New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 264—NO. 92
TUESDAY, NOVEMBER 10, 2020

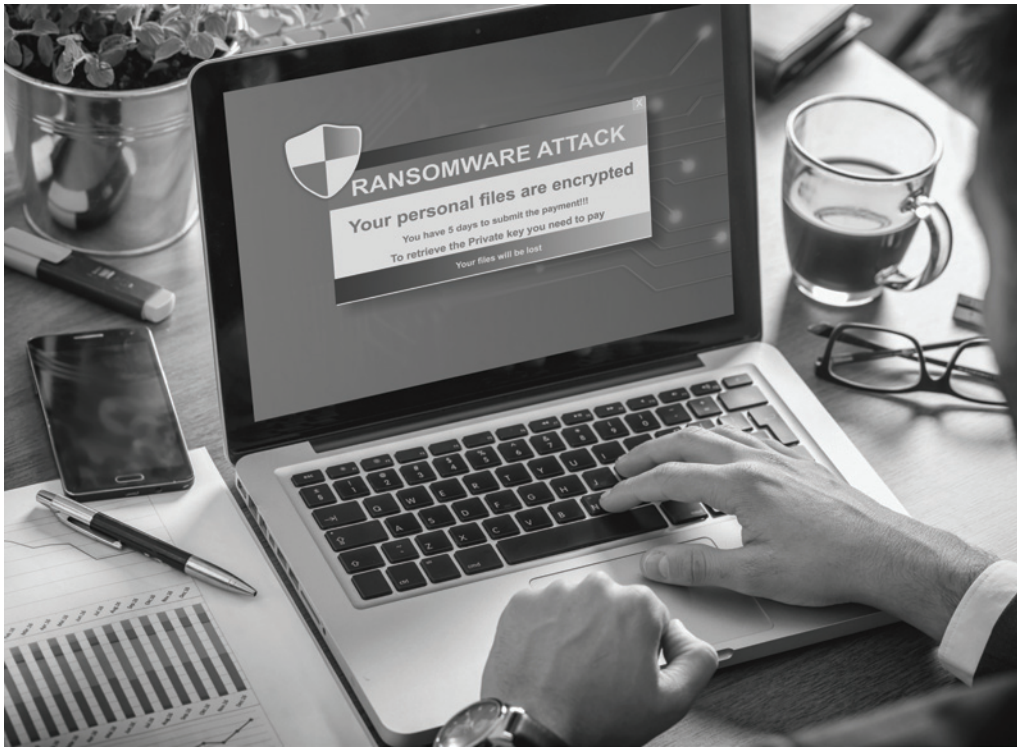
BEST PRACTICES

Refine Your Legal Toolkit Before Ransomware Strikes

By **F. Paul Greene**

And **Daniel J. Altieri**

Ransomware is more prevalent than ever, and it is getting worse. Rare is the organization that has not either experienced a network extortion event or dealt with another that has. Yet most organizations are ill prepared when hit with ransomware, losing precious time, and thereby increasing legal risk, all because of a failure to adequately plan for the potential disruptions that a ransomware attack may bring. Even after the attack subsides, the legal repercussions of ransomware can often dwarf the attack itself, considering such things as reporting duties, investigations, indemnification claims, and lawsuits.



Organizations are best served by preparing for these challenges in advance and honing the appropriate legal tools for use in an attack before the attack occurs. These tools include, amongst others, an Incident Response Plan keyed to the organization's specific regulatory concerns; appropriate third-party relationships to provide support in a ransomware attack; and a thorough risk management analysis, addressing everything from risk transfer strategies, such as insurance, to the all-important question of whether or not to pay a ransom demand, if such payment is even possible.

Developing an Appropriate Incident Response Plan

Incident Response Plans have been familiar in highly regulated industries, such as health care and financial services, for years. Only recently, however, have they become a requirement for the masses, with many organizations facing recent statutory or regulatory mandates to adopt a plan. Case in point, the recently implemented N.Y. SHIELD Act, which added a new §899-bb to the General Business Law, requiring any person or business that owns or licenses the computerized private information of a New Yorker to "develop, implement and maintain

F. PAUL GREENE *partner and chair of the privacy and data security practice group, and* DANIEL J. ALTIERI, *senior associate, are attorneys at Harter Secrest & Emery, a full-service business law firm with offices throughout New York. They can be reached at fgreene@hselaw.com and daltieri@hselaw.com.*

reasonable safeguards to protect the security, confidentiality and integrity of [such] information including, but not limited to, disposal of data." See N.Y. Gen. Bus. Law §899-bb(2).

Section 899-bb goes on to list 14 separate administrative, technical, and physical safeguards necessary for an information security program to comply with the statute, mentioning twice the need to "detect[], prevent[] and respond[] to" attacks. See N.Y. Gen. Bus. Law §§899-bb(2)(b)(ii)(B)(2); 899-bb(2)(b)(ii)(C)(2). Although §899-bb does not reference an Incident Response Plan by name, it is difficult, if not impossible, to appropriately document and guide efforts to "detect[], prevent[] and respond[] to" attacks without a written plan in place.

