A SPECIAL EXCERPT FROM THE
AMAZON.COM BESTSELLING BOOK

ON THIN ICE

CHAPTER 26

DO YOU KNOW WHAT YOU HAVE, AND WILL YOU KNOW IF IT CHANGES?

BY JAY FERRON

If you don’t know what’s on your network today, how will you know what has changed if you get hacked? You won’t. If you don’t know the configurations of your machines and which machines are working, how will you know what’s changed? Do you know what’s in your server room? Do you have a diagram of how everything connects? If today, you don’t know precisely what hardware and apps your business utilizes, which versions of those apps are running, and how and why the network is configured the way it is, your business could be in trouble. In the event of a disaster, you will need to rebuild. No baseline means no blueprint to reconstruct what you had. How will you get to know what you’ve got?

If you don’t know the details of your server configuration or if your version of QuickBooks is up to date, you are not alone. Many small to medium companies don’t know their configurations because nobody bothers to document it. They have no idea what the server configuration is supposed to be; therefore, they won’t know if they’ve been hacked. Two hundred days later—when the breach is discovered—the risk to the business will have compounded.

It’s easy to see how this can happen. A small to medium-sized business probably doesn’t care about what their computers do or how they are configured. They just need their applications. Most of the time, they hire somebody to set up their system and expect that person to know what they installed. Maybe they hire a managed service provider that is also a security specialist to document those settings. They might just pick up the phone when something breaks.

You might think that large companies always know what's going on with their networks because they have IT departments handling those issues. Realistically, however, the larger the company, the more users and workstations they have, and the harder it is for anyone to keep track of what they've got. Who should be tracking it? Generally, it's either the IT department, if they have one, or the security vendor if the company has hired somebody to manage that. With any size company, the same foundational security rules apply:

1. **Understand, prioritize, and manage what you have.**
2. **Patch and update when necessary.**
3. **Get rid of anything you no longer need.**

Locking valuables in a safe isn't of any value if you cannot prove what was in the safe if someone breaks in. No cybersecurity efforts will be worthwhile without an inventory. If you don't do this, I don't care what you do in security, you're still going to be vulnerable. Even if you do all your patching and everything else, you won't know what's there. Here's a technical example: DNS works on port 53. If I installed a piece of malware software on your computer that gave me remote access and I connect it to port 53, would you say, “Oh, that's just DNS“ and forget it, or would you say, “““Wait a minute, DNS wasn't running here. What's running here? That's a hole that somebody got access to.“““ That's the mindset that I'm trying to drive. Knowledge is power.

When hackers gain access or when computers are compromised, typically, there are two types of compromises. One is ransomware, in which they encrypt all of a company's files. In the other, a hacker breaks in—potentially even a nation such as China, Iraq, North Korea, or Russia—trying to harvest information. However, once somebody breaks in, they become what's called an advanced persistent threat. What that means is they give themselves ways to come back and forth. So, if you plug the first hole, there are other holes where they can get in. They can go back and forth in that network as much as they want, whenever they want. If I'm a hacker, I am going to make a hole in the network, and it’s going to be a service, a port, or something that’s open, which is going to allow me to connect to it. If a business doesn’t know what it has and how its network is configured, how will it know what I’ve added there?

It isn’t unheard of for hackers to be in a network for nearly a year before somebody figures out what’s going on. That’s a long time for somebody to have access to your company’s data. Businesses must start thinking about what they have, what they need, how it’s configured, and what to do if that changes. You can’t have proper security without answering those questions.

Your primary business might not focus on the network or the server. If you own a catering company, your primary focus is probably on food, clients, and the equipment in your commercial kitchen; however, if you own a server, you have it for a reason. The server houses the information for the thousands of clients whose events you host annually. What value do you place on those records? Without your client records, all the accouterments of food preparation will be completely unnecessary.

Building on the catering company example, if someone recalibrated the oven you use to prepare catered meals so it was 50 degrees hotter than normal, you would want to know that information because that’s your business line. If you didn’t know and suddenly somebody changed it, that would be a big issue, right? You could burn thousands of meals, losing revenue and, potentially, the clients who trusted you to do the job correctly.

