

# Protecting Your IBM i from Administrative Risks

Terry Ford  
[taford@us.ibm.com](mailto:taford@us.ibm.com)



## Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. **No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access.** IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. **IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.**



# IBM Security

# Industry Observations

## Sony Breach Has Cybersecurity Industry Scrambling for Answers

By Chris Nolter

12/05/14 - 04:31 PM EST

NEW YORK -- The baffling, prolonged cyber-breach at **Sony** highlights the frailty of corporate networks, if a string of high-profile attacks against **Home Depot**, **Neiman Marcus**, **Target**, **Bank of America** and others.

The Sony hack breaks the mold of some of the recent cases, in which cybercriminals looted troves of customer information and in some cases credit card details.

"In the old days it was kind of like this social misfit hacker stereotype who was largely self-taught. A computer geek," said Norwest Venture Partners managing partner Matt Howard, who was the first general manager of security at Cisco Systems. "Now it has become extremely professionalized."

Nation states and criminal groups have recruited sophisticated computer scientists. The goal is not to infect a legion of computers worldwide with a signature worm, but to target a select organization, inhabit its systems and collect sensitive data for political or financial ends.

The attackers also posted archive files online containing at least 25 gigabytes of data from Sony's network. [**Update:** in an e-mail to Ars that included a link to an archive of some of the stolen Sony Pictures data, an individual claiming to be "the boss" of the attackers known as GOP claimed that "tens of TB" of files had been exfiltrated and would be shared as soon as possible.] Some of those files included Excel spreadsheets and screen grabs from mainframe terminal sessions including employee payroll and medical data.

## Have We Entered the Age of Brand Terrorism?

By Robert Klara, Technology Today – Nov 30, 2014

In October, FBI director James Comey no doubt caused a sleepless night for many an executive when he told CBS' 60 Minutes that "there are two kinds of big companies in the United States ... those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese."

Comey was saying, more or less, that every U.S. corporation has already been attacked—a fact that lengthens the list of brands whose high-profile breaches have made news lately, among them Neiman Marcus, The Home Depot, Dairy Queen, Target and Kmart. According to research from cyber security firm Trustwave large retail brands now make up close to half of the hacking targets out there.

But behind the headlines and the fear of stolen identities, observers say there's something even darker going on. In the old days, hacking used to be about making mischief and stealing money. Hackers who targeted "America" mostly attacked federal agencies. Today, increasingly, it's companies that symbolize America on the global stage, and attacking the U.S. means attacking its brands. Are we experiencing an age of brand terrorism?

Herjavec believes that hacking has entered a new stage in which the perpetrators are state actors whose goals have moved beyond mere larceny. "In the last 24 months, we've been seeing an absolute surge of state-sponsored cyber attacks," he said. "We're no longer dealing with individuals who want to steal your money. We're dealing with foreign national governments that want to hurt America." And in an age of viral content, there are few better ways to make the country look vulnerable than to cut down its famous brand names.

Nobody's arguing that money isn't behind at least some of the high-profile hacking. The malware implanted in Target's mainframe just before last year's holiday shopping season siphoned off as many as 40 million credit card numbers. The attack on The Home Depot two months ago affected 56 million. But according to Herjavec's data, only 40 percent of computer attacks are financially motivated.

According to the FBI, state-sponsored cyber attacks are often launched to steal intellectual property, but the chaos caused by a breach has become an end in itself. Speaking at a symposium held at New York's John Jay College of Criminal Justice earlier this month, K2 Intelligence executive director

# Industry Observations

## FBI Warns of Rise in Disgruntled Employees Stealing Data

By  
Devlin Barrett – Wall Street Journal  
Sept. 23, 2014 7:53 p.m. ET

WASHINGTON—The Federal Bureau of Investigation issued a warning to U.S. companies Tuesday about a recent spike in the number of disgruntled employees stealing company information sometimes to try to extort money from their old bosses.

"There has been an increase in computer network exploitation and disruption by disgruntled and/or former employees," the FBI and Department of Homeland Security wrote in the computer security bulletin.

Such employees have led to "several significant FBI investigations in which individuals used their access to destroy data, steal proprietary software, obtain customer information, purchase unauthorized goods and services using customer accounts, and gain a competitive edge at a new company," the bulletin continued.

"Additionally, multiple incidents were reported in which disgruntled or former employees attempted to extort their employer for financial gain by modifying and restricting access to company websites, disabling content management system functions, and conducting distributed denial of service attacks."

## Hey CIO, CEO: You're Leaking Data

By Virginia Backaitis | Nov 3, 2014

Of all the vital responsibilities C-level executives have, keeping data secure is a big one. Especially today, when many managers consider data to be the "new gold" or the "new oil"... feel free to add your own metaphor.

The Harvard Business Review has published a number of articles that say that those who leverage their data best will be at a competitive advantage.

"Data-driven decisions tend to be better decisions. Leaders will either embrace this fact or be replaced by others who do," wrote Andrew McAfee and Erik Brynjolfsson in an article in 2012.

But what happens when your strategic data is at someone else's disposal as well? And we're not just talking about data that's been hacked or deliberately open sourced and shared with select parties, but also the stuff that your employees lob over company firewalls for convenience sake.

If you're a manager this kind of behavior should be cause for concern because we could be talking about the very strategic assets and intellectual property you've been charged to protect.

### Time to Reassess

Left unchecked, this situation isn't likely to get better. And, it goes without saying, that it will cause problems. What's an IT manager to do?

While reigning in shadow IT may seem like the obvious answer, Sanjay Beri, CEO and co-founder of Netskope said that it's not enough.

