MICHAEL ESPOSITO, INC.

Hello I'm
Michael Esposito
Vice President and Insurance Broker
at USI Insurance Services, LLC

USI Cyber Risk Update

Cyber Exposures and the COVID-19 Quarantine

March 26, 2020

USI Executive and Professional Risk Services (EPS) COVID-19 Risk Series - Cyber Exposures and the COVID-19 Quarantine

Given the COVID-19 pandemic impacting the globe, most organizations will likely face increased cyber risk due to:

- Remote workforces (workers accessing networks through company and personal devices, public wi-fi, etc.)
- COVID-19-targeted ransomware and phishing attempts and
- Overall strains on IT departments, third-party providers and support staff

These major threats require risk mitigation, risk management and/or risk transfer strategies as the crisis unfolds.

Malware and Bad Actors – the Threat is Real and Growing

- The Johns Hopkins COVID-19 infection rate map was laced with suspicious malware - that targeted people looking for information about the pandemic.
- A spike in ransomware attacks tailored to look like informative statements regarding the COVID-19 virus has been noted (and growing).
- The work of specific industries/organizations related to COVID-19 treatments are being targeted and the number of malicious sites involving COVID-19 being set up is staggering.
- Additionally, threat actors are using the COVID-19 event and remote workforce to gain a foothold for later exploits against "highly valued targets" – defense contractors, healthcare organizations and other entities with large amounts of sensitive data.

IMPACT – both immediate and future financial and operational impacts can be expected by many organizations.

Employer and Employee Practice Considerations – Critical Remote Workforce Considerations

As indicated in USI's Corona virus FAQ's document released in March 2020, a remote workforce raises potential cyber risks from both an employer and employee practices standpoint. Key risks and mitigation strategies for each include:

Employers: Work with IT, legal and HR departments to understand your company's:

- **Remote Access Practices:**
  - Test remote access solutions capacity and increase capacity to allow increased functionality.
  - Ensure Virtual Private Networks (VPN) are up to date w/access systems fully patched.
  - Implement the use of Multi-factor authentication (MFA) for remote access in conjunction with VPN.
  - Avoid use of RDP (Remote Desktop Protocol); replace with VPN/MFA combination.
  - Consider prohibiting/limiting access to certain assets and systems via any public Wi-Fi use.
  - Company provided devices should only be used by employees themselves, for company business.

  - BYOD (Bring Your Own Device) policy optimization best practices include updates on anti-virus usage, use of personal VPN's, version update automation, and use of device security features.
  - Note approved services for file-sharing and collaboration tools so employees don't find their own.
  - Implement Mobile Device Management (MDM) and Mobile Application Management (MAM).

- **Network Protection Practices**
  - Are the following enabled?
    - Endpoint detection and protection?
    - Network segmentation and backup segmentation?
    - Intrusion Detection System usage and monitoring?
    - Data Loss Prevention (DLP)?
    - Focus logging and monitoring efforts on VPN or other remote access; access to critical SaaS applications and logging around your most critical data stores.
    - Ensure all devices have properly configured firewalls; instruct employees on personal VPN items.
    - Data classification and collaboration with DLP?
    - Encryption utilization – data at rest and in transit? Homomorphic encryption for Healthcare?
    - Patch management – process and cadence should be reviewed and increased as necessary.

- **Training and Preparedness Practices**
  - Increase awareness of information technology support and "incident reporting" procedures.

- Remind employees of information they need to safeguard (Personal, Health and Corporate data).
- Continue security Awareness Program efforts, but shift focus to phishing awareness, device security, physical security of data.
- Disaster Recovery/Business Continuity Plan (DR/BCP) - does one exist and is it regularly updated? Has it been amended to contemplate a mostly remote workforce including the key DR/BCP stakeholders?
  - Current Vendor Management considerations (IT and non-IT vendors) – example of need for alternate option planning is India's announced 21-day lockdown.
  - Could a Managed Service Provider (MSP) provide back-up to any cybersecurity DR/BCP?
  - Document what changes (new practices, i.e.) are being made and why.

- Prepare for return to normalcy now -- what needs to change upon return to office work.