Every business needs a baseline for the system so that they know ‘what’ and ‘where’ everything is. Take an inventory of the hardware, the software, and the configurations, so you can say, ““Okay, wait a minute, something is not right.““

A cybersecurity professional needs to know what you have before they can protect what you have. So, the first thing they should do when a business calls with a problem is to take an inventory of their network to find out what is there: what services they have, what they are doing, and why they are doing it. Do they have an application they haven’t used in ten years that is still talking to the internet? Maybe that needs to be eliminated. Only after an inventory can you make intelligent choices. When your car breaks down, the mechanic runs a diagnostic test on the vehicle to see what it says and proceeds from there. That's the recommended approach for cybersecurity as well.

If you don't know what you have, you're not thinking about it, patching it, updating it, or managing it. This increases the risk to the business because the more issues that it has that are not managed or understood, the more vulnerabilities it has, and the easier it is for somebody to attack it. Potential security issues begin the minute the system is installed. The operating system and driver updates are regularly released, and a missed update equals a hacker opportunity. Update notifications are like car recall notifications. If you received a recall notice from your auto manufacturer that said there's a problem with your car's steering wheel assembly and it could randomly fall off, would you drive your car? Probably not. However, if you never paid attention to the recall notice to know that you have a problem with your car, you're an accident waiting to happen.

Simple inconsistencies can result in significant cybersecurity issues. I recently serviced a customer whose small business had several seemingly trivial issues. The software was stored on computers, not a server. Everyone had administrative privileges. One employee had Adobe Photoshop Version 1, and somebody else had Adobe Photoshop Version 3. No one considered the possible vulnerabilities in Photoshop Version 1. Understandably, people are busy working the business that they run, and they're not thinking about if Windows is regularly updating on every machine, if the antivirus is updating, or if the backup is working.

A business might add an external hard drive to the laptop, and make it backup files to that hard drive. That sounds reasonable, except if you get ransomware, it's also going to take down the hard drive to which you backup files, right? From the hacker's perspective, if he can find a hole that's well known that the business hasn't patched, why should he work harder to break in when he could work smarter and easier? If he can exploit the vulnerabilities of the old version of Photoshop, he can waltz right into all the files backed up on the external hard drive too.

So, exploited holes in any system can lead to disaster. A recent example in the news involved Android cell phones. Android phones that are two years old, or older, have a security hole in them. They are unpatched—most carriers don’t patch the phones—so there are over a million Android phones with this glitch—any hacker can direct the user to a webpage and take over the phone. Now, you’re probably saying, ““‘So what? It’s just my phone?““‘ Oh, but the phone is also your contact list. It’s your email. It’s probably the same password you use to log in to social media and half of your credit cards. How about if the hacker just downloads your phonebook and then sends an email to your boss telling him that you quit?

To be fair, the same can be said of a PC, a Mac, and a Linux machine. It doesn’t make a difference which tools you’re using. If you have an inventory of what you have and how it should function, then you can prioritize based on the risks of the organization and take care of those things that are critical and not worry about those things that are minor. Once you know what you have, then you can say, “Okay, what’s the most critical thing to my business? What are the risks of that thing? How do I protect that thing?” Sadly, too often, people go the other way around and try to fix all the little patches first, when some of those might be minor, instead of addressing the critical issues first. It makes sense to methodically prioritize and address the concerns after a risk assessment with a security professional.

Even devices like printers have vulnerabilities. Older network protocols that once facilitated communication between devices require upgrading to current protocols. Older ones still in use could allow a bad actor to access the buffer overflow attached to a printer and use that to gain access to the data on the printer. If that printer has a hard drive storing frequently used documents, etc., as many of the larger models do, essential data could be stored on it. Do you know what’s stored on the printer in your office? If the service technician must replace the old hard drive, would you know what information he could be carrying out of the building if he takes the old hard drive with him?

Knowing what you have is critical, so you can say with certainty, “Wait a minute, you can work on my printer, but I won’t allow you to leave the building with a storage device. You can replace it, but you can’t take the old one away with you because I’m worried about my confidential data.” A doctor’s office, a law firm, and a small financial organization all have regulations with which to comply, but they don’t think about the risk of a printer on their network.

