Cybercrime, Cyber Security, and Surveillance Operations

By

Derk J. Boss, CFE, CPP, CSP

There has been an increasing number of incidents occurring at casino properties involving cybercrime. Recent attacks have included gaining unauthorized entry into a gaming property's computer system and gaining access to sensitive information that is either then released into the public domain to damage the entity's reputation or is held for ransom by the attackers until thousands or millions of dollars are paid to them. Two attacks against two Las Vegas-based gaming corporations made international news and resulted in substantial losses.

Another method used by attackers is phishing. Using this method, attackers pose as a trusted organization or individual to obtain sensitive information or, in recent cases, cash from unsuspecting employees, focusing particularly on Cage employees. These scams have happened despite the safeguards in place and the security measures taken, such as surveillance cameras everywhere within the cage!

It is not my intention in this article to discuss each incident that occurred. Most of us, if not all, have followed these crimes in the news and know that they exist. In most cases, gaming properties have already taken steps to focus their IT staff on this issue to do what they can to protect and seal their systems from attack, as well as increase their ability to detect intrusions. Training for employees to recognize attempts to access IT systems and/or phishing attacks is on the rise.

However, we can only prepare for the crimes and methods we know and must be ever vigilant for the next twist to be made by the bad guys. Security and surveillance professionals already know this from the crime-fighting they do on a regular basis.

Over the last three years, the Surveillance Directors Survey conducted by the International Association of Certified Surveillance Professionals, Raving Consulting, and eConnect has found that cyber security concerns have ranked among the top five threats for surveillance directors. This is not to say that they are concerned only about their surveillance systems being hacked (although that

is a concern); they are worried that their property could be attacked by such means.

For security and surveillance departments, this is a new type of threat. One that we never felt was an area we could or should be involved in and lacked the knowledge, expertise, and resources to do so even if we did. Overall, that was believed to be an IT function, and we were hands-off. In other words, what could we do anyway?

I think that our mindset must change. If the property we protect is vulnerable to cybercrime, then we in security and surveillance who are charged with loss prevention must find ways to become involved and find ways to detect and/or deter cybercrime. We cannot stand by and watch as a significant amount of the company or the tribe's money is taken.

I think that we change our outlook on cybercrime and our capability to be part of the solution by:

1. Realize that we are the security experts and must step up to the table to offer security solutions. Yes, IT and others understand the technology and what can or should be done in that area. However, we understand the human factor. We know that much good can be done, and deterrence levels can be set by ensuring security measures are in place, such as controls, policies, and procedures, and that they are adhered to. Think how hundreds of thousands of dollars can leave the cage without security or surveillance leave the cage without one or both departments being involved? A simple required notification to surveillance that cash of a certain amount is being issued and the reason why would stop that scam (and has).
2. Monitor our vendors and those employees who use our systems to access sensitive information or operations. As an example, I think we are all guilty of not paying attention to a vendor working on slot or player rating systems. The same goes for slot technicians working on devices on the floor or, even worse, in their shop. We don't, and we should. Think of how many scams slot techs have been involved in over the years and the tremendous losses that were sustained. Think about the scams or even unintentional mistakes made by vendors working inside our systems and the losses they generated. Now, think about if we had a plan to monitor such activity. Do you think

that trained surveillance personnel might observe some type of suspicious activity that, if reported, could be the means to initiate a response or to ask the right questions? I do. In fact, I am aware of surveillance teams that have done so, resulting in the detection of illicit activity.

3. Ensuring that cyber security is part of the surveillance audit program. Yes, I know that we monitor vendors while they are on property and doing whatever it is they do. However, that usually means that we place cameras on them to record their activities and then forget them. We often don't even know what they should be doing. This is not routine anymore if it ever was. Now, we must be involved and ask questions. An audit observation of the slot shop, may detect unusual or suspicious activity and must be part of your operations.

Please bear in mind that surveillance cannot and should not be the primary team leading the efforts against cybercrime. IT and senior executives should be in that role. However, surveillance can serve as a supporting department to aid in the effort. As always, we see what others don't. We just have to look for it.

In conclusion, we, as surveillance and security professionals, can play a significant role in the prevention and detection of cybercrime. And we don't have to be IT experts. We have those. What will work, as it always does, is to ensure that the necessary controls, policies, procedures, and tripwires (notifications to surveillance or security) and a prepared and engaged surveillance agent. We do that through effective observation and audits of those activities and individuals involving our information, key operations, and transactions.

Originally published in TG&H Magazine (2024 Spring Edition).