Fact or Fiction: IBM i has Never Been Hacked

Carol Woodbury
VP of Global Security
Services

helpsystems

Agenda – Bringing Reality to the Situation

Why are We Talking About This?

- An “AS/400” was hacked – as documented in the article, “smoke on the Water [plant] in the “Data Breach Digest” from Verizon.

Data breach digest.

Scenarios from the field.

verizon✓

What Happened?

- A hacker was able to make use of a known vulnerability in the payment (credit card) software
  - Over 2.5 million records were exfiltrated
- The AS/400 administrator’s user id and password were stored in cleartext (and discovered) in an .ini file on a web server running on the AS/400. These were used to gain access to the Supervisory Control and Data Acquisition (SCADA) application which controls the community’s water supply.
  - The mixture of chemicals going into the water supply was manipulated, affecting times to replenish water supplies
- No network segmentation existed. The organization’s AS/400 was directly attached to the Internet and the internal network was exposed.

Others

- Call the FBI or your country’s investigative branch!

Was this Incident a Failure of AS/400, iSeries, IBM i?

“I Thought We Were Already Secure!”

IBM i has a well-deserved reputation as one of the most **securable** operating systems available.

But, **securable** does not imply you simply plug in the system and take no further action.

It takes a joint effort by:

- IBM (who supplies the OS),
- Your software vendors (who supply the application),
- And YOU (who has ultimate responsibility for the server and data)

Securable

Secure

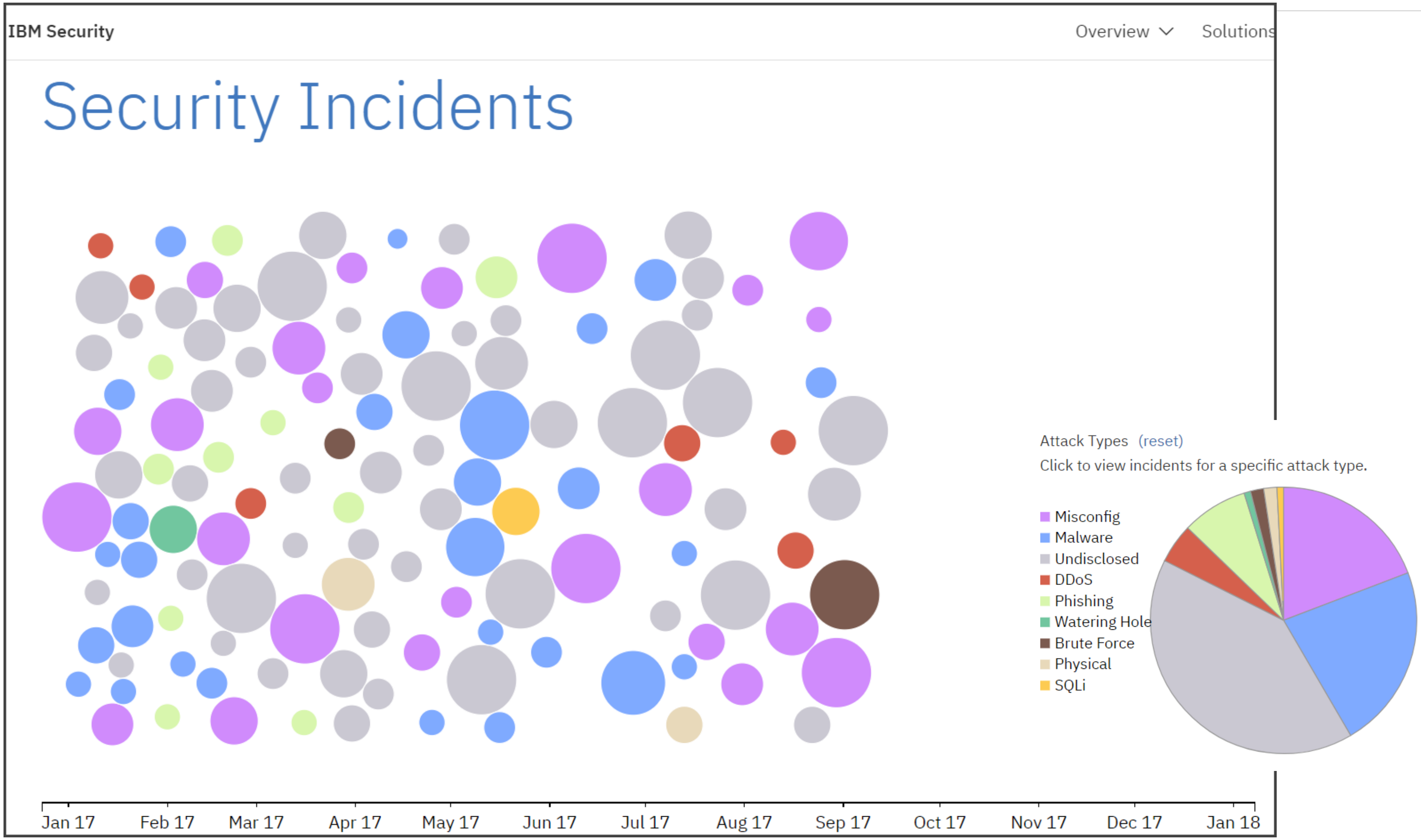
So, what was the Cause?