Know your risk. *Risk equals asset-with-value x(times) threats x(times) vulnerabilities.* Once you find a risk, there are only four things you can do.

- One, deny the risk. If you're not jumping out of an airplane, it doesn't matter whether the parachute works.
- Two, share transfer the risk. Auto insurance is an example of share transfer. You have auto insurance so that if you get in an accident, the insurance company will pay for a percentage of my damage.
- The third option is to reduce the risk to an acceptable level. You will never eliminate all risks, but you can minimize the risk to an acceptable level.
- What's leftover, the fourth option, is residual risk? How can you make those decisions, those risk decisions, around your computer, network, and phone infrastructure unless you know what you've got? You can't.

Sometimes the simplest services can create serious risk. Take the office phone, for instance. Do you have a traditional landline or VoIP? If you cannot answer that question, that could become a problem. If it is VoIP, it is connected through the network to the internet. What are the holes? Is the VoIP secure or not? Do we need a patch? I've had clients say to me, "What do you mean you need to patch our telephones?" Well, they are network devices now, so they need security patches. What is the risk to your business if somebody can get in and take call manager down, preventing employees from conducting business?

When providing cybersecurity, I begin with a simple investigation into the network for IP addresses or services that are running. That tells me how many computers a business has. Sometimes, they may not even know where their computers are. When I scan the network for hardware, then I locate the servers.

It is certainly possible, especially in larger organizations, that hardware goes missing. While inventorying at a client's office, I asked, "Where's the Novell file server?" The owner looked at me, puzzled, and said they no longer had a Novell server. However, there was a Novell server currently online. I asked to speak to the employee who had been there the longest and asked him, “Did you have a server called Nile, because it’s still running?” He denied that was possible but eventually directed me to where there used to be a room that housed that server. We walked around the walls, but we couldn’t see anything. We finally poked our heads up in the drop ceiling and looked down, and in the middle of what used to be a closet was a server sitting on the floor. It was still running. Talk about skeletons in the closet.

Do you know what’s still running on your network? Learn what you have. Identify the risks to the business. Rank those items from most critical to least critical and address them in that order. Address them in that order because most companies don’t have an unlimited budget for their cybersecurity. You prioritize because you might have the budget to fix thirty little things or one critical thing in your business. The most critical thing to the business is what you should address first.

About Jay

Jay Ferron is the founder of Interactive Security Training, LLC. Interactive Security Training has been in business for over 30 years, with the goal of helping customers to secure business and company data. Interactive Security Training listens to customer's needs, helps them develop solutions, implements those solutions, and then trains staff to maintain those solutions. Interactive Security Training customers include Cigna Insurance, Travelers Insurance, Microsoft, Rogers Communications, AT&T, US Marine Corps, US Air Force, US Army, and Defense Information Systems Agency. Other customers include banks, government agencies, health agencies, and service providers.

Jay Ferron is a multi-certified Information Security Subject-Matter-Expert (SME) with more than 40 years of professional experience, including Security & Compliance, Integration and Transformation Initiatives, IS Management Process and Operational Metrics Definition and Documentation. Jay's extensive certifications include: CDPSE, CEHI, CISSP, CHFIi, COBIT, C)PTEi, CISM, CRISC, CVEi, MCITP, MCSE, MCT, MVP, & NSA-IAM.

Jay has written over 19 technical courses for Microsoft, Global Knowledge, and others. Jay is quoted in *Channel Pro*, a reseller publication, and his blog is at: https://www.channelpronetwork.com/blog/231/Jay-Ferron. Jay is a Microsoft MVP and President of the Connecticut chapter of ISACA. Jay is also Co-Director of the NY Metro Joint Cyber Security Conference (NYMJCSC.org). NYMJCSC is now in its seventh year—featuring keynote speakers, educational panels, and sessions aimed at various aspects of information security and technology.

Jay's blog is: http://Blog.mir.net, and you can find information about the conference at: http:// nymjcsc.org.

You can connect with Jay and his team at:

- 203-675-8900
- Info@interactivesecuritytraining.com
- www.interactivesecuritytraining.com