

Achieving Compliance with Bsafe/Enterprise Security

**Banking
Financial Markets
Insurance**

- Basel II Accord, USA Patriot Act, Anti money laundering
- Basel II Accord, USA Patriot Act, SEC 17-a-4 / NASD 3010, 3110
- ACORD, GLBA

**Automotive
Electronics**

- Tread Act, European Block Exemption, End of Life (AP)
- RosettaNet, Waste for Electronics and Electronics Equipment (WEEE),
- Wassenaar Agreement

**Retail
Consumer Products**

- Retail Event Management, ARTS for POS data
- Global data synchronization, RFID, Sunrise 2005
- UCCNet

**Government
Healthcare
Life Sciences**

- Homeland Security, Freedom of Information Act, DOD5015.2
- HIPAA
- FDA/21CFRp11

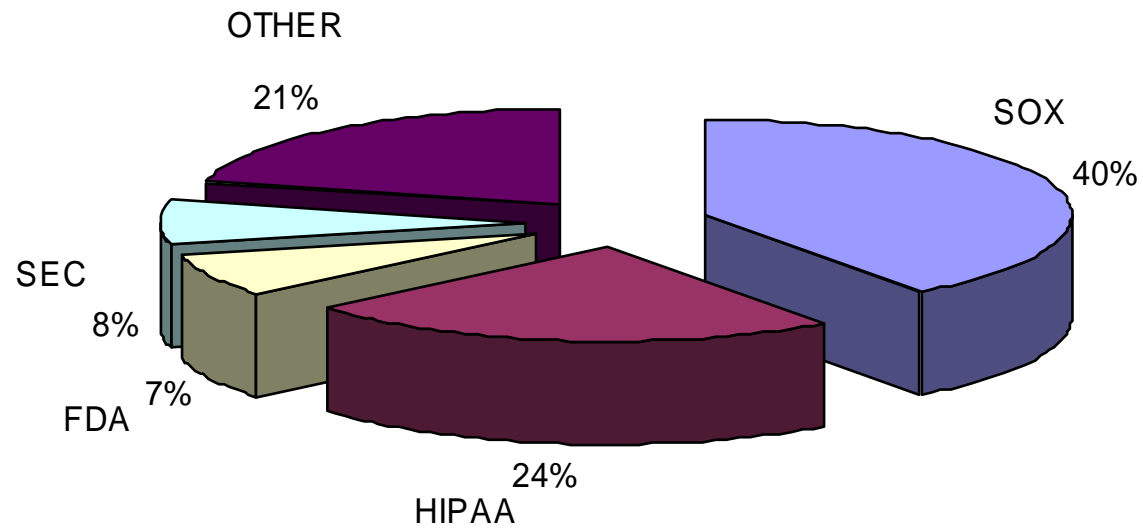
**Energy and Utilities
Telecommunications**

- NERC 1200
- Number Portability

**All US Publicly
Traded
Companies**

- Sarbanes-Oxley

Compliance Spending - 2005



Source : AMR Research Group

- A recent study conducted by the Securities Industry Association estimated that the cost of compliance has nearly doubled in the past three years
- The cost of compliance went up from \$13 billion in 2002 to more than \$25 billion in 2005

- CIO's estimate that, during the past twelve months, their organizations have spent on compliance with SOX :
 - Just under 2% of gross revenue
 - An average of \$1,450,000 of their information technology (IT) budget
- Majority of CIO's believe SOX compliance costs will either increase (21%) or stay the same (49%) in the next year.

To be compliant, Security Officers must quantify:

- Prevention of access for users without a demonstrable need to access data.
- Existence of a clear recognizable audit trail for transactions.
- A real-time intrusion alerting mechanism

- The OS/400 was architected before the advent of PC connectivity.
- Therefore, it can not inherently track or secure all of a PC user's transactions without additional assistance.
- Without such assistance a user is able to access the iSeries through the network, change or delete any data he wants without being detected

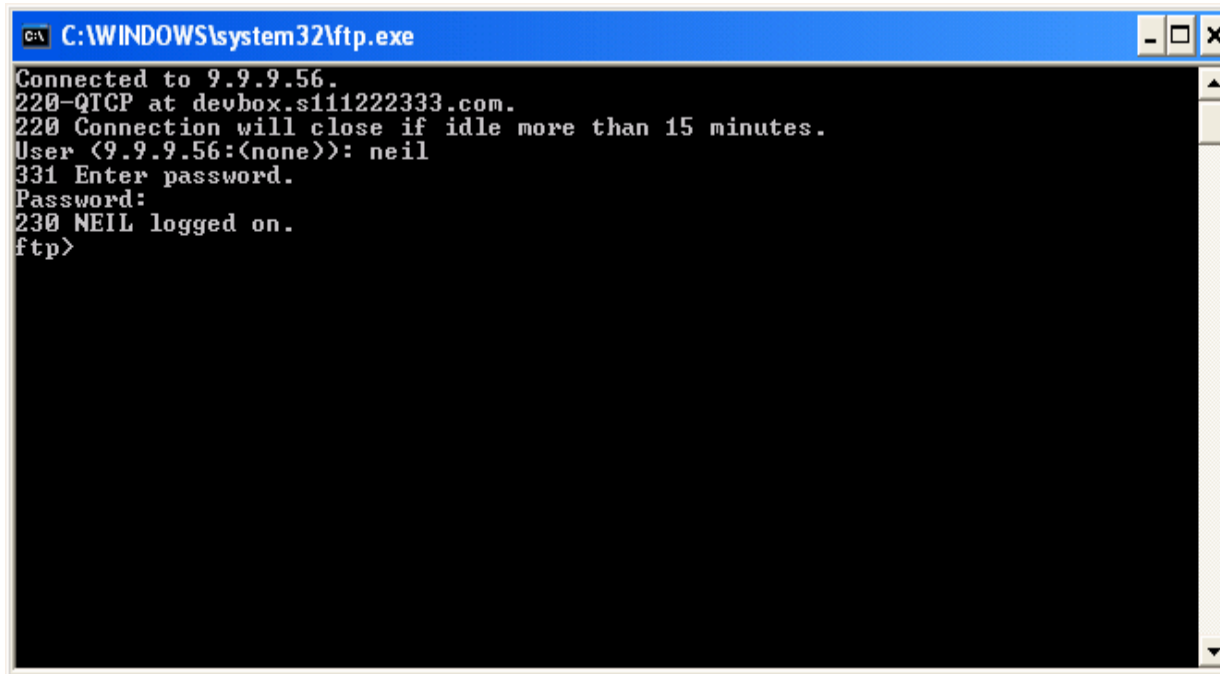
Compliance rulings came into effect following manipulation of company data by executives *inside the company*

***Trusted people* in an organization naturally have access to sensitive information**

Compliance is about ensuring those entrusted people do not *abuse their authority*.

Take FTP for example.