- Failure to:
  - Use the features readily available in IBM i
  - Follow any sort of security ‘best practices’
    - The write-up clearly pointed out that the single AS/400 administrator made no consideration for the security implications of the configuration settings chosen
  - Keep applications patched
  - Use common sense!

Types of Hackers

- Drive-by
- Exploiting known vulnerabilities
- Targeted attack
  - Nation-state, Professional hackers, Hackivists

Security Incidents by Attack Type, Time, & Impact



IBM Security

Security Incidents

Attack Types (reset)

Click to view incidents for a specific attack type.

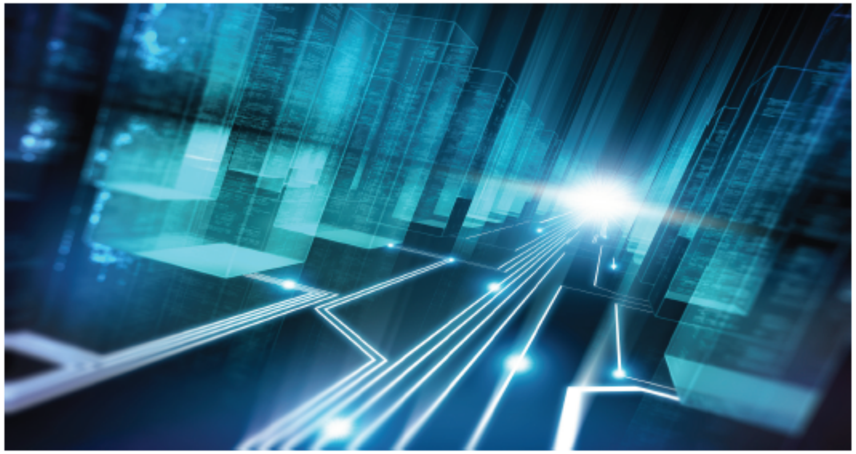
https://www.ibm.com/security/xforce/xfisi/

Ponemon Institute – 2016 Cost of Insider Threats

Three types of insider threats

- A careless or negligent employee or contractor
- A criminal or malicious insider
- A credential thief

Ponemon INSTITUTE



2016 Cost of Insider Threats

2016 Cost of Insider Threats – Interesting facts

- Total number of benchmarked organizations – 54
- Total number of insider incidents – 874
- Percentage by type:
  - Negligence - 68% (average per incident $206,933)
  - Criminal insider – 22% (average cost per incident $347,130)
  - Credential theft – 10% (average cost per incident $493,093)

Examples of Misconfiguration from the IBM i world

UP NEXT

Modified IBM i Profiles

Additional special authorities are often granted to IBM i-provided profiles:

- QSYSOPR
- QUSER
- QPGMR

Or private authorities are granted or *PUBLIC authority is changed to *USE or granter.

IBM i-supplied Profiles with a Password

IBM i-supplied profiles have shipped without a password for many, many years. While QSECOFR must have a password, the others should not.