# Industry Observations

## Target CEO out as data breach fallout goes on Hadley Malcolm, USA TODAY May 5, 2014

Target President and CEO Gregg Steinhafel resigned Monday as the retailer continues to recover its image nearly five months after a massive holiday-season data breach.

Steinhafel also resigned as chairman of the board of directors. John Mulligan, Target's chief financial officer, will serve as interim president and CEO, while current board member Roxanne Austin will take over as interim chair.

"Today we are announcing that, after extensive discussions, the board and Gregg Steinhafel have decided that now is the right time for new leadership at Target," a company statement posted on its website Monday morning says.

Steinhafel, a 35-year veteran of Target, will serve as an advisor during the transition. In an SEC filing Monday, Target said Steinhafel is entitled to severance pay but that the board "has not made a final determination on other compensation-related aspects" of Steinhafel's departure.

Target hired executive recruitment firm Korn Ferry to assist in finding its next CEO.

Some say Steinhafel's resignation should have come sooner. "It would have been better to start the year with fresh eyes and a fresh approach," says Brian Sozzi, CEO of Belus Capital Advisors.

## Protecting Data "At Rest" – Encryption Is Not Enough

- Computer data spends most of its life "at rest." Whether it is stored on your desktop hard drive or somewhere in the cloud, "data at rest" is any data that is not, at a particular moment, being transmitted or acted upon.
- Encryption is often regarded as a main line of protection for sensitive data. But historically encryption has been associated with *messages* – that is to say, "data in motion," being transmitted, and encrypted to protect it from eavesdroppers during the transmission process.
- Computer technology reinforces this association of encryption with "data in motion." Encryption keys can be created on the fly, and destroyed when the message-sending process is completed. But "data at rest" is inherently persistent, and any encryption keys used to protect it must also be persistent. The key must be stored along with the data it protects, and is therefore itself vulnerable to theft. (If a key is encrypted, some other non-encrypted key is needed to make use of it.)
- In particular, encryption offers no protection against unauthorized use of data by insiders, who have access to the keys, and thus to the data a key is supposed to protect. Other means of protection are therefore needed to ensure the security of "data at rest."

# Industry Observations

No easy fix to most risks unless you just unplug. Majority of risks require a extensive root cause and dependency analysis followed by detailed planning, testing and implementation of fixes and mitigating controls.



# What's the Data Worth?

- Is the data an asset?
  - YES!!!
  - <https://www-03.ibm.com/press/us/en/pressrelease/24585.wss>
- Is it listed on the books?
  - Probably Not
- What's it worth?
  - Most likely more than all those other IT assets (servers, workstations, routers, switches, networks etc.) combined!





# Cost of Insecurity

## BUSINESS CONTINUITY

DISASTER RECOVERY/BUSINESS CONTINUITY RANKS #4 ON THE LIST OF THE TOP BUSINESS ISSUES AFFECTING IT



**\$5,000/  
MINUTE**

AVERAGE COST  
**OF DATA  
CENTER  
DOWNTIME**

## COMPLIANCE

..... COST OF .....

COMPLIANCE



**\$222**

PER EMPLOYEE

NON-COMPLIANCE



**\$820**

PER EMPLOYEE



COPPA UK DATA PROTECTION ACT 1988 U.K. BRIBERY ACT  
FOREIGN CORRUPT PRACTICES ACT SARBANES-OXLEY  
DO NOT TRACK INFORMATION TECHNOLOGY RULES  
HIPPA EUROPE DATA PROTECTION DIRECTIVE DODD-FRANK  
SAFE HARBOR ACT PERSONAL INFORMATION PROTECTION LAW

