MARSH & McLENNAN AGENCY

It's our business
to be there for you in the
MOMENTS THAT MATTER.

Client Advisory

Cyber security and privacy concerns: COVID-19

In response to the inquiries from many of our insureds concerning the business impact that organizations are facing under the COVID-19 pandemic, the following are some best practices that may be helpful regarding security and privacy concerns. As remote desktop protocol is a frequent threat vector, we recommend these reminders for employers and employees:

1. Ensure privacy of employee information. Remind employees not to share sensitive information publicly if an employee (or family member) has been, or is suspected to have been diagnosed with Coronavirus.

2. With the increased numbers of employees working from home, especially for those who may not be accustomed to doing so, it is recommended to remind employees of corporate mobile device and remote access policies (i.e. mobile device policies, email/internet usage). Also, if not already implemented, require Security Application Gateway or VPN (Virtual Private Network) to access corporate systems and ensure multifactor authentication (MFA) where applicable.

   Additional tips from CSOonline.com: 8 Key Security Considerations For Protecting Remote Workers.

REMOTE DESKTOP PROTOCOL IS A FREQUENT THREAT VECTOR.

3. Remind your employees of your organization's data security policies, including the policy that we see many organizations have in place that mandates not sharing corporate information with non-approved and/or personal email systems.

4. Be wary of coronavirus related emails that may lure employees to click on malicious links and download malware/ransomware which may further interrupt your technology infrastructure by encrypting your network files and subjecting your organization to a potential ransom demand.

5. Do not connect nor download corporate documents/materials via non-approved or non-corporate managed devices (i.e. flash drives).

6. Protect mobile devices and sensitive paper document in transit (to avoid car theft) and at home in compliance with mobile device policies.

7. Presuming employees' increased reliance on teleconferencing, review contracts with mobile conference systems providers (i.e. Skype, Zoom, etc.) pertaining to the security/privacy safeguards they employ. Review responsibility, collaboration and indemnity provisions in the event of a system or security disruption and/or privacy event (i.e. eavesdropping, etc.).

   National Institute of Standards & Technology (NIST) Virtual Meetings Best Practices

8. If you are faced with supply chain disruption, maintain due diligence in seeking alternative suppliers/vendors from a systems and connectivity standpoint, without sacrificing security controls, data integrity and contractual standards.

9. Review your cyber liability insurance policy to ensure how it will respond to security/privacy infiltrations within a remote desktop employee environment. Most updated policy forms affirmatively cover unauthorized access into the organization's network/system/environment via remote desktop protocol (for example), although each policy differs in coverage. Remind employees to report suspected activity or infiltrations of their home network to their IT/Information Security team in accordance with your incident response plan and cyber liability policy.

10. For multinational organizations and organizations that may have care, custody or control of non-US citizen data, be mindful of the individual collection, retention and safeguarding guidelines by various Data Protection Authorities, especially in light of COVID-19. Guidelines from International Association of Privacy Professionals (IAPP) Global Data Protection Authorities.

FOR ADDITIONAL INSIGHT ON CYBER SECURITY AND PRIVACY, CONTACT YOUR LOCAL MARSH & MCLENNAN AGENCY REPRESENTATIVE.

Lisa Dickinson – Sr. Vice President, Executive and Professional Liability Practice
MMA Cyber Center of Excellence, Co-Chair
+1 470 337 1192 | lisa.dickinson@MarshMMA.com

Terry Lavoie – Sr. Vice President, Executive and Professional Liability Practice
+1 470 342 5911 | terry.lavoie@MarshMMA.com

Sam Stern – Sr. Vice President, Executive and Professional Liability Practice
+1 770 622 7235 | sam.stern@marshMMA.com

WE'RE HERE FOR YOU

BUSINESS INSURANCE

EMPLOYEE HEALTH & BENEFITS

EXECUTIVE BENEFITS

PRIVATE CLIENT SERVICES

RETIREMENT SERVICES

RISK MANAGEMENT

SURETY

Scott Boyett

Senior VP

Huntsville, AL

256-890-9068