



helpsystems

Top 10 IBM i Configuration Mistakes that Leave your System Vulnerable

Carol Woodbury, CISSP, CRISC, PCIP
VP, Global Security Services
Carol.Woodbury@helpsystems.com

IBMCHAMPION 


© HelpSystems LLC. All rights reserved.
All trademarks and registered trademarks are the property of their respective owners.

2018
www.helpsystems.com

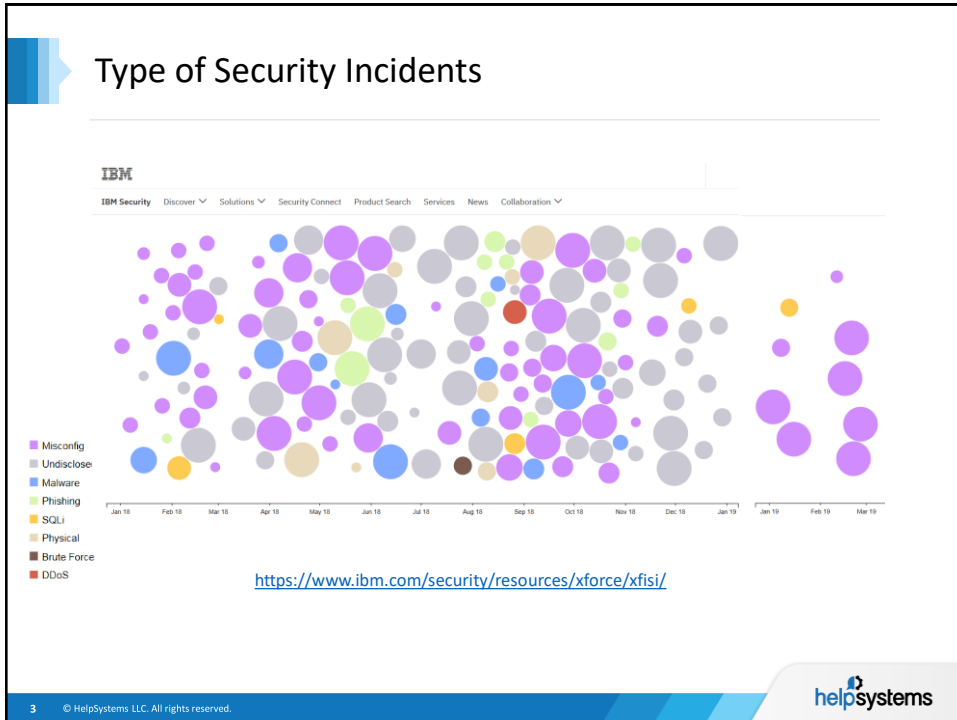
1

Three Types of Hackers

- Targeted attack
- Attack of opportunity
 - Takes advantage of known vulnerabilities in applications, operating systems or protocols or servers/applications that are out-of-date (missing patches)
- Attack for 'fun'

2 © HelpSystems LLC. All rights reserved. 

2



3

Exploiting misconfigurations

- Hacker scans for misconfigured AWS containers
 - <https://www.secureworldexpo.com/industry-news/capital-one-hacker-other-companies-indictment>

4 © HelpSystems LLC. All rights reserved. helpsystems

4

The Insider Threat



- Inadvertent threat actors are **insiders in your company who unwittingly compromise the environment.**
- Two of the most prolific ways X-Force researchers have observed inadvertent insiders leaving organizations open to attack is by **falling for phishing scams** or social engineering, and through the **improper configuration of systems, servers, and cloud environments**, and by **foregoing password best practices.**
- - IBM X-Force Threat Intelligence Index 2019

5

© HelpSystems LLC. All rights reserved.

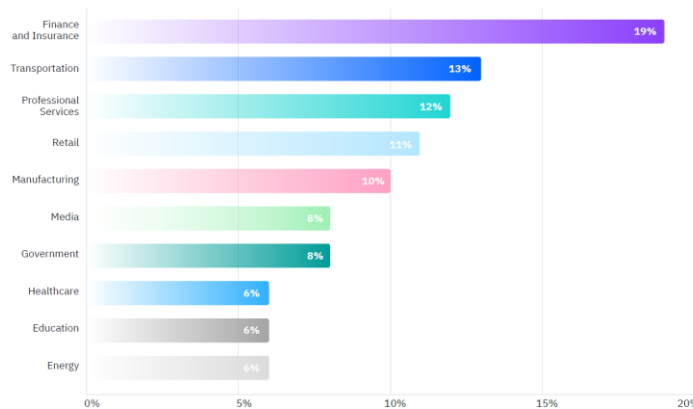


5

Who's the Target?

