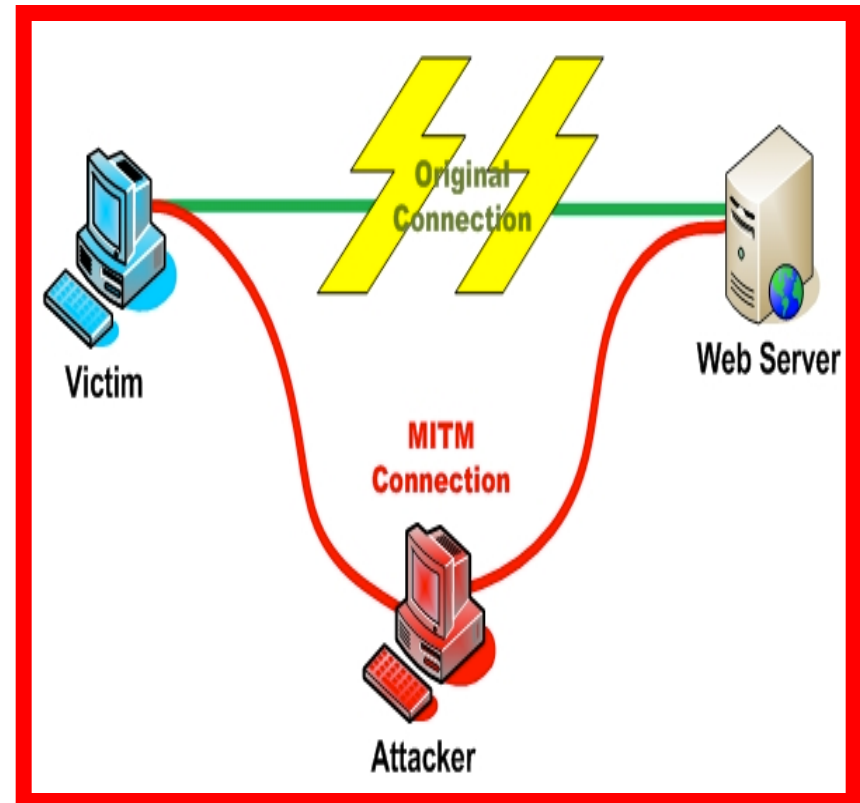
- Integrity

*Ensuring that the received data is the data that was actually sent.*

- Authenticity

*Proving the identity of the end point to ensure that the end point is the intended entity to communicate with.*

✓ All network attacks, i.e. Man-in-the Middle attacks, attempt to defeat and/or compromise these goals.



# Legacy Security is Just Not Enough!



<http://www.stuhenderson.com/StuTop12f.pdf>

## Stu Henderson - His Top 12 Mainframe Security Exposures!

### *Advanced Persistent Threat APT The Hacker's Guide*

- *Scan Server Farm for open Ports*
- *Send a malformed Packet*
- *Open the Packet to activate Port*
- *Send a Trojan through open Port*
- *Harvest user credentials on Server*
- *Exploit open mainframe Port*
- *Send Exploit Findings to Adversary*
- *Harvest credentials on LPAR*
- *Implant Remote Access Tool - RAT*
- *Seek and copy target data*
- *FTP Data to Internet Drop Box*
- *Terminate and Erase*

### *12 Mainframe Security Exposures By Stu Henderson*

- *MVS Program Integrity*
- *Excess Defaults/Privileges*
- *Job Entry Security*
- *Tape Security*
- *Residual Data (Copies)*
- *DB2 Internal Security*
- *Access to Production Data*
- *Windows Sniffer Programs*
- *VTAM Security*
- *Batch with Another's UserId*
- *Hardware Configuration*
- *TCP/IP Connections*

Source: *Top 12 Mainframe Security Exposures and Lessons From A Real Mainframe Break-In*

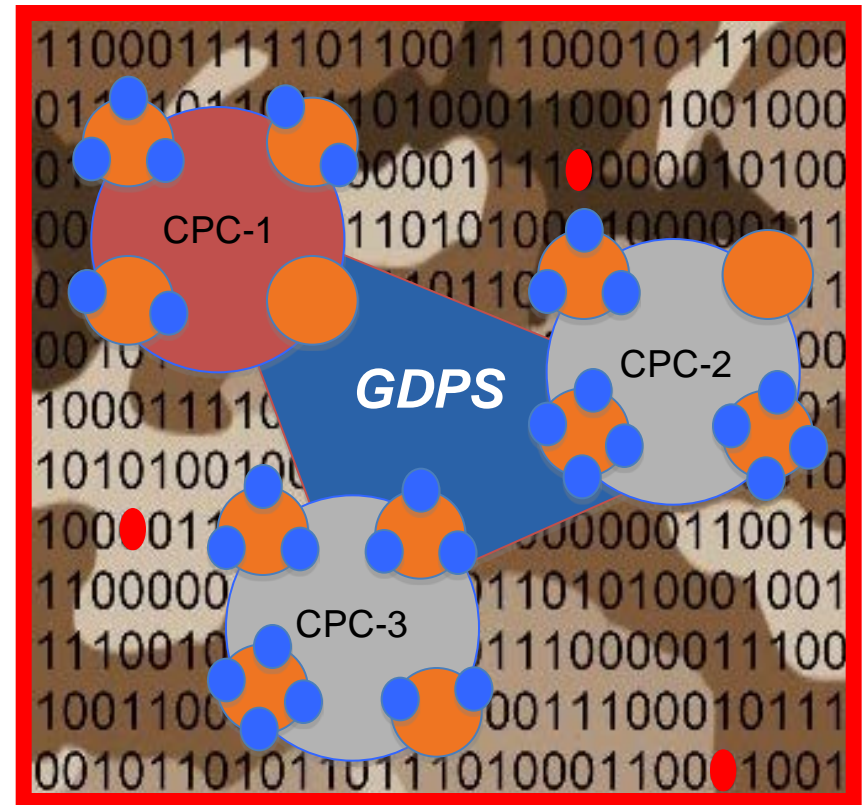


# Legacy Security is Just Not Enough!

<http://www.newera-info.com/z-OS-Crypto.html>

*Any Network, without Crypto will Lack Confidentiality, Integrity or Authenticity!*

- ✓ *Data Encryption Standard<sup>1</sup> (DES) is a symmetric-key algorithm for the encryption of data. It is advanced modern “Crypto” but is not considered adequate - 56-Bit Key.*
- ✓ *Triple DES (TDEA) applies the DES cipher algorithm three times, a relatively simple method of increasing the key size of DES to protect without the need to design a completely new block cipher.*
- ✓ *Advanced Encryption Standard (AES) supersedes DES. AES is based on a design principle known as a substitution-permutation network. Its block and key sizes are any multiple of 32 bits, with a minimum of 128 and maximum of 256 bits.*



<sup>1</sup>DES = 1975 > IBM > NBS > NSA > FIPS > Federal Information Processing Standard

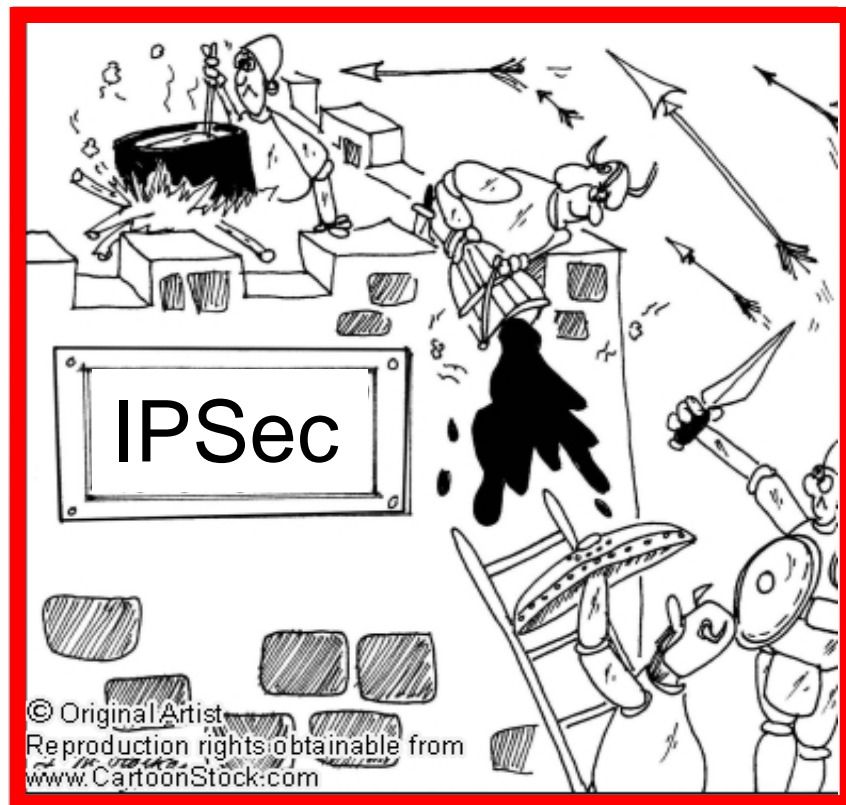
NIST      Reduced Key Size

Source: Wikipedia - Data Encryption Standard

# Legacy Security is Just Not Enough!

*Open, Raw and/or Un defended Ports are a real NO-NO!*

- ✓ Identifying that scanning missions are underway can alert a security analyst as to what services or types of computers are being targeted for possible attack.
- ✓ Knowing what services are targeted allows an administrator to take preventative IPSec measures, e.g. installing patches, fire walling services from the outside, or removing services on machines which do not need to be running on them.
- ✓ Port Scan detection systems count distinct destination IPs attempting to connect to a given Port within a certain time window. False Positives a Problem!



