IT FOR THE C
By Dave Moorman

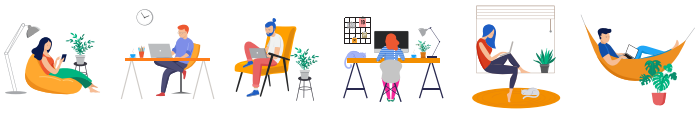
NOVATECH
BRING EVERYTHING UP TO SPEED

Corporate Cyberattacks Are Out of Control.

Don't Let Work from Home Policies Be a Factor

In January 2021, Security Magazine predicted the pandemic-driven rush to deploy remote and hybrid work environments would have significant implications for cybersecurity. With the increased attack surface, the authors noted, criminals would expend even more effort to identify and capitalize on companies' weak points. As it turns out, the predictions were spot on. In the past 12 months, per a study by Forrester Consulting, 94% of businesses have been the target of a cyberattack, with 74% of the attacks attributed to vulnerabilities in technology adopted during the pandemic.

Furthermore, it doesn't appear things will get better anytime soon. Initial assumptions that COVID-19 would be controlled and companies could return to a more normal working environment have turned out to be woefully wrong. As of July 2021, only one-third of company leaders indicated their workers would be "in-person first," with approximately half using a hybrid model.



As of late August 2021, 66% of organizations surveyed had announced delayed office reopening due to the continued arrival of COVID-19 variants. In September, the news became so pervasive that experts began calling the "return to work" (RTW) movement "the great wait.

Behemoths such as Amazon, Apple, Facebook, Google and Starbucks have now announced they are delaying their return to the office date. (Google has delayed it until January 2022 or later — the third delay since its original date of July 2021.)

Navigating the Future of Home and Hybrid Workspaces

When COVID-19 hit, some people were already working full-time from their homes or local business centers and coffee shops, but the unprecedented uptick in remote working from the pandemic has caught many business leaders by surprise. Here at Novatech, we watched as organizations large and small moved a significant number of workers from centralized locations to home offices. We have also learned of the dire consequences many suffered due to lack of preparation.

The good news is that it is not too late. Given the current "great wait," it makes sense for business leaders to implement key technologies that will not only serve remote workers now and in the future but will also support traveling workers, hybrid workers and potentially even trusted partners and vendors who need access to corporate systems. All of these solutions are designed with two ideals in mind: ensure rock-solid security without compromising productivity.

No matter where you and your company are on the "remote work continuum," — or where your staff works — I urge you to address five critical exposure points: User Awareness, Network Security, Endpoint Security, Data Security, and Wireless Connectivity. Following are my recommendations with a summary of each item. Functionality (and value) goes well beyond these brief listings. If needed, Novatech experts would be happy to explain them in greater detail.

User Awareness Training

There is no dispute that end users are the weakest security link in the cybersecurity chain. Hackers prey on human curiosity, trust, negligence and greed to introduce malware into networks. (So prevalent has phishing become that one in every 99 emails is now a phishing attack.) Fortunately, users are also the first line of defense. User awareness training ensures proper education regarding malware sources, ransomware and other potential threats — and how the user should respond.

Next Generation Firewall (NGFW)

Most tech-savvy business leaders recognize their firewall is a primary bulwark against attack. What's different about a NGFW? Like regular firewalls, NGFW use both static and dynamic packet filtering and VPN support to ensure that all connections and encrypted traffic between the network, Internet and firewall are valid and secure. Both can also translate network and port addresses in order to map IPs. However, NGFWs provide other network device filtering functions, conducting deep-packet inspection (DPI-SSL) that moves beyond port/protocol inspection and blocking to add application-level inspection and intrusion prevention.

This capability enables NGFWs to analyze external data, such as white lists, and match them to application signatures. With this information, they can distinguish between safe applications and unwanted ones and either allow or block them. Given that web application breaches account for approximately 43% of all breaches, this capability is significant.

Endpoint Detection and Response

The news is full of stories of "network vulnerabilities" and "network compromise," but they don't always mention the primary source of intrusion — endpoints. Endpoint attacks are no longer limited to targeting careless users or unprotected thumb drives. Although both remain an issue, business equipment, such as networked printers that scan and store documents, are also prime targets. All endpoints must be identified and secured.

Some firms have so much exposure that they require XDR — Extended Detection and Response, a service that Novatech also provides. XDR products combine multiple security products in a cohesive, unified security incident detection and

response platform, thereby enhancing security (and value). This approach not only increases the detection surface but also enables evaluation of streams of alerts to identify more serious incidents for manual investigation.

Multi-Factor Authentication (MFA)

The days when a strong password was sufficient to secure data and systems is long gone. Multi-factor authentication requires users to provide two of authentication factors from three possibilities — something they know (like a password), something they have (such as their smartphone) and something they are, like a fingerprint). Best practices dictate the use of MFA to secure access to all corporate resources, from networks to Microsoft Office, Salesforce and Google documents.

Secure Wi-Fi Connections

So many devices are now connected via Wi-Fi networks that the damage a hack could do is incalculable. Attackers have accessed one company's network and then used that access to leverage partner and vendor networks as well. Although some of the protections listed above can help secure Wi-Fi networks, business owners should also incorporate data encryption, hiding SSIDs (service set identifiers, your network's unique name), access restriction (e.g. the use of limited-privilege "guest accounts" for third-party entities that need access) and other controls.

Who Has Your Back? We Do.

If this sounds like a lot to digest, it can be. Yet, no organization is safe if they do not implement these basic protections. We actually recommend more, including ensuring an IT specialist trained in remote working issues and security is available to answer worker questions and help them avoid foolish, expensive mistakes.

This resource can be direct (email or call response) or it can be orchestrated through an automated ticketing system that incorporates security advice. If you have implemented either of those approaches, we salute you. The majority of business leaders with whom I speak have not. Many rely on an in-house staffer who handles other technology needs, such as managing a sales database or maintaining the software that integrates mission-critical technical systems.