**14,215**

REGULATORY ANNOUNCEMENTS IN 2011

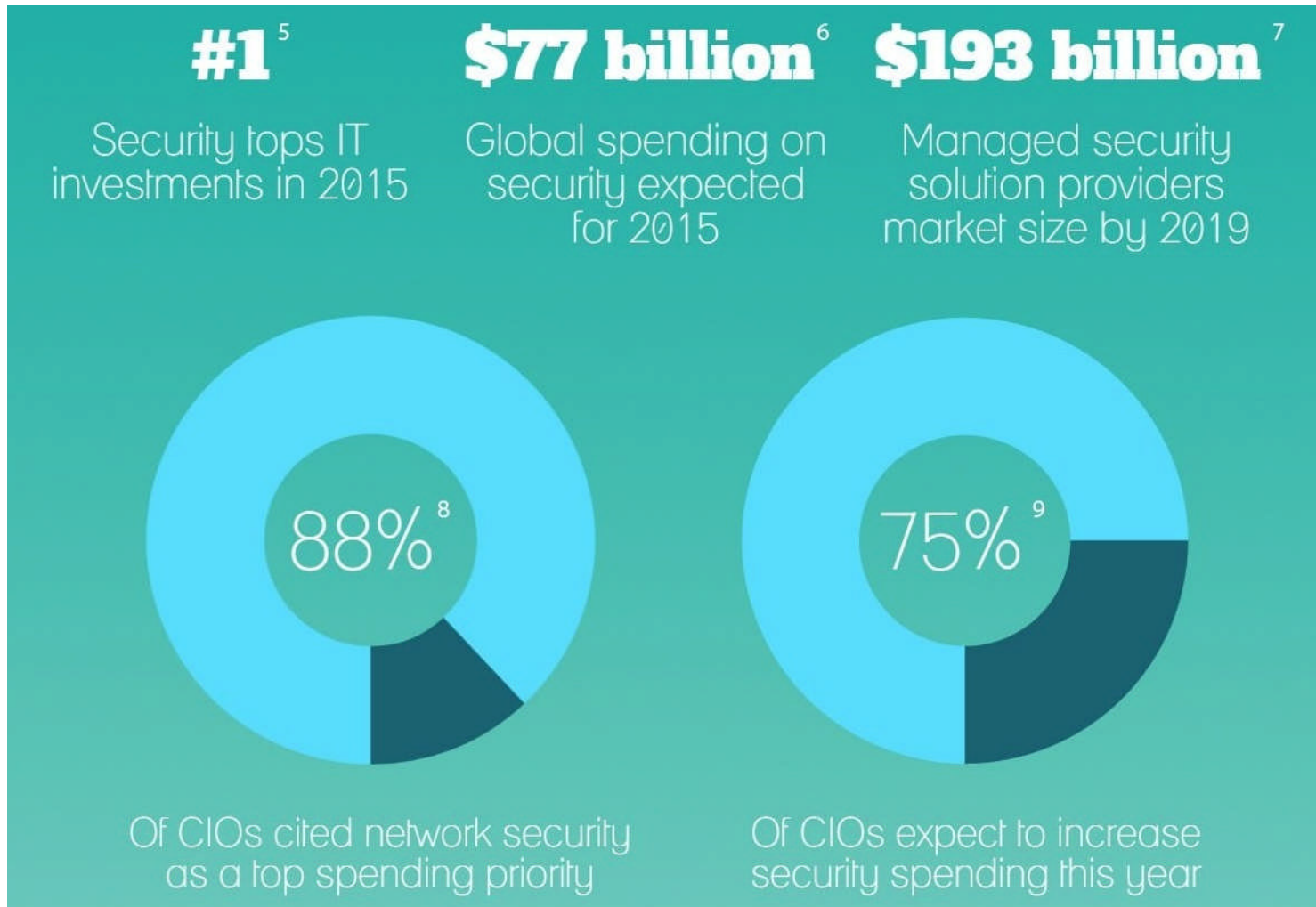
### SOURCES

Ponemon Institute 2011 Cost of Data Breach Study: United States  
Verizon 2012 Data Breach Investigations Report  
Reuters, <http://reut.rs/zrcec>  
Symantec Internal Threat Report 17  
WIRED, <http://www.wired.com/threatlevel/2012/05/flame/all/1>  
European Commission-Justice, Data Protection  
Ponemon Institute Second Annual Benchmark Study on Patient  
Privacy and Data Security

ISACA 2011 Top Business/Technology Issues Survey  
Symantec 2012 SMB Disaster Preparedness Survey  
Ponemon Institute True Cost of Compliance Report  
Thomson Reuters State of Regulatory Reform 2012  
eWeek, <http://www.eweek.com/c/a/IT-Infrastructure/Unplanned-IT-Downtime-Can-Cost-5K-Per-Minute-Report-549007/>



# What Is Being Done!



<sup>5</sup> "2015 Piper Jaffray CIO Survey"

<sup>6</sup> MarketsandMarkets 2014 survey

<sup>7</sup> Gartner/FierceIT Security

# Risk Conclusions

- Today, the majority of organizations could not operate if they were to lose their computing capabilities.
- For each risk, you can choose to:
  - Reduce the risk
  - Transfer the risk
  - Accept the risk
  - Avoid the risk
- Each choice has a cost. You can budget for risk reduction, transfer or avoidance, but you may find it difficult if not impossible to budget for the acceptance of risk and the associated pain and possible loss of industry reputation if the risk is exploited and data is stolen or compromised.

# Special Authorities

# Special Authorities (Privileged Users)

Privileged users should be minimized, tightly controlled and audited.  
Special Authority Privileges can come from several places

- Defined in the user profile's special authority value
- Inherited from one or more groups
- Unsecured Adopted and Swapped Authority Programs
- \*PUBLICly and Privately authorized user profile accounts

# \*JOBCTL Special Authority

The Job control (\*JOBCTL) special authority allows a user to change the priority of jobs and of printing, end a job before it has finished, or delete output before it has printed. \*JOBCTL special authority can also give a user access to confidential spooled output, if output queues are specified OPRCTL(\*YES).

Job control (\*JOBCTL) special authority allows the user to:

✓ Stop subsystems:

```
ENDSBS SBS(QINTER) OPTION(*IMMED) ENDSBSOPT(*NOJOBLOG)
```

✓ Perform an initial program load (IPL).

# \*SPLCTL Special Authority

Spool control (\*SPLCTL) special authority allows a user to perform all spool control functions, such as changing, deleting, displaying, holding and releasing spooled files.

The user can perform these functions on all output queues, regardless of any authorities for the output queue or the OPRCTL parameter for the output queue. \*SPLCTL special authority also allows the user to manage job queues, including holding, releasing, and clearing the job queue regardless of any authorities for the job queue or the OPRCTL parameter for the job queue.

**Risks:** The user with \*SPLCTL special authority can perform any operation on any spooled file in the system. Confidential spooled files cannot be protected from a user with \*SPLCTL special authority.



## **\*IOSYSCFG Special Authority**

Allows a user to configure and manage system configuration objects (e.g. line descriptions, TCP/IP attributes, host tables, interfaces etc.).

## **\*SAVSYS Special Authority**

Allows a user to save and restore any object on the system, regardless of the user's authority to that object. This includes the ability to clear (\*FREE storage) any object saved on the system.

## **\*AUDIT Special Authority**

Allows users to change system values that affect auditing (e.g. turn auditing on/off) and to change user and object auditing values and manage other aspects of system, object and user auditing.

## \*SECADM Special Authority

Allows a user to create, change and delete user profiles. Also enables a \*SECADM administrator to:

- ✓ Add users to the system distribution directory
- ✓ Add and remove access codes to the system
- ✓ Grant and remove a user's access code authority
- ✓ Display authority for folders and documents
- ✓ Delete documents and folders

## \*SERVICE Special Authority

Allows a user to start system service tools, debug programs and perform trace functions.