Source: Scan Detection: A Data Mining Approach – 2006 - By György J. Simon , Hui Xiong  
University of Minnesota, Rutgers University



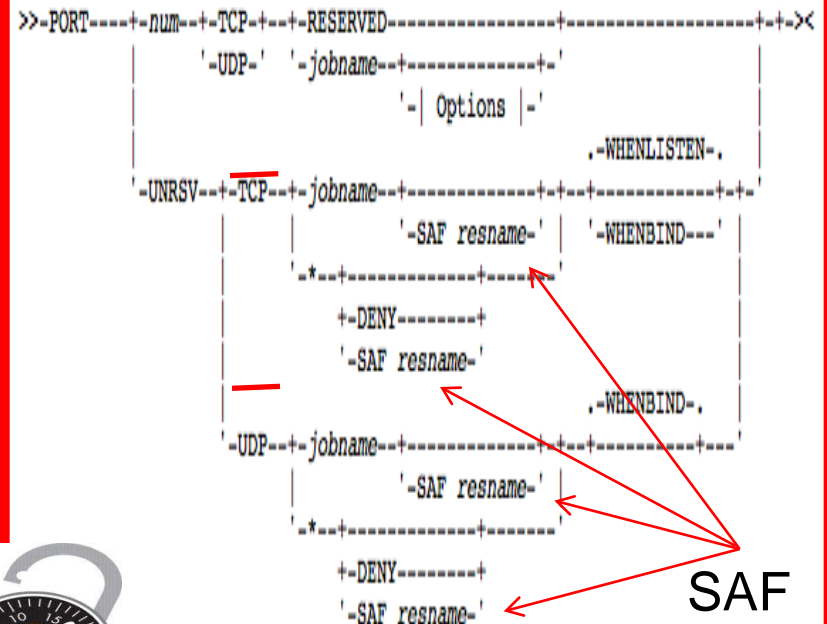
# Legacy Security is Just Not Enough!

## What's Currently Available - Use SAF Call to Validate Access!

- ✓ The *PORT* statement is used to reserve a port for one/more job names or to control application access to unreserved ports.
- ✓ For example, use the *PORT* statement to control the port that will be used by the SMTP server for receiving mail. If *PORT* is not coded, SMTP defaults to the value 25, the well known port for mail service.
- ✓ Note that port 25 is typically reserved in *hlq.PROFILE.TCPIP* for the SMTP server to accept incoming mail. If another port number is selected for the SMTP server, then update the *hlq.PROFILE.TCPIP* file accordingly.

### TCP/IP - Port Configuration Statement Syntax

```
>>PORT-----num---TCP---RESERVED-----+-----+<<X
      '-UDP-'  '-jobname-----+'
                    '| Options |-'
                                '-WHENLISTEN-'
-UNRSV---TCP---jobname-----+-----+
      '-SAF resname-'  '-WHENBIND---'
      +-----+
      '-DENY-----+'
      '-SAF resname-'
      +-----+
      '-UDP---jobname-----+'
      '-SAF resname-'
      +-----+
      '-DENY-----+'
      '-SAF resname-'
```



SAF



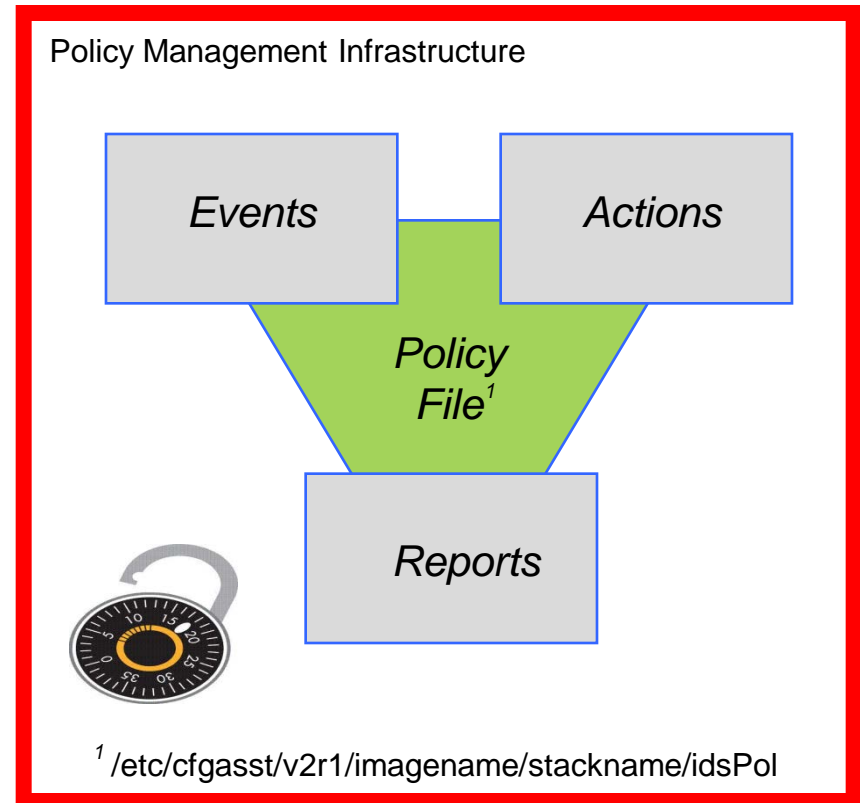
Source: IBM z/OS V2R1 CS TCP/IP Implementation

Note – TCP/IP Profile DECK, **IPSECURITY Keyword** on the IPCONFIG Statement

# Legacy Security is Just Not Enough!

## Exploiting the Policy Management Infrastructure!

- ✓ Management Policies are a pre-defined set of network Events, corresponding reply Actions, related Notifications and Reports.
- ✓ Policy files are created and maintained using the z/OSMF Configuration Assistant, or the PC-based Configuration Assistant for the z/OS Communication Server. (Gone in V2R1)
- ✓ The same Policy Configuration can be applied across multiple IP Stacks in the same underlying LPAR and or LPARs.
- ✓ Alternatively a Unique Policy Configuration can be deployed to each IP Stack in an LPAR.



# Legacy Security is Just Not Enough!

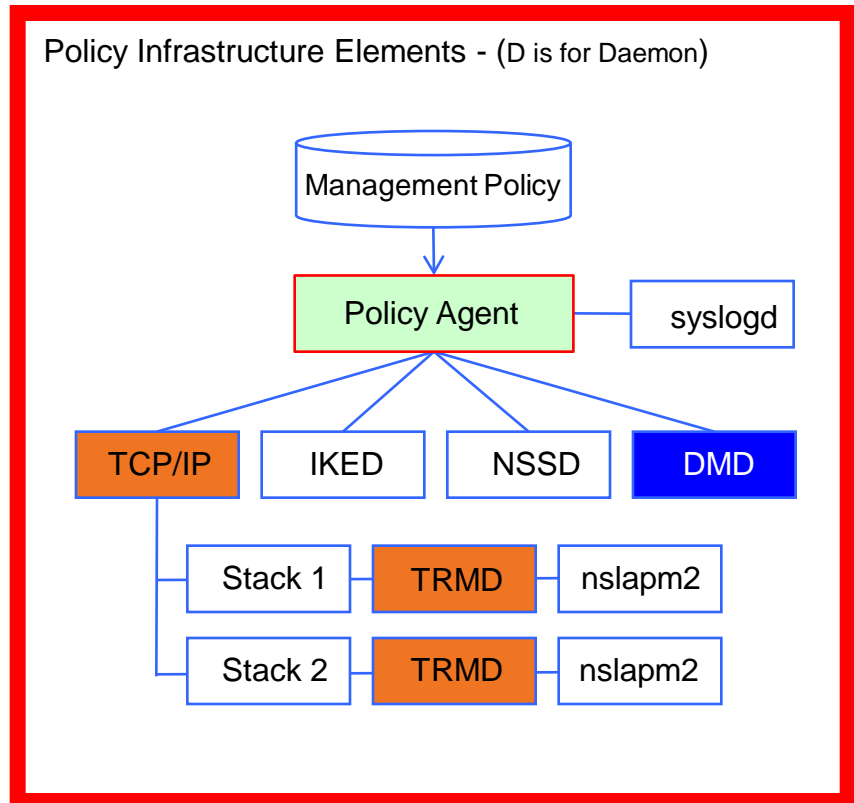
## Get Up-Close and Personal with PAGENT!

