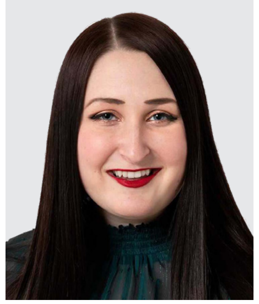
TechChannel

Why Knowing Your Organization's Security Needs Can Help Keep Data Locked Down

→ Patrick Botz on determining which security best practices apply to your organization's needs

→ Rob McNelly on what questions you and your AIX network team should be asking to make sure data is locked down contents

Keep Data Guarded With a Multilayered Security Approach



IBM Power Systems hardware and AIX are innately secure—but even top-notch security requires monitoring, patching and security planning to guard against bad actors and keep data locked down.

Complacency is a recipe for disaster when it comes to security. An effective security plan requires a multilayered approach that starts with people, then physical security measures, then other various layers. With a cross-functional approach where everyone works together, a security team can keep data guarded from cyberhacks, internal security threats and more.

Many organizations believe that following security best practices can help guard against breaches. In some cases—they're right. However, when adopting a best practice it's key to know whether or not it applies to your organization, where it should be applied and when. Compare best practices against your security policies and your business needs. Understand the details, and get feedback from your team and other organizations in your industry.

In this TechChannel e-book, you'll learn the importance of implementing a multilayered security approach, avoiding security complacency and researching effective (and relevant) security best practices.

Keelia Estrada Moeller, Senior Editor

Key AIX Security Considerations

Rob McNelly explains what questions you and your team should be asking to make sure data is locked down

BY ROB MCNELLY

You've seen the headlines about malware attacks and cyberhacks. Whether it's a competitor looking to steal your secrets or criminals looking to extort money, system administrators have myriad reasons to be wary. After all, the only absolutely secure system is one that is powered off.

Luckily, if you're running AIX on IBM Power Systems hardware, you are officially "secure" and don't need to take further action (in case you couldn't tell, that's sarcasm).

Don’t get me wrong; AIX is great. **It's my favorite OS.** But it still requires monitoring and patching, and that's for starters. If you don't believe me, check IBM's **APAR security information** or **CVE vulnerability data.**

It may be true that Windows and Linux systems, which number in the millions, are higher profile and thus more commonly targeted. However, that's no reason for AIX admins to be complacent. If anything, systems running AIX make more tempting targets for bad actors. Look at it this way: The data held on AIX systems is incredibly valuable.

These machines typically run mission-critical workloads and essential databases and applications for some of the world's largest enterprises. What are the ramifications of someone gaining access to or corrupting this data? What happens if records are deleted or destroyed? Yes, most AIX systems are behind a firewall, and most large corporate environments have disaster recovery sites and detailed recovery plans. Again though, that's not enough. More must be done to reduce the chances of a damaging attack.

Put Yourself on Notice: IBM Support

I like to keep up to date on the latest known vulnerabilities by subscribing to IBM's notifications. You can bookmark the links I cited earlier, or just do what I do and register for IBM updates. I receive weekly emails from IBM. Go to the **IBM Support site** to subscribe and **manage your subscriptions** and delivery preferences.

While I prefer weekly updates, you can opt for daily email. You can also limit update topics to ensure the information you receive is relevant.

Once you check these boxes, ask yourself some questions about your own environment. For instance, if an attacker gains access to your internal network,

The data held on AIX systems is incredibly valuable. These machines typically run mission-critical workloads and essential databases and applications for some of the world's largest enterprises. What are the ramifications of someone gaining access to or corrupting this data?

how quickly or easily could you identify the vulnerability? Are unnecessary services running on your machine? It’s harder to attack a system that's listening on only a limited number of ports.

I mentioned firewalls: They're a nice line of defense, but attackers can still beat them and gain access via the network. They could gain a foothold by compromising VPN credentials or some Windows or Linux machine on the network, and then move laterally within your organization by behaving as an authorized network user. Your network team should be watchful for unusual behavior such as logins at odd hours or atypical actions.

