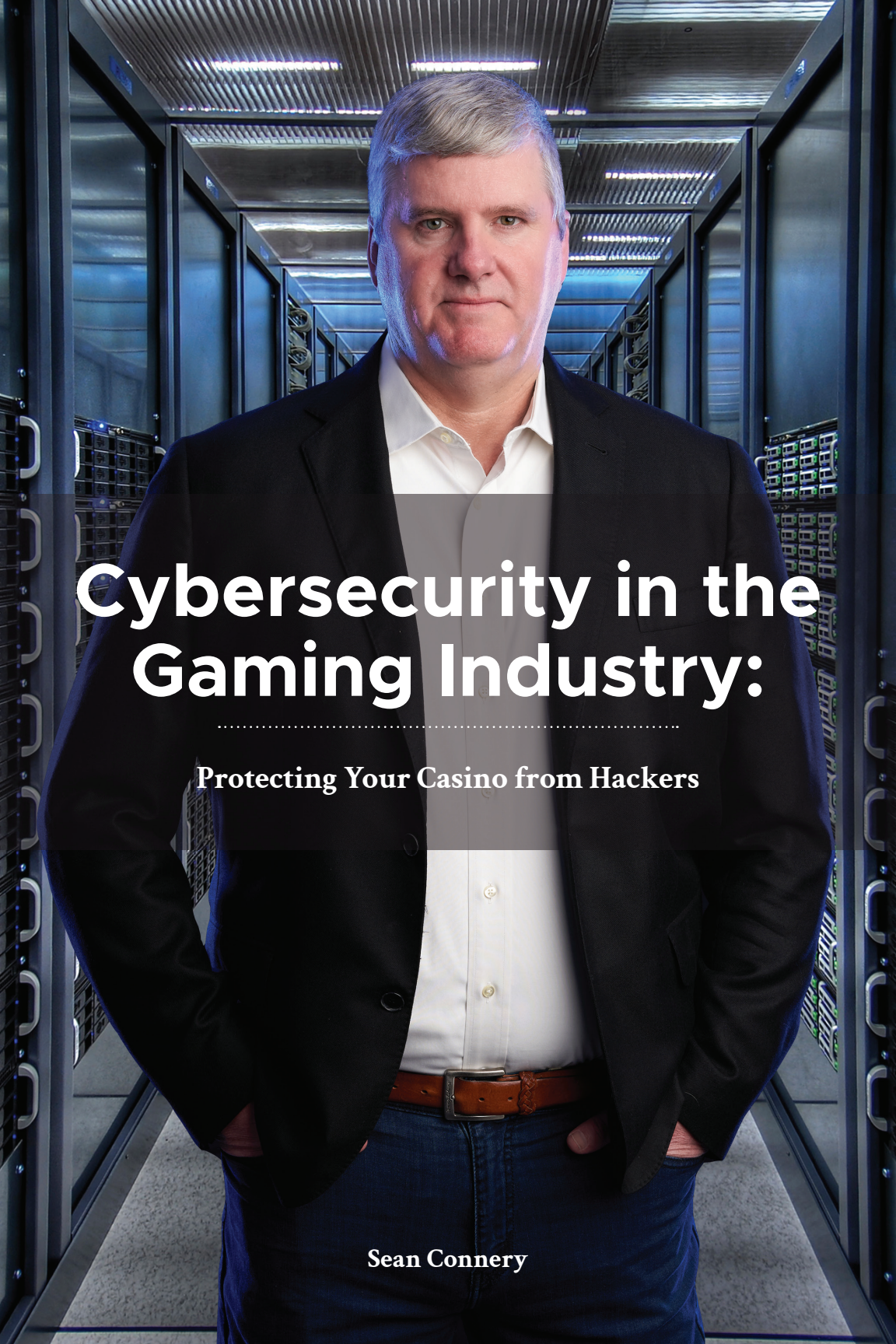

Cybersecurity in the Gaming Industry:

Protecting Your Casino from Hackers

Sean Connery

CGC Publishing House

Printed in the United States of America

Cybersecurity in the Gaming Industry:

Protecting Your Casino from Hackers

Sean Connery

Contents

Author's Note

As I reflect on my journey in the gaming industry and the world of cybersecurity, I am reminded of the countless experiences and lessons that have shaped my understanding and approach to protecting casinos from cyber threats. This book, "Cybersecurity in the Gaming Industry: Protecting Your Casino from Hackers," is a culmination of those experiences and the knowledge I have gained over the years.

