CLCT

WILLIAM & MARY LAW SCHOOL

Cybersecurity and Information Security Newsletter

Issue 21 | August 15, 2022

Table of Contents

Daniel Shin, research scientist with the Commonwealth Cyber Initiative (CCI) Coastal Virginia region, wants to hear from you! Submit any cybersecurity and information security news items or request related topics, via e-mail to dshin01@wm.edu.

This newsletter supports the mission of CCI. To learn more about CCI, including upcoming events, funded research, and news, please visit cyberinitiative.org.

Internet critical infrastructure calls for attention; are undersea cables possible points of failure?

Our ever-increasing reliance on data means that we are also increasingly dependent upon our data infrastructure. On July 8, 2022, Rogers Communications (Rogers), a Canadian telecommunication company, suffered a near-total outage of Internet and communication services that led to a nationwide Internet disruption in Canada. *Rogers outage knocks out Canadian internet service*, available here. The outage not only prevented Internet access to most parts of the nation but it also disrupted financial payment transactions and some emergency call systems. *Rogers outage points to need for greater oversight of critical industry*, available here. On July 9, 2022, the company announced that Internet and communication services had been restored, and Rogers' CEO Tony Staffieri disclosed that a maintenance update involving its network may have caused the nationwide communication outage. *A Message from Rogers President and CEO*, available here. Rogers did not share any further details as of the time of this newsletter's publication.

In response, Canada's Minister of Innovation, Science, and Industry François-Philippe Champagne convened the CEOs of Canada's major telecommunication companies, including Staffieri, to discuss ways how to prevent such nationwide outages in the future. *Ottawa calls on telecom companies to shore up networks after Rogers outage*, available here. Minister Champagne asked the telecommunication leaders to draft a plan that would allow telecommunication companies to provide mutual assistance during an outage and ensure that 911 call services would remain undisrupted.

Analysis

Rogers' Internet outage highlights the need to safeguard Internet critical infrastructure. Although Canada's nationwide disruption was likely caused by a malfunction within Rogers' network routing infrastructure, there have been other nationwide Internet outages caused by other infrastructure components, namely undersea cable communication networks (also known as submarine cables).

For example, on January 13, 2022, Hunga Tonga-Hunga Ha'apai, a submarine volcano located in the Kingdom of Tonga, erupted, causing ash, steam, and gas to spread across the region while also causing atmospheric shock waves and tsunami waves that traveled globally. *The Hunga Tonga-Hunga Ha'apai Eruption, a Multi-Hazard Event*, available here. The volcano eruption caused serious damage to the islands, including many injuries and fatalities. *First official update following the Volcanic Eruption*, available here. As a result of the natural disaster, the Government of the Kingdom of Tonga noted that the nation's access to international communication was severely hampered due to damages to its submarine communication cable that carried most of the nation's Internet and communication data. *Id.* Although satellite-based Internet was available, Internet and communication connectivity was severely hampered while the submarine cable was being repaired. After over a month from the eruption, the Tonga government announced that the cable was successfully repaired and the Internet connectivity and communication systems of the nation were restored successfully. *Tonga reconnects with outside world after data cable cut off by volcanic eruption, tsunami repaired*, available here.

Natural disasters are a clear risk but so too are criminal cyber attacks. On September 28, 2017, the U.S. Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) issued a joint publication that identified threats to the nation's undersea cable communications. *Threats to Undersea Cable Communications [DHS & DNI]*, available here. The report highlighted natural disasters and inadvertent accidents as major causes of undersea cable damage. *Id.* at 19-20. However, it also emphasized deliberate attacks on the infrastructure as a potential risk of causing disruptions. Specifically, cyber attacks involving "sniffing" communication signals on the fiber optic lines may allow threat actors to tap all insecure data transmissions routed through the compromised cable. *Id.* at 22. Threat actors can also cut undersea cable lines, which can lead to significant communication outages that can cascade to nationwide network disruption. *Id.* at 23.

In April 2022, Homeland Security Investigations of DHS announced that federal agents disrupted a cyberattack targeting an unidentified telecommunication company's server that was associated with undersea cables connecting Hawaii to other regions. *DHS investigators say they foiled cyberattack on undersea internet cable in Hawaii*, available here. Although details of the cyberattack were not disclosed to the public, if threat actors successfully disrupted the island's undersea cable infrastructure, the communication outages may have been disastrous.