Asking the Tough Security Questions

To see if you are covered, ask yourself these 18 questions:

1. Do the user IDs on your system have strong passwords?
2. Have you changed your default password algorithm?
3. Have you disabled or deleted accounts that are no longer needed?
4. Are you authenticating via LDAP or some other central service, or are you trying to manually manage user IDs across your machines?
5. Once users log in, are they allowed to escalate their privileges via sudo or some other mechanism?
6. Are those permissions regularly audited?
7. Are the sudo logs themselves audited?
8. Are you tracking attempts, successful or not, to log into your system? Put a machine on port 22 on the public facing internet and see how quickly it gets inundated. If you're seeing that sort of activity behind your firewall, something may not be right.
9. If you're tracking logins, are log files being monitored and reviewed?
10. Do you have a security information and event management (SIEM) server that actively checks logs across your environment?
11. Are log files growing without being rotated, or are they allowed to grow indefinitely? Considering the huge amount of disk that we can allocate to file systems these days, log file size may seem insignificant, but rotating these logs is still a good idea.
12. Do you keep logs locally or send the files to a central system? This information can help diagnose an intrusion, particularly if an attacker gains access to a machine and alters the files stored there. Of course, if an attacker accesses the logging machines and deletes those files, that's another matter.
13. Are your systems regularly patched? Besides the OS, are you up to date on patching system firmware, device firmware and any VIO servers that are in use?
14. For those who continue to rely on legacy applications and older AIX versions, are you taking extra precautions? Those using unsupported hardware and software don't have the options of opening a problem ticket with IBM support or applying security patches. If you're dealing with these limitations, you must be extra vigilant in assessing and monitoring risks to your environment.

Most AIX systems are behind a firewall, and most large corporate environments have disaster recovery sites and detailed recovery plans. Again though, that's not enough. More must be done to reduce the chances of a damaging attack.

15. What are your procedures, who gets notified, and what actions are taken when an intrusion attempt is detected or recognized after the fact?

16. Who determines when systems should be removed from the network, and who decides how to analyze the system after an event occurs?

17. At what point do you declare a disaster and move operations to another location?

18. Do you have a disaster recovery plan?

Help From the Outside: Lab Services and Documentation

IBM Lab Services for Power Systems or your IBM Business Partner can help you assess your organization's security and compliance practices and procedures.

Another option is to engage a penetration testing company. Penetration testers simulate attacks to determine how your system would hold up against the real thing, and how well your staff responds to notifications of anomalies in real time. Knowing that there was no detection of an attack is valuable information as well.

While this overview offers a few things to keep in mind as far as managing the security of your systems, it is by no means intended to be an exhaustive list. Rather it is meant to help jump start conversations in your organization to start considering how important your data is and what you can do it keep it safe. I encourage you to read **this detailed look at AIX security strategies** authored by lifetime IBM Power Champion Jaqui Lynch (see a sneak peek of this article on **page 8**).

ROB MCNELLY is a senior AIX solutions architect and IBM Power Systems Champion.

Basic AIX Security Strategies and Best Practices: Locking Down LPARs

BY JAQUI LYNCH

So much of our personally identifiable information is now being stored that the security break-ins that have been happening have most likely affected everyone reading this article. Additionally, the penalties now for breaches of the various standards (e.g., HIPAA, PCI, etc.) are significant. Good security requires a multilayered approach that starts with people, then physical security, and then the various layers. It's critical to look at the whole environment and see how security can be applied at each level.

Here, you'll learn some of the basics of locking down your LPARs. This isn't done by default, but it's fairly easy to do. It ranges from default permissions and umasks, good usernames and passwords, logging, patching, and removing insecure daemons to integration with LDAP or active directory (AD). Jaqui Lynch explains how you can protect your LPARs through:

- Usernames and passwords
- Logging
- Securing daemons
- Time synchronization
- Patching
- Fix Level Recommendation Tool Vulnerability Checker (efixes and ifixes)
- Server and I/O firmware
- AD/LDAP integration
- Enhanced access
- Backups

Learn how to lock down LPARs in the full article

Going Beyond Security Best Practices

Patrick Botz explains how to determine which security best practices apply to your organization's specific needs

BY PATRICK BOTZ

It's been a while since I've had an opportunity to get on my high horse. And considering "best practices" is a term that has always made me uneasy—I'm happy to get this off my chest!