From the early days of my career, I have been driven by a mission to safeguard the gaming industry and its patrons from the ever-evolving landscape of cybercrime. I have witnessed firsthand the devastating impact that cyber-attacks can have on casinos, from financial losses to reputational damage. It is my hope that this book serves as a valuable resource for casino executives, IT professionals, and employees, providing them with the tools and strategies needed to defend against these threats.

Throughout the chapters, I have shared real-world examples, practical advice, and step-by-step instructions to help you navigate the complex world of cybersecurity. My goal is to empower you with the knowledge and confidence to protect your casino and ensure a safe and enjoyable experience for your patrons.

I would like to extend my gratitude to the many individuals and organizations who have supported me in this mission. Your dedication and commitment to cybersecurity have been an inspiration, and I am honored to share this journey with you.

Thank you for taking the time to read this book. Together, we can make a difference in the fight against cybercrime and create a safer gaming industry for all.

Chapter 1:

Have You Already Been Hacked?

In this chapter, I'm going to talk about how casinos have already been hacked, three surprisingly easy ways any casino executive can detect a security breach, and what exactly you can do about it.

You're probably wondering who the heck is this Sean Connery, and why should I care?

Let me tell you a little about myself before we dive in. I started out working in the gaming industry. My job was to keep the bets moving and protect data. Over many years, I learned how the bad guys were winning the battle and wreaking havoc in the casino sector by hacking networks, stealing data, and sometimes completely shutting down casinos.

I have made it my mission to protect a billion people. You may be wondering, "How is that even possible?" Don't worry, we'll get there.

One time while helping clean up a major security incident, a critical employee quit the job site due to overwhelming stress. Imagine losing valuable employees over a security breach simply because you were unprepared. Who will do their job if they walk away? I have seen this happen in the casino sector, and I want to prevent it from happening again.

Think about all the foot traffic from patrons in the gaming industry. By helping to protect them from security incidents, people can enjoy their time and simply be entertained. I want to help the gaming industry run as smoothly as possible to keep their customers coming back for more fun.

Imagine a security incident that shuts down an entire casino, prevents

the casino from paying its employees, or even cancels an event like a concert, sporting event, or convention. Each year, over 40 million people visit Las Vegas and spend more than $30 billion. So, you can see why my mission to protect one billion people in the casino industry is a reality, not just an arbitrary number.

I want to start this chapter by exploring two conflicting ideas. First, it's dangerous for a casino to be online. At the same time, you have to be online to get things that are important to the casino done. Let me give you an example. Email is a mission-critical application to communicate, but in 2020, 65% of organizations had their business email compromised. They might have done things like money transfers or tricked someone into giving someone else's social security numbers.

But the real problem is that the number is going up. In 2021, it went up to 77%. At the same time, the number of business email compromises continues to increase: from 2019 to 2021, that number increased by 65%, according to the FBI.

That means you have two problems when it comes to your email. First, there's the increased cost of an event. Then there's the increasing likelihood it happens. Think about that hacker for a minute. They're experiencing and witnessing more money per success, which increases their desire to do this stuff. They're being more successful more often. How does that happen? There are more vulnerabilities that keep popping up. In fact, 2022 was a record year for vulnerabilities.

Here's some quick context. First off, we need to establish what vulnerability means. Think about your car for a minute. A vulnerability might be your windows not being rolled up, your doors being unlocked, or your alarm not being set. These are obvious ones, but there is more to it than just the obvious vulnerabilities.

Let me give you an example. Between 2015 and 2019, Kias were twice

as likely to be stolen. Why? Because they were missing an anti-theft feature that verified the key really belonged to that car. Of course, thieves got wise to the fact that they could use the access to steal these cars. The bad guys definitely knew about this vulnerability, but the average driver didn't.