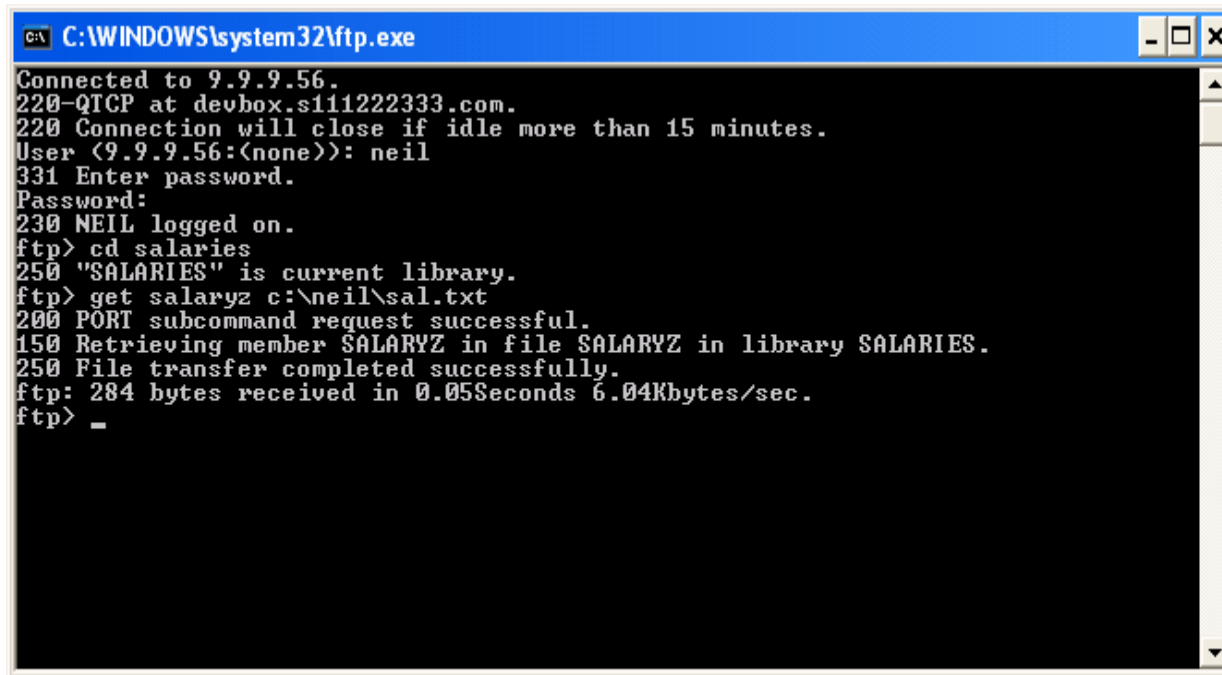
File transfer functions are just a mouse-click away from the Windows desktop. This worker in the Accounts department clicked Start, run and logged on to the iSeries



```
C:\WINDOWS\system32\ftp.exe
Connected to 9.9.9.56.
220-QTCP at devbox.s111222333.com.
220 Connection will close if idle more than 15 minutes.
User (9.9.9.56:(none>): neil
331 Enter password.
Password:
230 NEIL logged on.
ftp>
```

Vulnerability from the PC

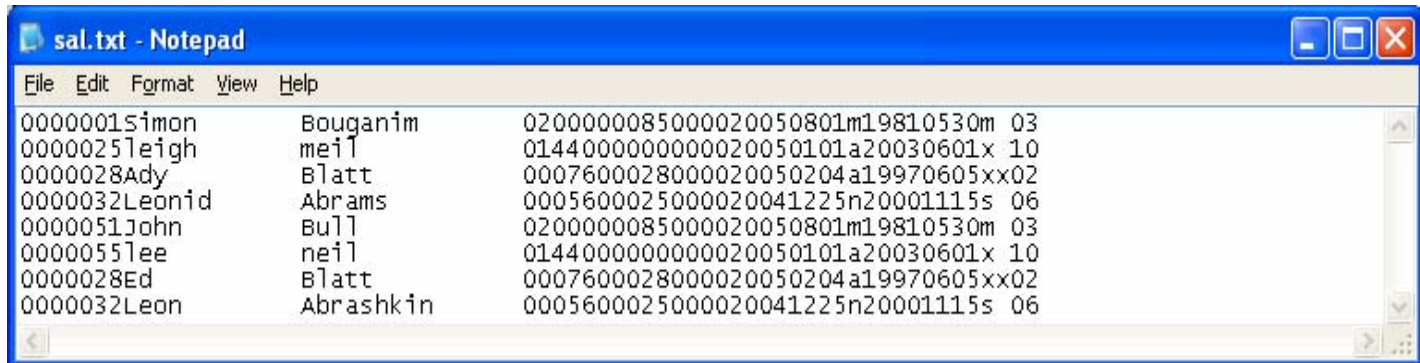
The worker downloads the salary file from the iSeries database to his PC



```
C:\WINDOWS\system32\ftp.exe
Connected to 9.9.9.56.
220-QTCP at devbox.s111222333.com.
220 Connection will close if idle more than 15 minutes.
User (9.9.9.56:(none)): neil
331 Enter password.
Password:
230 NEIL logged on.
ftp> cd salaries
250 "SALARIES" is current library.
ftp> get salaryz c:\neil\sals.txt
200 PORT subcommand request successful.
150 Retrieving member SALARYZ in file SALARYZ in library SALARIES.
250 File transfer completed successfully.
ftp: 284 bytes received in 0.055Seconds 6.04Kbytes/sec.
ftp> _
```

Vulnerability from the PC

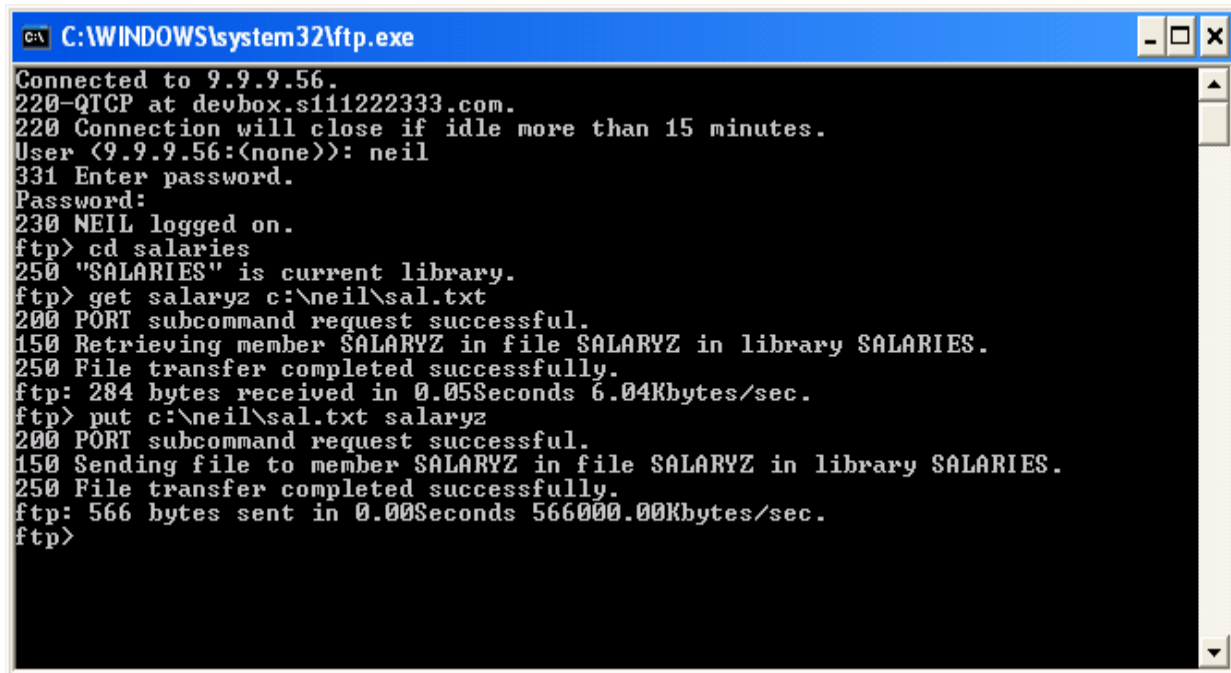
Once he has downloaded the salary file he can view and even change its contents



```
sal.txt - Notepad
File Edit Format View Help
0000001Simon      Bouganim      0200000085000020050801m19810530m 03
0000025leigh     meil         01440000000000020050101a20030601x 10
0000028Ady       Blatt        0007600028000020050204a19970605xx02
0000032Leonid   Abrams       0005600025000020041225n20001115s 06
0000051John      Bull         0200000085000020050801m19810530m 03
0000055lee       neil         01440000000000020050101a20030601x 10
0000028Ed        Blatt        0007600028000020050204a19970605xx02
0000032Leon     Abrashkin    0005600025000020041225n20001115s 06
```

