Thursday, 29 October 2020

TOP LINE

Cyberattacks are a constant presence in the modern digital economy. Few companies escape the barrage of intrusions and hacks that seek to take advantage of localized or lower threshold vulnerabilities. Many attacks go unnoticed and unreported; the invisible nature of these intrusions demonstrate the ease with which geopolitical or criminal actors can take advantage of digital vulnerabilities.

Digitization of data has provided technology companies with disproportionate power compared to that of democratic governments and other private enterprises. This imbalance has put technology companies in a unique position of best understanding and managing risk in the digital realm. However, policing cyberspace is not a well-defined function. Cyberspace is called the lawless realm for a reason; it is protected by an ad hoc web of private security software and user guidelines, without any clear penalties for violating normative behavior.

In a recognition of this lack of enforcement, an effort to bolster internet security in the U.S. through the development of new encryption standards is underway to counter both traditional and quantum computing cyberattacks. Current encryption algorithms outpace the power of existing quantum computers; however, some popular algorithms are particularly vulnerable to their exponential speedup capabilities. As such, cryptographers have been spending recent years developing new encryption algorithms to bolster internet security with a wary eye towards the potential power of quantum computing.

Business leaders should evaluate their cybersecurity procedures in terms of both cyber defense and response. The Federal Bureau of Investigation is also warning hospitals of an imminent wave of ransomware attacks. This comes just as the second wave of COVID is hitting Europe and cases are surging here in the US. Ensuring software is updated, data is protected, and employees are trained on cybersecurity practices is only a first step. Business leaders should consider how they plan to

respond to the near inevitability of a cybersecurity incident or attack that compromises their systems and data.

Question to Consider:
How can business leaders prepare for an increase in cybersecurity incidents including ransomware attacks that threaten information security and the operational viability of the organization?

COVID-19: THE HIGHLIGHTS

As fall continues, France announced plans to reimpose a nationwide lockdown of nonessential businesses until at least December 1. Meanwhile, Germany announced that bars and restaurants would be closed effective Monday, even as schools, stores, and supermarkets remained open. In the United States, hospitals are seeing a 46 percent spike in hospitalizations of Covid patients within the past month. This increase in case numbers is stretching the resources of regional health systems that were spared the worst of the virus in the spring.

BEYOND THE NOISE: THE NEW NORMAL

The increasing sophistication of cyberattacks was demonstrated by the anticipation of U.S. cybersecurity officials that Russian cyber actors would interfere in the 2020 U.S. elections, and their inability to stop them from breaching state and local computer systems. In September 2020, officials observed a Russian FSB affiliated group in government computers. The group is known to have breached airport WiFi systems, the U.S. power grid, water treatment facilities, and nuclear power plants, but is not known for targeting states and countries. With that said, it has demonstrated the capability to conduct sabotage and there is little that can be done to prevent such disruption.

TRUSTED RESOURCES: for numbers & guidance

Johns Hopkins University – Coronavirus Resource Center
World Health Organization – COVID-19 Pandemic
Center for Disease Control – Coronavirus (COVID-19)

Please contact Secure Source International at info@securesource.com to schedule a leadership roundtable with our intelligence and security experts to dive into these topics and discuss security and safety related best-practices..