Well-known profiles:

- QUSER
- QSYSOPR
- QSRV
- QSRVBAS
- QPGMR

New *ALLOBJ Profiles

No monitoring or recognition/approval of new profiles with *ALLOBJ (and other special authorities)

- Service accounts
- Copied profiles
- Vendor profiles
  - Take control of vendor access!

Default Passwords

Passwords the same as the user profile name

- Profile creation process
- Service accounts
- Vendor profiles
- No password rules

Specify:

QPWDRULES and include *LMTPRFNAME and *ALLCRTCHG (V7R2)

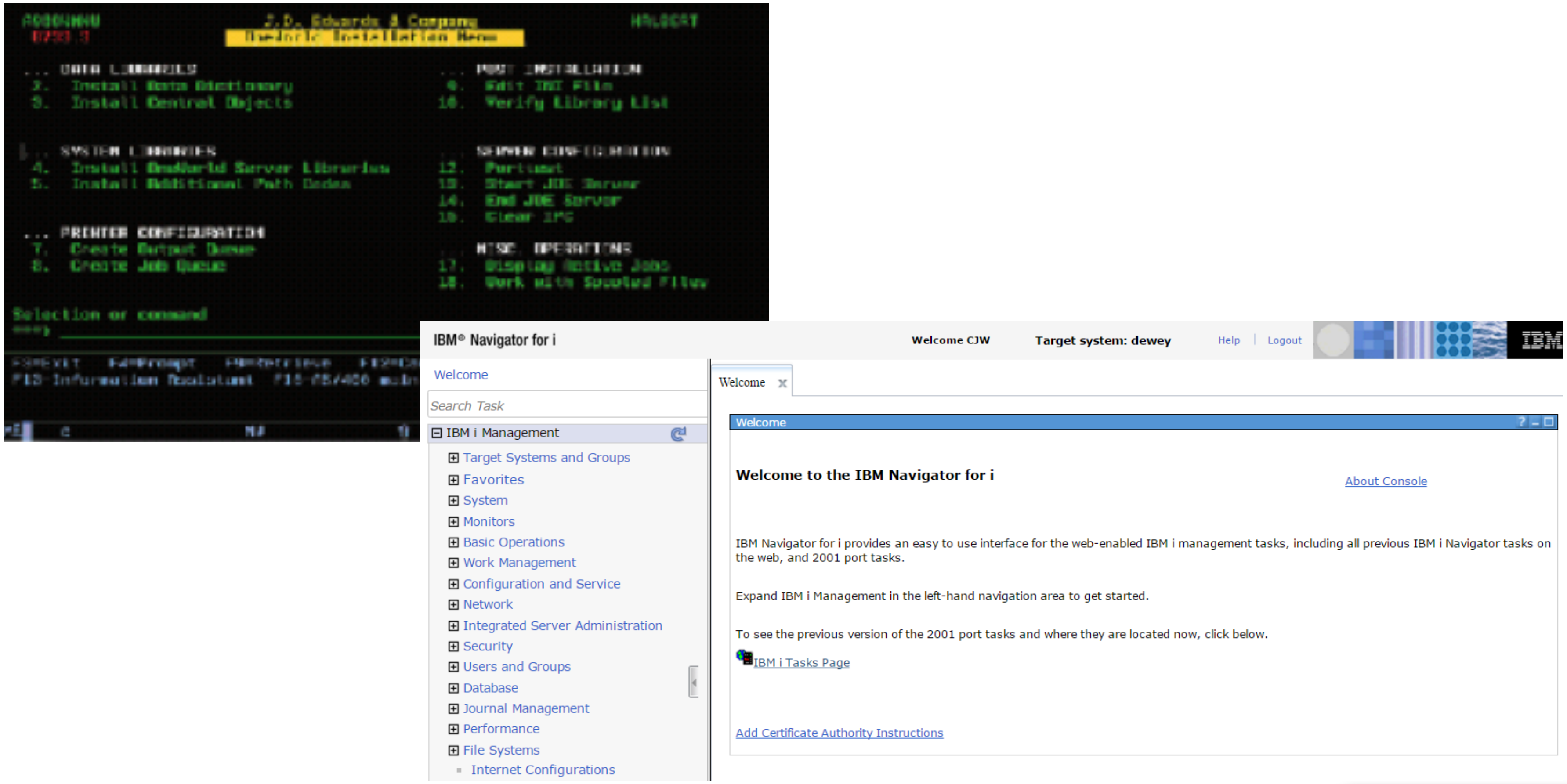
Service Accounts

Service accounts are often automatically created with *ALLOBJ (and often, all special authorities) because no one is sure what authority is required.