Vulnerability from the PC

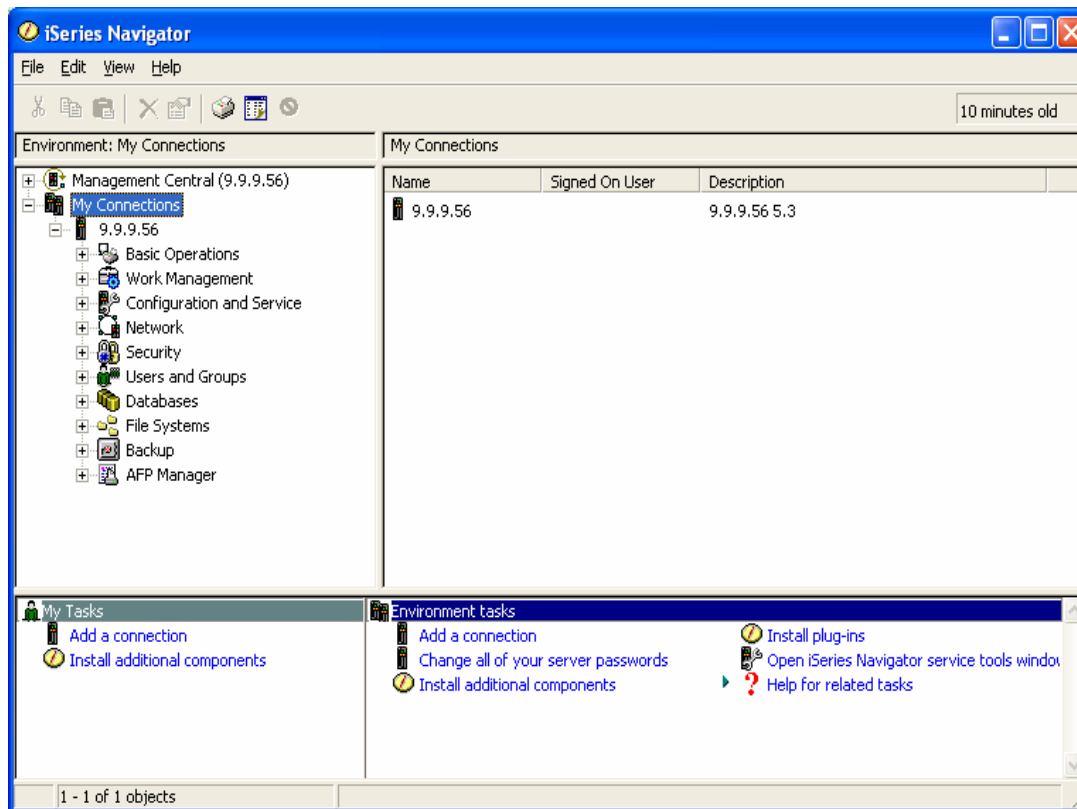
Finally, he can replace the original file in the iSeries database with his changed version



```
C:\WINDOWS\system32\ftp.exe
Connected to 9.9.9.56.
220-QTCP at devbox.s111222333.com.
220 Connection will close if idle more than 15 minutes.
User (9.9.9.56:(none)): neil
331 Enter password.
Password:
230 NEIL logged on.
ftp> cd salaries
250 "SALARIES" is current library.
ftp> get salaryz c:\neil\sal.txt
200 PORT subcommand request successful.
150 Retrieving member SALARYZ in file SALARYZ in library SALARIES.
250 File transfer completed successfully.
ftp: 284 bytes received in 0.055Seconds 6.04Kbytes/sec.
ftp> put c:\neil\sal.txt salaryz
200 PORT subcommand request successful.
150 Sending file to member SALARYZ in file SALARYZ in library SALARIES.
250 File transfer completed successfully.
ftp: 566 bytes sent in 0.000Seconds 566000.00Kbytes/sec.
ftp>
```

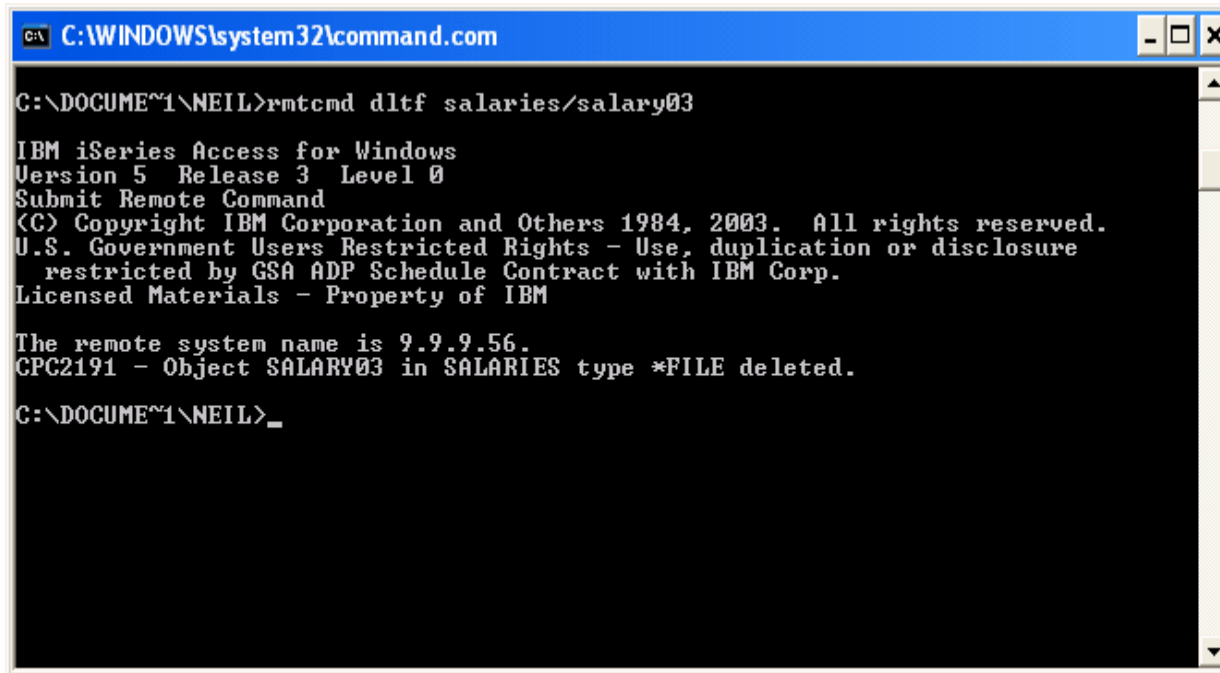
Another example...

Ever heard of the IBM Operations Navigator ? It provides many tools for accessing the iSeries from a PC



For example...

