Cybersecurity in the Time of COVID-19

Keys to Embracing (and Securing) a Remote Workforce

The declaration of a global pandemic forcing the immediate need to protect the health of employees underscores what we are all coming to realize: that the COVID-19 disease, is going to continue to cause a level of social and economic upheaval that is unprecedented in modern times. At Atlantic, Tomorrow's Office we have risen to the significant challenge from our customers as they continue to face these sudden and profound challenges, seeking ways to quickly mobilize and support the sudden need for employees to vacate offices and work from home.

Maintaining security in the face of this office exodus magnifies the threats and presents additional significant risks for most organizations.

The COVID-19 crisis is likely to be with us for a while. Organizations and their employees have been be forced to make tough decisions rapidly, and enabling a remote workforce is one of those decisions. There are risks involved in accomplishing this at speed, but the security of your employees, data, networks, devices shouldn't be among them. Aside from the pressure this office exodus puts on management and employees, there are real cybersecurity challenges organizations must now consider.

In recent weeks, Atlantic has assisted organizations who are trying to rapidly deploy large fleets of new systems. These emergency deployments need to be secured just like any other corporate asset, with the additional challenge of keeping remote users diligent of their responsibilities to continue practicing safe cybersecurity habits. Extraordinary times call for extraordinary responses. As our customers respond to the challenge posed by **COVID-19** by requiring remote work for employees, Atlantic wants to do its part to help companies stay secure and focus on their business continuity.

Due to the speed at which organizations were forced to move employees to remote / home-work environments, security becomes more challenging. In many cases, many organizations are force to quickly purchase new systems and/or are asking employees to leverage their own devices to do their work, which may or may not have adequate endpoint protection. Unfortunately, the rush to deploy this new work environment can supersede the diligence to ensure proper security measures have been put in place. And since personal devices may be used to access sensitive company data and applications, they also require appropriate and heightened protection from cyber threats.

Security solutions for remote devices and users need to be simple to deploy and manage. The Atlantic team rises to these challenges with solutions to minimize employee and organizational security risks.

How Atlantic, Tomorrow's Office Is Helping Ensuring Security Across Your Remote Workforce

In order to help organizations cope with these new and unexpected challenges, it is imperative to have a ***Managed* Security Suite** to address increased risks introduced by the large numbers of managed and unmanaged devices being used by new remote workers.

These are the core security components of Atlantic's Managed Security Suite to maintain compliance and minimize risks of financial loss, business interruption and potential liabilities

- **User Awareness Education & Training -** Continued education is crucial, as coronavirus-themed scams escalate. The World Health Organization (WHO) and the U.S. Federal Trade Commission (FTC) have already warned about ongoing coronavirus-themed phishing attacks and scam campaigns. Magnified by the additional distraction from working at home, employees need to more diligent than ever to practice safe email and social media habit to avoid falling victim to phishing emails, ransomware and other email and internet borne threats. Continuous end-user education and communication are extremely important and should include ensuring that remote workers can contact IT/Atlantic quickly for advice. Organizations should also consider employing more stringent email security measures.

- **Advanced Email Security** - To help minimize the risk of phishing, ransomware and other malware-laced emails making it to your users, it is imperative that effective systems and processes are employed to prevent threats from even making it into users email. Managed email security solutions are designed to minimize email threats by successfully filtering spam email, identifying phishing, ransomware, malware and other malicious links and attachments. Additionally, our solution automatically will backup and archive email and can provide email encryption to help secure sensitive communication if needed.

- **Multi-Factor Authentication (MFA)** – As employees work remotely, now more than ever it is imperative that their identity be validated before they are granted access to your network, applications and data. Our managed security includes MFA, which will send a verification code to a predefined cell phone or email, requiring employees to confirm they are an authorized user by entering the code on their system before access is granted.

- **Dark Web Monitoring** – It is inevitable that user credentials will become exposed to breaches, whether directly from your organization, or more likely as part of a larger breach at a financial company, credit agency, store, vendor, Facebook, healthcare provider or any number of other companies. The trick is know if your employees credential have been stolen and are now being sold on the Dark Web – which is how hackers monetize their nefarious efforts! At Atlantic, we will monitor the Dark Web and be quickly alerted to any occurrence of user emails and potentially passwords – providing us with actionable information to take proactive measures to secure your accounts.

The Atlantic Difference - **The glue that unifies, monitors and manages this solution for our customers is our world-class support and technical team! From our 24 x 7 help desk and professional engineering team, we do all the heavy lifting to ensure our customers stay safe, resilient and operational at all times, especially during today's challenging world! Managed Security needs to be part of every organizations solution.**