SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

COVID-19 Decision Insight

Issue: Cyberattacks Resulting from COVID-19: Information Security Risks

Contributors: Herbert J. Mattord, PhD, SEC Subject Matter Expert, Professor of Information Security and Assurance, Kennesaw State University and Keith Jones, SEC Subject Matter Expert, former CSO for The Charles Stark Draper Laboratory, Inc.

Where this issue fits in the phases of the pandemic: Hot spots, flare-ups, next waves, business resumption

Summary: Security leaders and other stakeholders can have a positive impact on employees and the workplace by considering and implementing risk control and mitigation techniques designed to protect computers, technology, and the company brand.

Many employees have been sequestered with shelter-in-place orders with little notice (and if fortunate enough to still be employed) are working remotely. Given the situation we are all in, security leaders can mitigate risk by evaluating, identifying, and improving their information security policies to counter the aggressive actions of cybercriminals and advance persistent threat (APT) groups taking advantage of the COVID-19 pandemic. According to the Verizon 2019 Data Breach Investigations Report (https://enterprise.verizon.com/resources/reports/dbir/):

Threat actors consist primarily of three types - and involve the corresponding threat actions that are focused on data breaches:

1. **Actors external to the company**: Account for ~ 65% of data breaches (social engineering, accessing unsecured networks, physical theft, or data exfiltration).
2. **Actors internal to the company**: Account for ~ 30% of data breaches (insider and privilege misuse, ignorance of policy existence, physical loss, or data exfiltration for unauthorized use).
3. **Partners of the company**: Account for ~ 5% of data breaches (negligence, data misuse, malicious intent, or accidents).

Alarmingly, the report also highlights that 56% of breaches had long periods of activity taking months or longer to discover. Prior to the pandemic, some companies implemented well-defined and mature information protection controls. These controls include multi-factor authentication, end-point protection, unified threat management, VPN connectivity, data loss prevention), and security event and incident management (SEIM). Many also have implemented bring your own device programs that provide partitioned and controlled access from personally owned hardware. The most mature companies maintain security operations centers (SOC) or global security operation centers (GSOC) to monitor, detect, and respond to cyber incidents.

However, some organizations have implemented only a few of these controls. Meanwhile, cybercriminals and APT groups have done everything but shelter in place; they are moving boldly across the globe at internet speed while actively taking advantage of the COVID-19 pandemic to gain access to companies sensitive, proprietary, and customer information. A recent FBI report stated that "Scammers have used websites and mobile apps to implant malware to steal financial and personal information. Other criminals have used COVID-19 as a lure to deploy ransomware for payments." (https://www.fbi.gov/news/pressrel/press-releases/fbi-and-secret-service-working-against-covid-19-threats).

Technical systems, even if equipped with all the "best-in-class" cyber defenses, are still vulnerable to cybercriminals who will leverage social engineering to compromise information technology resources and the information contained within. The best hardware and software cannot prevent people from being helpful on the phone, responding to emails they think come from their superiors, or clicking on a link and infecting their or the company's computers. The following recommendations should be considered now to minimize risk:

- Have a well-defined cyber-attack response plan that can be immediately implemented and acted upon. Given many labels, this is often called an incident response plan.
- Implement an augment awareness program; send policy and rules reminders to all employees regarding the use of information technology resources provided by the company and, if applicable, personally owned devices.
- Update and invigorate your end-point protection so that malware/virus scanning software is operating in all resources used for business purposes; this may require employees to connect to your network overnight, so that each device can be scanned, and patch management upgrades can be provided. This should be done periodically, or upon detection of a significant vulnerability.
- Give detailed instructions for the use (or restriction) of videoconference platforms such as Zoom and other online teleconference center services. Consider allowing only signed-in users to attend, turning off file transfer, locking the meeting, and requiring unique passwords for each meeting to reduce the chances of hackers eavesdropping on private sessions; not doing so is an easy path to corporate espionage.
- Increase network monitoring consistent with the threats facing your industry; update and dial up the sensitivity on every technical control system and augment staff accordingly.
- Provide education and training regarding phishing, social engineering - especially business email compromise using typo squatted domains, common attack vectors, or vectors that are specifically targeting your industry. Employees must be reminded to be cautious of all emails and text links. They should be required to examine the full content of a message looking for anomalies before opening or clicking. Remember: the best IT systems cannot prevent a person from clicking on a link that can compromise your or your customer's intellectual property and tarnish your companies name.
- Require employees to report any suspicious or anomalous activity related to any computer used for business purposes. Increase the degree and sensitivity of your SEIM logging as well as additional staffing levels at the call centers to enable highly vigilante responses.
- Contemplate cyber and ransomware insurance policies to cover losses, notification costs, credit monitoring, defending claims from customers and applicable regulators, as well as any fines or penalties.
- Implement mandatory and frequent password changes and specify complexity requirements.
- Ensure your call center and SOC/GSOC are fully staffed and ready to respond to, or escalate, a cyber-incident.

We recommend you collaborate, now, with stakeholders in IT, Legal, Audit, and perhaps others, to understand the capabilities you currently have in place. Then, identify any gaps and corresponding actions you can implement short-term that can reduce or prevent the risks such as outlined above.

Once the dust has settled, and things get nearer to a steady state, it will be time for an after action report. This should be a thorough macro-level, wide-area review of your information protection game plan. If that litany of technical control options we rattled off at the top of this article sounds like geek technobabble, you need to get your IT and InfoSec leadership in to explain why these features are missing from your environment. Ask some tough questions but be ready for the tough answers. You may find that insufficient resources or inadequate investment may have adversely impacted your organization's ability to reduce risk when it mattered most.

Related SEC resource: A Holistic Information Protection Program

Contact us if you need assistance in COVID-19 strategic planning, response or recovery at contact@secleader.com