Using Remote Command you can manipulate iSeries resources – even if you are denied access to the green screen command line



```
C:\WINDOWS\system32\command.com

C:\DOCUME~1\NEIL>rmtcmd dltf salaries/salary03

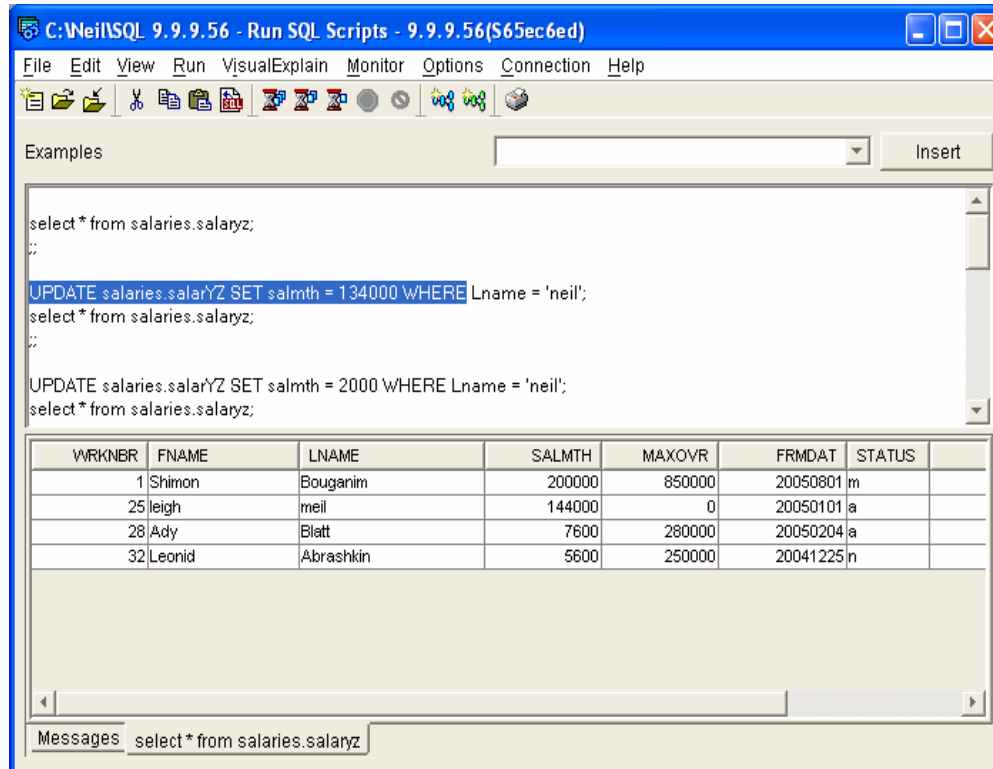
IBM iSeries Access for Windows
Version 5 Release 3 Level 0
Submit Remote Command
(C) Copyright IBM Corporation and Others 1984, 2003. All rights reserved.
U.S. Government Users Restricted Rights - Use, duplication or disclosure
restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM

The remote system name is 9.9.9.56.
CPC2191 - Object SALARY03 in SALARIES type *FILE deleted.

C:\DOCUME~1\NEIL>_
```

For example...

Using SQL scripts to access your iSeries through ODBC, there's almost nothing you can't do with your data...

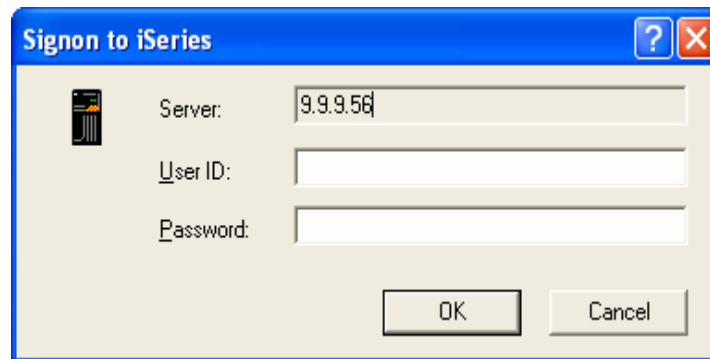


The screenshot shows a window titled "C:\Neil\SQL 9.9.9.56 - Run SQL Scripts - 9.9.9.56(S65ec6ed)". The window contains a menu bar (File, Edit, View, Run, Visual Explain, Monitor, Options, Connection, Help) and a toolbar. Below the toolbar is a text area with SQL scripts. The first script is "select * from salaries.salaryz;". The second script is "UPDATE salaries.salaryZ SET salmth = 134000 WHERE Lname = 'neil';" followed by "select * from salaries.salaryz;". The third script is "UPDATE salaries.salaryZ SET salmth = 2000 WHERE Lname = 'neil';" followed by "select * from salaries.salaryz;". Below the text area is a table with the following data:

WRKNBR	FNAME	LNAME	SALMTH	MAXOVR	FRMDAT	STATUS
1	Shimon	Bouganim	200000	850000	20050801	m
25	leigh	meil	144000	0	20050101	a
28	Ady	Blatt	7600	280000	20050204	a
32	Leonid	Abrashkin	5600	250000	20041225	n

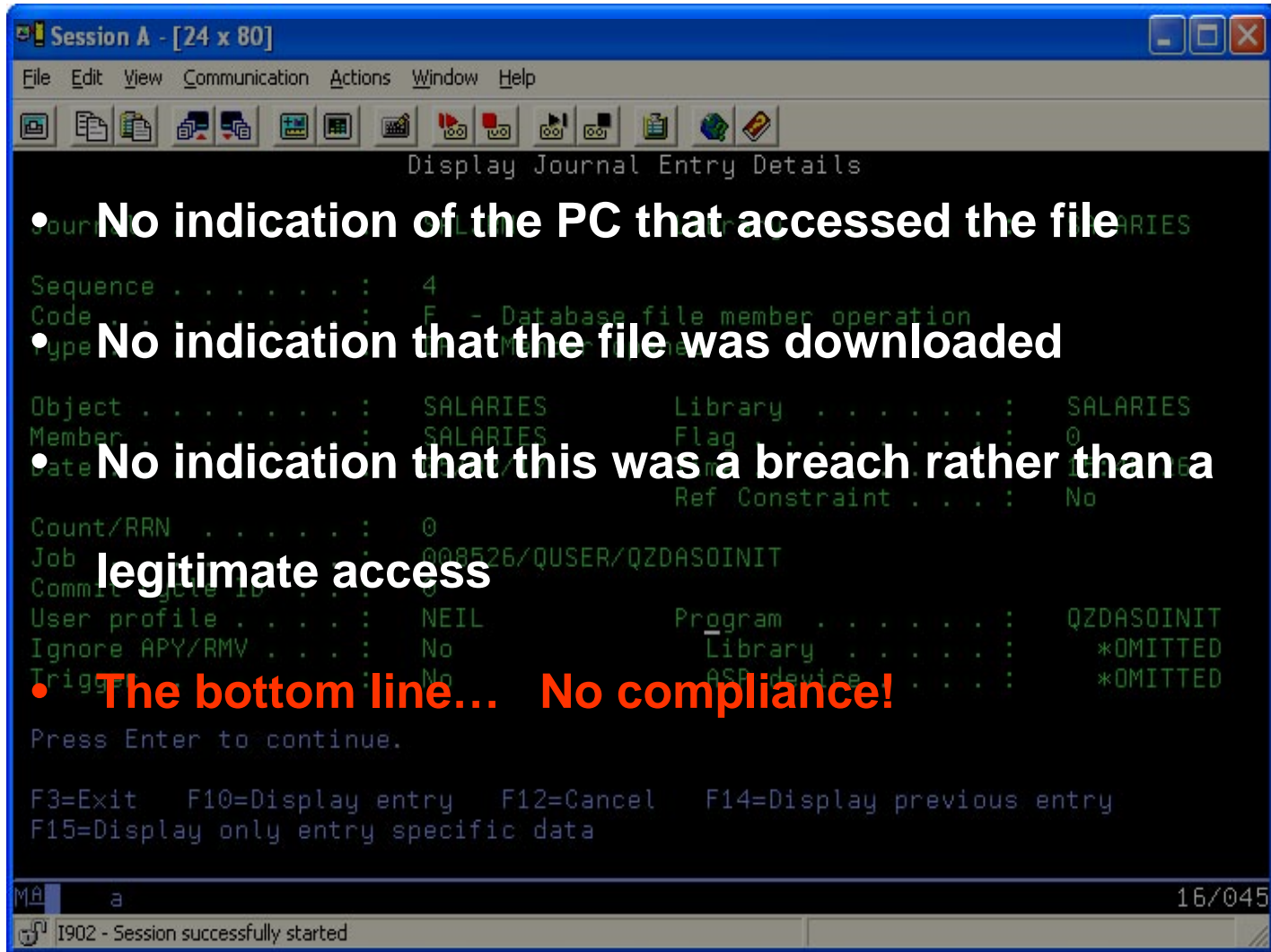
At the bottom of the window, there is a "Messages" pane showing "select * from salaries.salaryz".