- In V7R3, use the authority collection function to determine the authority required.
- In prior releases, make the service account a member of the application owning profile if it needs *ALL authority to application objects
  - This is a better option than granting the service account *ALLOBJ special authority.

Device Time-out

No device time-out implemented



```
A0004NHU                 J.D. Edwards & Company                 HALOCAT
                        OneWorld Installation Menu

... DATA LIBRARIES                            ... POST INSTALLATION
 2.  Install Data Dictionary                   9.  Edit INI File
 3.  Install Central Objects                  10.  Verify Library List

... SYSTEM LIBRARIES                          ... SERVER CONFIGURATION
 4.  Install OneWorld Server Libraries        12.  PortTest
 5.  Install Additional Path Codes            13.  Start JDE Server
                                              14.  End JDE Server
                                              15.  Clear IPC

... PRINTER CONFIGURATION                     ... MISC. OPERATIONS
 7.  Create Output Queue                      17.  Display Active Jobs
 8.  Create Job Queue                         18.  Work with Spooled Files

Selection or command
===>

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant   F16=AS/400 main menu
```

IBM® Navigator for i — Welcome CJW — Target system: dewey — Help | Logout

Welcome to the IBM Navigator for i

About Console

IBM Navigator for i provides an easy to use interface for the web-enabled IBM i management tasks, including all previous IBM i Navigator tasks on the web, and 2001 port tasks.

Expand IBM i Management in the left-hand navigation area to get started.

To see the previous version of the 2001 port tasks and where they are located now, click below.

IBM i Tasks Page

Add Certificate Authority Instructions

Development Not Secured Like Production

Whether auditors like it (or not) production data often resides on Development LPARs.

- Development is rarely secured the same as Production
  - Developers often have *ALLOBJ
  - Object authorities rarely match

- Options
  - RCAC to mask the data (V7R2)
    - http://www.redbooks.ibm.com/redpieces/pdfs/redp5110.pdf
  - FIELDPROC to encrypt the column (V7R1)
    - Linoma Cryto Complete

Testing Without Consideration to Security

Testing new function without security in mind then scared to change the profile when moving into production (especially with deadlines looming.)