✓ PAGENT, a z/OS address space, builds the Policy Infrastructure needed by the z/OS Communication Server to support Intrusion Detection Services (IDS). PAGENT acts as a:

- ✓ Policy Server: executes on a single system and installs policies for others
- ✓ Policy Client: retrieves remote policies from the Policy Server.

✓ The Policy Infrastructure Includes:

- ✓ Internet Key Exchange (IKED)
- ✓ Network Security Services (NSSD)
- ✓ Defense Manager (DMD)
- ✓ Traffic Regulation Management (TRMD)
- ✓ The Reporting Subagent (nslapm2)



Source: V1R13 IBM Configuration Assistant for z/OS Communications Server tool

Note - In V2R1, z/OSMF Takes over these configuration functions.

# Legacy Security is Just Not Enough!

## Hardware Management Console (HMC) – Rules of Engagement?

- ✓ HMC hardware is not serviced by the user, only IBM personnel perform this task.
- ✓ HMC is not an operating platform, not usable by an end user for other application execution.
- ✓ HMC uses a “Private Network” connection(s) to one or more z Server Frames in order to perform management functions.
- ✓ HMC must be tested for network security using procedures that include periodic network scans to detect intrusion attempts.
- ✓ HMC monitors and logs the activity of its users based on their pre-assigned roles.



**HMC**

“I’m a very special,  
User Friendly GUI,  
PC based but Networked  
System Management Platform”

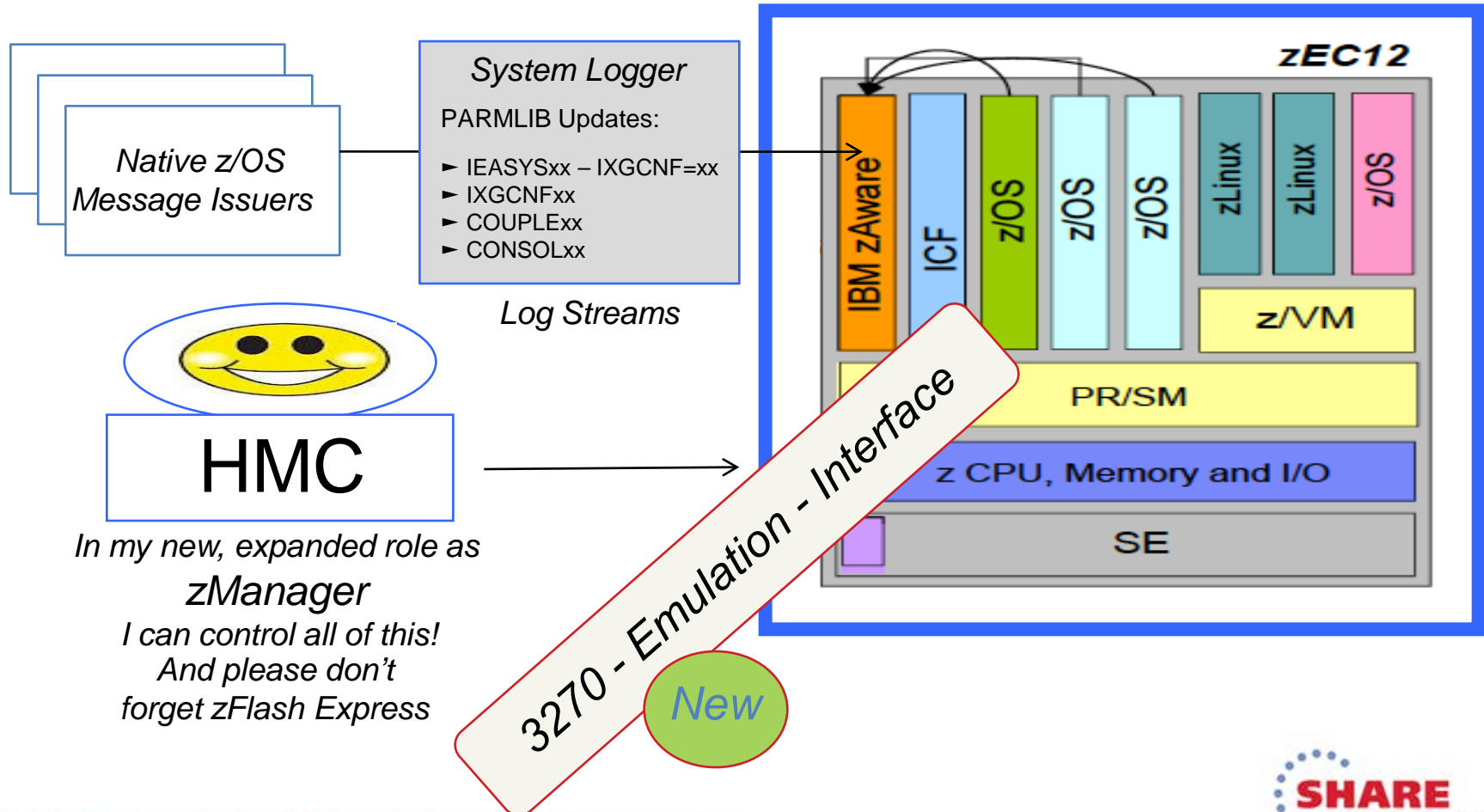
You can call me “The zManager”

Source: Introduction to the System z Hardware Management Console, [ibm.com/redbooks](http://ibm.com/redbooks)



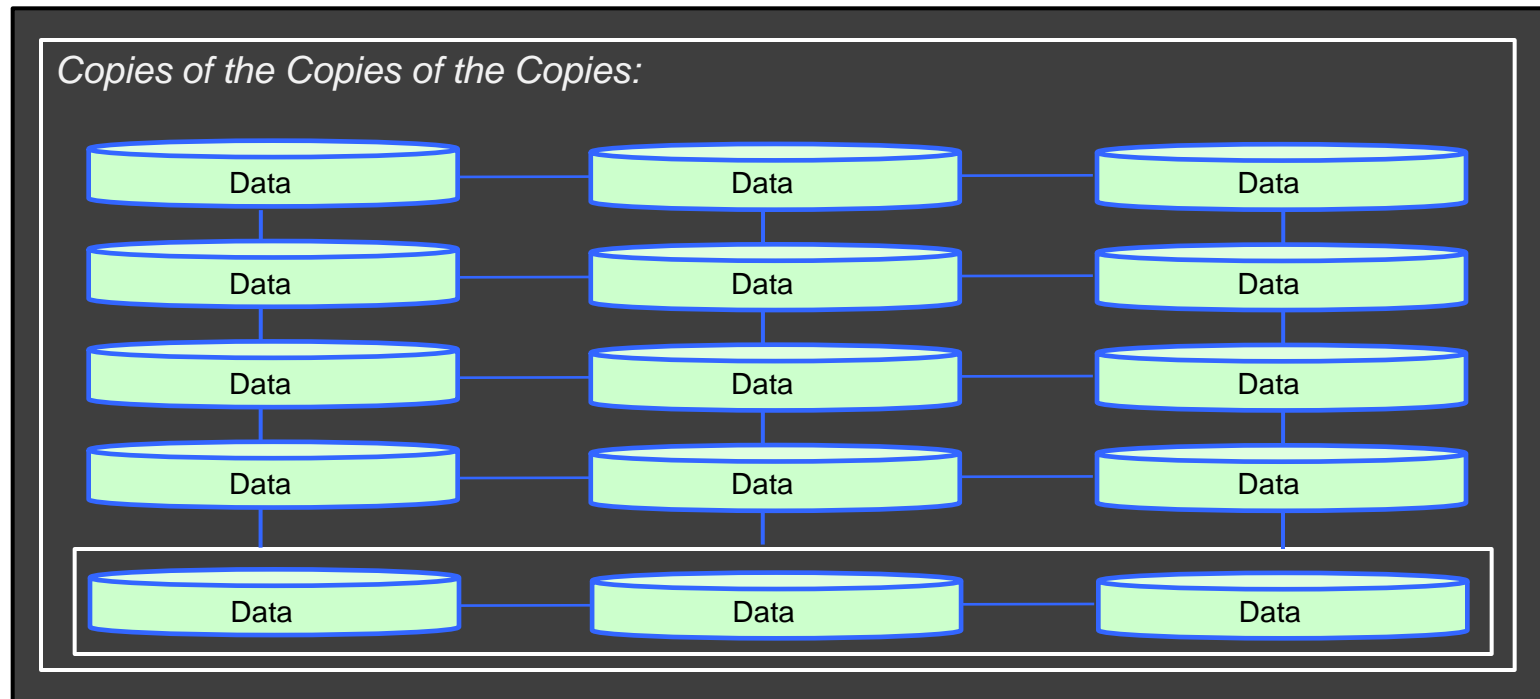
# Security - What's New in V2R1!

