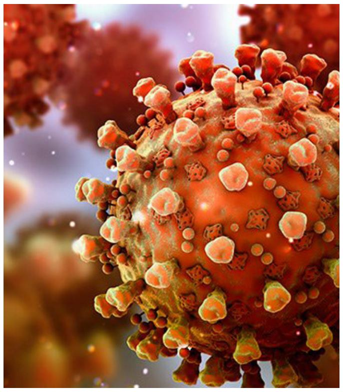
Quick Reference Guide

Functioning in the Age of Shelter in Place

How we're transitioning to virtual work @home & data security

Prepared by CONEXXUS

On March 11th, 2020 the World Health Organization (WHO) characterized the COVID-19 Virus as a global pandemic. Within two days, the planet was operating under an unprecedented State of Emergency, requiring a majority to stay home and shelter in place.



"Our community is an essential service across North America. For the many of us sheltered in place at home, our ability to support our site staff and consumers is dependent on secure access to our critical information systems."

Please stay healthy and safe!

Gray Taylor – Conexxus Executive Director

Securing Our Work @Home

It is virtually impossible to secure everyone's homes to the same level as their work locations. Much will be learned from the COVID-19 emergency, and extended security policies and workflows will be reviewed and adjusted for working at home.

In the meantime, we suggest three practices to increase the security of work at home:

1. PERSONAL FOCUS / SEGREGATION OF TASKS

Make a conscious effort to separate work time from family time and household responsibilities. During focused work time, turn off your social networks, personal email, games and searches. Keep your attention, computer, and network activity on work related tasks, the most common being company related email, conference calls and collaboration tools. If possible, segregate work and personal use to different devices (computers, laptops, tablets), and do not permit family use of your work devices.

2. FUNCTIONAL BUSINESS SYSTEMS

Sensitive financial, customer, HR, product and operational data should only be accessed through a Virtual Private Network. A VPN is set up and implemented by IT administration, and permits your work device(s) remote access to company's secure internal network. For those who primarily work at the office, VPN access should be mandatory to work at home.

3. ESSENTIAL SERVICES SUPPORT STAFF

There are many critical office staff responsible for 24/7 support of the ESSENTIAL RETAIL SERVICES of the business. During the COVID-19 pandemic, home based monitoring of, and access to, mission critical infrastructure will be required. For retailers and vendors, the help desk, software development and QA teams, field technicians, back office and payment systems specialists must be able to operate with high availability and security.

Quick Reference Guide

During the COVID-19 crisis, many of our Conexxus members have securely installed fully operational support systems at the homes of the critical staff. These home installations require the same PCI safeguards as internal systems and workflow processes.

The following are a few examples of how Conexxus members are enabling Essential Service Support at home:

Essential Services support practices from home for critical IT and operational staff

- Securely prepped, tested and installed production point of sale systems. Lock-down hardware, secure Windows / Linux image, PA-DSS application software, printer, scanner, and payment terminal.
- Secure remote access to test and certification labs for quality assurance and development staff. Provide test cards (payment, loyalty, gift) and secure access to above site test systems.
- Prepped, shipped and installed pump dispenser and pay at pump simulators to critical developers and QA staff.
- Acquired smaller desktop versions of pay at pump simulators from pump manufacturers. These desktop devices are excellent for both office and home use, not only during emergency periods, but to facilitate 24/7 response to critical field issues.
- Technicians sent to install equipment, while ensuring their safety, and the safety of the families at home.

Conexxus is seeing a shift by Cybercriminals to exploit home attacks during COVID-19.

These recommendations are not only best practices that should be adopted at home, but necessary to stop an increase in business related cyberattacks to workers homes.

A recent Law360 article indicates a new spike in cyberthreats related to the disruption of COVID-19.

> *"Hackers are exploiting vulnerabilities stemming from the global coronavirus pandemic, including distracted workers and stretched-thin IT staff, as cybersecurity attorneys say the spread of COVID-19 has also brought with it a spike in data security incidents."* *Law360 (March 20, 2020)*

The article further states that companies need to double down on cyber-defense during the crisis, as the shift to remote work gives hackers more ways to infiltrate networks and take advantage of potentially panicked staff.

It's challenging to segregate work and family activities while sheltered in place at home. Unlike the office, where security policies restrict personal use of the company network, combined personal and work-related internet use is more the norm at home.

During the COVID-19 pandemic, the Conexxus Data Security Committee (DSC) has been advised of substantial increases in cyberattacks resulting from sudden, unplanned relocation to our homes.

- Over 50% decrease in office-related security events due to the sheer volume of offices moving employees to remote work.
- Over 80% increase in active phishing activities and 30% increase in active blocks of malicious content. People are at home surfing Facebook and other social networks.
- Over 200% increase in logged events from remote network equipment as IT departments put their teams at home, rapidly deploy VPN infrastructure, and in some cases decrease security controls all of which serves to increase vulnerability to attack.
- A surge in COVID-19 related phishing emails, ransomware and duping online payments and wire transfer services.

This article is co-authored by:

Gray Taylor – Executive Director, Conexxus
Dave de la Plante – Strategy and Program Director,
Bulloch Technologies