In fact, there are quite a few different ways to access and update the iSeries from the PC desktop – and they are all no more than a mouse-click away



A user and password meant for one thing could be used for something else - that wasn't intended

- Earlier we saw how easily users can download sensitive files to their PCs via FTP
- The system journal doesn't log FTP actions at all
- If the file is already journaled to a data journal it will log the opening of the file, but not the results of the FTP operations
- This is what you get...



Session A - [24 x 80]

File Edit View Communication Actions Window Help

Display Journal Entry Details

- **No indication of the PC that accessed the file**
- **No indication that the file was downloaded**
- **No indication that this was a breach rather than a legitimate access**
- **The bottom line... No compliance!**

```
Source: ... SALARIES
Sequence . . . . . : 4
Code . . . . . : F - Database file member operation
Type . . . . . : M - Member operation

Object . . . . . : SALARIES      Library . . . . . : SALARIES
Member . . . . . : SALARIES     Flag . . . . . : 0
Date . . . . . :                Ref Constraint . . . : No

Count/RRN . . . . . : 0
Job . . . . . : 008526/QUSER/QZDASOINIT
Commit . . . . . : 0
User profile . . . . : NEIL      Program . . . . . : QZDASOINIT
Ignore APY/RMV . . . : No       Library . . . . . : *OMITTED
Trigger . . . . . : No         ASP device . . . . : *OMITTED

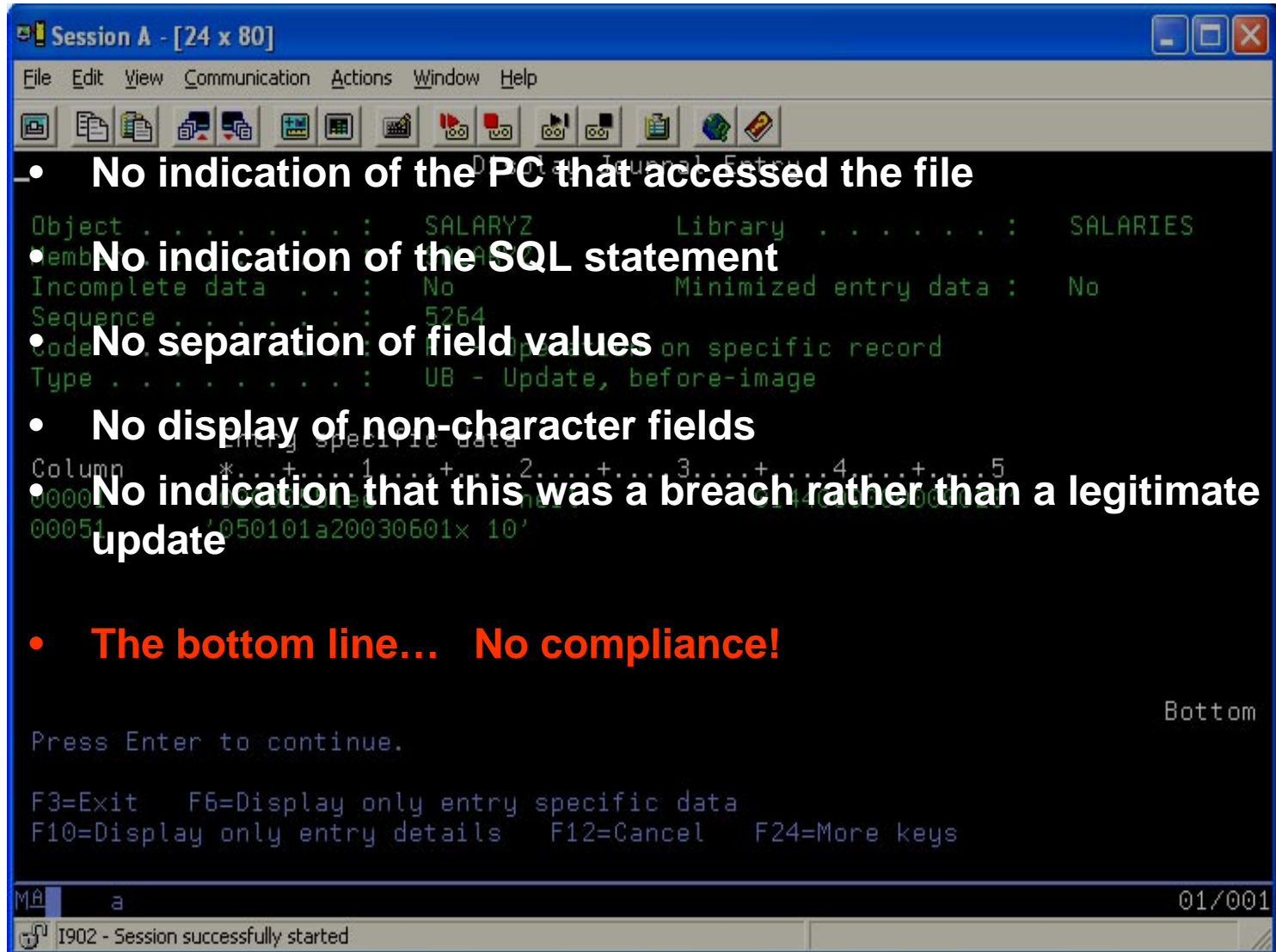
Press Enter to continue.

F3=Exit  F10=Display entry  F12=Cancel  F14=Display previous entry
F15=Display only entry specific data
```

Má a 16/045

I902 - Session successfully started

- We saw also how easily users can update data via ODBC
- The system journal doesn't log this action either
- If the file is journaled to a data journal it will log the record images, but little more
- This is what you get...



- **No indication of the PC that accessed the file**
- **No indication of the SQL statement**
- **No separation of field values**
- **No display of non-character fields**
- **No indication that this was a breach rather than a legitimate update**
- **The bottom line... No compliance!**

- These 'backdoor' means of access bypassing the more basic security afforded by menus
- Demonstrated lack of adequate logging
- As a result, companies using System i on the network can't be in compliance without an own-developed solution or a packaged solution like Bsafe/Enterprise Security Suite

Bsafe/Enterprise Security enables security administrators and auditors to:

- Monitor and secure users' activities.
- Automate the creation of clear and concise audit reports.
- Receive real-time security and system related alerts.

- You don't need to be a System i expert to **manage** System i **security**
- Nor do you need to be a System i expert to **audit** System i **activity**
- Let auditors directly access audit reports, on their PCs and print on their local printers
- The very features needed to achieve compliancy

“1. Prevention of access for users without a demonstrable need to access data”

Application Access Control

Restrict by:

- Organization level – system policy
- User/group of users
- Application server and function
- Library, object
- IP address
- File protection against power users like QSECOFR

Field Masking

- Block field values from view
- Match mask to user

Internal Security Management

- Object Authority Manager
- User profile manager

Port Restrictions Manager

- Restrict System i ports

Bsafe Enterprise Security Manager

File Host View Help

Field Encryption - 9.9.9.56 - Production i5

Options

Select Files for Encryption:

Library	File	Synchronization Mode	Status
SALARIES	SALARYZ1	Two-way	Active; Job name:
TZVILIB	ALLUSRPRF	Two-way	Inactive
TZVILIB	FLDTYPEP	No Synchronization	No File
TZVILIB3	ACSEMPSP	One-way	Inactive
TZVILIB5_2	ACSINVP	One-way	Inactive

Add Remove Start Encryption End Encryption

Select Fields for Encryption:

Field	Type	Length	Decimal	Mask	Description
LNAME	A	15		Blanks	LAST NAME
MAXOVR	S	7	00	All 9's	MAXIMUM OVERTIME
SALMTH	S	7	00	All 9's	MONTHLY SALARY