# \*ALLOBJ Special Authority

All-object (\*ALLOBJ) special authority allows a user to access any resource on the system. Even if the user has \*EXCLUDE authority to an object, \*ALLOBJ special authority still allows the user to access the object.

A user with \*ALLOBJ authority cannot directly perform operations that require another special authority. For example, \*ALLOBJ special authority does not allow a user to create another user profile, because creating user profiles requires \*SECADM special authority. However, a user with \*ALLOBJ special authority can submit a batch job to run using a profile that has the needed special authority. Giving \*ALLOBJ special authority essentially gives a user access to all functions on the system.

**Risks:** \*ALLOBJ special authority gives a user extensive authority over all resources on the system. The user can view, change, or delete any object. The user can also grant to other users the authority to use objects.

# \*PUBLICly and PRIVATEly Authorized Profiles

# \*PUBLIC authorized profiles

Three IBM supplied User Profile objects are shipped with \*PUBLIC authority that is not \*EXCLUDE. They are:

- QDBSHR
- QDBSHRDO
- QTMPLPD

Any User Profile object other than the 3 listed above that grants \*PUBLIC or PRIVATE authorities should be carefully examined to determine the risk level.

**PRT PUBAUT OBJTYPE(\*USRPRF)**

# Default profile \*PUBLIC authority

User Profile objects should be created with the default authority equal to \*EXCLUDE. The following slides display a User Profile object and the recommended authorities.

## Note:

- The \*PUBLIC has \*EXCLUDE
- The Owner has \*ALL
- The User has USER DEF authority to its own profile

```
CRTUSRPRF USRPRF(APENDUSER) PWDEXP(*YES) LMTCPB(*YES) AUT(*EXCLUDE)
```





# \*PUBLIC and PRIVATE Authorized Profiles

User Profile objects that grant \*PUBLIC or PRIVATE authorities to user profiles other than themselves, their owner or their group members should never:

- Have any Special Authorities
- Own application objects
- Own or have private authority to any data file that contains confidential or highly restricted information.
- Own or have private authority to any executable that accesses data files that contain confidential or highly restricted information.

# \*PUBLIC and PRIVATE Authorized Profiles

APPSECOFR is a \*PUBLIC authorized profile. It is \*DISABLED with a password of \*NONE.

APPSECOFR can be used by any authenticated user profile on the SBMJOB command or used to swap authorities using swap APIs.

Users submitting jobs as APPSECOFR will have all eight Special Authorities available and will be able to perform any function on any object on the system.

```
CHGSECAUD *NONE  
DLTJRN QAUDJRN  
CRTUSRPRF USRCLS (*SECOFR)
```

...

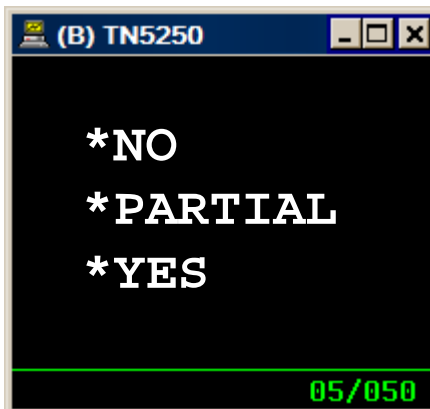
```
SBMJOB CMD(DTLIB LIB(PCIDATA)) USER(APPSECOFR)
```

```
SBMJOB CMD(CHGUSRPRF USRPRF(BRUCE) (SPCAUT(*ALLOBJ)) USER(APPSECOFR)
```

# Command Line Capabilities

# Command Line Capabilities

Pay careful attention to user's command line capabilities. The LMTCPB parameter specifies the limit to which a user can control the program, menu, current library, and the ATTN key handling program values. It also determines whether a user can run commands from a command line. Three allowed values:



**LMTCPB = \*NO:** User can change their initial program, menu and current library when signing on and in their profile with the CHGPRF command. **Any authorized command can be run from a command line.**

**LMTCPB = \*PARTIAL:** Users can change their initial menu when signing on and in their profile with the CHGPRF command. **Any authorized command can be run from a command line.**

**LMTCPB = \*YES:** Users cannot change their initial program, menu or current library. Only commands that allow limited users can be run from a command line.