The HMC V2R1 - Specific Identification now Possible



# Legacy Security is Just Not Enough!

*You Cannot Protect Data that You Don't Know Exists!*



*Copies of Data now represent 70% of all Mainframe Data. Such Copies are rarely Deleted!*

# Legacy Security is Just Not Enough!

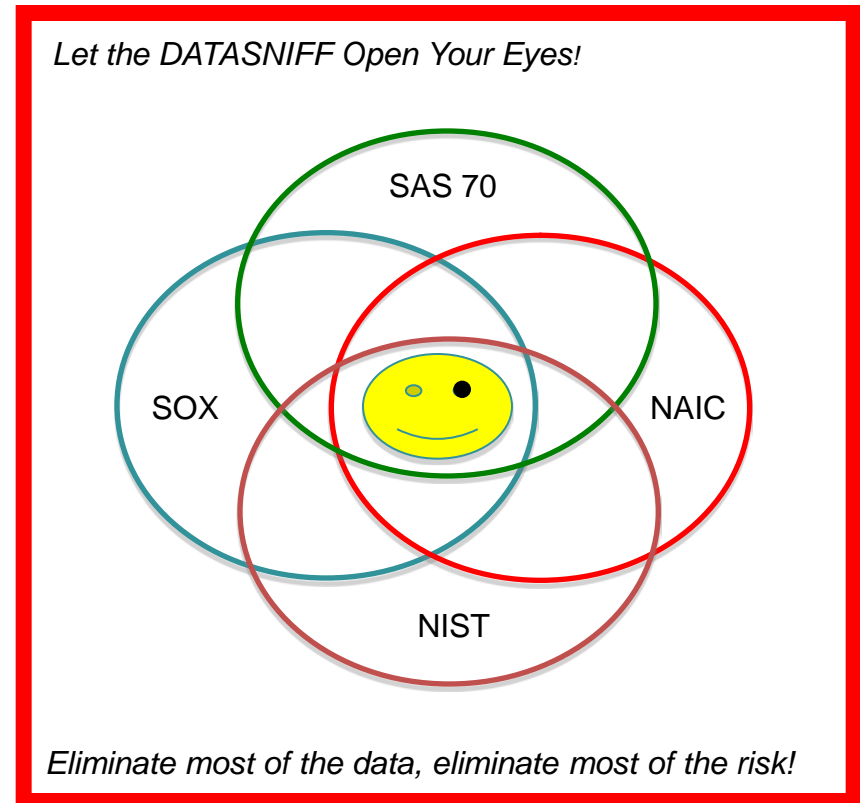


<http://www.xbridgesystems.com/about-us/>

[http://www.xbridgesystems.com/wp-content/uploads/2013/05/interview\\_primerica\\_final\\_edge\\_to-edge.pdf](http://www.xbridgesystems.com/wp-content/uploads/2013/05/interview_primerica_final_edge_to-edge.pdf)

## Regulatory Threats > Xbridge Systems

- ✓ *The right tools can help you to eliminate most of the “Copies” and in doing so the Regulatory Threat. They automatically:*
  - *Locate Sensitive Dataset Copies.*
  - *Isolate Sensitive Database Tables.*
  - *Deal with Data Migration Issues.*
  
- ✓ *Best Practices can help as well:*
  - *Datasets not recently referenced identified and stored securely.*
  - *Database tables currently in use should have access authorities validated.*
  - *Maintain a record of all Datasets by Type with a reference to the date of last use.*



# Legacy Security is Just Not Enough!



*Not Knowing the Requirements can be a Very Risky Business!*

## System z Configuration

*What “Bad News” Really Looks Like:*

*“...Although progress has been made in correcting previously reported Information Security weaknesses, system control material weaknesses continue to jeopardize the confidentiality, integrity and availability of those formal processes intended to safeguard access to financial, intellectual property and customer data..”*

*“...A material weakness is a deficiency, or a combination of deficiencies, in internal controls such that there is a reasonable possibility that material misstatement may result...”*

Audit Sub-Committed of  
The Board of Directors

### **Information Security**

#### Audit Findings:

Noted Information System Weaknesses Indicate a Need to Enhance the Internal Controls over:

- Financial Reporting
- Intellectual Property
- Customer Data

Audit 12/31/13 - Report 04/06/14

*Regulatory Compliance requires oversight to ensure that approved IS controls are in place and stay that way.*



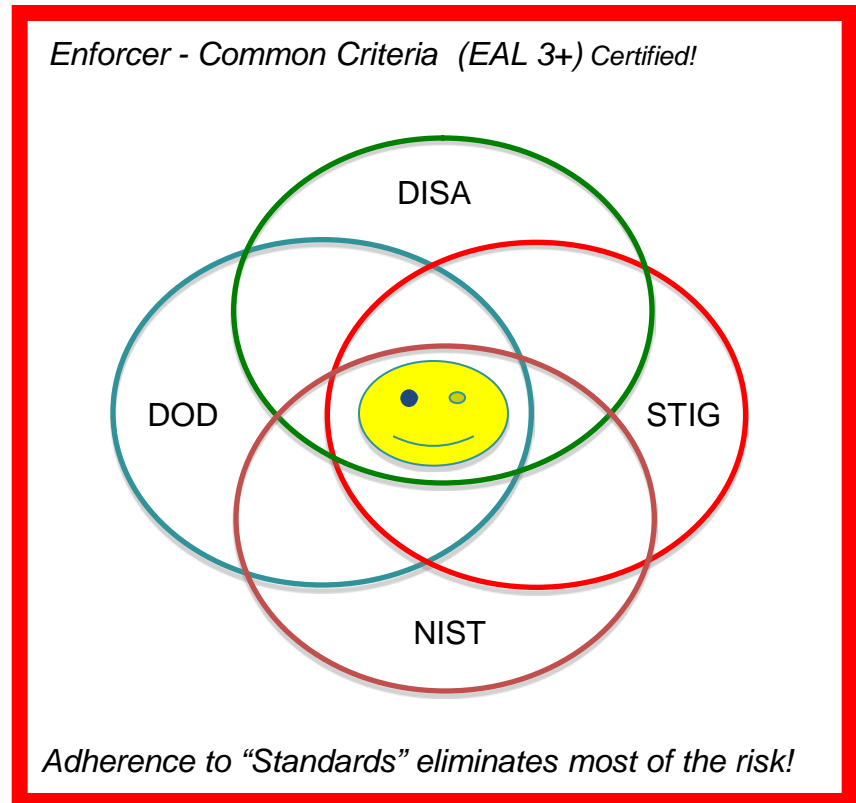
# Legacy Security is Just Not Enough!

<http://www.go2vanguard.com/>

<http://www.youtube.com/watch?v=8jEJfrNUOJM&list=UUW0IEUY-gQauvur6bWPySSA>

## Regulatory Threats > Vanguard Integrity Professionals

- ✓ Automatically detect and notify personnel when threat events on the mainframe and network occur, then respond to deviations from the security baseline with corrective actions that reassert the approved security policy.
- ✓ Satisfy the demands of Regulatory Compliance Standards (i.e. STIG) that require continuous oversight to ensure that approved IS controls (i.e. DOD) are in place and will stay that way.
- ✓ Gain confidence that their z/OS and RACF security implementations are protecting critical data and resources and adhere to z/OS best practices.