Add Change Remove Remove All

Navigation: Left arrow, Right arrow, Home icon

Untitled - Run SQL Scripts - 9.9.9.56(S65ec6ed) *

File Edit View Run VisualExplain Monitor Options Connection Help

Examples Insert

```
select * from salaries.salary1
```

WRKNBR	FNAME	LNAME	SALMTH	MAXOVR	FRMDAT	STATUS	STRDAT	FAMSTS	CHILD
25	leigh	neil	128000	0	20050101	a	20030601	x	3
28	Ady	Blatt	7500	250000	20050204	a	19970605	xx	2
32	Leonid	Abrashkin	5600	250000	20041225	n	20001115	s	6
1	Shimon	Bouganim	200000	850000	20050801	m	19810530	m	3

Untitled - Run SQL Scripts - 9.9.9.56(S65ec6ed) *

File Edit View Run VisualExplain Monitor Options Connection Help

Examples Insert

```
select * from production.salary1
```

WRKNBR	FNAME	LNAME	SALMTH	MAXOVR	FRMDAT	STATUS	STRDAT	FAMSTS	CHILD
25	leigh		9999999	9999999	20050101	a	20030601	x	3
28	Ady		9999999	9999999	20050204	a	19970605	xx	2
32	Leonid		9999999	9999999	20041225	n	20001115	s	6
1	Shimon		9999999	9999999	20050801	m	19810530	m	3

“2. Existence of a clear recognizable audit trail for transactions”

Application Audit

Network & exit point log

Central Audit

Multiple sources
Long term history

Application Analyzer

Graphics to pinpoint trends

Read-record Audit

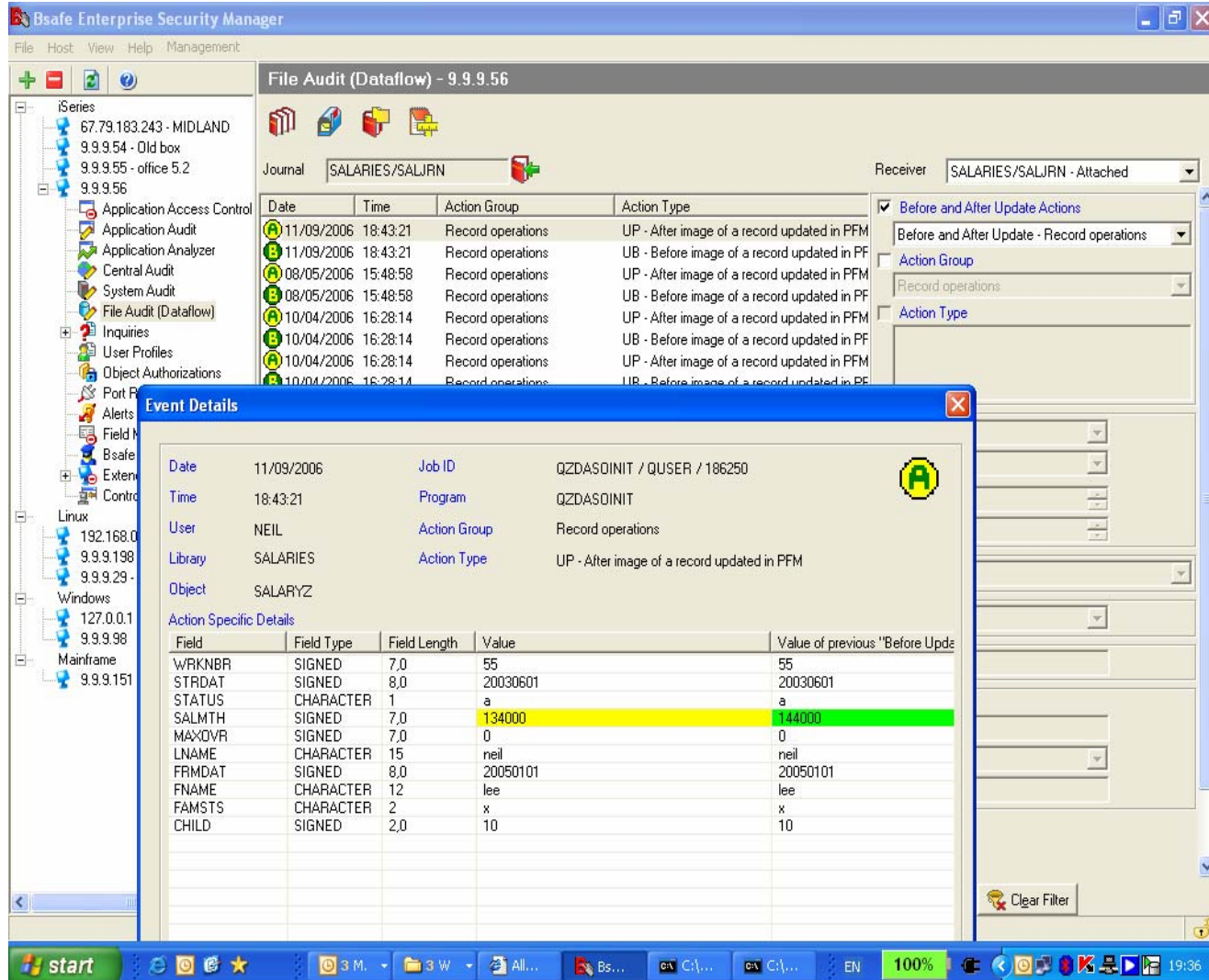
Log of read data

File Audit

Database changes by field

System Audit

All system activity, incl. internal transaction on i5 OS



The screenshot displays the BSAFE Enterprise Security Manager interface. The main window is titled "File Audit (Dataflow) - 9.9.9.56". It shows a list of audit events with columns for Date, Time, Action Group, and Action Type. The "Event Details" window is open, showing the following information:

Event Details

- Date: 11/09/2006
- Time: 18:43:21
- User: NEIL
- Library: SALARIES
- Object: SALARYZ
- Job ID: QZDASQINIT / QUSER / 186250
- Program: QZDASQINIT
- Action Group: Record operations
- Action Type: UP - After image of a record updated in PFM

Action Specific Details

Field	Field Type	Field Length	Value	Value of previous "Before Update"
WRKNBR	SIGNED	7,0	55	55
STRDAT	SIGNED	8,0	20030601	20030601
STATUS	CHARACTER	1	a	a
SALMTH	SIGNED	7,0	134000	0
MAXDVR	SIGNED	7,0	0	0
LNAME	CHARACTER	15	neil	neil
FRMDAT	SIGNED	8,0	20050101	20050101
FNAME	CHARACTER	12	lee	lee
FAMSTS	CHARACTER	2	x	x
CHILD	SIGNED	2,0	10	10

“2. Existence of a clear recognizable audit trail for transactions”

- Rich array of shipped audit reports
- Variety of formats including Excel files, on-screen inquiries, printing on PC printer
- Report generator for creating custom audit reports
- All done from easy to use PC GUI screens

