THE COUNCIL

What Brokers Need to Know About Cybersecurity During COVID-19

Jody R. Westby, Esq.
CEO, Global Cyber Risk LLC

COVID-19 Changed Cyber Threat Environment

- Coronavirus was boon to cybercriminals.
- Phony coronavirus news websites
- Phishing email campaigns posing as WHO, CDC, Government Agencies
- Malware spam campaigns
- Ransomware – more sophisticated attacks
- Mobile phone tracking malware
- Nation states are also conducting or sponsoring cyberattacks
  - Russia disinformation using fake online personas to exploit aspects of pandemic
  - Chinese spearphishing targeting Vietnam, Taiwan, Philippines, & Mongolia
  - DOJ memo to all U.S. Attorneys to prioritize detection, investigation & prosecution
- Attacks are global

Bottom Line: The bad guys are not just winning; they are really winning

Operational Changes Impact Cybersecurity Program

- Cybersecurity policies & procedures, including Acceptable Use of IT
- Technology used (personal v corporate) and access controls
- Controls in cybersecurity program
- Systems monitoring
- While the cats away….Analysis of logs, outputs from tools
- System patching & updates
- Incident response
- Backup and recovery
- Heightened Risk Area: Insider Threat

Bottom Line: Gaps and vulnerabilities created by operational changes will be exploited

Governance & Compliance Considerations

- Working remotely is not just IT & cybersecurity problem: It is a governance problem
- D&Os need to review governance of information security, business continuity plans, and risk transfer strategies
- Not just a general concept: ISO standard for information security governance, ISO 27014
- Included in most cybersecurity best practices (NIST, ISACA, FFIEC, SEC, etc.)
- Numerous laws & regulations require specific governance actions
- Need to exercise oversight to ensure cybersecurity program amended
- Must ensure compliance obligations are met in new working environment
- Investor notifications: SEC chairman says “provide investors with insight regarding their assessment of, and plans for addressing, material risk to their business and operations resulting from the coronavirus to the fullest extent practicable.”
- Internal reporting and D&O Monitoring: Caremark & Marchand v. Barnhill

Bottom Line: D&O lawsuits after most major incidents; governance is defence.

Risk Transfer Considerations

- Cyber attacks now require notification of most policies
- Not just breaches; multi-pronged attacks are the new normal
- D&O coverage may be silent, but legal fees may absorb full amount allowed
- Is cyber coverage limit adequate? Quantify risks
- Business interruption: Q of whether carriers will pay or government will backstop, but if it is due to cyber attack, claim will be stronger for coverage
- Property & Casualty: Usually throw out some hardware to rebuild after an attack
- CGL: May also have a liability claim or coverage under policy terms
- E&O: If offering services, E&O policies may be triggered
- Are your clients adequately covered?

Bottom Line: Bring added value to client by helping them review risk transfer strategy for COVID-19 threat and operational environment.

Q&A

THANK YOU!

Jody R. Westby
+1.202.255.2700
westby@globalcyberrisk.com