# THE SIMPLE GUIDE TO CYBERSECURITY POST-COVID

The COVID-19 pandemic changed things on many human and cultural dimensions. And what is more tied to culture in America than work? Our work underwent a digital transformation.

# 2020 Created Cybersecurity Triage

For many of us, the timeframe was March or April of 2020. The pandemic sent thousands of us home to work - all at the same time, with limited digital infrastructure in place. We worked from dining room tables, our kids in the next room trying to get enthused about virtual pre-algebra lessons. Employees found themselves trouble-shooting their own IT issues and lacking the sometimes underappreciated security blanket of that corporate digital infrastructure and in-house IT support staff. Working remote accelerated the adoption of applications like Zoom, Slack and other cloud-based computing applications. With these transformative changes in work culture, cybersecurity, and our need for it, changed as well.

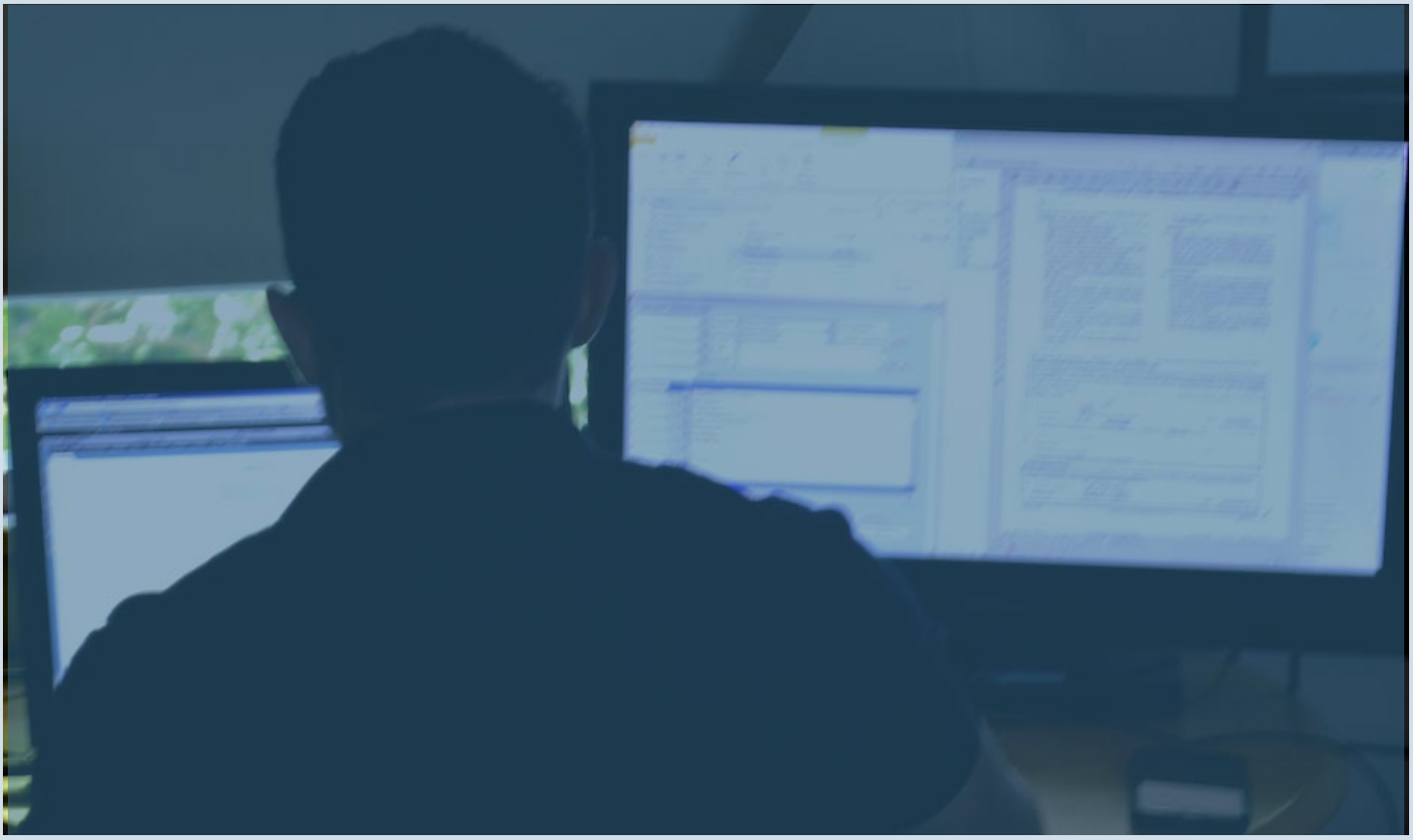
# The Attacks That Came With It

Those entrusted with cybersecurity at firms of every size had to alter plans on the fly as exposure to cyber risk heightened. Supply chains were targeted, ransomware attacks proliferated and cybersecurity was suddenly on the tip of everyone's tongue due to high-profile cyber crimes like the SolarWinds attack, suspected to be the work of Russian-government-backed hackers. Money allocated elsewhere was moved to the procurement or upgrade of VPNs, remote-work applications and other cloud-based security technology. Some of these investments were in the long-range plans as remote-work was trending prior to COVID - the pandemic put those investments on a very fast track.