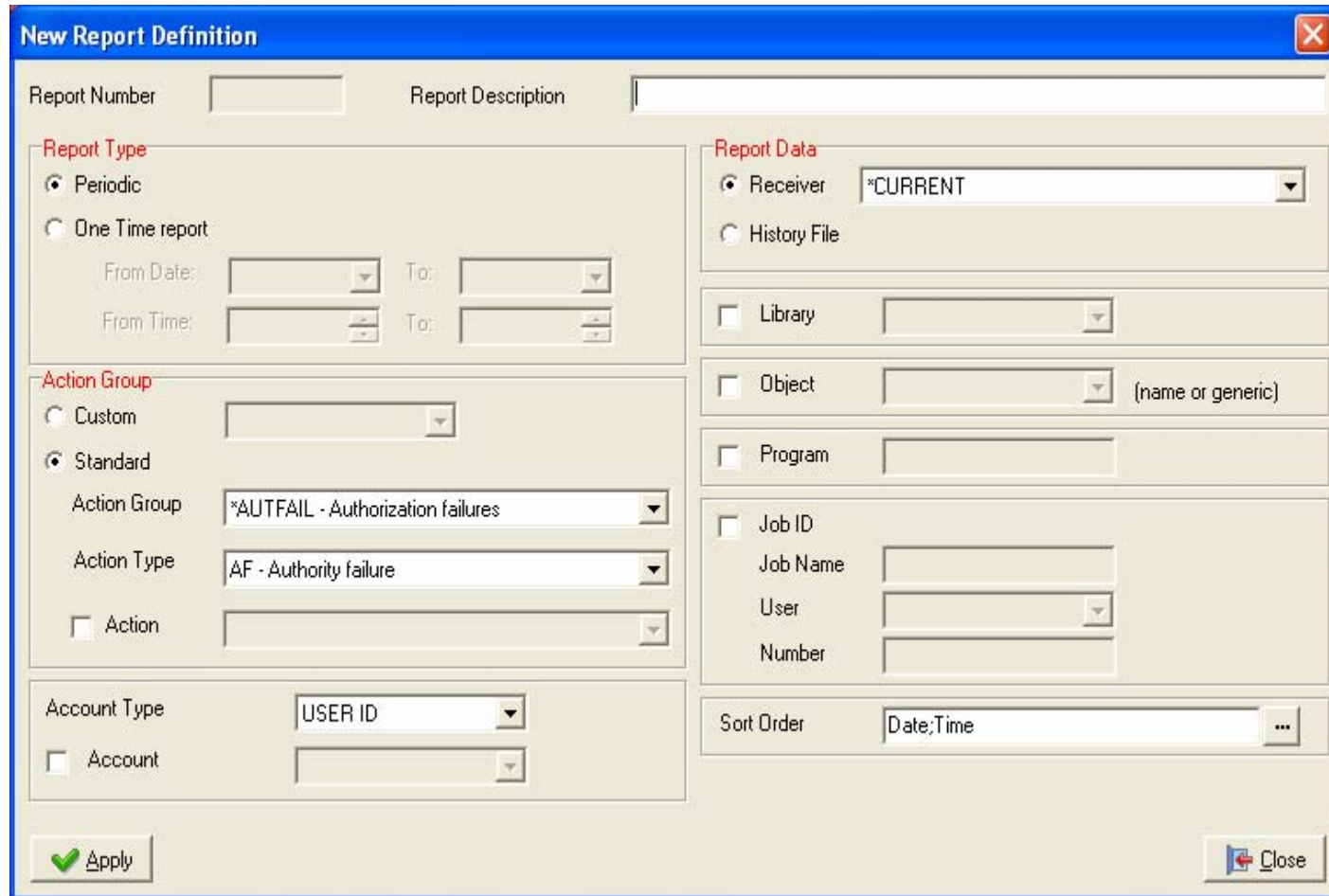
System Audit Reports

Report Scheduler Report Jobs Action Groups

Number	Report Description	Report Data	Group Type	Action Group	Action Type	Action	Report Type	Fr
1	SYSTEM VALUE CHANGES	Online Receivers	Standard	*SECURITY - Securi...	SV - System value c...	A - A system value w...	One Time	01
2	INCORRECT USER	Online Receivers	Standard	*AUTFAIL - Authoriz...	PW - Invalid password	U - User name not v...	One Time	01
3	INCORRECT PASSWORD	Online Receivers	Standard	*AUTFAIL - Authoriz...	PW - Invalid password	P - An incorrect pass...	One Time	01
4	OBJECTS AUTHORITY CHANGES	Online Receivers	Standard	*SECURITY - Securi...	CA - Authority changes	A - Changes to auth...	One Time	01
5	DELETE OBJECTS	Online Receivers	Standard	*DELETE - Deleting ...	DO - Delete object	A - All delete operat...	One Time	01
6	CREATE OBJECTS - NEW	Online Receivers	Standard	*CREATE - Creating ...	CO - Create object	N - Creation of a ne...	One Time	01
7	OBJECT OWNERSHIP CHANGED	Online Receivers	Standard	*SECURITY - Securi...	DW - Object owners...	A - Object ownership...	One Time	01
8	AUTHORITY FAILURE	Online Receivers	Standard	*AUTFAIL - Authoriz...	AF - Authority failure	A - Attempt made to ...	One Time	01
9	PROGRAM ADOPTED AUTHORITY	Online Receivers	Standard	*PGMADP - Adoptin...	AP - Obtaining adopt...	A - Adopted authority...	One Time	01
10	USER PROFILE CREATE / CHANGE / RESTORE	Online Receivers	Standard	*SECURITY - Securi...	CP - User profile cha...	A - Create, change o...	One Time	01
11	CHANGE OBJECT AUDIT	Online Receivers	Standard	*SECURITY - Securi...	AD - Auditing changes	O - Object Auditing ...	One Time	01
12	RESTORED OBJECTS (REPLACE EXISTING)	Online Receivers	Standard	*SAVRST - Save an...	OR - Object restore	E - An obj was restor...	One Time	01
13	RESTORED OBJECTS (NEW)	Online Receivers	Standard	*SAVRST - Save an...	OR - Object restore	N - New obj was rest...	One Time	01
14	CHANGES TO THE USER PARAMETER OF A JOB D...	Online Receivers	Standard	*SECURITY - Securi...	JD - Change to user ...	A - The USER para...	One Time	01
15	NETWORK ATTRIBUTES CHANGED	Online Receivers	Standard	*SECURITY - Securi...	NA - Network attribut...	A - A network attribut...	One Time	01
16	USER COMMANDS	Online Receivers	Standard	*CMD - Commands	CD - Command string...	C - A command was ...	One Time	17
17	MOVE OBJECTS	Online Receivers	Standard	*OBJMGT - Object m...	DM - Object move or...	M - An object was re...	One Time	01
18	RENAME OBJECTS	Online Receivers	Standard	*OBJMGT - Object m...	DM - Object move or...	R - An object was re...	One Time	01
19	A PROGRAM WAS CHANGED TO ADOPT OWNER ...	Online Receivers	Standard	*SECURITY - Securi...	PA - Program chang...	A - A PGM was chan...	One Time	01
20	DELETED SPOOLFILES	Online Receivers	Standard	*SPLFDTA - Operati...	SF - Actions to spool...	D - A spooled file wa...	One Time	01
21	RESTORED ADOPTING AUTHORITY PROGRAMS	Online Receivers	Standard	*SAVRST - Save an...	RP - Restoring adopt...	A - A program that a...	One Time	01
22	CHANGE OBJECT AUTHORITY DURING RESTORE	Online Receivers	Standard	*SAVRST - Save an...	RA - Authority chang...	A - System change a...	One Time	01
23	RESTORED JOB DESCRIPTION	Online Receivers	Standard	*SAVRST - Save an...	RJ - Restoring job de...	A - A job desc. conta...	One Time	01
24	RESTORED OBJECTS (CHANGE OBJECT OWNER...	Online Receivers	Standard	*SAVRST - Save an...	RO - Change of obje...	A - The OBJDOWN w...	One Time	01
25	RESTORED OBJECTS (CHANGE PRIMARY GROUP)	Online Receivers	Standard	*SAVRST - Save an...	RZ - Changing a pri...	A - Object restored. ...	One Time	01
26	CREATE SPOOLED FILES	Online Receivers	Standard	*SPLFDTA - Operati...	SF - Actions to spool...	C - A spooled file wa...	One Time	01
27	HOLD SPOOLED FILES	Online Receivers	Standard	*SPLFDTA - Operati...	SF - Actions to spool...	H - A spooled file wa...	One Time	01
28	RELEASE SPOOLED FILES	Online Receivers	Standard	*SPLFDTA - Operati...	SF - Actions to spool...	R - A spooled file wa...	One Time	01
29	CHANGE DLO AUDITING (CHGDLOAUD)	Online Receivers	Standard	*SECURITY - Securi...	AD - Auditing changes	D - Auditing of a DL...	One Time	01
30	CHANGE AUDIT ATTRIBUTES (CHGUSRAUD)	Online Receivers	Standard	*SECURITY - Securi...	AD - Auditing changes	U - Audit. for a user ...	One Time	01
31	JOB TO WHICH WAS GIVEN DESCRIPTOR	Online Receivers	Standard	*SECURITY - Securi...	GS - Socket descrip...	G - A descriptor was ...	One Time	01
32	ADOPTED AUTHORITY PROGRAM STARTED	Online Receivers	Standard	*PGMADP - Adoptin...	AP - Obtaining adopt...	S - A program started...	One Time	01
33	ADOPTED AUTHORITY PROGRAM ENDED	Online Receivers	Standard	*PGMADP - Adoptin...	AP - Obtaining adopt...	E - A program ended...	One Time	01
34	SUBMITTED JOBS	Online Receivers	Standard	*JOBDTA - Job tasks	JS - Actions that affe...	B - A job was submit...	One Time	01
35	CHANGED JOBS	Online Receivers	Standard	*JOBDTA - Job tasks	JS - Actions that affe...	C - A job was chang...	One Time	01
36	JOBS ENDED SUCCESSFULLY	Online Receivers	Standard	*JOBDTA - Job tasks	JS - Actions that affe...	E - A job was ended...	One Time	01
37	HOLD JOBS	Online Receivers	Standard	*JOBDTA - Job tasks	JS - Actions that affe...	H - A job was held...	One Time	01
38	DISCONNECTED JOBS	Online Receivers	Standard	*JOBDTA - Job tasks	JS - Actions that affe...	I - A job was disconn...	One Time	01
39	END JOB COMMANDS USED	Online Receivers	Standard	*JOBDTA - Job tasks	JS - Actions that affe...	N - The ENDJOB co...	One Time	01
40	RELEASED JOBS	Online Receivers	Standard	*JOBDTA - Job tasks	JS - Actions that affe...	R - A held job was re...	One Time	01
41	STARTED JOBS	Online Receivers	Standard	*JOBDTA - Job tasks	JS - Actions that affe...	S - A job was started...	One Time	01
42	RESTART JOB STARTED	Online Receivers	Standard	*JOBDTA - Job tasks	JS - Actions that affe...	R - PGM start reque...	One Time	01

