SpencerFane®

Never Too Early: Olympics 2028 Preparation. Part IV: IT and Cybersecurity Issues

The world is coming to Oklahoma City in 2028. Not all of it, of course, but a large and connected slice of it is headed our way. During the 2028 Summer Olympics, Devon Park, home of the Softball World Series and Riversport OKC, a venue at which international rowing and paddling competitions occur, will host competitions. Oklahoma City University will serve as a satellite Olympic Village, housing athletes from around the world.

That's tens of thousands of competitors, spectators, and vendors, along with their smartphones, payment cards, browsing habits and very attractive profiles for cybercriminals who will be here in Oklahoma City and may be distracted by the excitement of the Olympic Games. If you own a business near these venues, now is the time to think seriously about your IT and cybersecurity preparedness.

Previous installments in this series on preparing for the Olympics covered topics like intellectual property, insurance, and employment issues. Now let's spend few minutes on topics that often don't get the attention they should . . . until after something goes wrong.

The Olympics Make You a Target

You might think, "I run a law firm / accounting firm / coffee shop / gift store or boutique. Why would hackers care about me?" The answer is that hackers care because of proximity and opportunity. The Canadian Center for Cyber Security puts it this way, cybercriminals will "very likely target large organizations associated with major international sporting events and local businesses around the events. . .." And because international travelers are often people of means, they are especially

attractive targets.

Protecting My Customers

Your customers put their trust in you every time you process a transaction. You may have access to personal information and credit card numbers. International visitors may be more vulnerable to frauds with which they are unfamiliar.

If you are in hospitality, make sure the Wi-Fi to which customers connect is secure and keeps their browsing completely separate from your business operations, including your point-of-sale activities. Consider offering them a secure, password-protected guest network that is insulated from your internal business network.

On the payment side, ensure that your point-of-sale (POS) systems are fully patched. Running outdated payment software puts your customers and your business at risk.

Make certain that your Google Business profile is claimed and accurate. If not, it could be a target for scammers. Review your business website. Does it have valid electronic security like appropriate encryption and sensitive information storage?

Your Greatest Asset and Your Biggest Risk

Your employees are amazing. They do an incredible job serving your customers every single day. They are also the number one way cybercriminals attack businesses. According to *Security Magazine*, "67% of all breaches start with someone clicking on a seemingly safe link, which explains why adversaries begin 80-95% of all attacks with a phish."

The phishing attempts are appealing, "click here to claim your free tickets," or "your vendor account requires verification." Some initially look like legitimate invoices or video call links. One modern example was a malicious link sent through SMS texts, giving fake information about a package delivery. Attackers now use AI to "generate convincing fake multimedia content, blurring the lines between reality and deception."

The good news is that training your employees to avoid social engineering attacks works. Make sure your employees know not to open emails from unrecognized accounts. For example, an email promising you a refund from Amazon that is from an address that has nothing to do with Amazon is fraudulent. Messages asking you to verify personal data are also likely to be phishing attempts. And often, the message looks like it will come from your CEO or CFO, who needs you to act urgently.

One often overlooked topic is what your protocols are when an employee leaves your organization. Do you immediately revoke all logins and credentials? If you don't have a formal offboarding checklist, now is the time to create it. Make sure that IT issues are addressed, along with turning in the computer, the key and the uniform.

Cyber Insurance: A Safety Net

Seventy-five percent of U.S. small businesses have a website, use online payments, and email thus giving them heightened exposure to cyber risk. Many erroneously believe their systems are secure or they are too small to be attacked. The reality is that the global average cost of a data breach is almost $5 million.

In the near future, have a discussion with your insurance agent. Make sure you understand what, if anything, your insurance policy covers if you are subject to a cyber attack. You may want to consider a standalone policy and make sure the policy covers the costs of a data breach response. That's where the dollars really add up and not all policies cover cyber and data breaches.

The Technical Stuff

Handling a Crowd. In the introduction, we discussed the crowds heading toward Olympic venues. When you have 10,000 neighbors, all carrying smartphones, your business's internet connection might not be sufficient.

Talk with your internet service provider *now* about available upgrades to bandwidth. Understand what the lead time is. Make certain that if you are offering Wi-Fi to your customers, your access points are able to handle the load from the increased level of concurrent devices.

Also talk to your internet service provider about whether signal strength will remain strong when thousands of internet connected devices are shoulder-to-shoulder in or near your business. Also recognize that the cellular infrastructure can be stressed with large crowds, so ensure your business has multiple ways to connect for your sales. An IT professional can help you plan for a network architecture with appropriate resilience.

If your business is crowded with customers, that's great. But you need assurance that your business operations, like your POS system, have a redundant connection. Just in case.

Network and POS Security. Your network and POS systems will have patches on top of patches. That's because cyber criminals keep finding new ways around the patches. Make sure all patches have been installed on all software, firmware, third-party applications, and the router. Software updates come out regularly and a best practice is to ensure everything has been appropriately updated the week before a big event for the most current protections.

With respect to your employees, each employee should only have access to the systems they need to perform their job. Your wait staff doesn't need access to your payroll system, for example. It is also a good idea to have a disciplined onboarding and off-boarding process for employees to ensure appropriate access and to remove it at the right time. And make sure that strong, unique passwords exist for every account and system. If you haven't moved to multi-factor authentication, now is the time.

Website and Email Security. Your business website should be running on HTTPS and not HTTP. The "s" stands for security! If your business domain expires soon, consider renewing early to avoid the possibility of a lapse, that can be capitalized on by bad actors who impersonate your legitimate business. Talk to your website provider and host to ensure you have the appropriate security in place as part of your agreement.

Redundancy and Business Continuity. If your business is subject to a ransomware attack right before or during the Olympics, what should you do? You need to have a plan in place *before* the unthinkable happens.

You and your senior team should know which systems and data are mission critical, how often backups are performed, and how quickly you can restore your systems from a backup. If you have never tested your system backups, now is the time. Start with a tabletop exercise where you game out the steps you would take in the event of a breach – but be sure to follow that up by actually exercising the technical steps, and ensuring the appropriate agreements are in place ahead of an actual event.

Staff Expertise. Is your business's IT person a part time high-school student who also handles A/V for your events? You might want to consider hiring someone with a few appropriate cybersecurity certificate credentials. You might also want to consider hiring a managed service provider, who can manager your IT, serve as a "help desk", and manage cybersecurity. Numerous companies can do that sort of work and can scale the services they provide to your needs.

Start Now. Seriously.

Two years until the 2028 Olympics sounds like plenty of time. But IT and cybersecurity upgrades often take longer and cost more than you anticipate. For example, if you are planning to get cyber insurance, you will need to spend time documenting your current security practices. And if you aren't, for example, training your employees, you might be uninsurable.

Oklahoma City is ready to step onto the global stage. The athletes will be ready. Make certain that your business is ready, too. Start today so that you can celebrate during the Olympics, rather than scrambling to deal with disaster.

This blog was drafted by Allison Garrett, an attorney in the Spencer Fane Oklahoma City office, and Rob Lyman, a retired U.S. Air Force Brigadier General who served as Assistant Deputy Chief of Staff for Cyber Effects Operations at Headquarters Air Force, and as Director, Command Control, Communications, and Cyber Systems at U.S. Transportation Command. For more information, visit spencerfane.com.

*Click **here** to subscribe to Spencer Fane communications to ensure you receive timely updates like this directly in your inbox.*