Most Frequently Targeted Industries in 2018

Source: IBM X-Force



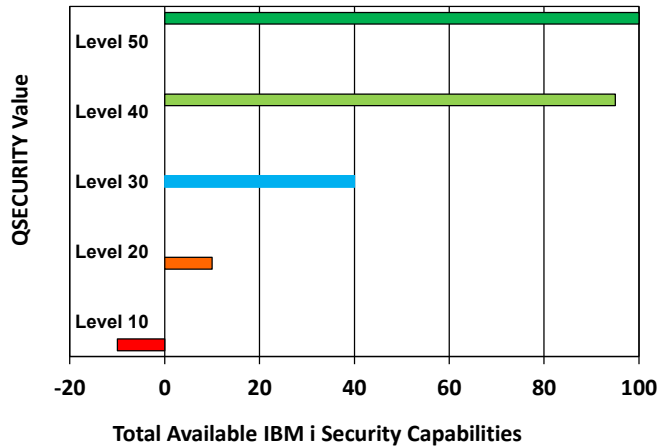
6

© HelpSystems LLC. All rights reserved.



6

#1: Running at the Wrong Security Level (QSECURITY)



© HelpSystems LLC. All rights reserved.

helpsystems

7

#2: Allowing Weak Passwords

- Password composition rules aren't set or are weak
 - Use QPWDRULES
- Users use the same password everywhere
- Users re-use passwords that have been compromised
 - User education !

Change Password

Please use 8 or more characters with a mix of letters, numbers and symbols.

8

© HelpSystems LLC. All rights reserved.

helpsystems

8

#3: Running at the Wrong Password Level (QPWDLVL)

System value	
0	Default Character set: A-Z, 0-9, \$, @, # and _ Maximum length: 10
→ 1	Same as level 0 but gets rid of old NetServer password- Safe to move if you are not using NetServer or not connecting with Windows 95, 98, ME or Windows 2000 server – end users will see no difference
2	Character set: Upper / lower case, all punctuation and special characters, numbers and spaces Maximum length: 128 Keeps NetServer password, encrypts with old and new algorithms Sign on screen changed to accommodate longer password, CHGPWD and CRT/CHGUSRPRF pwd field changed
→ 3	Same as level 2, gets rid of old encrypted password and old NetServer password Safe to move if you are not using NetServer or not connecting with Windows 95, 98, ME or Windows 2000 server – end users will see no difference

Changes require an IPL

<https://www.helpsystems.com/resources/on-demand-webinars/moving-password-level-2-or-3-and-other-password-tips-and-tricks>

© HelpSystems LLC. All rights reserved.

helpsystems

9

Passwords – Get Rid of Them!!!

- Switch to use SSO (Single Sign-on)
- IBM i passwords can be eliminated because AD credentials are used for authentication
- <https://www.helpsystems.com/resources/on-demand-webinars/how-achieve-single-sign-ss0-day>

10

© HelpSystems LLC. All rights reserved.

helpsystems

10

#4: Not Using 2FA (Two-Factor or Multi-Factor (MFA)) Authentication

- Authenticating with at least two of the following:
 - Something you know
 - Something you have
 - Something you are
- Required by several laws and regulations including PCI DSS

11

Encrypt Data in Motion

- Make sure all communications – even internal communications – are encrypted
- For internal communications
 - Use DCM (Digital Certificate Manager) to create and/or assign certificates
 - Use the Certificate Authority certificate in the deployment of Access Client Solutions (ACS)
 - Configure clients to use an encrypted session
 - For guidance:
 - <https://www.helpsystems.com/resources/on-demand-webinars/configuring-accs-access-client-solutions-use-ssl-tls>
 - <https://www.helpsystems.com/resources/on-demand-webinars/securely-deploying-ibms-access-client-solutions-accs>
- For secure file transfer and communications outside of the organization use GoAnywhere.
 - <https://www.helpsystems.com/product-lines/goanywhere>

14

#6: Using Weak Encryption (QSSL* System Values)

- ▣ QSSLPCL – list of SSL protocols on the system
 - ▣ *OPSYS – list is determined by the system and can vary by release. This is the default. Or to control, specify one or more of the following:
 - ▣ *TLSV13 (V7R4)
 - ▣ *TLSV12
 - ▣ *TLSV11
 - ▣ *TLSV1
 - ▣ *SSLV3
 - ▣ *SSLV2
- ▣ QSSLCSLCTL – who controls the list specified in QSSLCSL – the system (*OPSYS - default) or user (*USRDFN)
- ▣ QSSLCSL – contains list of ordered cipher suites to be used on an SSL connection. Can only be modified if QSSLCSLCTL is *USRDFN.