# Legacy Security is Just Not Enough!

*We Identify the Value and Erect Boundaries to Protect it:*

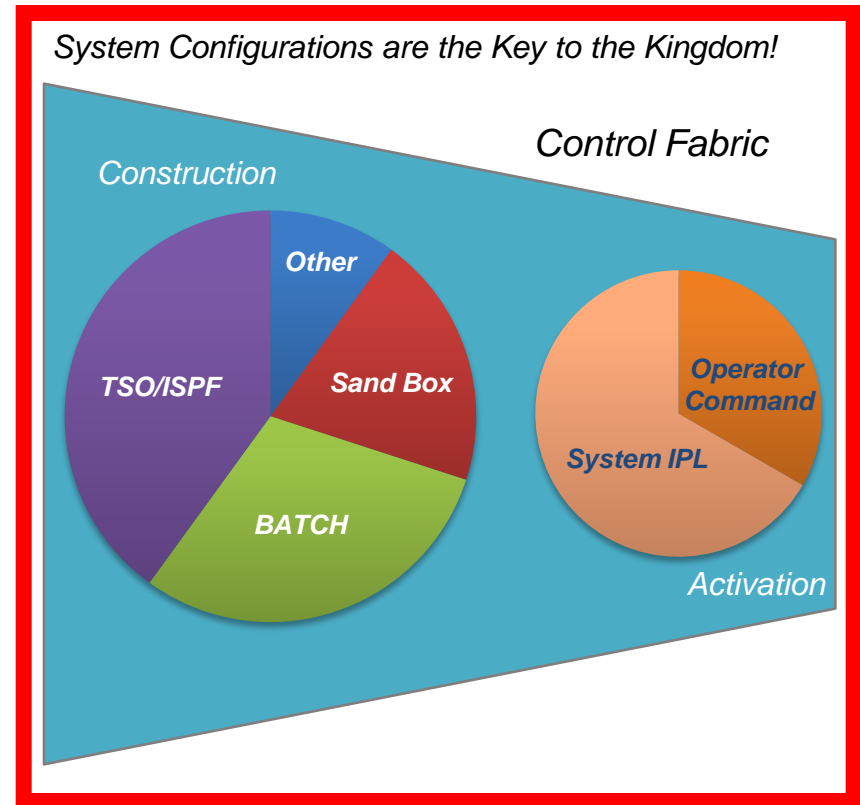
*System z Configuration*



# Legacy Security is Just Not Enough!

## Configuration Control “Gap” Makes Compliance Difficult!

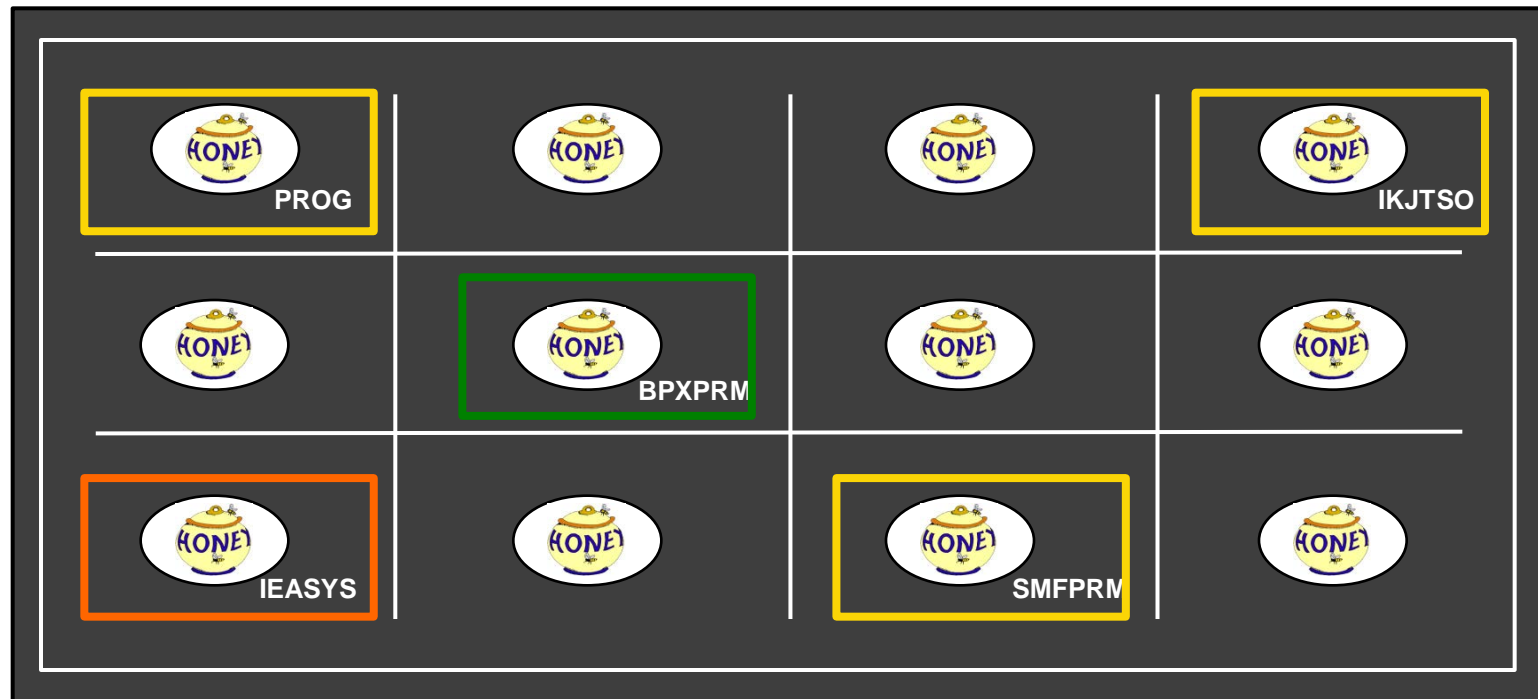
- ✓ A Control and Productivity gap exists between conventional Change Management Systems and your External Security Manager (IBM-RACF, CA-ACF2, CA-Top Secret), making it difficult to comply with System Programming and System Security best practices.
- ✓ These practices, are intended to shield the z/OS System Configuration from unauthorized and/or undocumented changes but more often than not result in findings of non-compliance with industry and regulatory configuration control requirements.
- ✓ Without Adequate Operating System Controls all Other System z Controls become Questionable!



# Legacy Security is Just Not Enough!

*We Identify the Value and Erect Boundaries to Protect it:*

System z Configuration





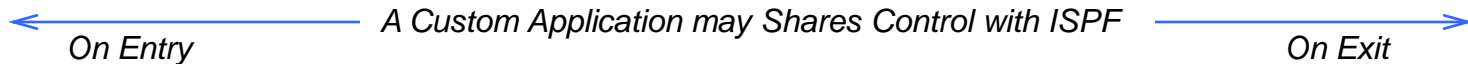
# Legacy Security is Just Not Enough!



We Identify the Value and Erect Boundaries to Protect it:

```

EDIT      SYS1.IPLPARM(LOADAC) - 01.00          Columns 00001 00072
***** Top of Data *****
==MSG> -Warning- The UNDO command is not available until you change
==MSG>      your edit profile using the command RECOVERY ON.
000001 IODF      99 SYS1
000002 SYSCAT    ZDSYS1113CCATALOG.Z113.MASTER
000003 SYSPARM   AC
000004 IEASYM    00
000005 NUCLST    00
000006 PARMLIB   USER.PARMLIB                  ZDSYS1
000007 PARMLIB   ADCD.Z113.PARMLIB             ZDRES1
000008 PARMLIB   SYS1.PARMLIB                 ZDRES1
000009 NUCLEUS   1
000010 SYSPLEX   ADCDPL
***** Bottom of Data *****
    
```



- Take Over Control from ISPF
- Check for “Out of Policy” Changes
- Make a Temporary Member Backup
- Check Conditional Access Rights

- Limit use of Copy, Submit, etc.
- Enforce your Doc Standards
- Supplemental Commands
- Access to Restore Points
- Sysplex-Wide Impact Analysis
- Full Member Change History
- Change Testing and Validation

- Detect if Member has Changed
- Enforce Documentation Standards
- Record/Backup/Notify Changes
- Return Control to ISPF