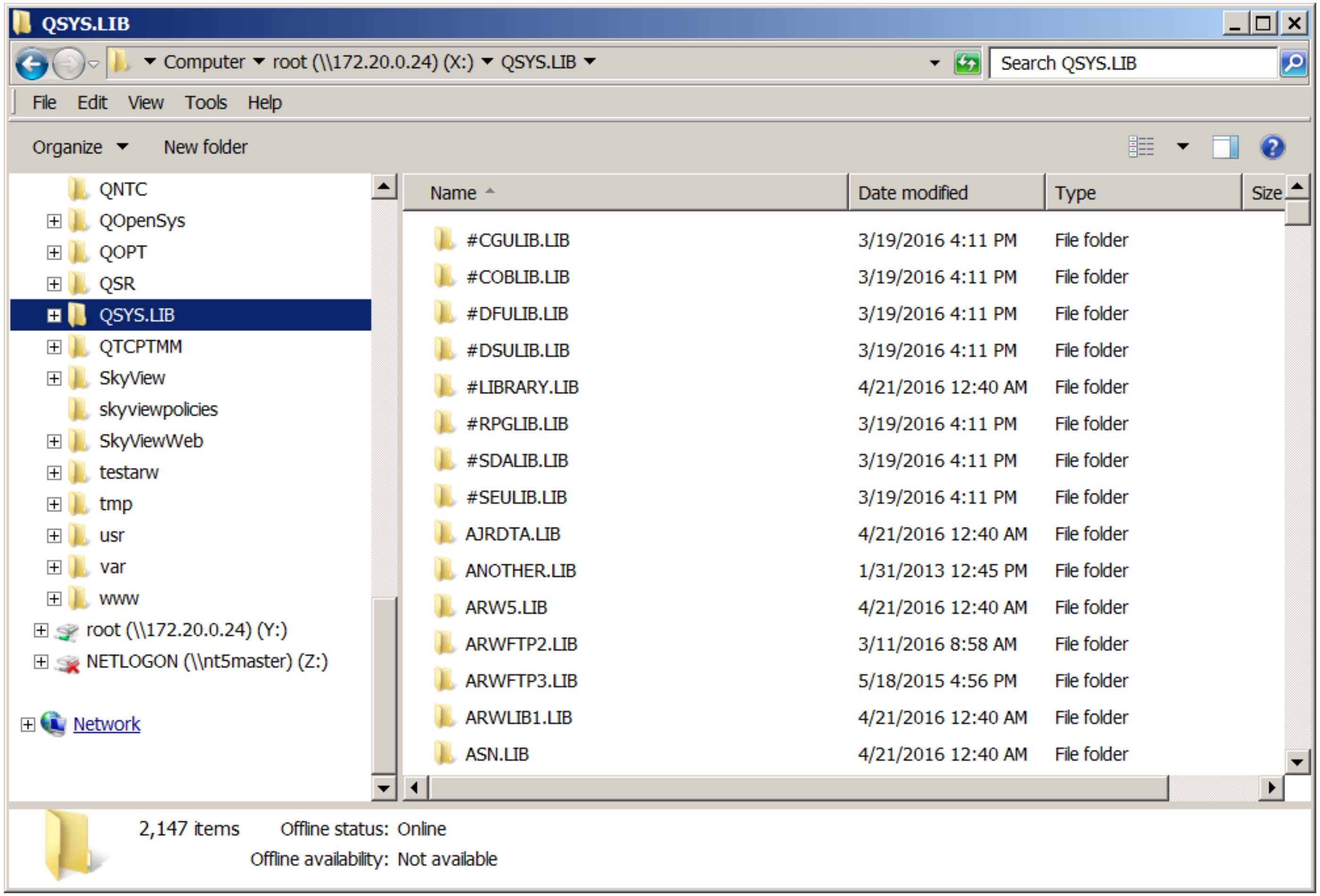
- Test profiles will often have too much authority – justified because you need to first get the application to work – then you'll think about security
  - When does that happen….?

Authorities Left After Debugging a Failure

Failures are often attributed to an “authority problem.”

- Authorities get added to debug a problem and never removed when it proves not to be the problem.
  - *ALLOBJ is added
  - *PUBLIC authority is opened up
  - Authorities are added to an authorization list

Shares to /root or QSYS.LIB



Name	Date modified	Type	Size
#CGULIB.LIB	3/19/2016 4:11 PM	File folder	
#COBLIB.LIB	3/19/2016 4:11 PM	File folder	
#DFULIB.LIB	3/19/2016 4:11 PM	File folder	
#DSULIB.LIB	3/19/2016 4:11 PM	File folder	
#LIBRARY.LIB	4/21/2016 12:40 AM	File folder	
#RPGLIB.LIB	3/19/2016 4:11 PM	File folder	
#SDALIB.LIB	3/19/2016 4:11 PM	File folder	
#SEULIB.LIB	3/19/2016 4:11 PM	File folder	
AJRDTA.LIB	4/21/2016 12:40 AM	File folder	
ANOTHER.LIB	1/31/2013 12:45 PM	File folder	
ARW5.LIB	4/21/2016 12:40 AM	File folder	
ARWFTP2.LIB	3/11/2016 8:58 AM	File folder	
ARWFTP3.LIB	5/18/2015 4:56 PM	File folder	
ARWLIB1.LIB	4/21/2016 12:40 AM	File folder	
ASN.LIB	4/21/2016 12:40 AM	File folder	

