How to Protect You Organization from Cyber Risk Amid COVID-19

Adrienne Ehrhardt, Michael Best
Derek Laczniak, M3
Michael Sias, Northwestern Mutual

August 2020

Agenda

Introductions & Overview

The COVID-19 Impact on Your Cyber-Risk Profile

- Evolving Cyber Attack Techniques
- Cyber Risks of a Remote Workforce
- Unique Challenges by Sector and Jurisdiction
- Practical Considerations for All Organizations

Cyber-Insurance Implications

- Cyber-Insurance Concerns Related to COVID-19
- How to Plug Insurance Coverage Gaps

Michael Best

M3 INSURANCE

Northwestern Mutual®

Introductions & Overview

Michael Best

M3 INSURANCE

Northwestern Mutual®

The Covid-19 Impact on Your Cyber-Risk Profile

Current Landscape & Trends

Current Landscape

- Cyber-attacks have increased with the rapid and worldwide spread of COVID-19
  - Social engineering campaigns that prey upon fear of the virus began appearing as early as late January
  - Rise of Phishing/Business Email Compromise (BEC) scams designed to trick recipients into transferring sensitive data or funds, particularly in industries that have been disrupted by COVID-19
- Rapid increase in need for telecommuting led to targeting vulnerabilities caused by remote access of organizations' systems
  - Many organizations were forced to rapidly switch to remote work for business continuity purposes, sometimes before proper protocols and IT infrastructure was in place

Cyber-Attack Techniques Are Evolving

- Social engineering scams proliferate in the wake of natural disasters, terror attacks, and pandemics. Here are some COVID-19-related tactics that have emerged:

  - **Emails masquerading as government announcements**
  - **Hidden malware** – malicious emails directing recipients to educational and health-related websites containing malware
  - **False advice and cures** – communications purporting to come from medical providers and other phishing attacks inviting recipients to download attachments containing “secret cures”
  - **False charity** – communications mimicking the CDC and soliciting donations to fight the spread of COVID-19
  - **Operational and industry disruption** – emails targeting specific disrupted industries with lines like “brief note for the shipping industry on COVID-19” or by sending false invoices

Help Your Employees Fight Cyber-Attacks

- Threat-aware employees are the first line of defense against cyber attacks

- Train employees to do the following:

  - Be skeptical of emails from unknown senders or familiar people (your company's CEO) who do not usually communicate directly with you
  - Think before you click – don't open any links or attachments from those senders
  - Don't forward any suspicious emails to co-workers
  - Examine the sender's address- hover over links to look for slight character changes that make an address appear visually accurate
  - Note grammatical errors in the text of body of an email- they can indicate fraud

Michael Best

M3 INSURANCE

Northwestern Mutual®

The Risk of Remote Work

Risks

- **Lack of IT Visibility –** rapid shift to remote connectivity likely resulted in new internet connected assets (e.g., personal devices) that may be insecure and open to attack
- **Accidental Data Exposure –** a large amount of new, remote workers accessing data outside the office, increased use of cloud storage and other third-party services
- **Phishing and other Cyber Attacks –** new attacks and techniques that prey on fear surrounding COVID-19
- **Increased Third Party Risk –** partners and suppliers are also going through rapid digital transformations and enabling remote work, with all associate risk

Additional Challenges by Sector/Jurisdiction

No U.S. Omnibus Privacy or Security Regulation

- Privacy and Security laws regulated by sector in the U.S. (e.g., HIPAA for Healthcare, GLBA for Financial Institutions)
- 50 state breach notification/data security laws with varying requirements
- New California Consumer Protection Act of 2018 (CCPA) with “reasonable security” requirements and a private right of action for data breach became enforceable July 1, 2020.

Healthcare

- HIPAA Covered Entities and Business Associates face unique risks when it comes to the access and transmission of Protected Health Information (PHI) remotely
- HHS guidance states security rule requirements still apply to remote work (e.g., access controls-automatic log-off settings.)
- Update policies, procedures, and training to highlight the unique risks associated with remote work (e.g., preventing family members or guests from overhearing or viewing PHI, no-printing policy, etc.)
- Check that employees have access to a secure connection and update security risk assessment to reflect additional controls (e.g., transmission security and encryption).

Financial Institutions

- Gramm-Leach-Bliley Act (GLBA) and state financial privacy laws govern the processing of Nonpublic Personal Information (NPI) by a “financial institution”
- “Safeguards Rule” requires administrative, physical, and technical security to protect NPI, but does not specifically address remote working or access
- Enhanced challenges for organizations trying to enforce the required physical security of NPI while employees are working from their own homes
- BYOD Issues and storage of sensitive customer information on personal devices

Practical Considerations Applicable to All

01

Assess and document new risks associated with COVID-19 and new digital work environment

02

Review and update security controls (e.g., administrative, physical, and technical safeguards)

03

Update policies, procedures, and training to address new risks

04

Monitor and audit new and existing safeguards for continued effectiveness

Cyber-Insurance Implications

How to Plug Insurance Gaps

Does COVID-19 Warrant Changes to My Coverage?

- **The Situation:** Cyberattacks have increased during the COVID-19 crisis as malicious actors have exploited network vulnerabilities resulting from remote work environments.

- **The Result:** Many current cyber insurance policies may fail to provide complete protection for the risk of data breach, network shutdowns, and civil and regulatory actions created by these new network vulnerabilities.

- **Looking Ahead:** Expanded remote work arrangements will remain with us for the foreseeable future. Corporate policyholders should review their cyber insurance programs and make modifications as necessary to cover the associated risks and defeat potential coverage defenses

Cyber-Insurance Concerns Specific to COVID-19

- With regard to new risks created by remote working environments, some cyber policies may have coverage gaps or imprecise wording that insurers can exploit to avoid coverage.

- Sharp increase in two types of cyberattacks during the COVID-19 crisis: (i) ransomware attacks; and (ii) phishing/ fraudulent transfer schemes.
  - These events may not fall within the standard insuring agreements and often must be added by endorsement, and the specific wording of the endorsement could determine whether coverage is available.

- Many cyber policies include exclusions for negligent network security practices (e.g., exclusions for delayed patches or use of unencrypted portable devices).
  - Such exclusions can be highly problematic, particularly during COVID-19 when network IT resources are strained.

Plug Potential Gaps

- Given the rapid evolution of cyber insurance coupled with COVID-19 data security concerns, corporate policyholders should consider conducting a close review of their policies every renewal cycle to determine the adequacy of coverage.

- Expanded remote work arrangements will persist for the foreseeable future and, in some sectors, become part of the "new normal." Businesses should consider modifying their cyber policies to address the emerging risks, with a focus on the specific wording of key policy terms that can make the difference between an insured loss and an uninsured loss.

- Corporate policyholders should review their cyber insurance programs, with the help of experienced insurance counsel, to assess the adequacy of coverage for the emerging threats created by the new digital work environment and minimize their insurer's ability to avoid coverage for cyber losses.

Michael Best

M3 INSURANCE

Northwestern Mutual®

Presenters

Adrienne Ehrhardt, CIPP/US, CIPM

Michael Best
Partner, Practice Group Chair, Privacy & Cybersecurity
asehrhardt@michaelbest.com
T. 608.283.0103

Derek Laczniak, CIC, CRM

M3
Sr. Account Executive, Partner, Director of Cyber Practice
Derek.laczniak@m3ins.com
T. 608.288.2752

Michael Sias, Esq.

Northwestern Mutual
Assistant General Counsel,
michaelsias@northwesternmutual.com