© HelpSystems LLC. All rights reserved.

helpsystems

15

Protocols by Release

OS Release	SSLv2	SSLv3	TLS1.0	TLS1.1	TLS1.2	TLS1.3
V5R4	A	X	X			
V6R1	A	X	X			
V7R1	A	X	X			
V7R1 w/TR6	A	X	X	A	A	
V7R2	A	A	X	X	X	
V7R3	A	A	X	X	X	
V7R4		A	A	A	X	X

X = Enabled by default
 A = Available but not by default
 Blank = Not available

© HelpSystems LLC. All rights reserved.

helpsystems

16

Weak Protocols and Ciphers – as of April 2019

- Protocols: SSLv2, SSLv3, TLS1.0 and TLS1.1

- Ciphers:

- *RSA_RC4_128_SHA
- *RSA_RC4_128_MD5
- *RSA_NULL_MD5
- *RSA_NULL_SHA
- *RSA_NULL_SHA256
- *RSA_DES_CBC_SHA
- *RSA_EXPORT_RC4_40_MD5
- *RSA_EXPORT_RC2_CBC_40_MD5
- *RSA_RC2_CBC_128_MD5
- *RSA_DES_CBC_MD5
- *RSA_3DES_EDE_CBC_MD5
- *RSA_3DES_EDE_CBC_SHA
- *ECDHE_ECDSA_NULL_SHA
- *ECDHE_ECDSA_RC4_128_SHA
- *ECDHE_RSA_NULL_SHA
- *ECDHE_RSA_RC4_128_SHA
- *ECDHE_RSA_3DES_EDE_CBC_SHA
- *ECDHE_ECDSA_3DES_EDE_CBC_SHA

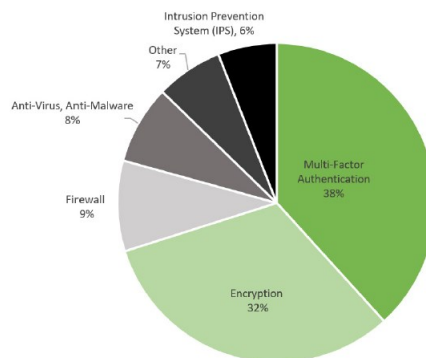
- <http://www-01.ibm.com/support/docview.wss?uid=nas8N1020876>

© HelpSystems LLC. All rights reserved.

helpsystems

18

Why the Emphasis on Encryption and 2FA?



- According to a 2017 Black Hat Hacker Survey by Thycotic, encryption and 2FA were the most difficult to get through
- Secureworks Incident Response Insight Report 2019 - <https://www.securityweek.com/failures-cybersecurity-fundamentals-still-primary-cause-compromise-report>

19 © HelpSystems LLC. All rights reserved.


helpsystems

19

Coffee with Carol Webinars

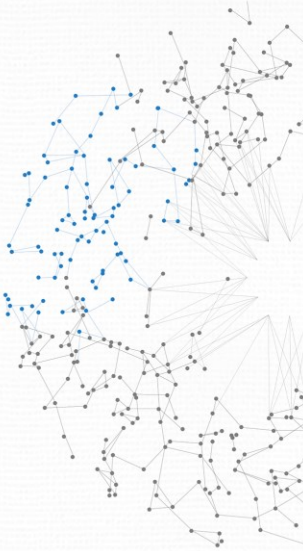
- Making the Move from SSL to TLS
 - <https://www.helpsystems.com/resources/on-demand-webinars/making-move-ssl-tls11-and-tls12>
- Configuring ACS to use SSL/TLS
 - <https://www.helpsystems.com/resources/on-demand-webinars/configuring-acs-access-client-solutions-use-ssl-tls>

© HelpSystems LLC. All rights reserved.




20

User Profiles



UP NEXT

HelpSystems Corporate Overview. All rights reserved. 

21

Too.Much.Power.



22

© HelpSystems LLC. All rights reserved.

