Encryption, Exfiltration, Extortion – Executive Order:
Ransomware's Rise, a Call to Action

By Armstrong Teasdale Partners Romaine Marshall, Scott Galt and Jeffrey Schultz

In the past several weeks, the digital scourge known as ransomware has gained considerable worldwide attention. In the U.S., Colonial Pipeline paid cyber criminals $4.4 million to regain access to its information systems[i]; in Ireland, a group of hospitals was forced to go back to using paper files after its IT systems were encrypted by cyber criminals[ii]; and in New Zealand, a provincial hospital is considering flying cancer patients to Australia because cyber criminals have demanded a ransom in exchange for access to its IT systems.[iii]

The attention ransomware has garnered has been so white-hot, that even cyber criminals appeared caught off guard. As reported by Krebs on Security, after a $5 million ransom payment was obtained from Colonial Pipeline, the administrator of a Russian cybercrime forum stated "[t]here's too much publicity" with ransomware and that it has "become dangerous and toxic."[iv]

Setting aside the questionable consciences of cyber criminals, these cybersecurity incidents demonstrate that despite their attention, and the legal obligations that have followed as a result, readiness for foes so formidable they have coined new terms and ecosystems – e.g., disruptionware, ransomware-as-a-service (RaaS), and ransomware recovery specialists – remains elusive.

But it is the Colonial Pipeline incident more than other recent high-profile cybersecurity incidents – e.g., SolarWinds, Microsoft and Accellion – that is likely to be the main catalyst for expanded legal obligations relating to cybersecurity, along with notable events that occurred before, during and after the incident.

Ransomware's 'Evolution'

In early 2020, several reports chronicled the devastating impact that ransomware was having on organizations.[v] Back then, according to the New York Times:

> In 2019, 205,280 organizations submitted files that had been hacked in a ransomware attack — a 41 percent increase from the year before, according to information provided to The New York Times by Emsisoft, a security firm that helps companies hit by ransomware.[vi]

But shortly thereafter, new and more destructive variants of ransomware began emerging. For example, Maze ransomware came to the fore not only to encrypt networks and require payment for decryption, but also to infiltrate networks and exfiltrate data beforehand. After exfiltration occurred, the cyber criminals would deploy the ransomware and threaten to publicly post the exfiltrated data (which is usually proprietary or personal) if the ransom payment is not promptly paid through an untraceable bitcoin account. This type of ransomware, now adopted by gangs who have taken on such monikers as DarkSide, Conti and Clop, is what crippled Colonial Pipeline, and Irish and New Zealand hospitals.

To make matters worse, while the cyber criminals will only steal a segment of the data they encrypt – a few GB, random emails, etc. – the victim will likely have no idea which portion of the encrypted files were stolen and will have to consider all data that was accessed as "breached," unless they can assess that there is a reasonably low risk that certain data was not extracted.[vii]

An Enforcer Against Ransomware Emerges

On March 31, 2021, the Department of Homeland Security's (DHS) Secretary, Alejandro Mayorkas, outlined a roadmap for DHS' cybersecurity strategy.[viii] Referring to a series of 60-day "sprints" to begin implementing the strategy, he stated that DHS' first focus is on raising ransomware awareness and disrupting those who launch the attacks.

DHS has designated the Cybersecurity & Infrastructure Security Agency (CISA) as its cybersecurity quarterback. On its website, CISA has a substantial library of ransomware resources including ransomware prevention best practices and a response checklist.[ix] These resources have evolved just as the types of ransomware variants have evolved and provide important information that should be considered when developing and refining cybersecurity incident response plans.

A Task Force Proposes a Ransomware Response Framework

On April 29, 2021, a team of more than 60 experts from software companies, cybersecurity vendors, government agencies, non-profits and academic institutions released an 81-page report titled "Combating Ransomware."[x]

The goal of the task force, similar to DHS and CISA's, is "to proactively and relentlessly disrupt the ransomware business model through a series of coordinated actions." In its report, the task force published 48 actions divided into four categories, the last two relating to how organizations (1) prepare for and (2) respond to ransomware attacks.

The task force noted that in 2020 nearly 2,400 organizations were victims of ransomware, and that they:

- averaged 21 days of downtime;
- averaged 287 days to fully recover;
- altogether paid $350 million in ransoms; and
- averaged $312,493 per payment.

The task force then recommended the following:

- Being Prepared
    - A framework should be developed to provide organizations with a ransomware-specific risk assessment tool.

    - Awareness materials should be developed to assist organizational leaders about the needs and risks of ransomware.
    - Regulatory guidance on how organizations can reduce the likelihood of fines or other penalties should be provided with preparation recommendations.
    - Incentivizing alignment with an established risk management framework should be encouraged, including tax breaks for meeting certain baseline standards.

- Knowing How to Respond

    - Rapid information sharing should occur between organizations that are affected by a ransomware incident.
    - A standardized incident reporting format and network should be created.
    - Organizations should be required to conduct a cost-benefit assessment prior to making a ransom payment.

