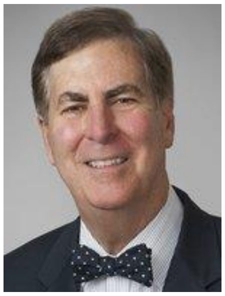
Health Cos. Must Prepare For Growing Ransomware Threat

By **Alaap Shah and Stuart Gerson** (June 21, 2021)

Alaap Shah



Stuart Gerson

Ransomware attacks have become big business, and they are on the rise. And entities in the health care and life sciences space have become primary targets of opportunity for attackers.

As the recent Colonial Pipeline Co. ransomware event[1] illustrates, a small group of black hat hackers, living in protected status in nation states hostile to U.S. interests, can create massive disruption in our country's infrastructure and well-being, and significant economic and other benefit for themselves and for the governments that support them.

Why is it that health care is such a prime target? The reason lies in the nature of the data that health care and life sciences companies and institutions create and store, and their relative vulnerability in the way they maintain and communicate it.

Health care entities are a treasure trove of cutting-edge research and information regarding pharmaceuticals, medical devices and other intellectual property that command great value. The protected health information that they store is of immense value, less with respect to identity theft, as is the popular notion, than it is as an enabler of fraudulent billing schemes that can quickly produce millions in revenue for hacking organizations.

And in the broadest sense, imagine, for example, the societal dislocation that a hostile digital intruder, or its sponsors, could cause if hospitals couldn't provide services because their patient records were made inaccessible by ransomware encryption code. That kind of potentiality has been the reason why so many institutions and companies have caved in to ransomware demands.

To keep their malicious economic engine running, hackers have become increasingly creative in their extortion schemes. Not only do they conduct ransomware attacks, but some offer ransomware as a service,[2] selling the means for others to conduct exploits.

In short, the tactics, techniques and procedures employed by hackers exhibit ever greater sophistication and can leave victims struggling operationally, financially and from a reputational perspective. This is in large part due to the fact that hackers are increasingly trying to take three bites at the apple when extorting ransom payment.

Triple Extortion Threat Explained

As a first bite at the apple, hackers use ransomware to lock systems and restrict access to data by encrypting systems and files across an organization. In simpler times, ransom payment, typically via cryptocurrency such as Bitcoin, would be exchanged anonymously for a decryption key.

The potential end game in this scenario that would leave an organization crippled and unable to operate, is especially problematic for health care and life sciences organizations that serve vulnerable patients.

However, as health care and life sciences organizations have appropriately focused attention on resiliency and resorted to restoring systems from robust data backups to avoid paying ransom, the hackers pivoted to exfiltrating an organization's sensitive data as the second bite at the apple.

The hackers typically share proof-of-life evidence of such exfiltration in the form or screen shots with the victim organization. In this scenario, hackers threaten to release the sensitive data[3] onto the dark web or to the public.

In essence, while organizations increasingly have moved toward thwarting ransomware with a backup strategy, the hackers have followed suit by using data exfiltration as their backup strategy to gain leverage and extort ransom payment.

Hackers have often succeeded in obtaining acquiescence. For example, in some cases, where a victim refuses to pay despite exfiltration of data, hackers have released the data publicly[4] or sought to monetize it through the dark web.[5] The leak of an organization's data can lead to reputational damage as well as regulatory risk related to the data breach involving personal information.

These leaks are often amplified by the media and can result in long-lasting loss of trust by customers, patients, business partners and regulators in an organization's ability to protect sensitive data, as well as class actions, even in cases without economic injury.

To make matters worse, hackers lately are taking a troubling third bite at the apple. If data encryption and exfiltration fail to produce payment, some brazen hackers have taken the radical approach of launching distributed denial-of-service attacks against an organization's information technology infrastructure in an effort to force the organization back to the negotiating table.

In essence, this third tactic has been referred to as a ransom denial of service,[6] which involves hackers demanding ransom payment to stop the attack. Such attacks at the heels of a failed ransomware extortion attempt has been rare thus far, but organizations need to be aware of this new development and implement additional resiliency measures.

Increased Scrutiny of Ransomware Payments

Another problem that has surfaced relates to ransomware payments. In times past, government enforcers tended to turn a blind eye to organizations that have chosen to pay off their attackers.

Insurance companies, finding that the cost of the bitcoin ransom might be less than the cost of dislocation and reconstruction that the exploit would occasion if payment were withheld, often have gone along. But ransomware attacks have become so prevalent, and law enforcement, insurers and outside analysts have concluded that payment simply is too much of an incentive for even more penetrations, that priorities have changed.

The U.S. Department of Justice, FBI and other enforcement agencies have made ransomware a priority[7] and now oppose payment in most circumstances where ransomware does not threaten the existence of an organization. This has led to greater pressure on all entities to magnify their compliance efforts.

