SDG

[technology + passion] – risk

- 55 North Water Street
  Norwalk, CT 06854
- 203.866.8886
- sdgc.com

Beyond COVID-19: 7 Security Focal Points for 2021

Over the last several months, our team has talked to CISOs across multiple industries to find out how they navigated the COVID-19 crisis. The answers we got became so repetitive that we stopped asking the questions. The common response from most of these security professionals was simple: They were prepared. No, they didn't predict COVID-19—but they had built their security to be ready for the unknown and flexible enough to handle sudden change.

Of course, there were pandemic-induced hiccups and challenges as organizations rushed to adapt to remote work. CISOs nationwide encountered everything from operational delays to serious gaps in the security footprint. But most were confident enough in their systems and team to weather the storm.

Now that the wave of chaos from the global pandemic has settled, the most pressing question is this: What comes next? How do you prepare for the next global crisis, hacker intrusion or insider security breach that may potentially cripple your organization's ability to do business? Consider the recent security breach on Twitter, which led to several verified accounts being hacked in order to scam followers out of their money. With breaches like this happening on a regular basis, every CISO must be on top of the next generation of threats. Which systems are deficient? Who needs to be retrained, or what steps can you take to firm up the gaps in your security architecture? And, perhaps most importantly: **Where do you start?**

Through conversations with clients and prospects about the lessons learned from COVID-19 and their vision for security in 2021, several threads emerged. Some are simple remedies; others are complex changes—but all of them are critical points of maturity to ensure that CISOs remain confident that they have prepared their firms and security infrastructures for the next onset of unknown challenges.

The top seven focal points for security maturity in a post-COVID-19 world are both strategic and operational in nature. They are essential for building a robust security footprint for 2021.

1. **Multifactor Authentication (MFA):** Ransomware attacks are increasingly crippling corporate systems—and they are just one of many threats to protect against. The sudden move to working remotely exposed a lot of devices, passwords and systems to threats that don't usually affect the business community. Having best practices and password policies in place may not be enough when you consider the move to remote work. Now, working at Starbucks with prying eyes sitting at the next table is a sure-fire way for a threat to gain access if you do not have MFA in place.

2. **Passwordless Authentication:** Password authentication has always been challenging for organizations, and according to the Verizon Breach Investigations Report, compromised credentials are responsible for more than 80% of all breaches. The COVID-19 crisis has resulted in increased attacks due to stolen and hacked passwords. Twitter and LinkedIn have been the most recent victims of ineffective password security. While these organizations are moving towards adoption of MFA to make static credentials more secure by utilizing OTPs, SMS or hardware tokens, these added layers still leave organizations vulnerable to keylogging, phishing attacks, and more. Passwordless authentication

enhances an organization's cybersecurity by significantly reducing the overall attack surface and virtually eliminating the risk of credential breaches.

3. **Privilege Access Management (PAM):** The increase in unauthorized access to corporate systems due to poor password policies and protection has elevated the risk of breaches to critical systems. The internal and external threats combatted by cybersecurity teams require an organization to have a handle on which critical systems are being accessed and what users are doing with the data they are accessing. Lack of visibility into your company's most precious assets leaves you vulnerable to catastrophic breaches. Establishing simple steps to monitor your organization's critical systems is not only prudent, but required in a time where just one breach can threaten your business and ruin your corporation's public image.

4. **Security Operations Center (SOC):** Most organizations are confident that their SOC, whether it is managed internally or externally, is being serviced by professionals. But how do you know when something needs to change? If you wait until after a breach, it's already too late. When was the last time you tested the effectiveness of your SOC? Are they maintaining the vigilance necessary to protect your assets? Or are they asleep at the wheel? Most CISOs have their SOC testing the business community to see if the users are following security protocols. Have you initiated a breach or inserted a threat in a system to ensure your SOC is responding quickly and diligently? How else will you remain confident that they will act appropriately during the next crisis?

5. **Identity and Access Management (IAM):** The value of Identity Governance is not a new issue. Publications and conferences have been stressing its importance to your organization for years. Most organizations have some sort of solution—but some are old and outdated, and others are only partially implemented or not fully functional. The lack of functionality and security associated with old or underutilized IAM implementations presents a unique problem for security professionals. These systems are designed to build confidence in your organization's security, but poor implementation or inefficient systems increase the likelihood of a breach. Waiting to repair or replace a deficient IAM program may be the greatest threat to your organizational security.

6. **Zero-Trust Network Access (ZTNA):** If there is one critical vulnerability that the novel coronavirus pandemic has highlighted, it is the deficiencies in the traditional VPN setup. The emergence of the remote workforce en masse has exposed many corporate applications to the internet and its lurking threats. Maturing your infrastructure and network security with ZTNA is the first step in securing and controlling remote access to specific applications. The capacity to "hide" applications from the internet may be the best way to expand your workforce's ability to work without exposing your systems to greater risk.

7. **Social Engineering Assessment:** Social Engineering attacks have risen sharply, and attackers continue to improve tactics. Psychologically speaking, social engineering attacks always bypass the analytical tools of the mind. It operates primarily at the level of the emotional sphere, which is habitually suppressed when most people engage in mental work. That is why social engineering techniques often succeed, even when the attacker's intelligence is notably lower than the victim's. Even if an insignificant percentage of employees launch malware on an organization's network (especially the privileged employees, such as top management and system administrators), this will compromise the entire company. Humanity will always be vulnerable, which means ongoing training is a necessity.

In this post-COVID-19 world, a time that many are calling the "New Normal," maturing your security capabilities is becoming even more important. As insider and outsider threats evolve, your team and systems must be assessed continually. Now is not the time to learn the lesson that Twitter recently learned. Verified, credible accounts once thought to be secure were deficient—and hackers manipulated the unsuspecting public to make off with hundreds of thousands of dollars in Bitcoin.

Where will your next breach come from? It's impossible to know—which is why you must evaluate where you are today and initiate the process of maturing your capabilities to meet tomorrow's unknown threats head-on. It's time to be confident in your risk management initiatives, so that no matter what comes your way, you are ready.

[technology + passion] – risk

- 55 North Water Street
  Norwalk, CT 06854
- 203.866.8886
- sdgc.com