EXPLOSION OF RANSOMWARE ATTACKS ADDRESSED BY DFS

Shari Claire Lewis Rivkin Radler LLP

On June 30, 2021, New York State's Department of Financial Services (DFS) issued its Ransomware Guidance to alert the financial industry to the upsurge in ransomware attacks and to provide education and standards for addressing cybersecurity issues. The Guidance provides valuable information for all businesses and organizations, not just for the financial industry that DFS regulates. The Guidance may be found here.

THE RANSOMWARE CRISIS

An explosion of the number and severity of ransomware incidences has been reported on by news outlets almost daily. Nevertheless, because news reports focus on massive ransomware attacks on Fortune 500 companies, other companies may underestimate the risk that ransomware presents to their businesses. The Guidance's analysis starkly demonstrates the pervasiveness of the problem. It notes that, according to U.S. Homeland Security Secretary Alejandro Mayorkas, ransomware attacks increased by 300% in 2020.

The Guidance also describes the crippling impact that a ransomware attack may have, as it sidelines organizations and prevents them from performing key functions, such as providing consumer services or patient care or enabling employees to work. Magnifying the problem, since mid-2020, ransomware criminals have more frequently engaged in "double extortion," whereby they steal the victim's data before deploying ransomware, which they then use to extort the victim a second time by threatening to publish the data after the ransomware event has concluded.

In addition to the growth in the frequency of attacks, DFS reported that the amounts demanded as ransom have increased 171% from 2019 through 2020 and are expected to continue to grow. Nevertheless, DFS, like the FBI, recommends against paying ransom for a variety of reasons:

- The payment funds ever more sophisticated attacks;
- The payment may violate a variety of laws, so that the victim may itself risk fines and sanctions, such as under the Office of Foreign Assets Control;
- Victims who have paid have not been able to gain access to all their data or have had the data leaked anyway; and
- 80% of victim organizations that paid experienced subsequent attacks.

WHAT IS AN ORGANIZATION TO DO?

Depending on the event and type of business, organizations may have obligations to promptly report any ransomware attacks on its systems to criminal, government or regulatory agencies, such as DFS. Additionally, the Guidance identifies nine actions that organizations should take to either prevent or respond to a ransomware incident.

DFS recommends that businesses employ a "multilayered approach" using a combination of security tools to reduce the risk of a ransomware attack and minimize its damage. DFS "expects" regulated companies to implement a "defense in depth" approach, when possible, as set forth in DFS' Cybersecurity Regulation (23 NYCRR § 500 et seq). The multilayered approach includes:

1. DFS' Recommendations for "Protecting Ransomware"

A. Email Filtering and Anti-Phishing Training – According to DFS, employee training is critical. Thus, employers should have robust cybersecurity awareness programs for employees, such as recurrent and remedial phishing training, periodic phishing exercises and testing. 23 NYCRR § 500.14(b). At the same time, emails should be filtered to block spam and malicious attachments from reaching users, as set forth in 23 NYCRR § 500.3(h).

B. Vulnerability/Patch Management – Companies should establish and document programs to identify, track and remediate vulnerabilities (23 NYCRR § 500.03(g)) that should include periodic penetration testing. 23 NYCRR § 500.05(b). When possible, regulated companies should enable automatic updates.

C. Multi-Factor Authentication (MFA) – DFS requires MFA for remote access to an organization's network and third-party applications or other external programs that may expose the organization's systems. 23 NYCRR § 500.12. DFS also recommends MFA be enabled for logins to all privileged accounts (whether remote or internal). 23 NYCRR § 500.3(d) & (g); 500.12.

D. Disable RDP – DFS recommends that regulated entities disable Remote Desktop Protocol (RDP) access from the internet when possible. 23 NYCRR § 500.03(g). If RDP access is deemed necessary, as it has become for businesses that are operating remotely, access should nevertheless be restricted to only approved (whitelisted) originating sources and should require MFA and strong passwords.

E. Password Management – Regulated entities should ensure that strong, unique passwords are used. 23 NYCRR § 500.03(d). DFS suggests that organizations ensure that privileged user accounts require passwords that are at least 16 characters and ban commonly used passwords entirely. Additionally, in larger organizations with dozens or hundreds of privileged accounts, organizations are encouraged to consider a "password vaulting PAM" (privileged access management solution) to require employees to request and check out passwords. In all cases, password caching should be turned off.

F. Privileged Access Management – Privileged access refers to increased access or abilities given to certain users (or computer programs) beyond that given to standard users, to enable them to perform their job functions. DFS encourages organizations to implement the principle of "least privileged access" and give users only the minimum access necessary to perform their job. 23 NYCRR § 500.03(d). 23 NYCRR § 500.07. Moreover, because privileged accounts are a frequent source of compromise, privileged accounts should be highly protected, universally require MFA and strong passwords, and should be periodically audited and inventoried.

G. Monitoring and Response – It is essential that companies have a way to monitor their systems for intruders and respond to alerts of suspicious activity. 23 NYCRR § 500.03(h). DFS recommends that all companies employ an "Endpoint Detection and Response (EDR) solution" to detect anomalous activity. EDR, in certain versions, may be able to stop ransomware from executing and from encrypting the entire system.

2. DFS' Recommendations for "Preparing for An Incident"

A. Tested and Segregated Backup – It is recommended that companies maintain comprehensive, segregated backups that will allow recovery in the event of a ransomware attack. 23 NYCRR §§ 500.03(e), (f) and (n). Having at least one set of offline backups that is segregated from the company's network is the best way to avoid ransomware criminals from being able to delete or encrypt the backups. Backups should be tested – before an event occurs – to make sure they will function in the event of an attack.

B. Incident Response Plan – Regulated companies are required to have an incident response plan that explicitly addresses ransomware attacks. 23 NYCRR § 500.16. This is something that all companies should do. The plan should be regularly revisited and tested to ensure that it will, in fact, work if needed.

The Guidance provides concrete steps that all organizations should consider in response to the explosive growth of ransomware attacks. Commitment by multiple stakeholders in the organization (including leadership, information technology and employees) and consultation with appropriate cybersecurity and legal professionals may help an organization reduce the risk of a ransomware event and its impact if one occurs, as well as help an organization navigate the various regulations that may apply.

Shari Claire Lewis is a partner in Rivkin Radler LLP's Complex Torts & Product Liability; Privacy, Data & Cyber Law; and Professional Liability practice groups. She has focused her practice on the intersection of law and technology, often advising and representing clients on 21st Century technology challenges they face.