# **CAUTION !**

**The Network Servers may not honor the User Profile**

**Limit Capabilities (Command Line),**

**Initial Program,**

**and**

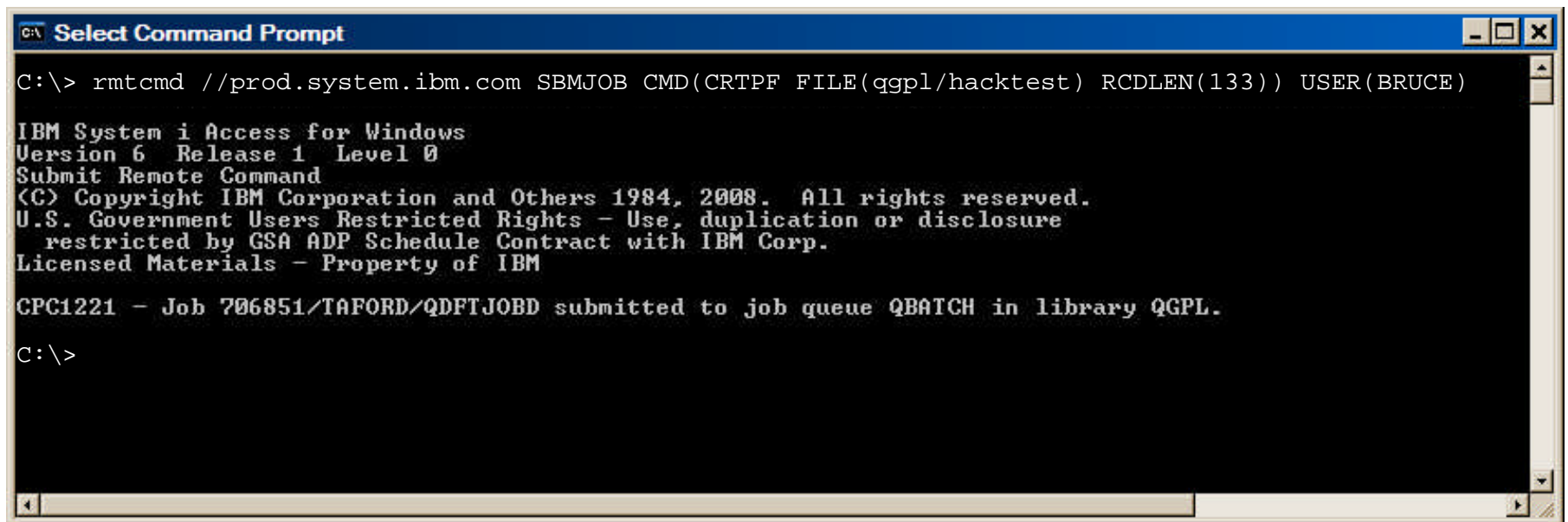
**Initial Menu parameters**

# Command Line Capabilities

## “Danger, Will Robinson!”

The DOS RMTCMD Does not honor Limited Capabilities  
(True for many other remote servers)

```
C:\> rmtcmd //prod.system.ibm.com SBMJOB CMD(CRTPF FILE(qgpl/hacktest) RCDLEN(133)) USER(BRUCE)
```



```
C:\> rmtcmd //prod.system.ibm.com SBMJOB CMD(CRTPF FILE(qgpl/hacktest) RCDLEN(133)) USER(BRUCE)

IBM System i Access for Windows
Version 6  Release 1  Level 0
Submit Remote Command
(C) Copyright IBM Corporation and Others 1984, 2008.  All rights reserved.
U.S. Government Users Restricted Rights - Use, duplication or disclosure
  restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM

CPC1221 - Job 706851/TAFORD/QDFTJOB submitted to job queue QBATCH in library QGPL.

C:\>
```



**Don't worry ...  
Simply plug in your IBM i  
and it protects your data flawlessly  
from any Network Access**

**As long as your 'network' only has these ...**



# For everyone else ...

- Network Servers are likely to be your single biggest threat
- Activities that come through the TCP servers are ubiquitous – you may not be able to tell who is downloading (or uploading), running SQL statements, or even executing remote commands
- Some servers allow command functions and IGNORE a profile's 5250 command line restriction



# For everyone else ...



# Turn off Servers you are not using

What gets started with STRTCPSVR?

- **Apache Tomcat Server**
- **Bootstrap Protocol**
- **Common Information Model Object Manager**
- **Debug Server**
- **DDM Server**
- **Dynamic Host Configuration Protocol**
- **LDAP**
- **DataLink File Manager**
- **Domain Name Server**
- **Domino**
- **Extended Dynamic Remote SQL**
- **File Transfer Protocol**
- **Host on Demand**
- **HTTP Server**
- **Internet Daemon**
- **Line Printer Daemon**
- **Management Central**
- **Net Server**
- **Network Station Login Daemon**
- **Simple Network Time Protocol**
- **On Demand Platform Authentication**
- **On Demand Server**
- **Post Office Protocol**
- **Quality of Service Server**
- **Remote Execution Servers**
- **Router Daemon**
- **Simple Mail Transfer Protocol**
- **Simple Network Management Protocol**
- **Trigger Cache Manager**
- **Telnet**
- **Trivial FTP**
- **Virtual Private Networking**
- **Webfacing Server**

# ODBC-JDBC-REXEC-RCMD-FTP-IFS Hacks

System i Scan

File Options Actions Help

cto00sc.rchland.ibm.com

Scan Run Query Capture

Library	Public	Files	Text
HLSBND	*CHANGE	2	Lee Sandstrom 3-7356
HLSHUBER	*CHANGE	1	Lee Sandstrom
HLSYNCPRF	*CHANGE	2	Lee Sandstrom
HMS	*CHANGE	345	X-Analysis/4 X-Reference Database Library
HOMDDMLIB	*CHANGE	2	Lib to manage DDM files
IASPTOOL	*CHANGE	12	
IBCQZDALIB	*CHANGE	1	NGS American
IBMLIB	*CHANGE		
IBMRST	*CHANGE		
IBMSHIP	*CHANGE		
ICCCODELIB	*CHANGE		
ICEBREAK	*CHANGE		
ICS	*CHANGE		
ICSWF	*CHANGE		
IES	*CHANGE		
IES_PTF83C	*CHANGE		
IESFILE	*CHANGE		
IESHELP	*USE		
IESMTINTR8	*USE	2	INTERFACE LIBRARY COMPILED OVER R8
IESSYN	*CHANGE	13	IES Software Standard Syn-on Library
IESWORK	*ALL	33	(C) Copyright ICC, Inc. 2003, All rights reserved.
IESKAN	*CHANGE	453	X-Analysis/4 X-Reference Database Library
IESXSP	*CHANGE	56	Innovative computing xsp library
ILEDOCS	*CHANGE	7	
ILPGMR	*USE	23	IES Standard ILPGMR library for latest Development
INFOSYSKR	*CHANGE	4	DNR Library for LMS Kerzner Request
INFILE	*CHANGE	1	
IRAT	*CHANGE	3	TEMPORARY for IRAT analysis
IRAT&&&	*CHANGE	18	TEMPORARY for IRAT analysis