Best practices are a great tool for helping you secure your environment. They can be useful as a temporary stopgap measure if your organization lacks a well-defined set of security policies. But they can easily be misused or applied in inappropriate situations. Be careful before blindly accepting or attempting to apply best practices.

What Are 'Best Practices?'

How would you react if someone told you, "Best practices indicate that you need to bring three pairs of shorts and a swimming suit on vacation?" Not having a well-defined set of vacation packing policies, before I accepted this input as gospel, I would certainly ask myself several questions starting with, "Says who?" Closely followed by questions like: "Where am I going?" or "How long am I staying?" and "Will I want or have any time to go swimming?" This "best practice" may or may not apply to me and my specific vacation plans.

Adopting a “best practice” makes a lot of sense when you know if they apply, and where and when to apply them. Compare it against your security policy. Make sure best practices apply to your specific circumstances, understand who has established them, that other organizations like yours accept them, understand the details and get a lot of other input, including legal advice.

Now—how would you react if someone told you, “Security best practices indicate that you must use exit point software to secure your system.” I know a few people, including at least one auditor, who accept this statement as fact. But is it? How do you know if it is? If it’s a best practice, does it apply to your unique situation?

Before addressing these questions, I’d like to note that “best practices” **are defined as** “commercial or professional procedures that are accepted or prescribed as being correct or most effective.”

Note the phrase “are accepted or prescribed.” Two questions to ask yourself about any best practice are:

1. By whom is it accepted or prescribed?
2. For whom is it intended or does it apply?

Just because you often hear it stated doesn’t mean it’s a best practice or that it applies to you.

Using military-grade encryption, for example, is surely a best practice for many organizations and institutions. But what about the family-owned restaurant down the street? Does this best practice apply to them? Is this practice accepted or prescribed by most family-owned restaurants or the family-owned restaurant industry? Was this best practice intended to be applied to these types of entities?

Determining Best Practices for Your Organization

To determine if a best practice applies to you and your organization, you should address these five questions:

1. **Is it a legal or industry requirement? (Is it prescribed?)** Get good legal advice from a corporate attorney or a lawyer practicing in your industry. Check with industry organizations, businesses, etc., to ensure it is generally accepted by your industry.

2. **Who or which organization(s) prescribe this practice? (Says who?)** Is this practice prescribed by government? How large a segment of my industry does the organization that prescribes this practice represent? Do other businesses/business owners accept this practice? Check with your auditors (but follow up with your own research).

3. **Is there evidence that organizations like mine generally accept this practice? (What is the evidence?)** Is the practice documented anywhere? If so, see Questions 1 and 2. Check with industry organizations, other businesses/business owners. Check with your financial and security auditors—but follow up with your own research as well.

4. **What are the details?** Take time to fully understand the details. Using military-grade encryption, for example, may only apply to specific types of information. It might only apply to information your organization stores or it might apply to information that merely transits your environment. Further, what does military-grade encryption mean? So, you use AES-256. If you don't generate and protect the keys properly, you aren't practicing military-grade encryption.

5. **Does the practice tell you what to do or how to do it?** I apply this rule of thumb when considering the validity of a purported best practice.

Question 5 is a good one to address first. In general, best practices should tell you the behavior(s) you need to enforce to appropriately secure your environment. Consider this statement: "Prevent unauthorized employees from accessing protected information." (As an aside—I'm sure this is a best practice—i.e. legally required for healthcare organizations—although it isn't specifically worded like this.) Note how this practice tells you what to do—prevent unauthorized access by employees to some type of data or resource. However, it doesn't tell you how to enforce this behavior.

Another way to think of this, rather loosely, is: Does the practice represent a policy to be enforced or does it try to tell me how I should enforce some unstated policy? The latter is suspect.

Define Behaviors: Beyond the 'How'

Now consider the purported best practice I mentioned earlier: Security best practices indicate that you must use exit point software to secure your system. Note how this statement tells you HOW to make your system secure—not the behavior you need to enforce to secure your system. A few red flags in this statement indicate that it isn't a best practice—even if most organizations do so. First, it specifies a platform-specific tool or technology. Because it's limited to a specific platform, it's unlikely to be generally accepted across an entire industry. It can't be. It only applies to one platform. Second, it defines no behavior to allow or prevent.