22

#7: Not Reviewing User Profiles

- Group assignments need to be reviewed periodically (e.g., quarterly)
 - DSPUSRPRF USRPRF(QPGMR) TYPE(*GRPMBR)
 - DSPAUTUSR SEQ(*GRPPRF)
- Special authorities
 - Start creating new profiles with only the special authorities required to do their jobs
 - PRTUSRPRF
 - DSPUSRPRF USRPRF(*ALL) OUTPUT(*OUTFILE) OUTFILE(MY_LIB/PROFILES)
 - QSYS2.USER_INFO view
- Limited capability setting
 - Most users should be LMTCPB(*YES)

© HelpSystems LLC. All rights reserved.

23

#8: Leaving Inactive Profiles on the System

- Inactive
 - Look at the Last used date (not the Last signon date!)
 - GO SECTOOLS, options 2-4

© HelpSystems LLC. All rights reserved.

helpsystems

25

Profile Clean-up Hints

- If PASSWORD(*NONE) then set PWDEXPIV to *SYSVAL
- If profile is only used for batch processing it doesn't need a password and can be set to STATUS(*DISABLED)
- You can't delete (the system will prevent the deletion of) a
 - Group profile that has members
 - Profile that owns objects

© HelpSystems LLC. All rights reserved.

helpsystems

26



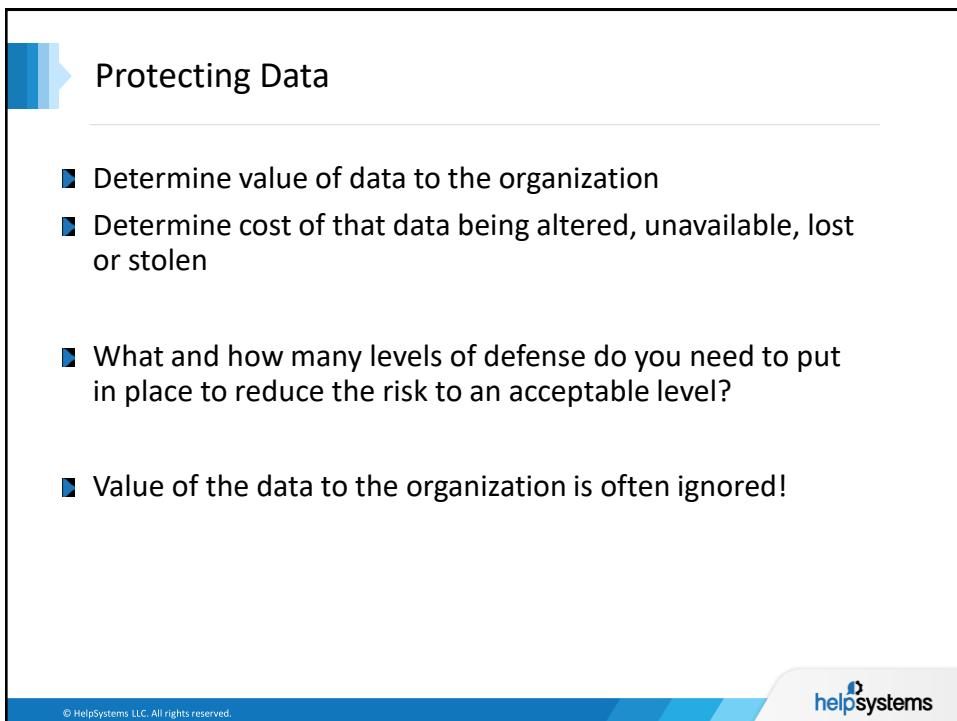
Protecting Data

UP NEXT

HelpSystems Corporate Overview. All rights reserved. helpsystems

The slide features a background of faint binary code (0s and 1s) and a network diagram on the right side consisting of numerous nodes connected by lines, with some nodes highlighted in blue.

27



Protecting Data

- Determine value of data to the organization
- Determine cost of that data being altered, unavailable, lost or stolen
- What and how many levels of defense do you need to put in place to reduce the risk to an acceptable level?
- Value of the data to the organization is often ignored!

© HelpSystems LLC. All rights reserved. helpsystems

The slide has a blue arrow graphic pointing right next to the title 'Protecting Data'.