2,147 items Offline status: Online
Offline availability: Not available

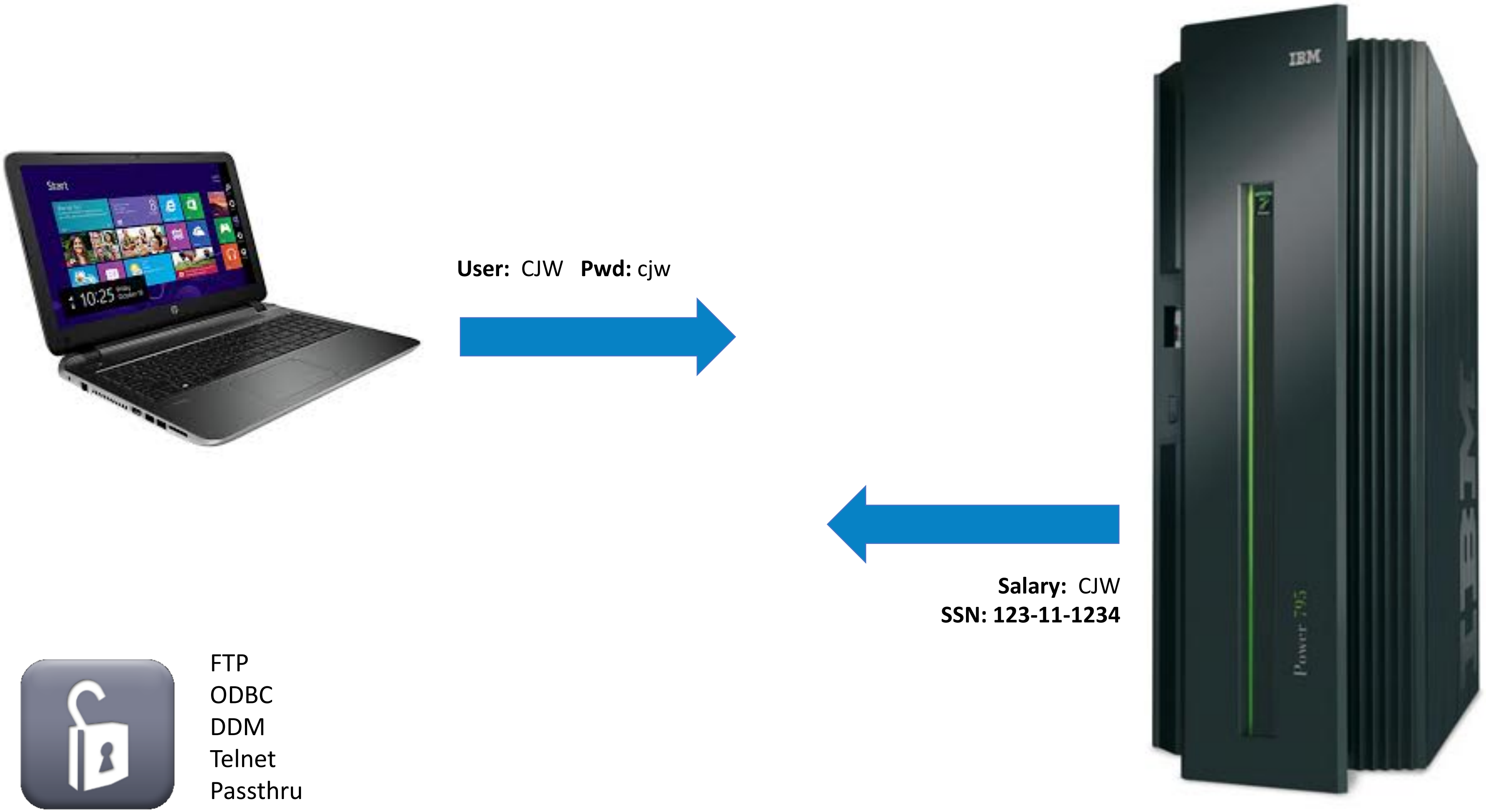
Sharing /root shares QSYS.LIB

/QSYS.LIB contains all libraries on the system.

Not Patching Known Vulnerabilities

- Integrity / Security PTFs
- Java group PTFs
- Anything to do with Open Source
- Moving from SSL to TLS1.2

Unencrypted Sessions



User: CJW **Pwd:** cjw

Salary: CJW
SSN: 123-11-1234

FTP
ODBC
DDM
Telnet
Passthru
SNA connections

Think 'Sniffing' Doesn't Happen…?

