2020 Cybersecurity Postmortem

by Justin Hall, Director Security Services

Are you a security practitioner that was blindsided by 2020? You're obviously not alone.

As we noted earlier in the year (man, I wrote that nine months ago? Feels like nine years), it's unlikely that a global pandemic was on your risk radar. With the year drawing to a close, it's a good time to reflect on how things have changed for your business' risk priorities and what you'll need to do next to keep pace with those changes. Here are a few questions you can pose to your security team:

Question 1: How are you reevaluating your risk priorities?

Let's first think about why a pandemic wasn't high on your list of risk priorities. If you don't have a list of risk priorities, that's a good reason, and the absolute first thing you should address. Document your business' risk—including "cyber" risk that affects your data and assets—and stack-rank them in terms of priority. As you're doing so, consider where your list came from. What were the sources of the risk you documented? Did it just come from your own imagination?

Comprehensive risk management looks at a wide range of factors. Certainly other stakeholders in the business need to weigh in. You also want to look at the output of security and risk assessments which are designed to highlight gaps that need to be addressed. Most of all, look at the assets that are most valuable—your customer database, your IP, your reputation, your third-party relationships—and determine what actions could damage those. Don't just focus on current events, either—do some research. Examine what historically has affected others in your industry or region. Those may bring some risk ideas to light that you hadn't previously considered.

Question 2: How are you protecting your remote workforce?

Did your users take their company workstations home during the pandemic? Who knows what kind of coffee stains are on them now? On top of that, it's likely that their home Internet connections do not have the same network defenses you might have on your company network. That might mean malware has found itself on that machine. It also might mean your company's sensitive data has found itself places it doesn't belong—a home printer, a recycle bin on the curb, or your employees' personal iPad.

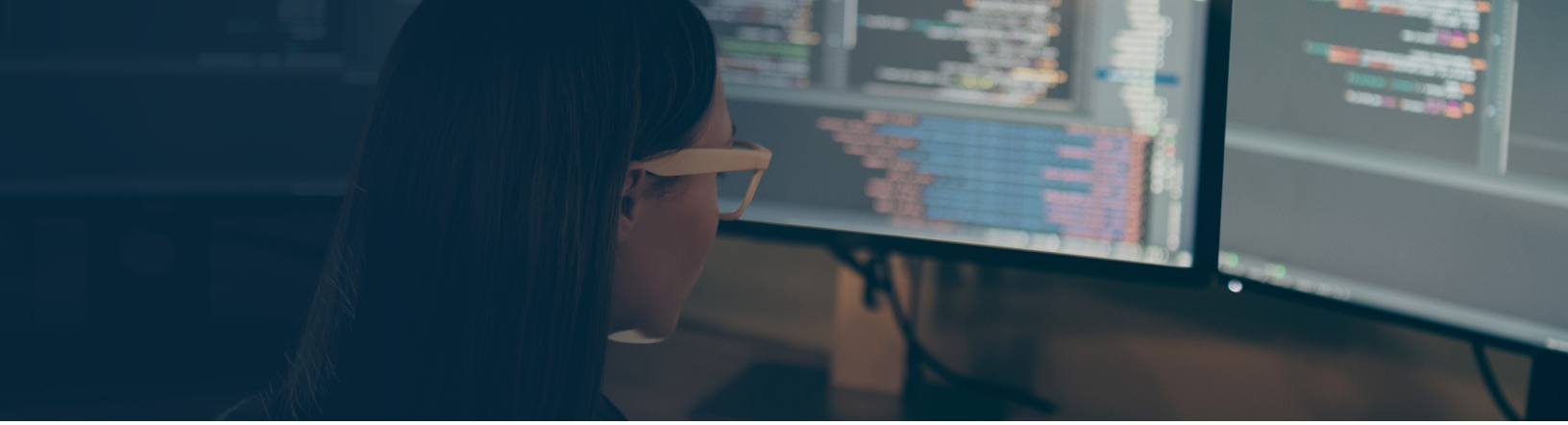
Many security teams build their controls with the assumption that sensitive data, or company assets, won't be far from the office for very long, Have you reconsidered that strategy since the pandemic? If there is a breach or incident, how will you approach the incident response process if the device in question is remote?

Question 3: What is your ransomware strategy?

One of the most pervasive threats to the enterprise network today is ransomware. Cyber criminals continue to develop more effective ransomware kits, with more sophisticated features. Their methodology is changing, too—many human attackers are stealing sensitive data before encrypting it, and threatening to expose that data publicly, doubling the incentive for a victim to pay up.

Cyber criminals are also using "pay the ransom" tactics in threatening distributed denial-of-service attacks—using botnets they create or rent to point a massive amount of bandwidth at a target server or network to knock it offline.

It's helpful to decide ahead of time the decision tree you will follow if this happens, and prepare a response. It's also helpful to establish a set of controls to prevent this from happening in the first place!



Question 4: Are your users trained to spot social engineering?

We've seen an uptick in phishing, social networking, phone, text, and other social engineering campaigns using the U.S. elections, the pandemic, racial tension, and other issues as fuel. When your employees' e-mail boxes are blasted with convincing-looking messages that promise details of a problem with vaccines, do you trust them to avoid the scams? To report the attempts to the security team?

The key practice that addresses these issues is awareness training, and in that vein, we need to be made aware of current threats more often than once a year, as the threat landscape changes, and attacker tactics mimic the fears and concerns of the victims they target.

Question 5: Are your security operations running smoothly?

In our experience, most security teams aren't blessed with a ton of margin. They run lean and frenetic, tasked with keeping security controls healthy, monitoring their output, and putting out fires with the assistance of other IT operations teams. Isolating those teams, amping up the pressure, adding distractions at home—times are tough, and we are finding customers looking to managed security services to take over some core practices. Security monitoring, vulnerability management, incident response, BC/DR and backups are some of these core functions that are ripe for outsourcing, to achieve more cost-effective, scalable, and operationally rigorous and sound security practice.

This year has been painful and memorable, but if we're honest, intentional, and we muster our courage, it can present a tremendous opportunity to improve our security posture and the essential practices on which our business will depend. Our mission to protect data and assets isn't going away, it simply continues to mutate. Our "what" and "why" stay the same, our "how" shifts continually—and this won't be the last time! We continue to look for ways to help our partners stay current and grow their security programs.

Request to be contacted by one of our security experts: www.onx.ca.