As you can imagine, your computer network is way more complicated than that. As I mentioned earlier, last year was a record year for vulnerabilities. In 2022, there were 26,448 new vulnerabilities. 59% of those were critical, meaning that 59% of them could be used to break into your computer systems and steal your data. That means more successful attacks and more money out the window.

Hacking is big business. In 2019, it was a trillion-dollar industry. Let's look closer at what a trillion dollars was. If you were holding a hundred-dollar bill, ten thousand dollars would be a stack of money that could sit in your hand. A million dollars would be about the size of a pizza box. A hundred million would be a crate, and one billion would end up being ten crates. $1 trillion, therefore, would be ten thousand crates.

Effectively, cybercrime cost organizations around the world ten thousand crates of hundred-dollar bills in 2019. According to experts, it's going up. It will be $10.5 trillion dollars by 2025. That's just less than the top two economies in the world. It would be the number three economy right behind the United States and China.

As I said, hacking is big business, and there are a lot of folks who have already been victims out there. Did you know that three out of four organizations have already been infected or had somebody in their network that they didn't expect to be there? You might be thinking to yourself that your organization has a computer person, so it isn't your job. However, imagine for a minute a ransomware event. The hackers

got every single computer in your casino, and they're able to access every single device. They go through and destroy your backups. They hold your data hostage. Then they send you an email expressing the amount of money they want and how you can pay that money.

As you deliberate on whether you're going to pay it, they go through and email all of your contacts a message from you with a link that gives those contacts ransomware. Then they start posting your client's personal data on internet blackmailing sites, so you pay them. Imagine that happening to your casino. Would security quickly become your number one priority? Imagine you'll be negotiating with criminals. You'll be trying to clean up this big mess and dealing with the fallout from clients who are now infected with the ransomware.

It doesn't matter if you have cyber insurance. This is just something you do not want to experience. Let me give you an example. You probably drive with caution even though you have auto insurance. This is because you still understand how much trouble an accident causes. Time slows down, progress stops, focus changes.

What can you do to keep this from happening to you? It's very simple: be prepared. Know the different signs and make sure you're secure. I'm going to go through three different signs that will tell you if your casino has been hacked in this chapter. First, there's figuring out if your computer has been hacked. Next, we're going to dig into figuring out if your network has been hacked. Finally, you're going to figure out whether your organization's emails have been hacked.

Let's start with the computer side. To figure out if your computer has been hacked, look for these telltale signs indicating that something is going on with your device. The first sign is that your computer suddenly starts running slow. What I mean by this is that when you

open a different program, it takes a long time for things to come up on the screen. You might also notice that your computer starts running louder, with a buzzing sound as the fan turns on because the computer is overheating. This is a good indicator that something is wrong with your device.

Another sign is programs popping up or multiple windows flashing by unexpectedly. These are signs that your device might have an attacker on it. Additionally, if your updates stop working, you might see a little orange dot above one of the icons in the bottom right-hand corner of your screen indicating that something isn't getting updated. You might notice that one of your files doesn't open anymore, and suddenly other files stop opening as well. Finally, you might find a document asking you to send someone money, like a ransom note. That's a clear indicator that it's already too late and your computer has been hacked.

But what about figuring out if the network has been hacked? This means knowing that somebody is not just on your individual computer, but on every single computer in your environment. There are a couple of ways to determine this. The first one is straightforward: pay attention to when your password unexpectedly changes. Imagine you try to log onto your computer, put in your username and password, and it says, "password incorrect." You try a few more times, and it still doesn't work. Then, you have to reach out to someone in your IT team or support to get that taken care of. This is a good indicator that something is going on inside your network.

Another sign is that your internet slows down. You might notice that your internet is coming in and out, and web pages take a long time to load. Another indicator is receiving reports from other organizations that they are getting emails from you, or worse, from their security teams that your team is sending out spam or trying to attack one of their devices. The most obvious way to know your computer system has been hacked is a visit from the FBI.