Then you haven't met this guy

To Combat Credential Sniffing

- Encrypt sessions
- Use MFA (Multi-factor authentication)

Web Applications Running on IBM i

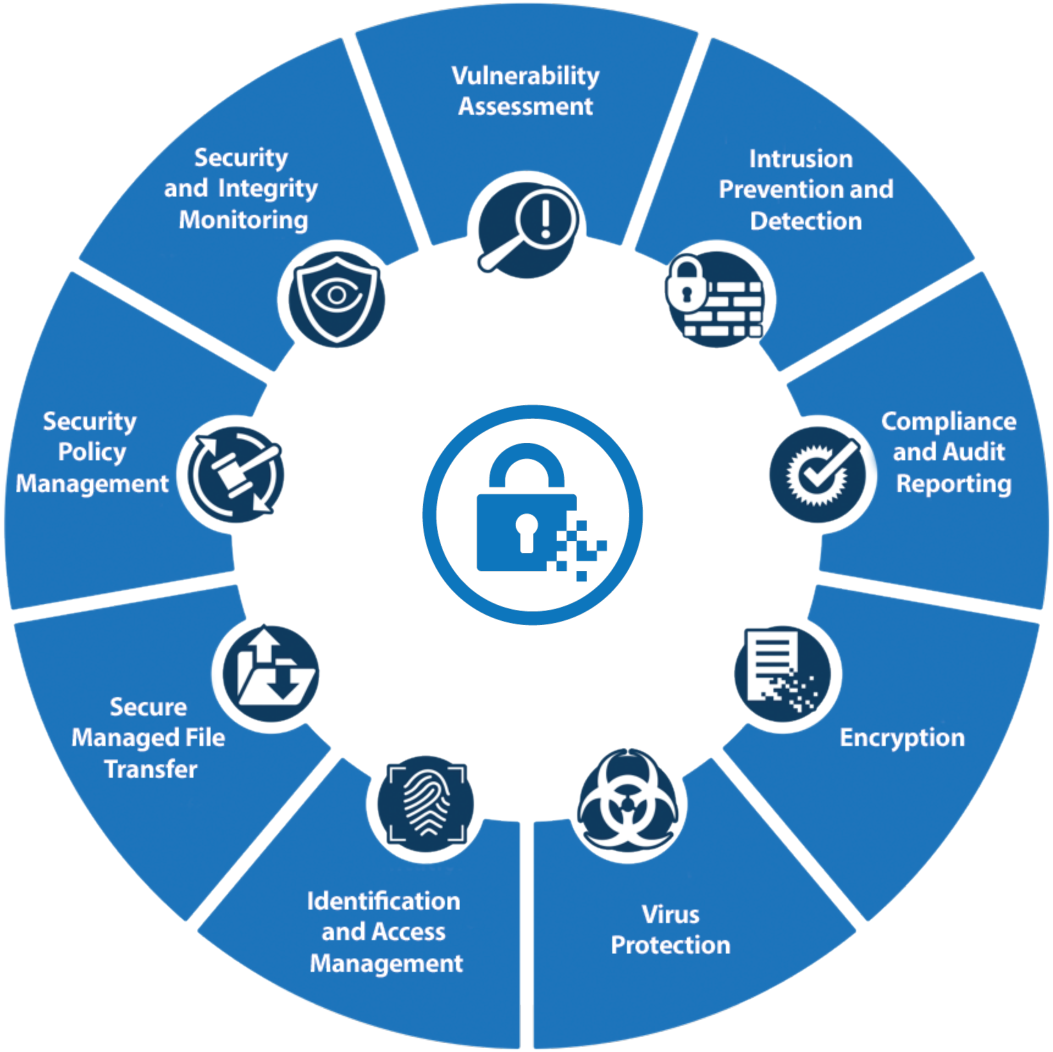
Impression that common exposures can’t occur on IBM i or best practices for web programming don’t apply.

Fiction!