28

Security Must be More than Menu 'Security'



Users downloading to an Excel spreadsheet

JDBC connections to WebSphere applications

FTP to banks, payroll processors, trading partners

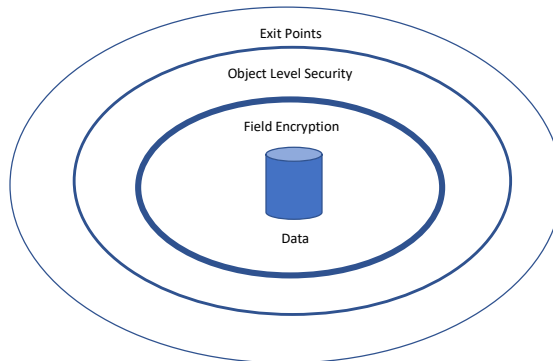
Developers updating data

Users running SQL or Queries

DDM

Administrators and Analysts with legitimate command line access

#9: Not Implementing Multiple Layers of Defense (Defense in Depth)



Secure the Data

- Start by considering how the data should be secured
 - For Integrity -> *PUBLIC(*USE)
 - For Confidentiality -> *PUBLIC(*EXCLUDE)
- Implement object level security to protect the data from unauthorized access
 - Determine how to secure the data without breaking other applications

© HelpSystems LLC. All rights reserved.

helpsystems

31

#10: Not Reviewing Authorization Lists

- Review (at least quarterly), profiles authorized to authorization lists
 - DSPAUTL
 - QSYS2.AUTHORIZATION_LIST_USER_INFO
- May also want to review objects secured by the list
 - DSPAUTLOBJ
 - QSYS2.AUTHORIZATION_LIST_INFO
 - <https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/IBM%20i%20Technology%20Updates/page/DB2%20for%20i%20-%20Services>

© HelpSystems LLC. All rights reserved.

helpsystems

32

#11: Not Reviewing Adopted Authority

- ▣ Not dangerous as long as it's used wisely
- ▣ Need process in place to review programs that adopt – especially an *ALLOBJ profile
- ▣ Caution!
 - ▣ Programs that put up a command line
 - ▣ Set Use adopted authority to *NO and User profile to *USER
 - ▣ Menu options that call an IBM command – WRKSPLF, WRKQRY, STRSQL
 - ▣ Put them into a CL program and set to USEADPAUT(*NO) USRPRF(*USER))
- ▣ PRTADPOBJ (Print Adopting Objects) to monitor/review

34

#11 – Not Reviewing Adopted Authority

- ▣ Not dangerous as long as it's used wisely
- ▣ Need process in place to review programs that adopt – especially an *ALLOBJ profile
- ▣ Be wary of:
 - ▣ Programs that put up a command line (set Use adopted authority to *NO and User profile to *USER)
 - ▣ Menu options that call an IBM command – WRKSPLF, WRKQRY, STRSQL (may be to add them to a CL program and set that program to be USEADPAUT(*NO) USRPRF(*USER))
 - ▣ PRTADPOBJ
- ➔ Use Policy Minder to establish a baseline and identify programs that adopt

35

#12: Configuring DDM to Connect without a Password

- Most DDM servers do not require a password on the connection
- ADDSVRAUTE (Add Server Authentication Entry) allows you to add an entry to connect as another (more powerful) user
- If you can't change the DDM server configuration:
 - Secure the ADDSVRAUTE, SBMRMTCMD and CRTDDMF commands
 - Use Exit Point Manager to block access to unauthorized users

© HelpSystems LLC. All rights reserved.




36



IFS



UP NEXT

HelpSystems Corporate Overview. All rights reserved. 

37

#13: Sharing root ("/")

The screenshot shows the File Shares console with a table of shares. The 'root' share is highlighted in yellow, and a red arrow points to its 'Current Users' column, which shows '1'.

Name	Path	Description	Current Users	Access
Qpbrsv	\\QIBMProdData\OS400\DirSrv	OS/400 - Directory Services	0	Read/Write
Qibm	\\QIBM		0	Read/Write
acs	\\ACS	Access Client Solutions	0	Read/Write
awshare	\\home\aw1	AW1 home folder share	0	Read/Write
b242	\\SkyView		0	Read/Write
Share1	\\SkyView	Test Share	0	Read/Write
aw1share	\\home\aw1		0	Read/Write
root	\\	Share to root	1	Read/Write
Arw1	\\arw1	testing moves	0	Read/Write
Testahr	\\testahr		0	Read/Write
Thisisanews	\\home		0	Read only
Zlungst	\\home\arw1\one\thisisa long directory		0	Read only
Zfour	\\arw1\testamy\testamy3		0	Read only

Remove read/write shares – especially to '/root'

38

Removing Shares

- Select the share
- Use the Actions dropdown to choose Properties
- Click on Sessions

The screenshot shows the Sessions table with one row selected. The 'Select' column has a checkbox checked, and the 'Workstation Name' is ':ffff:10.60.33.192'. The 'User Name' is '451 Cjw' and 'Time Active' is '233'.