The DHS and ODNI's undersea report recommends greater public awareness of how undersea cables support their infrastructure and the development of contingency plans in case of outages caused by undersea cable disruptions. *Threats to Undersea Cable Communications [DHS & DNI]*, *supra* at 24. For example, incorporating how key Internet infrastructure, such as undersea cables, play a role in maintaining network health continuity to cybersecurity training programs could facilitate the development of a resilient cybersecurity workforce ready to respond to widespread outages, including the one faced in Canada.

Also, following Internet infrastructure development in the region is critical to appreciate all cyber risks that can disrupt the operations of businesses and government entities. For example, on May 9, 2022, Globalinx, a data center and undersea cable company at Virginia Beach, announced the addition of four new subsea cable projects, connecting Virginia to Europe, Asia, the Caribbean, and the Americas. *Globalinx to add new subsea cable landing site in Va. Beach*, available here. Businesses and government entities near Virginia Beach should consider how the additional undersea connections affect their operations, especially in a widespread outage scenario.

As universities such as William & Mary (W&M) develop and emphasize data science programs and instruction and even offer, as W&M has, interdisciplinary cybersecurity courses, it is highly likely that they would be attracted to cutting-edge research into the vulnerabilities of our data infrastructure, including submarine transmission lines. Globalinx is only about 60 miles from W&M, for example, suggesting the possibility of a mutually beneficial public-private research collaboration.

The National Credit Union Board proposes cyber incident reporting rules

On July 27, 2022, the National Credit Union Board (Board) submitted to the Federal Register its proposed cyber incident reporting rules for federally insured credit unions (FICU). The proposed rules would require FICUs to report "substantial cyber incidents" to the National Credit Union Administration (NCUA). *Cyber Incident Notification Requirements for Federally Insured Credit Unions,* 87 FR 45029, available here. Citing the impact of cyber incidents within the financial services industry, the Board declared the importance of the NCUA being notified promptly of cyber incidents (1) impacting FICU operations; (2) leading to unauthorized access to sensitive data; or (3) disrupting FICU members' ability to access their accounts. (An FICU member refers to a customer of a FICU, similar to a bank customer of a bank.)

Under the proposed rule, FICU discovering a reportable cyber incident must notify the NCUA within 72 hours. A reportable cyber incident is any substantial cyber incident that leads to:

- a substantial loss of confidentiality, integrity, or availability of a member information system as a result of the exposure of sensitive data, disruption of vital member services, or that has a serious impact on the safety and resiliency of operational systems and processes;
- a disruption of business operations, vital member services, or a member information system; or
- a compromise of the FICU's sensitive data or business operations as a result of a cyber incident experienced by a third-party service provider, when either the third-party provider informed the FICU of the incident or the FICU has a reasonable belief that the incident has occurred.

The proposed rule would require a FICU to determine whether a cyber incident is substantial. According to the proposed regulation, what makes a cyber incident "substantial" depends on various factors, including the size of the FICU, the incident type and impact of loss, and incident duration. If a FICU is unsure whether a cyber incident is substantial, the proposed regulation encourages it to proactively report the cyber incidents to the NCUA.

As of this newsletter's publication, the proposed rule is in the public comment phase, which is scheduled to close on September 26, 2022. Pending the Board's revision, the proposed rule is expected to be implemented thereafter.

Analysis

The federal government is increasingly considering implementing cyber incident reporting requirements in various sectors. For example, on November 23, 2021, the Office of the Comptroller of the Currency, the Federal Reserve System, and the Federal Deposit Insurance Corporation jointly issued a cyber incident reporting regulation for banking organizations and their banking service providers. *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, 86 FR 66424, available here. Also, on March 23, 2022, the Securities and Exchange Commission proposed a more comprehensive regulation on cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies. *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, 87 FR 16590, available here.

One of the most impactful steps toward a resilient cyber incident reporting requirement took place on March 15, 2022, when President Biden signed the *Consolidated Appropriations Act, 2022*. *Bill Signed: H.R. 2471*, available here. The Act includes the *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, which paves the way for mandatory cyber incident reporting regulations for identified critical infrastructure operators from 16 critical infrastructure sectors. *Issue 17: CLCT Cybersecurity and Information Security Newsletter – Cyber Incident Reporting for Critical Infrastructure Act of 2022 signed into law*, available here.

It is notable that the Board issued the proposed cyber incident reporting rule for FICUs pursuant to its plenary grant of authority under the Federal Credit Union Act, signaling the importance of implementing cyber incident reporting requirements as a necessary regulatory component for covered entities. Following the Board's action, other federal regulatory agencies may propose their own cyber incident reporting rules for their sectors to bolster the visibility of the cybersecurity threat landscape.