GUIDEWIRE

COVID-19 Implications for Cyber Risk

WHITE PAPER

While humanitarian and economic concerns are rightfully taking center stage with the proliferation and uncertain containment of the COVID-19 global pandemic, the financial and insurance sectors should nonetheless be aware of the cyber risk spillover. The bad news is that we can reasonably expect corporate cyber risk exposure to mirror the generalized, global spread of COVID-19 across many sectors in regions where the virus has been transmitted. This is because most businesses in affected areas are migrating to telework and remote labor operations, thereby increasing the opportunities (the number of potentially vulnerable targets to exploit) for cyber adversaries. Similar to how the aftermath of natural disasters breeds scammers and fraudsters, the COVID-19 crisis promises to attract opportunistic cyber criminals. Despite the uncertainty of the infection rate and the absence of vaccines, the good news is that the anticipated threats and vulnerabilities are largely knowable, preventable, and defensible. There remains an open question, however, as to whether this altered cyber risk environment will be temporary or will mark an inflection point toward a new norm for corporate cyber exposures.

This document provides a concise preview of the main cyber risk factors that organizations should consider, recommendations for reducing exposure, and a sampling of the analytic capabilities that Guidewire Cyence products provide to quantify organizational and aggregated cyber risk and impact.

Cyber Risk Factors

Business susceptibility to cyber risk during the COVID-19 pandemic can result from the hasty or ill-prepared migration of the workforce to remote operations, where employees access internal corporate networks from outside the core corporate infrastructure. Causes of this susceptibility to cyber risk include the following:

- Insufficient **IT infrastructure capacity and expertise** to support large-scale transition of labor from centralized on-premises to distributed off-premises environments (for example, having inadequate or nonexistent VPN or server infrastructure to handle increased computational and bandwidth load)
- Immature or nonexistent **data governance and enterprise risk management** (policies, procedures, controls)
- Inadequate **security strategy, architecture, and controls** related to:
  - Continuous diagnostics and audit
  - Virtual and physical identity, credentials, and access and key management
  - Incident response plans
  - Identity, entitlement, and access management
  - Application programming interfaces (APIs) and permissions
  - Data storage and transmission
- Ineffective **enforcement of remote work policies** with technical and administrative controls, such as:
  - Improper VPN configurations to connect to corporate networks
  - Remote workers' use of non-employer-issued equipment, installing rogue or less robust versions of software, failure to install regular updates and patches, susceptibility to malware scans, failure to block malicious sites, BYOD risk

  - Remote employees leaving equipment unattended and accessible by family members or cohabitants
  - Exposure of protected information when in public spaces, both on-device and in-transmission (open Wi-Fi networks, coffee shops, libraries, co-working spaces)

Threat Vectors and Vulnerabilities

In light of the risk factors related to a COVID-19-induced remote workforce, the frequency of the following threats is likely to increase. The severity of their impact is a function of companies' success in implementing known countermeasures and establishing resiliency measures.

- **Social engineering and spear-phishing/spam-phishing scams** are known attack vectors for compromising business email accounts. Cybercrime statistics nearly unanimously show continued growth in both phishing frequency and detection challenges. Email compromise is a common way for cyber criminals to acquire sensitive information or perpetrate fraud.
  - Wire fraud may be a growing peril during the COVID-19 crisis. The confluence of financial pressures to move funds during the crisis along with shifting suppliers and vendors may force the relaxing of processing controls and amplify the opportunities for criminal exploitation.
  - Spam and phishing scams prey on fears and uncertainties related to COVID-19, luring individuals to click infected attachments or links in email messages that pretend to be updates on the coronavirus and often spoof authoritative organizations (such as the CDC and WHO). AZORult, for example, is malware that is contained in bogus Microsoft Word documents attached to email messages purporting to be about the coronavirus. It targets industries susceptible to shipping disruption (manufacturing, finance, transportation, pharmaceuticals, cosmetics) and can be used to install ransomware.
  - Phishing kits impersonate well-known, trusted service providers (e.g., Microsoft, Amazon, Google, Dropbox), vendors, suppliers, or partners to deceive employees. Victimization to account fraud or unwittingly revealing confidential business information, intellectual property, PII, or other resources will be heightened for employees who have less exposure in the traditional enterprise network.
- **Denial-of-service (DoS) attacks:** With expanded deployment of VPN and other communication applications (instant messaging, audio, web- and video-conferencing), dependencies on telecommunication infrastructures will be higher, and the frequency of malicious attacks intended to disrupt these services is likely to rise. Distributed DoS-driven complete outages or service disruptions for these infrastructures will increase aggregation exposure.
- **Ransomware attacks:** Ransomware success rates against organizations are not likely to increase if remote workers are properly segmented from production servers and databases where mission-critical data assets are stored.

Recommendations

Many resources are available to help businesses bolster the confidentiality, availability, and integrity of their business data and systems in a remote workforce regime.* As with the basic personal hygiene recommendations for addressing COVID-19, businesses should consider the following fundamental cyber hygiene practices in assessing and reducing cyber risk exposure for their remote workforce:

- Require multifactor authentication for company apps and networks.
- Implement a reputable and robust VPN infrastructure (accessed via multifactor authentication).
- Properly secure remote monitoring camera systems.
- Mandate employee use of private Wi-Fi networks. When work must be done in public places, require the use of the employee's mobile hotspot (smartphone or dedicated device) to access a secure connection.