As for the substance of such a plan, little regulatory guidance exists, whether under the SHIELD Act or otherwise. In Massachusetts, for example, the focus is on documenting "responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken," rather than developing a plan of action in advance. See 201 Mass. Code Regs. §17.03(j). The HIPAA Security Rule mandates "policies and procedures to address security incidents," and the ability to "identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents […] and document security incidents and their outcomes." See 45 C.F.R. §164.308(a)(6)(i)-(ii).

Regardless of the regulatory regime that applies, or any resulting lack of guidance, two considerations are key when developing an Incident Response Plan, especially when it comes to ransomware: ensuring that the team members entrusted with executing the plan know their roles and responsibilities, and properly tuning your plan to applicable reporting duties. As for an organization's incident response team, ignorance often reigns when it comes to activating the plan, who is responsible for what actions under the plan, and how best to assess and respond to an attack, once it occurs. Incident Response Plans often are delegated to an organization's IT department, or its Information Security department, if it has one. For this reason, other key stakeholders—like legal, finance, risk management, human resources, marketing and public relations—are either left out of planning entirely or only minimally aware of what role they may play when an attack strikes. In relation to ransomware, such a disconnect between the plan and the team can lead to the organization increasing rather than mitigating its legal risk, for example by failing to protect privileged communications, releasing unnecessary or inconsistent public statements, or otherwise breaching a contractual reporting or security covenant.

> Organizations are best served by preparing for these challenges in advance and honing the appropriate legal tools for use in an attack before the attack occurs.

As for potential reporting duties, a common misperception persists that an incident that does not involve actual exfiltration of data is not a reportable "breach." Yet the recent trend in the arena of data breach reporting is that mere access to reportable data, even without exfiltration, can be reportable. Case in point, the recent amendment to N.Y. G.B.L. §899-aa, effective as of October 2019, which specifically created a reporting duty when a bad actor accesses reportable data without authorization, regardless of whether the data is ultimately removed from the network or copied. See, e.g., N.Y. Gen. Bus. Law §899-aa(1)(c) ("'Breach of the security of the system' shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business … ."). Because of this, an Incident Response Plan, for example, that is only triggered when data is lost or stolen will not properly serve an organization when that data has been nonetheless accessed by a threat actor while conducting initial reconnaissance in a network. This can lead to missed reporting deadlines, failure to properly assess or mitigate risk, and loss of precious time, as the incident response team determines whether or not it should mobilize.

Third-Party Relationships

Many organizations have not yet established the various third-party relationships necessary for effective response to a ransomware attack. Security and legal relationships are key, of course, but—if an organization has cyber risk insurance—a gating decision must be made before these relationships can be fully leveraged: will the carrier pay for the insured's chosen vendors? Fortunately, nearly all forms of cyber risk insurance cover first-party security and legal costs in relation to a covered incident. The chief difference among competing forms in the industry, however, is whether the insured has choice of vendor, or instead must use vendors from the carrier's panel. For smaller organizations, these panel options can be a godsend, as such organizations may not have established relationships in place sufficient to help manage and respond to a ransomware event. For larger, more mature organizations, they are often surprised to learn that their choices may be limited. For example, if the organization has taken the laudable step of retaining a security vendor in advance with a guaranteed service level agreement, that security vendor may not be on the carrier's panel. The same holds true with the organization's preferred counsel. At a minimum, an organization should decide in advance whether choice of vendor is important to it. The last time an organization should be vetting new counsel or a new security vendor is in the heat and chaos of an encryption event.

Risk Management

The full effects of a ransomware attack can rarely be anticipated in advance. Many organizations are able to recover from an attack without public disclosure or materially adverse effect. Others are forced out of business because they are unable to recover crucial operational data. The one constant in relation to ransomware, however, is the question of whether or not to pay the ransom. Few organizations have contemplated this issue in detail in advance, however. If the ultimate decision is to pay, for example, risk can accompany that decision, as a ransom payment may not resound positively with either internal or external stakeholders. Further, as the Department of the Treasury has recently reminded, payment of a ransom or facilitation of such payment can lead to regulatory risk. If an attacker is listed on the Department's Office of Foreign Assets Control Specially Designated Nationals and Blocked Persons List or comes from an area subject to a comprehensive country or region embargo—including hacking hotspots Iran and North Korea—then the payment of a ransom, or the facilitation of payment, can be subject to regulatory action and fines. See U.S. Dep't of Treas., Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Oct. 1, 2020). These complexities only underscore the need to assess all relevant ransomware risks in advance, including the potential inability to pay a ransom, even if the organization wishes to.

> Planning for a ransomware event will always be imperfect, but failing to prepare could be catastrophic.

Preparation Is Your Best Defense

Against this backdrop, planning for a ransomware event will always be imperfect, but failing to prepare could be catastrophic. Some policy will be always be deficient, some relationship inadequate, some contingency not anticipated. That being said, by assessing its Incident Response Plan, third-party relationships, and risk management approach in advance of a ransomware attack, an organization can greatly increase its ability to respond to, and hopefully recover from, such a crisis. Failing to prepare only increases the attackers' advantage in relation to ransomware, as they prey off of the confusion and chaos that such an attack invariably brings.