The Federal Bureau of Investigation reported a 70% increase in digital cybercrime complaints from 2019 to 2020. Additionally, they estimated 2020 cybercrime losses at more than $4 billion. Is it real - at my level? Yes. Those FBI stats are reflective of broader trends - not just larger payouts. Deloitte, in their 2020 article outlining the impact of COVID-19 on cybersecurity, outlined a few reasons for this uptick including:

- Employees working from home can be tempted in this new environment to commit cyber crimes such as fraud.
- Opportunist cybercriminals pouncing on the vulnerability of those working from home.
- “Social engineering.” Cyber-attackers sensing that people concerned about a topic like the coronavirus will be inclined to open malicious fake email or visit fake sites.
- Hacktivists fighting for political and social issues, including those abroad.
- “Script Kiddies,” or junior hackers testing out their capabilities.

The instant ramp-up of work from home and bring-your-own-device exacerbated this trend, encouraging cybercriminals with a greater population of targets and networks offering less resistance to their attacks.



## The Alphabet Soup of Post-COVID Cybersecurity

With a new world of cybersecurity threats heightened by the pandemic crisis, we usher in an updated, good-to-know lexicon for employees in IT decision-making roles or at the C-level.

**1. WFH** - Work From Home. Gartner predicts that nearly half of employees will work remotely at least some of the time. That's up from 30% pre-pandemic. WFH has become a recruiting and retention necessity for many employers.

**2. BYOD** - Bring Your Own Device. Employees, especially in small to medium-sized businesses, rely on their personal mobile devices and computers to conduct corporate business.

**3. WAN** - Wide Area Network. Most are familiar with Local Area Network or LAN. WAN is simply the new reality - a large network of information not tied to a single location.

**4. SASE** - Secure Access Service Edge. SASE delivers security and wide-area networking as a cloud service directly to the source of connection rather than an enterprise data center.

**5. SWG** - Secure Web Gateway. A secure web gateway protects remote users from accessing malicious website traffic on their internet or cloud services that could infect their own devices or compromise their corporate network.

**5. SWG** - Secure Web Gateway. A secure web gateway protects remote users from accessing malicious website traffic on their internet or cloud services that could infect their own devices or compromise their corporate network.

**6. CASB** - Cloud Access Security Brokers. CASB is software that sits between the cloud service providers and cloud service users to provide a layer of enterprise security in that transaction.

**7. FWaaS** - Firewall as a Service. FWaaS are cloud-based services that include web filtering, advanced threat protection (ATP) and other security services to remote and hybrid workforces in particular.

**8. MDM** - Mobile Device Management. MDM is security software that allows a company to secure, manage and monitor end-user mobile devices and tablets, laptops and IoT (Internet of Things - e.g. smart monitors).

**9. XDR** - Extended Detection and Response. XDR collects and correlates data across multiple security layers to allow faster detection and mitigation of cybersecurity threats.

**10. ZTNA** - Zero Trust Network Access. ZTNA is a category of services that provide secure access to apps and services based on defined protocols such as authentication and authorization.

# What Do You Do to Be More CyberSecure?

Chief Information Security Officers and others charged with maintaining data security have a tall task. As futurist Gill Press noted, riffing on a Marc Andressen quote about software ten years prior, "Data is eating the world." Streaming, e-commerce, the digitization of work processes formerly conducted in person place enormous stress on the digital platforms and networks that we use. Cyber security experts and the employees and companies they are entrusted to protect need a new set of tools. Some recommendations:

- **Antivirus software.** Equip your team with antivirus or malware software that can monitor, analyze and alert to low-level cyber attacks.

- **Cybersecurity awareness.** We are all digital and employees need to know the risks. Do they know what phishing scams look like? Do they know how to report suspected scams? How to run security updates?

- **Cybersecurity training and support.** Acknowledge the real threats and what it will take to mitigate the risk within your organization. Then, if you don't have the internal resources, find a service provider with expertise in working with businesses of your size.

- **Home network security.** Find the services that can add a layer of protection between the corporate network and the home network. Use a VPN. Look for security that mitigates risk from the digital interaction with contract employees and key vendors.

- **Run a fire drill.** The average ransomware attack is reported to be between $200,000 to $400,000. In the same way, you might prepare your employee population for a fire drill, a simulated cyber attack is a drill worth considering.

- **Review your plans.** How fast are things changing in the digital space or in your industry? Consider conducting annual or spot reviews of your cyber security infrastructure and processes to stay ahead of the criminals.

- **Update your policies.** If you haven't already, consider more stringent authentication and authorization policies for employees working within your network. The Zero Trust approach sounds draconian, but is really just smart business.

There is no one-size-fits all solution here. If there is a universal message on the topic of cyber security post-COVID, it's this: be vigilant and fill in the gaps as they exist within your firm. This could mean extra commitment to process and protocols, equipment upgrades, the addition of specialized staff, or adding specialized training for existing staff - just to name a few. Whatever direction you go, it deserves your attention. We're not turning back!