- Files-Libraries retrieved
- Authorities retrieved
- File Formats retrieved
- Query capable
- Data retrieval capable

# Data Classification

Object authority is by far the most critical aspect of information security. As part of your security policy, there should be consideration for how data is classified. For many, industry regulation demands it. Data Classification is simply a mechanism which an organization uses to assign a level of sensitivity and an owner to each piece of information that it owns and maintains. The following is an example of a data classification scheme:

- **Public** everyone can read – information disclosed w/o impact
- **Internal Use** must authenticate – internal and client email
- **Confidential** exclusionary access - business, financial and technical info
- **Restricted** exclusionary access and fully audited - any info subject to restriction in access, storage or processing by law, or regulation, or by customer contract that could cause significant harm if inappropriately disclosed, accessed or modified

# Data Classification

## ISO/IEC 27001 2005 - section A.7.2.1

*“Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.”*

## COBIT 5 APO01.06 Define Information (data) and system ownership

*“Define and maintain responsibilities for ownership of information (data) and information systems. Ensure that owners make decisions about classifying information and systems and protecting them in line with this classification.”*



# Data Classification

Without a data classification scheme, an organization treats all information the same. As a result:

- There is an increased risk that sensitive data will not have adequate security controls,
- Increasing the risk of sensitive data being compromised
- An increased likelihood that less sensitive data will have more security controls than necessary,
- Leading to unnecessary restrictions, and
- Loss of efficiency for operational personnel

Manage your object authority according to your data classification scheme. Objects labeled confidential or restricted should use an exclusionary access model (Object Authority)

# Roles & Responsibilities

- Define user authorization roles
  - A user authorization role defines the tasks a user has to perform and the access he/she needs to objects
  - Try to keep the number of roles low, i.e. two roles per organization
  - Avoid “extra” authorities
  - Use one group profile per role
- Eliminate \*SECOFR profiles as much as possible
  - No programmer needs \*ALLOBJ
  - No programmer has all-time access to the production environment
  - When necessary, create utility programs for functions that require higher authorities and audit its use
- Document the requirements


# Subsystem Security Exposure

## CHGCFGL Secure Location Options:

- \***NO** – Default subsystem communication entry profile will be used if available
- \***YES** – Remote user verified, must exist on remote/target systems
- \***VFYENCPWD** – User ID and password must match on remote/target systems, password is verified, encrypted and sent

```
Change Configuration List                                DDMTARGT
                                                         09/03/13 10:56:22
Configuration list . . . : QAPPNRMT
Configuration list type : *APPNRMT

-----APPN Remote Locations-----
Remote   Remote   Remote   Control
Location Network Local   Control Point   Location   Secure
         ID      Location Point Net ID   Password  Loc
CTCTEST APPN   DDMTARGT RMTCP APPN   _____ *NO
         *NETATR *NETATR _____ *NETATR _____ *NO
```



# Subsystem Security Exposure

```
Display Communications Entries
Subsystem description: QSYSWRK  Status: ACTIVE

Device      Mode      Job      Default
*ALL        *ALL      *USRPRF  ALLUSER
```

- DSPSBSD QSYS/QSYSWRK

- DSPUSRPRF **ALLUSER**

```
Display User Profile - Basic
User profile . . . . . : ALLUSER
Special authority . . . . . : *ALLOBJ
                             *AUDIT
                             *IOSYSCFG
                             *JOBCTL
                             *SAVSYS
                             *SECADM
                             *SERVICE
                             *SPLCTL
```

# Subsystem Security Exposure

All remote DDM/DRDA and APPC communications will run anonymously as powerful account **ALLUSER** with all eight special authorities

- No password required

```
Display Job Log
System: DDMTARGT
Job . . . : DDMJOB      User . . . : ALLUSER      Number . . . : 634128

Job 634128/ALLUSER/DDMJOB started on 02/11/12 at 16:30:09 in subsystem QSYS
Target DDM job started by source system.
Local relational database accessed by DDMJOB.

Bottom
```

# Raising the bar against altered programs

## Program validation value:

A hash over security relevant parts of the program. The hash produces the same result on each system and is generated at program creation.

## Digital signing of program objects:

Signing of program objects using a secure private key. The public key is distributed to systems that need to verify the signature.

**NOTE:** The signature can be created after an object is altered.

# QVFYOBJRST system value

The 5 QVFYOBJRST options (default is 3): **Recommend 3 or 5**

1. Do not verify signatures on restore. Restore all objects regardless of their signature. **NOTE: Effectively trust everything**
2. Verify signatures on restore. Restore unsigned user-state objects. Restore signed user-state objects, even if the signatures are not valid.
3. Verify signatures on restore. Restore unsigned user-state objects. Restore signed user-state objects only if the signatures are valid.
4. Verify signatures on restore. Do not restore unsigned user-state objects. Restore signed user-state objects, even if the signatures are not valid.
5. Verify signatures on restore. Do not restore unsigned user-state objects. Restore signed user-state objects only if the signatures are valid. **NOTE: Effectively trust nothing**

# QFRCCVNRST system value

The 8 QFRCCVNRST options (default is 0): **Recommend 3**

0. Do not convert anything. **NOTE: Trust everything**
1. Objects with validation errors will be converted.
2. Objects requiring conversion to be used on the current version of the operating system and objects with validation errors will be converted.
3. Objects suspected of having been tampered with, objects containing validation errors, and objects requiring conversion to be used by the current version of the operating system will be converted.
4. Objects that contain sufficient creation data to be converted and do not have valid digital signatures will be converted.
5. Objects that contain sufficient creation data will be converted or else not restored.
6. All objects that do not have valid digital signatures will be converted.
7. All objects will be converted or else not restored. **NOTE: Trust nothing**



