COWBELL™ CYBER

Cyber resilience in times of COVID-19

MARCH 2020 | WWW.COWBELL.INSURE

RECOMMENDATIONS TO KEEP YOUR BUSINESS SAFE UNDER UNIQUE CIRCUMSTANCES

The disruptions created by COVID-19 are unprecedented. As we adjust to social distancing and a new way of interacting, we should not overlook disruptions that are less visible. Work is shifting to a virtual, online model wherever possible and it is imperative to remain vigilant and double down on cyber protection and basic security hygiene.

Two obvious examples of COVID-19 changing the threat landscape:

- Many employees are opting or required to work from home and connect to their workplace through personal devices, home router and WiFi network. These might or not be adequately protected.

- Many businesses are reaching out to offer online servicing, including banks inviting consumers to activate mobile banking.

Cyber criminals are also taking advantage of the chaos and uncertainty to launch email scams, phishing campaigns, and targeting vulnerable IT infrastructure left unattended.

The Cowbell team wanted to offer recommendations and resources to stay safe online and ensure the protection of your business:

Multi-factor authentication (MFA): Enable MFA on all services supporting it: payroll application, CRM system, online banking, email and more.

Patching: Keep devices, applications, and web site tools up-to-date and patched to the most recent versions of software.

Email scam and phishing: Remind employees to validate emails before downloading attachments or clicking on links. Diligently review email addresses - hackers will change one letter to a valid address and trick you into clicking on a malicious link. This Forbes article details the rise of phishing attacks and email scams that have emerged in the past two months.

Only visit secure websites: A secure website will have an address that starts with https, not http. Most browsers will raise an alert on suspicious sites granted that you're running the latest browser version.

Revisit your loss mitigation strategy: Review what your cyber insurance coverage includes or not, what type of event might be excluded. Check whether the limit, sublimits and deductibles you signed on for cyber still reflect the state of your business and your use of technology today.

Apply basic password hygiene: Do not share passwords, do not reuse passwords, especially between personal and professional services. Do not write them on sticker notes. Create passwords that are as long as possible.

Finally, get informed, don't hesitate to ask questions: if you need clarification on Business Interruption / Business Income coverage, what is covered or not, feel free to contact us.