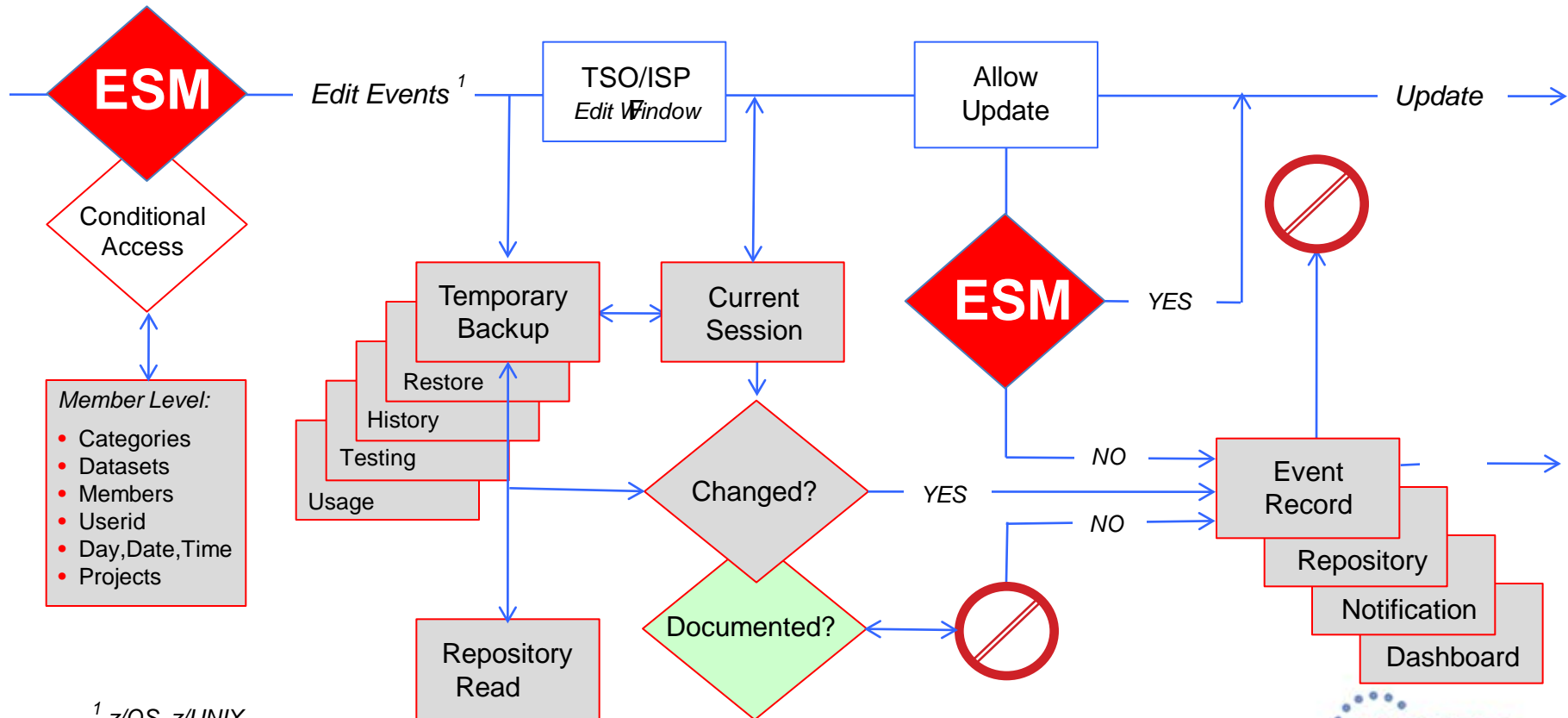


# Legacy Security is Just Not Enough!



*We're all under Attack! > Internal Threat > Closing "The Gap"*

*zEnterprise System Integrity - EDIF Services - Improving Work Flow*



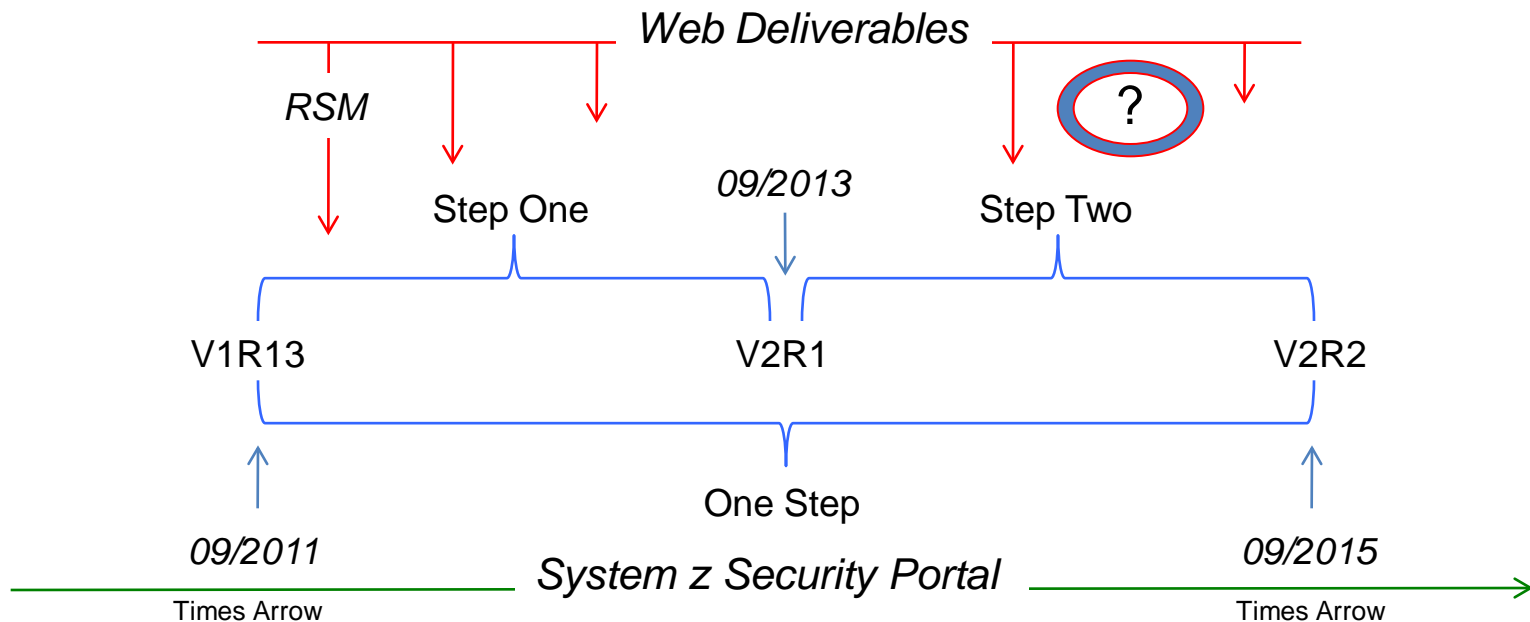
<sup>1</sup> z/OS, z/UNIX



# Legacy Security is Just Not Enough!



Get to V2R1 ASAP, and Stay Up-to-date, Please!



The System z Security Portal is intended to help you stay current with security and system integrity fixes by providing current SMP/E HOLDDATA you can use to identify security and system integrity fixes that you might not have installed on your z/OS systems before they are marked RSU. The System z Security Portal now also provides Associated Common Vulnerability Scoring System (CVSS) V2 ratings.<sup>1</sup>

<sup>1</sup> Source: IBM United States Software Announcement 213-292 - (V2R1 Announcement)



# Legacy Security is Just Not Enough!



<http://www.first.org/cvss> and <http://en.wikipedia.org/wiki/CVSS>

## System z Security Portal

A Common, Standardized, Free Vulnerability Scoring System (CVSS)

- ✓ Provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of 3 groups:
  - *The Base group represents the intrinsic qualities of a vulnerability.*
  - *The Temporal group reflects the characteristics of a vulnerability that change over time.*
  - *The Environmental group represents the characteristics of a vulnerability that are unique to any user's environment.*
- ✓ From each Group the following is produced:
  - *A numeric score ranging from 0 to 10, and*
  - *A Vector, a compressed textual representation that reflects the values used to derive the score.*
- ✓ This scoring process enables IT managers to more productively evaluate, recognize, prioritize and resolve System Threats across the entire organization.