# QALWOBJRST system value

The **QALWOBJRST** options (default is \*ALL): **Recommend \*NONE or \*ALWPTF**

- \*ALL - Allows all objects to be restored regardless of whether or not they have security-sensitive attributes or validation errors. **NOTE: Effectively trust everything**
- \*NONE - Does not allow objects with security-sensitive attributes to be restored. **NOTE: Effectively trust nothing**
- \*ALWSYSSTT - Allows programs, service programs, and modules with the system-state or inherit-state attribute to be restored.
- \*ALWPGMADP - Allows programs and service programs with the adopt attribute to be restored.
- \*ALWPTF - Allow system-state or inherit-state programs, service programs, modules, objects that adopt authority, objects that have the S\_ISUID (set-user-ID) attribute enabled, and objects that have the S\_ISGID (set-group-ID) attribute enabled to be restored to the system during a PTF install.
- \*ALWSETUID - Allow restore of files that have the S\_ISUID (set-user-ID) attribute
- \*ALWSETGID or the S\_ISGID (set-group-ID) enabled.
- \*ALWVLDERR - Allow objects with validation errors or suspected of having been tampered with to be restored. When the setting of the QFRCCVNRST system value causes the object to be converted any validation errors it may have had will be corrected.

# Security Level 30 – Not secure !

System interfaces perform appropriate authority checks but security exposures exist on this security level

Security level 30 is NOT a secure security level!

User written programs running at security level 30 can gain access to objects with minimal authority

# DDM/DRDA

# DDM (Distributed Data Management)

“DDM”



DDM does not honor limit capabilities **AND** can provide elevated (even QSECOFR) access if no password is required

```
Change DDM TCP/IP Attributes (CHGDDMTCPA)

Type choices, press Enter.

Autostart server . . . . . *YES          *NO, *YES, *SAME
Password required . . . . . *NO          *NO, *YES, *ENCRYPTED...
```

# DDM (Distributed Data Management)

**“DANGER, DANGER, DANGER”**

DDM Password Attributes to beware of:

**\*NO**

Do not require a password on a DDM connection request. If a password is sent, it is ignored.

**\*USRID**

Do not require a password on a DDM connection request. If a password is sent, it is ignored. See also \*VLDONLY description.

**\*VLDONLY**

Do not require a password on a DDM connection request. If a password is sent, however, it must be valid for the associated userid.

# “DDM – THE HACK!”

- User BRUCE is a standard \*USER class profile with no special authorities
- Bruce can use DDM to submit a job on the target system as QSECOFR to create the profile HACKME (and much more) without knowing QSECOFR's password

```
                Add Server Auth Entry (ADDSVRAUTE)

Type choices, press Enter.

User profile . . . . . > *CURRENT      Name, *CURRENT
Server . . . . . > QDDMSERVER

-----
User ID . . . . . QSECOFR
-----
User password . . . . . *NONE
-----
```

```
                Submit Remote Command (SBMRMTCMD)

Type choices, press Enter.

Command to run . . . . . > 'CRTUSRPRF USRPRF (HACKME) PASSWORD (HACKME1)
USRCLS (*SECOFR) '
-----
-----
-----
```

# “DDM/DRDA – THE HACK!”

## Part 2 - SQL

- **DB2 Connect uses DDM/DRDA. No need for:**
  - **Server Authentication Entry (ADDSVRAUTE)**
  - **DDM files (CRTDDMF)**
- **DB2 Connect is everywhere. Windows, UNIX, OS/400, etc, etc, etc.**
- **Only requires a Relational Database Entry (ADDRDBDIRE) which may already exist.**
  - **DDM Password = \*NO, \*USRID or \*VLDONLY**
- **CONNECT TO *rdbname* USER QSECOFR USING ‘ ‘**
  - **Now connected as QSECOFR without a password you can run any SQL statement/s and bypass any access control.**
  - **UPDATE**
  - **DELETE**
  - **INSERT**
  - **ALTER TABLE**
  - **CALL**

# DDM (Distributed Data Management)

DDM does not honor limited capabilities **AND** can provide elevated (even QSECOFR) access if no password is required

```
Change DDM TCP/IP Attributes (CHGDDMTCPA)

Type choices, press Enter.

Autostart server . . . . . *YES          *NO, *YES, *SAME
Password required . . . . . *NO          *NO, *YES, *ENCRYPTED...
```



# Risk Remediation

- Monitoring is great if you want to watch as the data is being extricated and stolen
- Firewalls are good at keeping the good guys out, **the bad guys are most likely already in**
- Encryption is excellent at keeping anyone who does not have access to the systems (already in ?) from stealing the data



# Application Access Protects Me?

True – only if...

- ✓ All application objects and libraries are \*PUBLIC \*EXCLUDE and NO private authorities exist
- ✓ All OS risks and backdoors are closed
- ✓ No elevated privilege is allowed
  - No \*PUBLIC or privately authorized profiles (identity theft)
  - All powerful adopted authority programs are secured
  - DDM/DRDA requires an encrypted password
  - Etc, etc.....
- ✓ All remote servers are disabled
- ✓ More, more, more.....