Referring to Colonial Pipeline, the White House Demands Better Cybersecurity

On May 12, 2021, President Biden issued the "Executive Order on Improving the Nation's Cybersecurity."[xi] The 18-page order includes numerous ambitious requirements with deadlines ranging from 14-360 days and divided into sections relating to, among other things, the:

- removal of contractual barriers to information sharing;
- mandated use of multifactor authentication and encryption and security best practices;
- building security into software from the ground up;
- requiring baseline incident response capabilities;
- enabling better endpoint detection and response systems to detect malicious activity; and
- creating event logging so that incidents can be better detected and mitigated.

While it pertains specifically to federal networks, in taking a bold step to chart a new course, the order encourages "private sector companies to follow the Federal government's lead and take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents."[xii]

Given the numerous deadlines established by the order, the coming days and weeks could see an unprecedented amount of activity in the development of cybersecurity standards.

Alignment with Basic Cybersecurity Standards

The Colonial Pipeline incident and the events and announcements discussed above shed light on how organizations can prepare for, and respond to, ransomware and other cybersecurity incidents that involve similar attack vectors and unauthorized access by cyber criminals. While the Executive Order is still being analyzed and further guidance will be provided, one thing is certain: lessons learned must be implemented.

As baseline requirements, organizations should at a minimum do the following to keep pace with the expanding cybersecurity legal obligations:

- Refine your Cybersecurity Incident Response Plans (IRP)
    - An IRP should include detailed response processes that articulate communication, documentation and evaluation activities.
        - For example, compare the NIST Computer Security Incident Handling Guide which has 20 recommendations for an incident response plan.[xiii]
    - According to the New York Department of Financial Services, an IRP should:
        - include a plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of information systems or the continuing functionality of any aspect of business or operations;
        - codify the internal processes for responding to a cybersecurity event;
        - address the goals of the IRP by defining clear roles, responsibilities and levels of decision-making authority;
        - provide a plan for external and internal communications and information sharing;
        - identify requirements for the mediation of any identified weaknesses in information systems and associated controls;
        - address documentation and reporting regarding cybersecurity events and related incident response activities; and
        - address the evaluation and revision as necessary of the incident response plan following a cybersecurity event.[xiv]
- Reassess your Cybersecurity Risk Assessment (RA)
    - Certain statutes and regulations mandate RAs and provide guidance and tools to assist organization.[xv]
        - For example, conduct an assessment to analyze your alignment with industry standards and ensure vulnerabilities targeted by ransomware have been addressed.
    - According to the New York Department of Financial Services, an RA should:
        - articulate any reasonably necessary changes, and then the plans to address any issues raised in the RA;
        - address any and all plans for revisions of controls to respond to technological developments and evolving threats, which should all consider the particular risks of the business's operations related to cybersecurity, personal or sensitive information collected or stored, the

information systems utilized and the availability and effectiveness of controls to protect personal and sensitive information and information systems;

- describe any and all plans for updating or creating written policies and procedures to include:
    - criteria for evaluation and categorization of identified cybersecurity risks or threats facing an organization;
    - criteria for the assessment of the confidentiality, integrity, security and availability of an organization's information systems and personal and sensitive information, including the adequacy of existing controls in the context of identified risks; and
    - requirements describing how identified risks will be mitigated or accepted based on the RA and how the cybersecurity program will address the risk.[1]

- Refocus your Written Information Security Program (WISP)

    - Check to see if your WISP includes updated administrative, technical and physical safeguards, as some states now require.[xvi]
    - For example, evaluate and adjust your program in light of any changes to your operations or business arrangements.

Just as organizations continue to embrace digital transformation – the process of leveraging technology, processes and people to innovate – so too will cyber criminals seek to exploit vulnerabilities for big paydays. Today it is ransomware, but tomorrow the attack vector could be new variants or be entirely different (e.g., deep fakes, disinformation, vulnerabilities within IoT devices). Thus, organizations must continue to evolve just as their cybersecurity legal obligations continue to evolve.

---

[i] https://www.bbc.com/news/business-57178503
[ii] https://www.nytimes.com/2021/05/20/technology/ransomware-attack-ireland-hospitals.html
[iii] https://www.nzherald.co.nz/nz/waikato-dhb-cyber-attack-cancer-patients-could-be-sent-to-australia/3J3VCVVZV5PQIP4KDC5KSKWOGA/
[iv] https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/
[v] *See, e.g.*, Sean Lyngaas, *FBI warns U.S. companies about Maze ransomware, appeals for victim data* (Jan. 2, 2020) https://www.cyberscoop.com/fbi-maze-ransomware/
[vi] https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html
[vii] https://www.jdsupra.com/legalnews/soon-all-ransomware-attacks-may-be-data-95481/
[viii] https://www.dhs.gov/news/2021/03/31/secretary-mayorkas-outlines-his-vision-cybersecurity-resilience
[ix] *See, e.g.*, https://www.cisa.gov/publication/ransomware-guide
[x] https://securityandtechnology.org/ransomwaretaskforce/report/
[xi] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[xii] https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/
[xiii] https://www.nist.gov/publications/computer-security-incident-handling-guide
[xiv] https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202104141

---

[1] *See* n.14.

[xv] *See, e.g.*, https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool (a security risk assessment tool provided by the Department of Health and Human Services).

[xvi] https://www.armstrongteasdale.com/romaine-marshall/thought-leadership/outlier-or-pioneer-utah-reconsiders-a-cybersecurity-safe-harbor/