TECHASSURE

www.techassure.org | info@techassure.org

Work-From-Home Cyber Risk Management

Employer Guide

Almost as quickly as the coronavirus/covid-19 pandemic took the world to its knees, cyber criminals begin using it to exploit the millions now forced to work-from-home (WFH). Weak home WiFi networks, a lack of encryption on personal devices and incorrect configuration of remote desk protocol (RDP) all bring massive cyber risks to employers that are now unable to monitor all workstations and employees directly.

A variety of phishing attacks have been discovered already and more are being created each day. Fake websites are being set up with false information, fraudulent stores selling medical equipment and fake charities - all in the effort to harvest credentials to cause harm. Cybercriminals know that company IT systems and resources are more strained than ever before and are using this to their advantage. The Cybersecurity and Infrastructure Security Agency (CISA), a department of US Homeland Security, recently announced key cyber security recommendations for employees working from home.

- *Update VPNs, network infrastructure and devices used for remote work – as all devices are variables*
- *Notify employees of increased phishing attacks and offer training/guidance*
- *Ensure IT Security teams are proactively monitoring logs/devices and are prepared for incident response/recovery*
- *Implement Multifactor Authentication (MFA) on all VPN connections and wherever possible*
- *Routinely test VPN network for limitations of mass usage*
- *Do not use Public WiFi, even with a VPN*

Phishing attempts are quickly increasing due to the work-from-home mandate from many employers. Phishing is the largest source of ransomware, one of the leading cyber threats. According to CFC Underwriting, 80% of all ransomware claims in 2019 were initiated through remote desktop protocol (RDP). Using MFA on all devices employee are using to access their work environment is critically important.

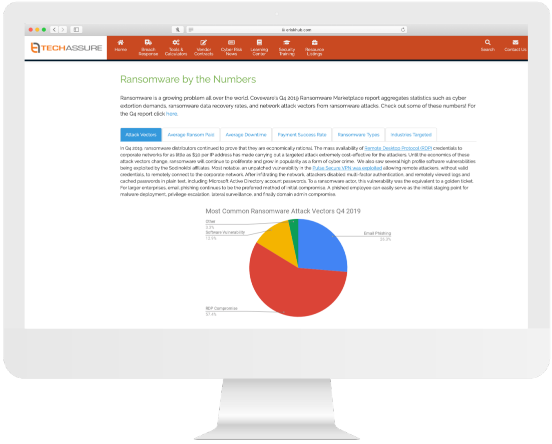
Additionally, alert employees that fraudulent websites and apps are appearing daily claiming to contain covid-19 resources, safety supplies, etc. Alert employees to stay vigilant.

ProTip: TechAssure member Brush Creek Partners' Emily Short advises employees to simply pick up the phone if something appears suspicious. "We tend to communicate almost exclusively via email and text in today's business environment but picking up the phone has averted many disasters. The client/vendor will appreciate you taking the extra step to confirm a request."

Additionally, password management is key. Short says, "Remind employees to use unique passwords for all accounts. Reusing passwords is an extremely common and can put all of your accounts at risk if one gets hacked." Use a password manager such as Dashlane, LastPass instead.

TECHASSURE

www.techassure.org | info@techassure.org

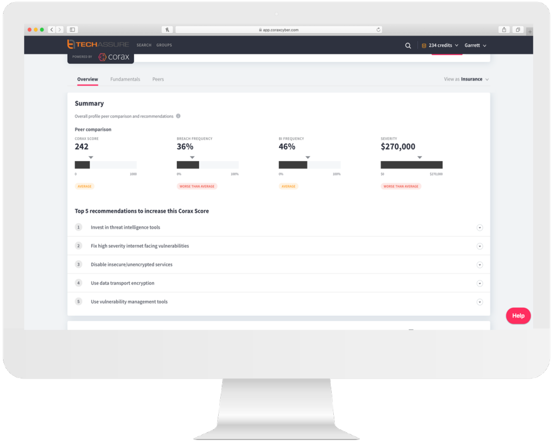


Ransomware by the Numbers

Ransomware is a growing problem all over the world. Coveware's Q4 2019 Ransomware Marketplace report aggregates statistics such as cyber extortion demands, ransomware data recovery rates, and network attack vectors from ransomware attacks. Check out some of these numbers! For the Q4 report click here.

In Q4 2019, ransomware distributors continued to prove that they are economically rational. The mass availability of Remote Desktop Protocol (RDP) credentials to corporate networks for as little as $30 per IP address has made carrying out a targeted attack extremely cost-effective for the attackers. Until the economics of these attack vectors change, ransomware will continue to proliferate and grow in popularity as a form of cyber crime. We also saw several high profile software vulnerabilities being exploited by the Sodinokibi affiliates. Most notable, an unpatched vulnerability in the Pulse Secure VPN was exploited allowing remote attackers, without valid credentials, to remotely connect to the corporate network. After infiltrating the network, attackers disabled multi-factor authentication, and remotely viewed logs and cached passwords in plain text, including Microsoft Active Directory account passwords. To a ransomware actor, this vulnerability was the equivalent to a golden ticket. For larger enterprises, email phishing continues to be the preferred method of initial compromise. A phished employee can easily serve as the initial staging point for malware deployment, privilege escalation, lateral surveillance, and finally domain admin compromise.

Most Common Ransomware Attack Vectors Q4 2019



Summary

Overall profile peer comparison and recommendations

Peer comparison

CORAX SCORE	BREACH FREQUENCY	BI FREQUENCY	SEVERITY
242	36%	46%	$270,000
0 – 1000	0% – 100%	0% – 100%	$0 – $270,000
AVERAGE	WORSE THAN AVERAGE	AVERAGE	WORSE THAN AVERAGE

Top 5 recommendations to increase this Corax Score

1 Invest in threat intelligence tools

2 Fix high severity internet facing vulnerabilities

3 Disable insecure/unencrypted services

4 Use data transport encryption

5 Use vulnerability management tools

eRiskHub®

corax

Tools | Resources | Guidance

TechAssure was founded in 2000 as a not-for-profit trade association for insurance brokers that specialize in technology-related risks. Our members are all peer-vetted top-ranking insurance brokerages that offer clients best-in-class service and guidance for cyber risks. TechAssure members have access to a number of resources and tools to better understand and manage cyber risks, including: eRiskHub pre/post breach services, Corax cyber assessments, benchmarking, coverage enhancements and more. Visit www.techassure.org to locate a TechAssure member nearby.