COSMOS
Navigate the Compliance Universe

Report on Supply Chain Compliance Volume 3, Number 17. September 03, 2020
Cybersecurity firm releases report on increased hacking during pandemic

By Sascha Matuszak

Resilience360 has released a report, COVID-19 Pandemic Creates Opportunity for Innovative Cyber Threat Campaigns,[1] that discusses the skyrocketing hacking attempts during the pandemic and ways to mitigate the risk of data breaches. The report found that the two most common methods of hacking during the pandemic are phishing and ransomware.

Phishing involves the impersonation of legitimate governmental, business, or personal entities in order to "fish" for a victim that will enable access to a network. This is often facilitated by tricking the victim into clicking a dubious link with embedded malicious software, or "malware." A successful phishing attempt can result in the threat of publishing sensitive data unless a ransom is paid, hence the term "ransomware."

"So long as the COVID-19 pandemic continues to drive high demand for remote work solutions, it is incumbent upon supply chain managers to understand the current commercial cybersecurity landscape, the ways cyber incidents manifest, and the novel intensity of the threat to supply chains," the report stated. "Supply chain managers can implement programs with suppliers that mitigate risk such as verifying data backups and implementing attack recovery plans to potentially outperform the competition if a cybersecurity crisis strikes."

1 Resilience360, *COVID-19 Pandemic Creates Opportunity for Innovative Cyber Threat Campaigns*, August 6, 2020, https://bit.ly/3hGbDsM.