* For details about telework, see https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf and https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf.

- Ensure robust password requirements (complexity, length, diversity), including trusted password managers and change management.
- Enforce the use of company-owned communication services (email, messaging, and conferencing via audio, web, and video) and prohibit the use of free online services.
- Implement and monitor intrusion detection system filters.
- Segment the company network by providing user access to data and systems directly related to users' tasks or departments.
- Assess and monitor identity, credential, access, and key management for third-party partners, vendors, and supply chain entities.
- Monitor the vulnerabilities of third-party service providers used by remote workers.
- Review and revise all relevant security policies and practices. Train employees on these policies and practices, and remind them especially about phishing and social engineering threats.

Implications and Analytics

Although the impact of COVID-19 on supply chains and global economies is still not fully understood, we should anticipate that the second-order effects on business cyber risk will follow the known attack patterns and susceptibilities outlined above. What is novel, however, are the scale and speed at which these threats and vulnerabilities will impact companies for which a large scale, distributed remote workforce is unprecedented. Although the IT sector is presumably prepared to handle increased risk factors, even tech-savvy businesses have exposure to cyber threats via their supply chains (labor, service, and product providers), which will be targets of compromise due to their unreadiness. Heightened litigation risk and business interruption stemming from cyber infrastructure disruption should be a top priority.

None of these COVID-19-derived cyber risks are novel for established cyber coverages at the firm level. None of these anticipated exposures pose unprecedented implications for the transfer of risk via cyber insurance from the standpoint of correlation with established coverages. Affected coverages might include:

- First-party data breach (breach coach, remediation, notification/ID monitoring, call center, public relations)
- Third-party liability (class action, regulatory fines, liability claims)
- Network interruption (income, remediation, forensics, business interruption)
- Cyber extortion (ransomware, forensics)
- Data asset practices (forensics; the cost to restore, recollect, or re-create stolen or destroyed data; remediation)

Other non-affirmative cyber coverages and lines of business that can be affected include:

- Property: BI/CBI related to a network outage, or property damage stemming from cyber attacks (ICS)
- Financial lines: D&O, professional liability, and commercial crime from cyber attacks
- General liability

However, one of the notable potential secondary effects of COVID-19 for insurance and financial service providers is cyber risk accumulation. Companies across industries are more reliant on information and telecommunications infrastructures. As we gain efficiencies from increased reliance on internet data and control planes (e.g., cloud IaaS-PaaS-SaaS, internet exchange points, broadband), we increase the technical dependencies and aggregate risk potential—along with the resulting frequency and magnitude of cascading and systemic harm. In addition, many insurance policies cover both malicious and nonmalicious incidents in service chain outages. These types of incidents are especially pernicious with increasing globalization and tight coupling of supply chains. They are particularly risky as companies struggle to identify their critical suppliers, the effects of disrupting that chain, and contingent alternative suppliers. This information asymmetry presents challenges for managing the potential for accumulation.

As with COVID-19 health strategies, the key to reducing cyber exposure lies in understanding the nature, scope, and projected impact of cyber risk. For insurers and other risk managers, this is essential in defining segments, tailoring prices, determining bad risks, understanding risk exposure across a portfolio, and determining the degree of claims automation.

The analytics and data science capabilities of Guidewire Cyence products can help policy administrators, underwriters, and risk and claims managers diagnose, quantify, forecast, and remedy these cyber risks by providing capabilities such as the following:

- Analyzing signals of the health of a business's remote services (VPN, RDP, HTTPS, SSH) correlated with a displaced workforce regime and segmented by geography (e.g., exposure of high-revenue regions)
- Segmenting signals of a business's remote services by sector, by proportion of customer portfolio, or by import/export dependencies on heavily impacted or incapacitated regions (Examples include sectors in the U.S. with major exports from China in electronics, furniture, machinery, apparel, printing, plastics, paper, metals, textiles, and nonmetallic minerals.)
- Understanding risk aggregation paths based on network dependencies such as ISP, cloud service providers, or DNS should one of these services suffer outages or disruptions
- Simulating and estimating ground-up financial losses for the following types of cyber perils that affect one or more institutions in a portfolio:
  - Mass vulnerability (observable) scenario
  - Mass ransomware scenario
  - Data breach

Although Guidewire has transitioned from prevention to mitigation in Cyence's analog response to COVID-19, we still have the opportunity to prevent and manage its secondary effects on cyber risk exposure. And—as we can corroborate with the biological reality of the coronavirus—testing for indicators of risk is the key to understanding and responding to the frequency, distribution, and severity of forthcoming exposures. In the cyber realm, the Cyence data and knowledge platform, along with our analytics and domain expertise, are well-positioned to bridge the disconnect in the interpretation of risk for the financial and insurance industries.

About Guidewire Software

Guidewire delivers the industry platform that Property and Casualty (P&C) insurers rely upon to adapt and succeed in a time of accelerating change. We provide the software, services, and partner ecosystem to enable our customers to run, differentiate, and grow their business. As of the end of our fiscal year 2019, we were privileged to serve more than 380 companies in 34 countries. For more information, please visit www.guidewire.com and follow us on twitter: @Guidewire_PandC.