Select	Workstation Name	Sessi...	User Na...	Time Active	Time Idle
<input checked="" type="checkbox"/>	:ffff:10.60.33.192	451	Cjw	233	

Page 1 of 1 | 1 | Go | Rows 1 | Total: 1 Filtered: 1 Selected: 0

Refresh

39

#14: Leaving Root at the Default *PUBLIC Authority

- Reduce the *PUBLIC authority of '/' from
 - DTAAUT(*RWX) OBJAUT(*ALL) to
 - DTAAUT(*RX) OBJAUT(*NONE)
- Review the CO and DO audit journal entries prior to making any changes to make sure you accommodate objects being created into (CO) / deleted out of (DO) '/root'

40

© HelpSystems LLC. All rights reserved.



40

Miscellaneous



UP NEXT

HelpSystems Corporate Overview. All rights reserved.

41

#15: Hoarding!



- ▀ Inactive profiles
- ▀ De-commissioned servers
- ▀ Archived data past retention schedule
- ▀ Copies made prior to updating a database
 - ▀ filenameX, filenameOld, filename2, filenameCopy
- ▀ File shares
- ▀ Past versions of vendor products
- ▀ Vendor products no longer in use

42

© HelpSystems LLC. All rights reserved.

42

#16: Not Saving and/or Not Verifying your Save Media

- ▀ How often are you saving security data (SAVSECDTA)?
 - ▀ User profiles
 - ▀ Private authorities
 - ▀ Authorization lists
- ▀ Note: Reducing the private authorities on your system reduces the SAVSECDTA and RSTAUT times
- ▀ Note: No one should have *SAVSYS special authority except Administrators and Operators
 - ▀ Can always save / restore what you own or have authority too
- ▀ Your ability to recover from malware infecting IBM i may depend on how good your back-ups are



© HelpSystems LLC. All rights reserved.

43

#17: Not Staying Current!

- OS level
 - Many security enhancements – including protocols and cipher suites that may be needed for compliance - aren't available in lower releases.
 - V7R1 out of support as of April 30, 2018
- Technology Refresh
 - <https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/IBM%20i%20Technology%20Updates/page/IBM%20i%20Technology%20Updates>
- PTFs (especially for Java, OpenSource, etc)
 - Use the SYSTOOLS.GROUP_PTF_CURRENCY
 - <https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/IBM%20i%20Technology%20Updates/page/DB2%20for%20i%20-%20Services>
 - Sign up for email alerts
 - https://static.helpsystems.com/powertech/pdfs/other/registering-for-ibm-i-security-bulletins.pdf?_ga=2.80461141.393372873.1518473394-983144696.1457057176
- iAccess (out of service as of April 30, 2019) -> Access Client Solutions

© HelpSystems LLC. All rights reserved.

helpsystems

44

Start Somewhere – Even if It's a Small Step!



© HelpSystems LLC. All rights reserved.

helpsystems

50

HelpSystems' Professional Security Services

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

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

Penetration Testing
Test your security defenses through penetration testing—ethical hacking required by auditors that highlights the danger of security vulnerabilities.

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.

Single Sign On Managed Services
Help implement and maintain Single Sign On, eliminating up to 80 percent of password management costs.

51 © HelpSystems LLC. All rights reserved.

51

HelpSystems' Solution-based Approach

Compliance Reporting
Compliance Monitor for IBM i

Privileged Access Management
Authority Broker for IBM i

Self-Service Password Reset
Password Self Help for IBM i

Database Monitoring
Database Monitor for IBM i

User Provisioning
Identity Manager for IBM i

Multi-Factor Authentication
Multi-Factor Authentication, SecurID Agent for IBM i

Native Encryption
Encryption for IBM i

Perimeter Access Control
Exit Point Manager for IBM i

Command Monitoring
Command Security for IBM i

Automated Risk Audit
Risk Assessor for IBM i

Security Information and Event Management
SIEM Agent for IBM i, Event Manager

Native Virus Protection
Antivirus for IBM i

InfoSec Policy Control
Policy Minder for IBM i

Secure Managed File Transfer
GoAnywhere

Security Scan
Free IBM i security snapshot

52 © HelpSystems LLC. All rights reserved.

52

Questions?



www.helpsystems.com/professional-security-services
www.helpsystems.com
info@helpsystems.com

© HelpSystems LLC. All rights reserved.



53