# YouTube videos and other links

**IBM i Security - Misconceptions Part 1 Limited Capabilities**

<https://www.youtube.com/watch?v=vW0pFUGstoM>

**IBM i Security Misconceptions Part 2 Authority to User Profiles**

<https://www.youtube.com/watch?v=cFaCfJDI7Hs>

**Hacking iSeries Network Servers**

<http://www.itjungle.com/tfh/tfh081903-story06.html>

**Hacking the Legacy**

<https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Bart-Kulach-Hack-the-Legacy-IBMi-revealed.pdf>

**IBM i Knowledge Center**

[https://www.ibm.com/support/knowledgecenter/ssw\\_ibm\\_i\\_72/rzarl/rzarlspcaut.htm?lang=en](https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_72/rzarl/rzarlspcaut.htm?lang=en)

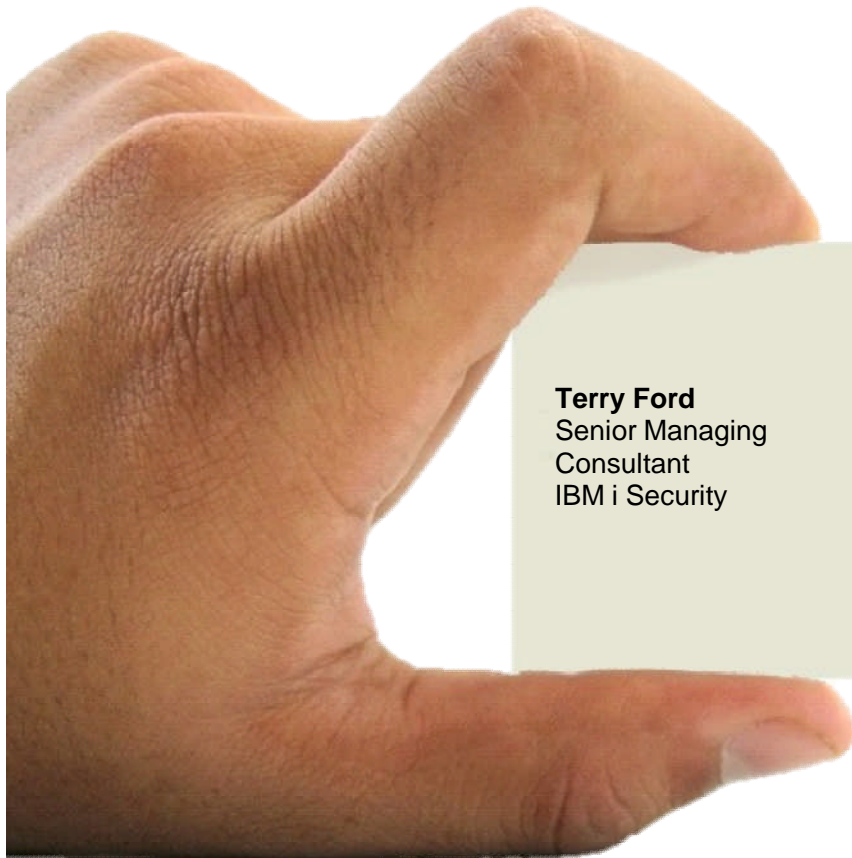
**Jeff Uehling – Best Practices**

[https://www-950.ibm.com/events/wwe/grp/grp017.nsf/vLookupPDFs/STL\\_2013\\_Best\\_Security\\_Practices/\\$file/STL\\_2013\\_Best\\_Security\\_Practices.pdf](https://www-950.ibm.com/events/wwe/grp/grp017.nsf/vLookupPDFs/STL_2013_Best_Security_Practices/$file/STL_2013_Best_Security_Practices.pdf)

## IBM Lab Services Can Help!



- IBM Lab Services can offer consulting and security services:
  - IBM i Security Assessment
  - IBM i Network Encryption (TLS)
  - IBM i Single Sign On Setup
  
- IBM Lab Services also has several security related tools:
  - IBM i Software Firewall (Exit Programs)
  - IBM i Privileged Elevation Tool
  - IBM i Compliance and Reporting Tool with Event Monitoring
  - IBM i Two Factor Authentication / Password Reset Utility
  - And many more non-network related tools
  
- Visit <http://ibm.biz/IBMiSecurity> to learn more about all of these offerings!



**IBM**

**Terry Ford**  
Senior Managing  
Consultant  
IBM i Security

Office: 1-507-253-7241  
Mobile: 1-507-358-1771  
taford@us.ibm.com

3605 Highway 52 N  
Bldg. 025-3 A113  
Rochester, MN 55901  
USA



**Statement of Good Security Practices:** IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

# THANK YOU

[www.ibm.com/security](http://www.ibm.com/security)



## IBM Security

Intelligence. Integration. Expertise.

© Copyright IBM Corporation 2015. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

# Notices and Disclaimers

Copyright © 2016 by International Business Machines Corporation (IBM). No part of this document may be reproduced or transmitted in any form without written permission from IBM.

## **U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IN NO EVENT SHALL IBM BE LIABLE FOR ANY DAMAGE ARISING FROM THE USE OF THIS INFORMATION, INCLUDING BUT NOT LIMITED TO, LOSS OF DATA, BUSINESS INTERRUPTION, LOSS OF PROFIT OR LOSS OF OPPORTUNITY. IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

## **Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of 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. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. IBM EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com, Aspera®, Bluemix, Blueworks Live, CICS, Clearcase, Cognos®, DOORS®, Emptoris®, Enterprise Document Management System™, FASP®, FileNet®, Global Business Services®, Global Technology Services®, IBM ExperienceOne™, IBM SmartCloud®, IBM Social Business®, Information on Demand, ILOG, Maximo®, MQIntegrator®, MQSeries®, Netcool®, OMEGAMON, OpenPower, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, Smarter Commerce®, SoDA, SPSS, Sterling Commerce®, StoredIQ, Tealeaf®, Tivoli®, Trusteer®, Unica®, urban{code}®, Watson, WebSphere®, Worklight®, X-Force® and System z® Z/OS, are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).