Employers: best practices include, but are not limited to:

- Exercise caution in handling any email ("phishing"), text message ("smishing") or voice calls ("vishing") with a COVID-19-related subject lines/attachment/hyperlink/topics or headers.
  - Topics with malware embedded have been noted as "CDC Update or Alert," "Best Health Practices for COVID-19," and "Workplace Policies or Workplace update."
  - Do not click on links or open attachments contained in unsolicited emails; do not open texts from unknown or suspicious numbers and be wary of unknown phone number calls.
- Be cautious of social media pleas/articles/links related to COVID-19 – these may be phishing items.
- Do not provide corporate/personal/financial information in response to online/offline solicitations.
- Use only trusted sources (hospitals, government websites) to obtain up-to-date information on the crisis.
- If you believe you have been a victim of a Phishing attack or potential malware attack:
  - Immediately report it to your employer, including network administrators.
  - Immediately contact your financial institution and watch for any unexplainable charges.
  - Immediately change any passwords you might have revealed – for each account. Do not use these passwords in the future.
  - Consider reporting the incident to the police, and file a report with the Federal Trade Commission.
- Employees should not use unapproved devices and cloud services for company business.
- Employees should keep their devices patched/updated, enabling automatic updates.
- Enable security features on any devices - PINs, fingerprint authentication, or facial recognition.
- Ensure home wi-fi networks are secure; use WPA2 or WPA3 security and a unique password.
- Disable all "smart home" devices with recording capability when discussing confidential matters, especially voice activated "smart speakers" such as Alexa, etc.
- Monitor the physical security of devices and files that go home. Ensure the disposal of hard-copy personal information and corporate data.
- "Remember password" functions should always be turned off when employees are logging into employer systems and apps from personal devices.

Cyber Insurance Considerations: Terms and Conditions and Representations

While no broad form COVID-19 direct exclusion has been seen in Cyber policies to date, it is important for clients to follow their Business Continuity Plan (BCP), Disaster Recovery (DR), risk management plans, vendor management, and protocols and practices as closely to the letter as possible. The reason - cyber insurance policies include a representation clause.

EXAMPLE: if there is a loss that could have been prevented by MFA (Multi-Factor Authentication) and a client represented in their application/supplement that they use MFA and forensics proves that they did not, any potential coverage may be impacted.

Other Important Cyber Coverage Issues: best practices include, but are not limited to:

- Awareness of the scope and definition of "Computer Network" (or "Network") or "Computer System" (or "System") is critical.
- Most policies will not respond to Internet Service Provider (ISP) or utility outages (seen as "Acts of God" or Force Majeure).
- For small and medium enterprises (SMEs): many policies include pre-event cyber loss controls, cyber best practices, cyber risk training and other cyber risk management tools. These additional services may assist with some of the topics noted above often at no or reduced cost to Insureds.
- COVID-19 will likely spark additional and specific underwriting questions that clients should be ready to address.

Other Resources

For more information about Coronavirus (COVID-19) including other helpful tools and resources, please visit our web page at www.usi.com/public-health-emergencies.

To further discuss any of the cyber threats covered in this update, or to learn more about how your organization can improve cyber awareness and the ability to respond to cyber threats optimally, please reach out to your local USI representative to access the cyber experts in the USI Executive and Professional Services Group (EPS). www.usi.com.

Sources

https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/

https://arstechnica.com/information-technology/2020/03/the-internet-is-drowning-in-covid-19-related-malware-and-phishing-scams/

https://threatpost.com/who-attacked-possible-apt-covid-19-cyberattacks-double/154083/

https://www.dataprivacymonitor.com/cybersecurity/covid-19-cybersecurity-exposure/, https://www.zdnet.com/article/working-fromhome-switch-off-amazons-alexa-say-lawyers/, https://www.insideprivacy.com/covid-19/covid-19-cybersecurity-advice-ftc-nist-and-cisarelease-guidance-on-secure-teleworking-and-critical-infrastructure-jobs/

https://www.natlawreview.com/article/coronavirus-covid-19-managing-cyber-security-risks-remote-work

https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

https://hbr.org/2020/03/will-coronavirus-lead-to-more-cyber-attacks

https://www.wired.com/story/coronavirus-cyberattacks-ransomware-phishing/