Of course, one can quibble with these descriptions. Does a best practice of encrypting all passwords represent a policy or is it telling me what to do? I would argue it tells you that encrypting all passwords defines a behavior. While it does

Best practices are a great tool for helping you secure your environment. They can be useful as a temporary stopgap measure if your organization lacks a well-defined set of security policies. But they can easily be misused or applied in inappropriate situations. Be careful before blindly accepting or attempting to apply best practices.

mandate a technology, it doesn't mandate a platform-specific capability. But one can also argue that encryption is something you do. With a little discretion on your part these differences should be easily discernible.

Behaviors You Enforce Impact Security

The behaviors you enforce on your system—your security policy—makes it secure. Assuming the enforcement is effective, how you enforce those policies is irrelevant. Cost is the determining factor for how a practice is enforced. If the behaviors allowed or prevented in your environment are inappropriate, perfect enforcement of those behaviors will not ensure a properly secured system.

Adopting a "best practice" makes a lot of sense when you know if they apply, and where and when to apply them. Compare it against your security policy. Make sure best practices apply to your specific circumstances, understand who has established them, that other organizations like yours accept them, understand the details and get a lot of other input, including legal advice.

Oh, and don't forget to pack your swimsuit for your vacation.

PATRICK BOTZ holds a master's degree in cybersecurity organization and leadership from the University of San Diego. He worked at IBM for 20 years where he held various information security roles including lead security architect for AS/400 and i5/OS.

Why Having a Backup and Recovery Plan Improves IBM i Vitality

BY JENNIFER GOFORTH GREGORY

Monitoring the vitality of your IBM i system is a cornerstone of keeping your business running 24-7. A key component of IBM i's vitality includes recovering quickly after a disaster with the least amount of disruption to your customers and revenue streams.

Debbie Saugen has heard all the excuses for why a company isn't prioritizing backup and recovery for their IBM i system. "Everyone says they aren't going to have a disaster, their business isn't like our other customers', or they don't live in a disaster-prone area," says Saugen, owner of Debbie Saugen Consulting. "But I've worked with hundreds of customers in real-life disasters over the years. It's not just natural disasters—it's hardware failures, it's user errors and now it's a problem with security. If you have a breach, you may need to recover your system in order to recover from that security breach. Every company needs a backup and recovery plan and solution for IBM i."

Saugen finds that most IBM i clients currently back up the IBM i locally to physical tapes. As clients realize the benefits of cloud backup, Saugen is increasingly helping organizations transition to a virtual tape library (VTL) solution.

Once you decide to move to the cloud, Saugen recommends focusing first on recovery and then backup. Because the entire focus of recovery is getting your business back online and fully operating, it's essential to understand exactly how quickly you need to recover your IBM i system.

Read the full article

This e-book was published by

TechChannel 901 N. 3rd St., Suite 195, Minneapolis, MN 55401 // (612) 339-7571

staff list

Publishing Director: Mari Adamson-Bray

Senior Content Director: Evelyn Hoover

Senior Editor: Keelia Estrada Moeller

Art Directors: Mike Kooiman & Kelsey Hanscom

Project Manager: Noelle Heaslip

Audience Development Director: Linda Holm

Account Executive: Kathy Ingulsrud
(612) 313-1785 // kingulsrud@techchannel.com

Account Executive: Darryl Rowell
(612) 313-1781 // drowell@techchannel.com

This e-book could contain technical inaccuracies or typographical errors. Also, illustrations shown herein may show prototype equipment. Your system configuration may vary slightly. This e-book may contain small programs that are furnished by MSPC as simple examples to provide an illustration. These examples have not been tested under all conditions. MSPC, therefore, cannot guarantee or imply reliability, serviceability or function of these programs. All programs contained herein are provided to you "AS IS." IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED.

All customer examples cited represent the results achieved by some customers. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

The articles in this e-book represent the views of the authors and are not necessarily those of MSPC or TechChannel.

TechChannel

TechChannel.com is home to a variety of content to help you get started on your security journey.

Learn more about SMB security