*FIRST = Forum of Incident Response and Security Teams*

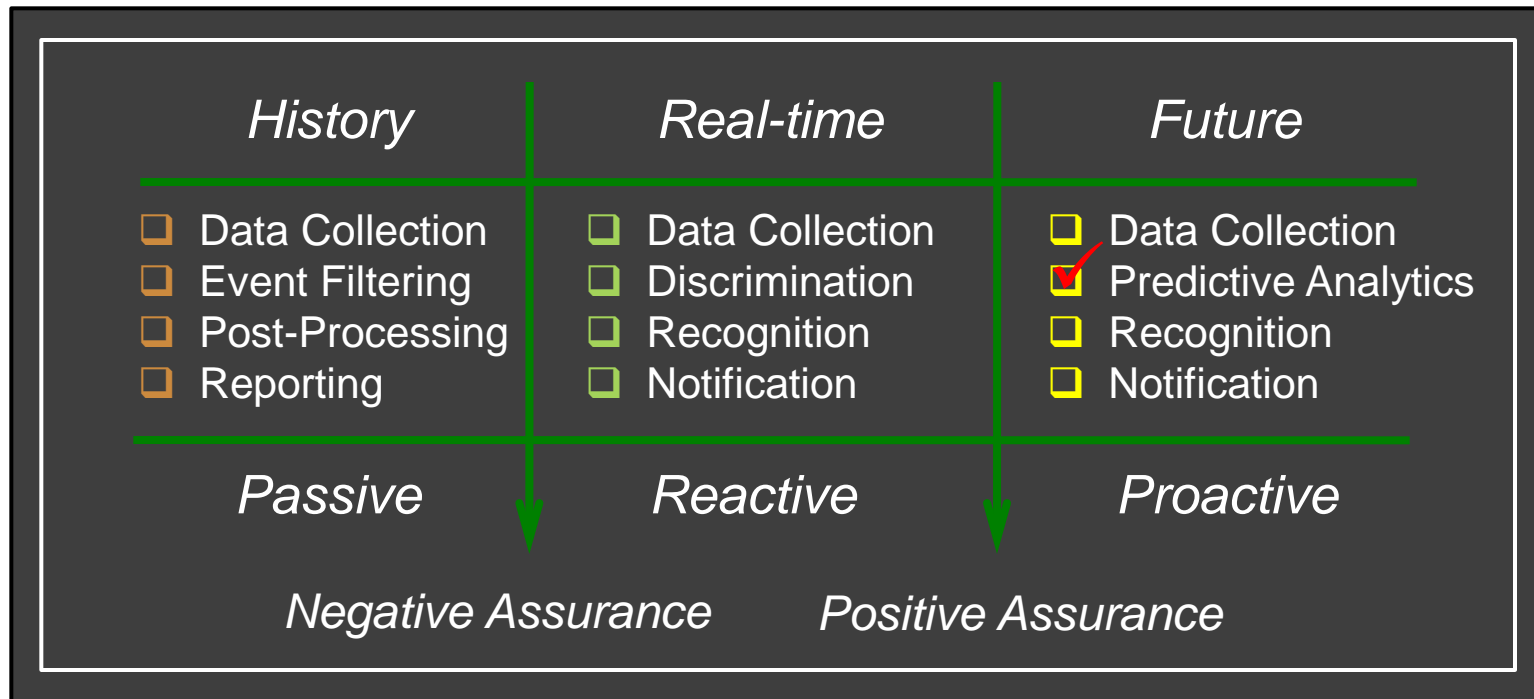


# Legacy Security is Just Not Enough!



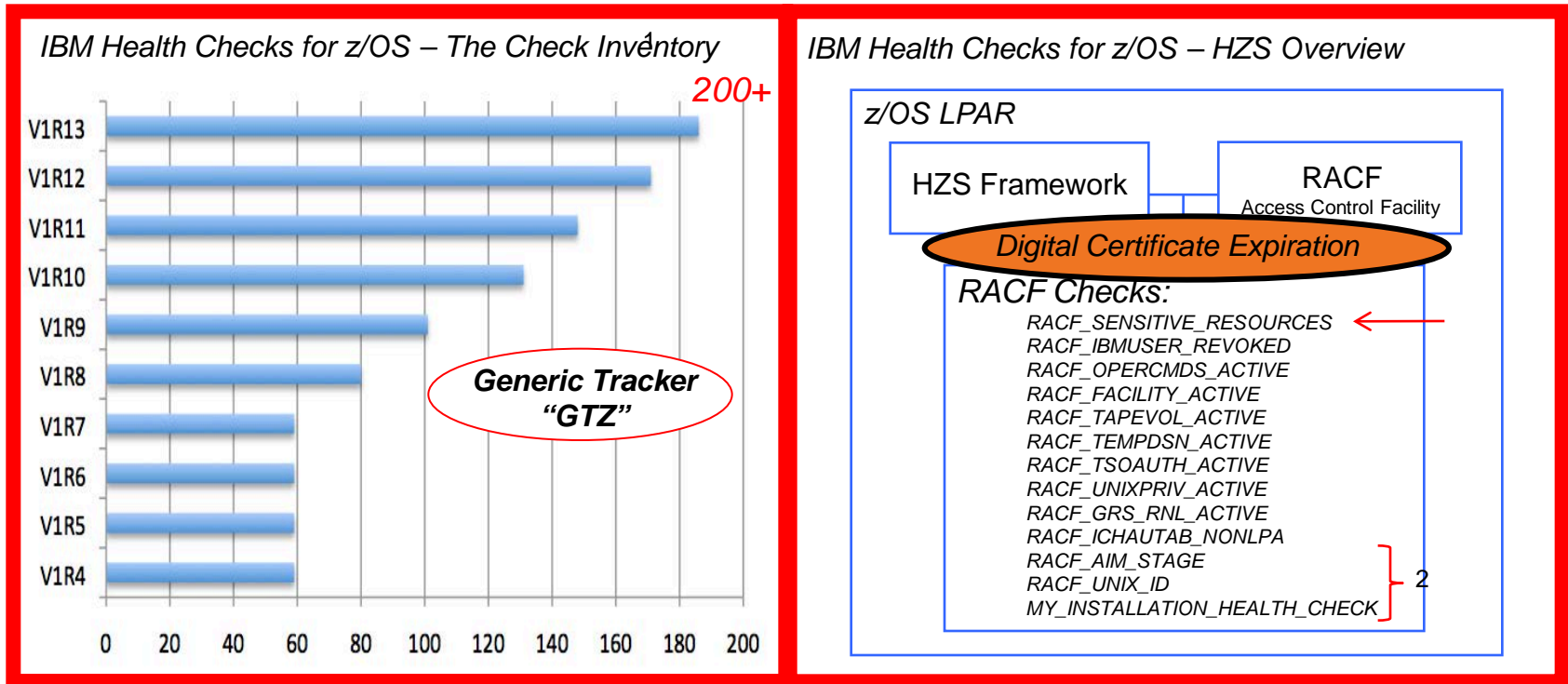
## The Future of Security > Predictive Failure Analysis

System z Configuration



# Legacy Security is Just Not Enough!

The Future of Security > Health Checker > A Security Necessity



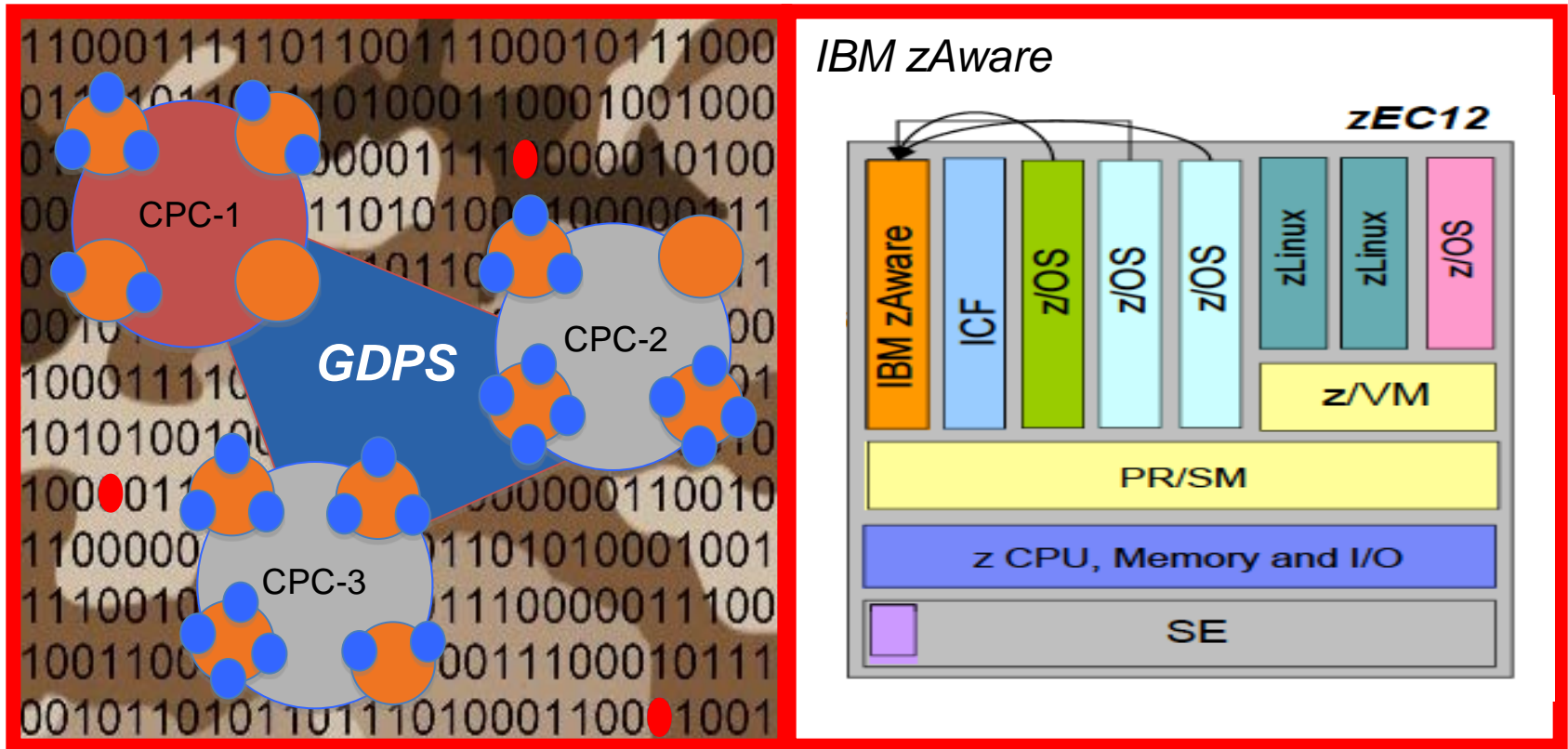
<sup>1</sup> zZS18 – The Latest in IBM Health Checker for z/OS - Marna Walle, IBM Corporation