Add Change Delete Submit Close

Dozens of audit reports ready-shipped



New Report Definition

Report Number: Report Description:

Report Type

Periodic

One Time report

From Date: To:

From Time: To:

Action Group

Custom

Standard

Action Group:

Action Type:

Action

Account Type:

Account

Report Data

Receiver

History File

Library

Object (name or generic)

Program

Job ID

Job Name:

User:

Number:

Sort Order:

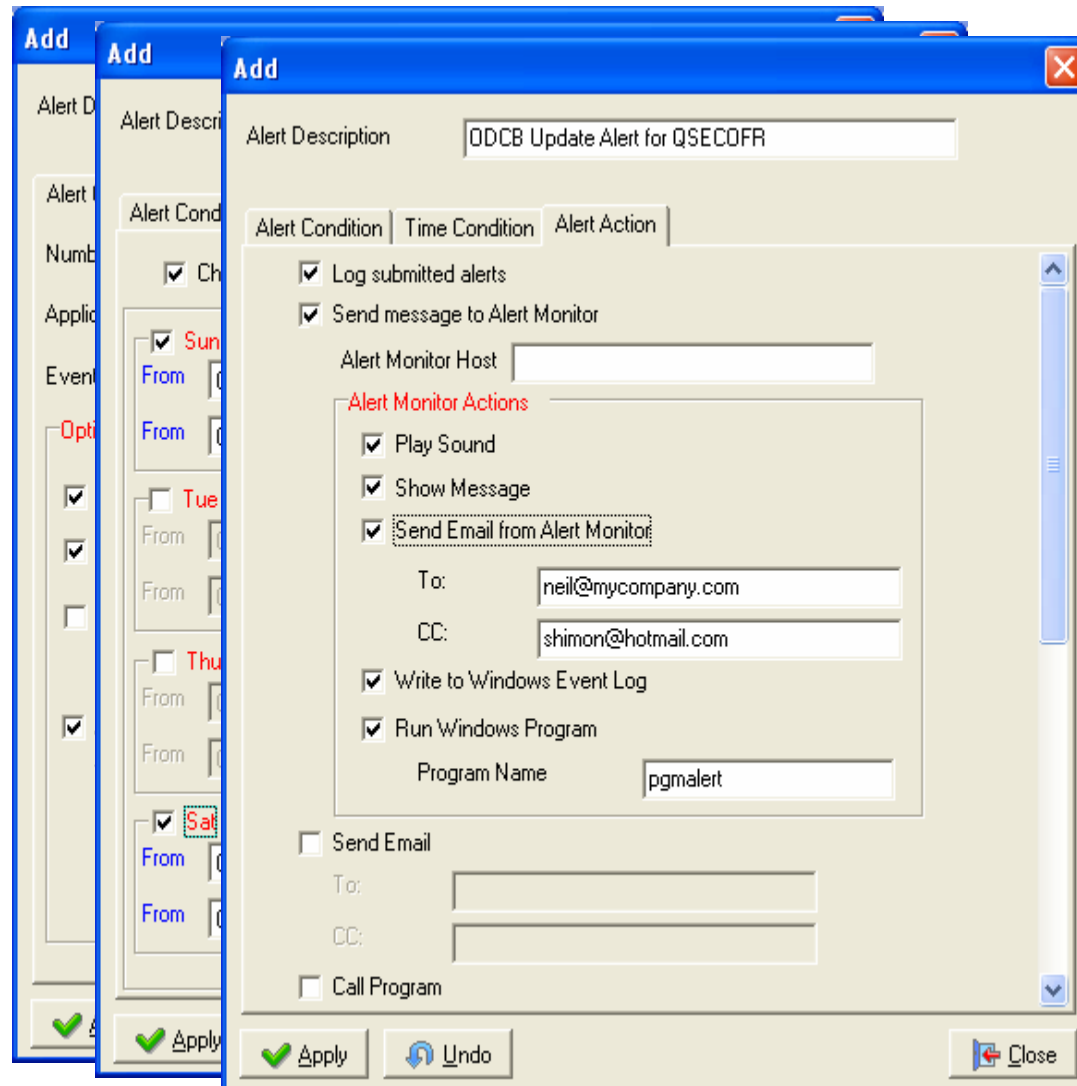
Apply Close

Report Generator to create tailored audit reports

“3. A real-time intrusion alerting mechanism”

Intrusion Detection System

- Alerts defined at granular level
- Alerts to any PC on the network
- Alerts to SNMP via IBM Tivoli, HP Openview, Tango/04 and others
- Alerts of access at a general or granular level
- System journal alerts
- Alerts linked to exit point control



Add

Alert Description: ODCB Update Alert for QSECOFR

Alert Condition | Time Condition | Alert Action

- Log submitted alerts
- Send message to Alert Monitor

Alert Monitor Host: [Text Box]

Alert Monitor Actions

- Play Sound
- Show Message
- Send Email from Alert Monitor
 - To: neil@mycompany.com
 - CC: shimon@hotmail.com
- Write to Windows Event Log
- Run Windows Program
 - Program Name: pgmaalert

Send Email

To: [Text Box]

CC: [Text Box]

Call Program

Buttons: Apply, Undo, Close

Some specific issues

1. Guarding the guards.
2. To know what data was viewed.
3. Keeping an appropriate audit trail over a long period.
4. Privacy - controlling what each user can see.
5. Temporary enhanced authority.

- Corporate responsibility, OK. But who guards the guards - who controls the administrators?
- Different authority levels for your administrators and auditors
- Role management built into the product to grant different authority levels for various Bsafe users

The issues:

- What data was viewed
- Keeping audit information over a long period
- Controlling what each user can see
- Temporary enhanced authority

The Solution:

- The read record audit
- The central audit module
- The field masking feature
- Account swapping module

A few references



Volkswagen Bank



Sony Financial Services