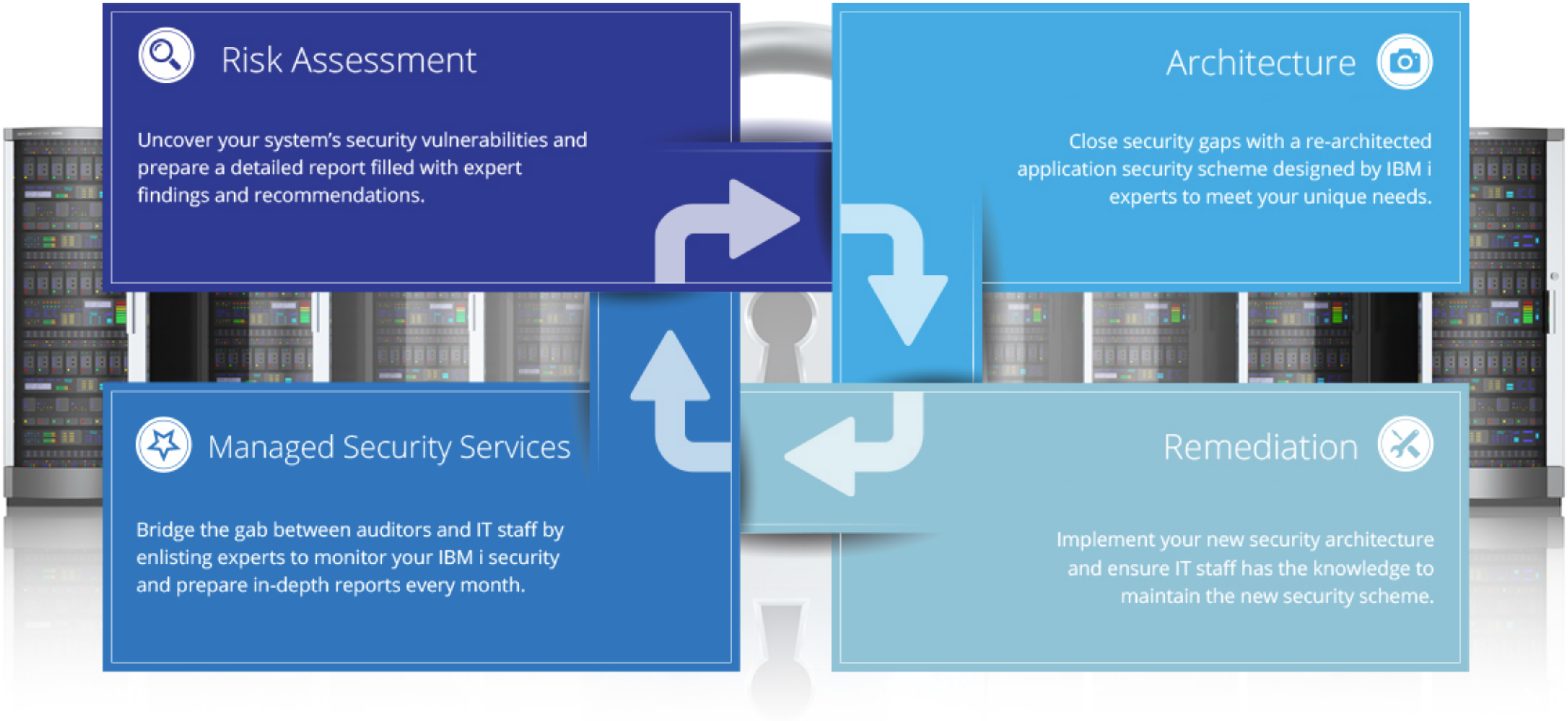
Do Any of These Situations Apply to Your Organization?

If so, are the security controls you have in place sufficient to protect the data and processes the organization depends on ?

HelpSystems’ Solution-Based Approach


Vulnerability Assessment
Intrusion Prevention and Detection
Compliance and Audit Reporting
Encryption
Virus Protection
Identification and Access Management
Secure Managed File Transfer
Security Policy Management
Security and Integrity Monitoring

Data Security Life Cycle



Risk Assessment

Uncover your system's security vulnerabilities and prepare a detailed report filled with expert findings and recommendations.

Architecture

Close security gaps with a re-architected application security scheme designed by IBM i experts to meet your unique needs.

Remediation

Implement your new security architecture and ensure IT staff has the knowledge to maintain the new security scheme.

Managed Security Services

Bridge the gab between auditors and IT staff by enlisting experts to monitor your IBM i security and prepare in-depth reports every month.

Questions?

www.helpsystems.com/professional-security-services

www.helpsystems.com

800-328-1000 | info@helpsystems.com