<sup>2</sup> Mark Nelson, z/OS Security Server (RACF) Design and Development - APAR OA37164



# Legacy Security is Just Not Enough!

*The Future of Security > Self-Aware, Self-Healing, Automated!*



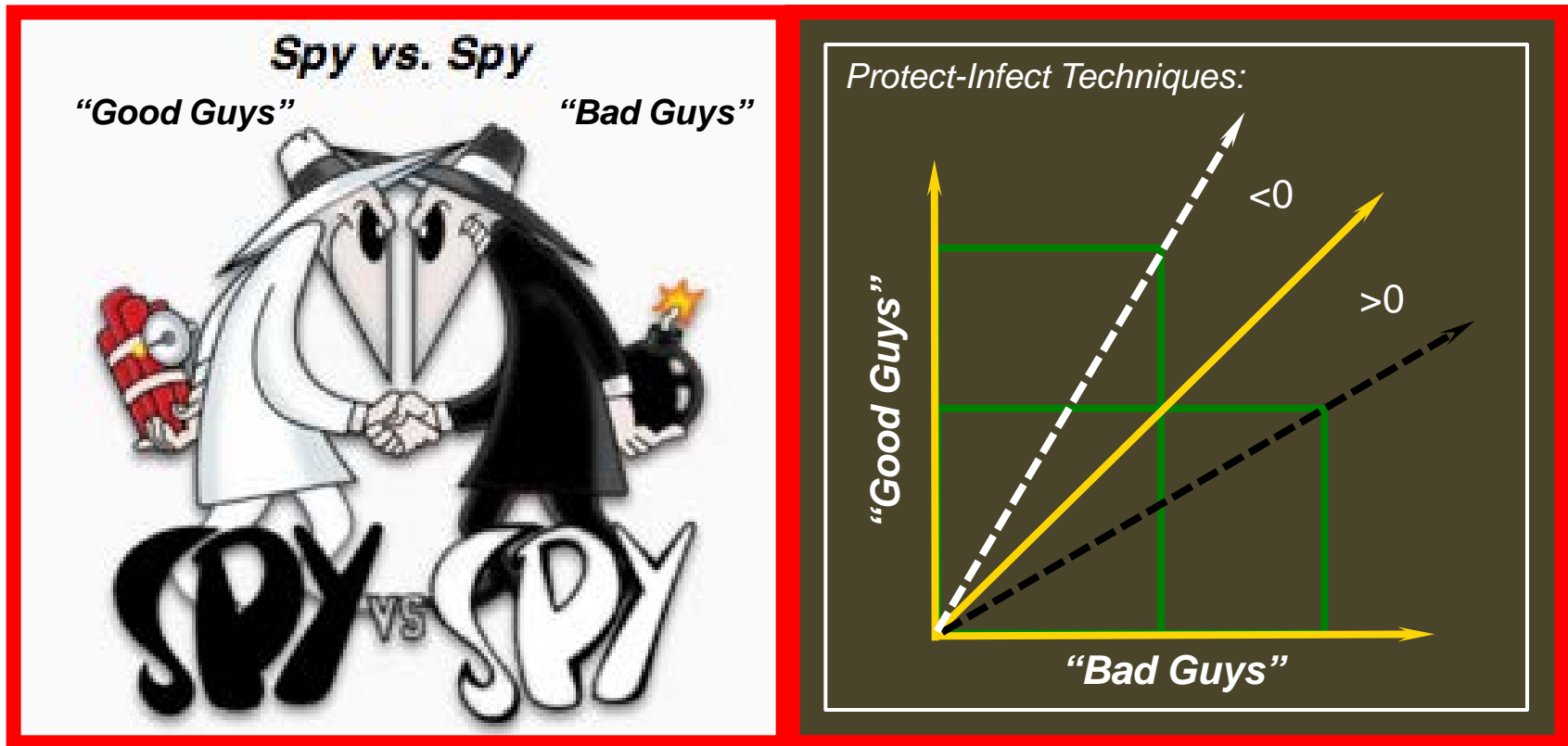
Sources: *The Father of IT Security, Founder of SHARE Security Project - Barry Schrage* President, Xbridge

# Legacy Security is Just Not Enough!

[http://en.wikipedia.org/wiki/Advantage\\_\(cryptography\)](http://en.wikipedia.org/wiki/Advantage_(cryptography))

<http://www.zdnet.com/mega-to-fill-secure-email-gap-left-by-lavabit-7000019232/>

*The Goal is to Reduce an Adversary's Advantage to "Zero"!*



*A System is Considered Secure when "Bad Guys" have a Negligible Advantage over "Good Guys".*

# Legacy Security is Just Not Enough!



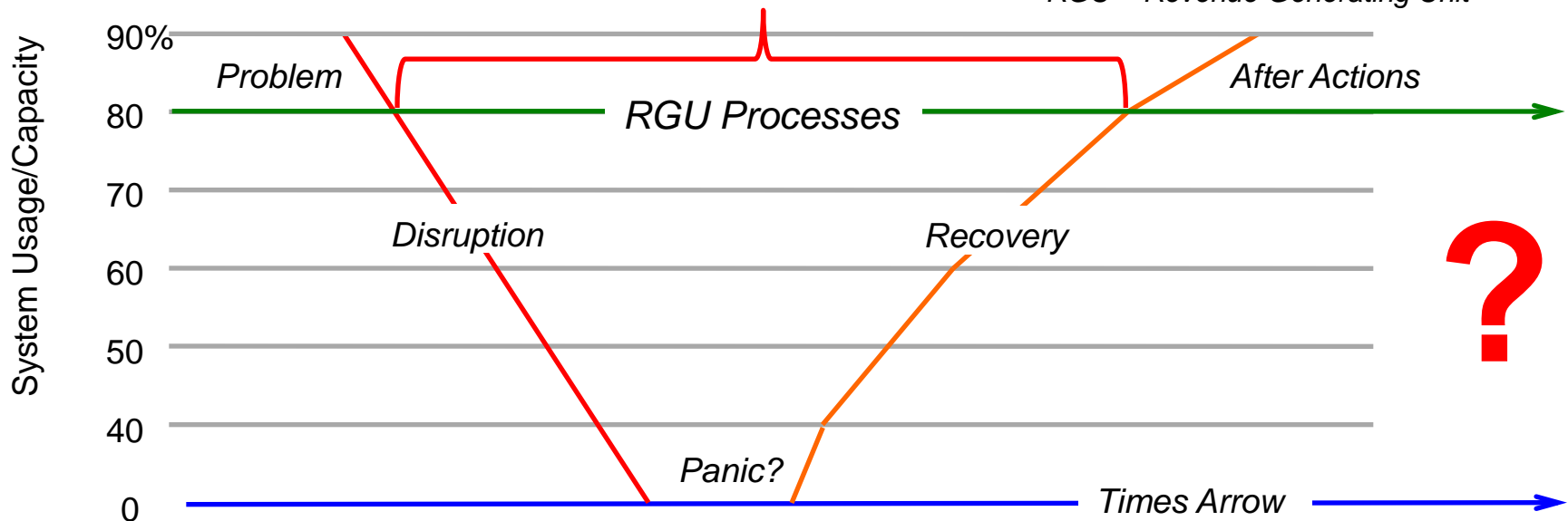
Security - What's New in V2R1 - Thursday, March 13, 2014 - 8:00AM

*This is all about RAS - Reliability, Availability and Securability*



The Bottom !

RGU = Revenue Generating Unit



*“...tracking and installing security and system integrity fixes will help to mitigate risk in the System z Environment. Recommended Service Upgrades (RSUs) help to minimize your exposure to security threats and system integrity issues.” What level are you at?*



# Legacy Security is Just Not Enough!



*Session Evaluation - Session Number - 14797*



Paul R. Robichaux  
NewEra Software, Inc.  
prr@newera.com

Monday, March 10, 2014 - 4:30PM  
Platinum Ballroom Salon 1  
Anaheim Marriott Hotel

Session Number - 14797



Visit [www.SHARE-SEC.com](http://www.SHARE-SEC.com)  
for more information on  
the SHARE Security &  
Compliance Project