When I was working at a casino, bad actors were in the network trying to log into the gaming servers. I and the other cyber heroes were stopping the attack while gathering as much evidence as possible. This type of situation can be avoided by paying attention to these first simple signs.

Next, we'll talk about how to figure out if your email has been hacked. The first sign might be unexpected. If you start noticing a whole bunch of spam suddenly coming into your mailbox, this is a good indicator that something is going on. When attackers get into your mailbox, they might start sending out messages while you're trying to communicate with other people, creating a smoke screen. They send out a whole bunch of spam to your account, making it difficult for you to keep up. Meanwhile, they can delete messages, modify messages, etc., right under your nose while you're busy dealing with all the spam.

Another sign inside casinos is when an attacker gets into one of their email addresses and changes the victim's email signature, such as the phone number. This is so that if an attacker sends out a message as you, and the recipient calls back on the phone number, the attacker can intercept the call. They also change your title or the organization you have listed. These steps are taken by attackers to get more information from others and trick them into doing things like wiring money to the wrong account.

Speaking of wiring money to the wrong account, the hacker might create a forwarding rule inside your email. If you notice that your email is alerting you to new forwarding rules being created, this is something you should investigate. It may be time to contact someone else on your team to look over your shoulder and figure out what is going on.

Another thing you can look for is emails in your sent items because hackers often use your email to trick other people by leveraging your

authority within the organization. They might send an email to your contacts, and you'll see an email in your sent items that you don't recognize. If the hacker is competent, they may delete those items, so you might find them in your deleted items folder as well.

You may also have people reaching out to tell you that you're sending them strange messages. Essentially, an attacker might send out a message to one of your contacts that includes an executable file, a zip file, or a link the attacker is using to spread more malicious software or gain access to additional information. If someone complains that you've been sending them such messages, this is a good sign that something's wrong. Take a moment to understand the situation before dismissing it.

So far, this chapter has covered three different areas: how to figure out if your computer has been hacked, how to determine if your network has been hacked, and how to figure out if your email has been hacked. All these things happen after the fact, though. By the time they happen, the attacker is already in your environment. The question is, what can you do to prevent this in the first place?

The answer is to ensure your security is working for you. You might think you're fine because you have a computer person. Do you think the victims of the events I've mentioned didn't have a computer person? Do you think someone who had to deal with ransomware and the recovery from a ransomware event hadn't previously thought they had their security in order?

These people thought they were secure. They had antivirus and a firewall. They had good backups. They had all these things in place and were spending good money to ensure their security was working.

But how do you know if your security is working? Ultimately, there are blind spots. These are the spots that you can't see when you're

in the middle of working inside a casino. We have a third party that analyzes our cybersecurity. They go through and analyze our network on a monthly and quarterly basis to ensure we don't have any blind spots we've missed.

There are spots you can't see when you're in the middle of working inside your casino. If you were to Google pen tests/security assessments, these assessments usually run about $10,000 – $30,000 per assessment. What we'll do is a free analysis of your cybersecurity risk. You might wonder, am I the right person for this? The answer is simple. If you experience an event, will you be the person who has to deal with the fallout? Will you be the person who has to talk to and deal with upset clients, partners, and regulators?

The next question is, are you completely protected? Do you know for sure that you have everything locked down and secure? When we do this assessment, we won't need credentials. We won't need to install anything. We'll analyze your security, then I'll meet with you to review the results. I'll give you a simple plan with steps you can take to protect yourself and your data. If this interests you, go to **OrbisSolutionsInc.com/analysis**. You might be wondering, what's the catch? There is no catch. I'm on a mission to protect one billion people. If you want to do this, go to **OrbisSolutionsInc.com/analysis** and get your free cybersecurity assessment.

Some of you might not be ready for this assessment. If you're wondering how you can figure out this stuff on your own and determine whether your security is working properly, we have a report. I spent some time putting together an easy-to-understand report with five simple signs that indicate you have weak cybersecurity. If you're interested in the report, go to **OrbisSolutionsInc.com/five-signs**.