Building a Comprehensive Ransomware Defense and Response Strategy

There is no silver bullet to prevent ransomware attacks, but an ounce of prevention can equal many pounds of cure when it comes to minimizing downside operational, financial and reputational risk.

Thus, health care and life sciences organizations must continue to pivot, as criminal ransomware activity has evolved, to determine how to beef up cybersecurity spend and deploy resources to thwart this ransomware triple threat.

It will likely require a robust layered defense strategy and solutions. Yet, no organization can solve this problem alone. It is likely that international government prioritization, cooperation and intervention relative to these threats will reduce these existential risks for victimized organizations.

In the near run, while hackers increasingly are turning to sophisticated technical means to gain access to organizations' databases, most exploits begin by attacking human weakness, often through things like phishing emails and other seemingly innocent ruses.

It is now a commonplace for organizations to take measures to control and monitor access to their systems, to employ encryption and multifactor authentication, to seek cloud-based solutions and vigorously to update and patch software.

These are steps in the right direction, but they are not enough. There is some good news out there, most recently the DOJ's announcement that it has been able to recover most of the ransom paid by Colonial Pipeline[8] and its insurer, that suggests that countermeasures can produce helpful results. At the same time, however, the compliance responsibilities of potential victims have continued to rise. We all must react accordingly.

Having declared ransomware to be a significant threat to national security, and a technical equivalent to terrorism, the DOJ has made this issue a law enforcement priority.

In that, as noted, most ransomware attacks originate with human error or malfeasance, it can be expected that the enforcement agencies will place great pressure on private organizations vigorously to adopt best practices in order to avoid regulatory sanction.

This is particularly true in the health care space, where the primary U.S. Department of Health and Human Services functionary in the field, the Office for Civil Rights, is not technically qualified or equipped directly to counter ransomware hackers, and can only deal with their prospective or actual victims.

Still on June 9, recognizing the rampant ransomware threats, the OCR issued guidance via its list serves to guide Health Insurance Portability and Accountability Act-subject entities regarding managing ransomware risks.

Prepare for the Inevitable Attack Including Compliance and Risk Management Activities

What then should a health care or life sciences organization do to prevent or deal with ransomware? Perhaps the best place to find actionable guidance is in the U.S. government technical guidance manual titled "How to Protect Your Network From Ransomware."[9]

This manual is a joint publication of the government's principal law enforcement agencies, including the DOJ and the FBI, as well as the member agencies of the intelligence community, including the U.S. Department of Homeland Security. DHS' cyber component, the Cybersecurity and Infrastructure Security Agency, has also published a helpful guide to ransomware.[10]

In short, all ransomware prevention is premised upon risk determination and awareness, followed by intensive training and testing.

There are many steps that even small organizations can undertake to reduce risk. Specifically organizations should consider employing spam filters to weed out phishing emails, firewall configuration, limitations and monitoring of network access, regular software update and patch management, automatic antivirus and anti-malware utilities; end-to-end encryption; and dual-factor authorization, among other cybersecurity best practices.[11]

Of course, larger, more sophisticated organizations can go further with technical means in terms of prevention and managed detection and response.

Every organization must, to the best of its ability, assure resilience, regularly backing up data to secure servers, offline or air-gapped if possible, or using cloud-based solutions.

And it is strongly encouraged to conduct at least annual penetration tests and vulnerability assessments. Law firms and insurers can provide useful assistance in that regard to put organizations in a defensible position relative to hackers and regulatory authorities.

If systems fail and an organization suffers a ransomware infection, it must immediately contain the threat by isolating infected computers, powering off all likely infected devices and securing cloud-based or remote backups. Shortly thereafter, an organization should contact the FBI or U.S. Secret Service as soon as possible.

Organizations will likely also have federal and state breach notification requirements and other administrative responsibilities flowing from a ransomware attack. But it may be that the critical decision that has to be made early on is whether to pay ransom. The lay of the land in this regard is changing, and any decision should be made after consultation with law enforcement and participation of the cyberinsurance carrier.

All in all, ransomware is a danger to public and private entities, and it will take a high level of public-private cooperation to combat it. As all segments of American society address that aim, the watchwords remain compliance and resilience.

Alaap Shah and Stuart Gerson are members at Epstein Becker Green.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://www.nytimes.com/2021/06/08/business/colonial-pipeline-hack.html.

[2] https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

[3] https://www.fincen.gov/sites/default/files/advisory/2020-10-

01/Advisory%20Ransomware%20FINAL%20508.pdf.

[4] https://www.forbes.com/sites/thomasbrewster/2021/05/13/ransomware-hackers-claim-to-leak-250gb-of-washington-dc-police-data-after-cops-dont-pay-4-million-ransom/?sh=49095bd158d0.

[5] https://www.healthcareitnews.com/news/tens-thousands-patient-records-posted-dark-web.

[6] https://heimdalsecurity.com/blog/avaddon-ransomware-hits-insurance-giant-axa/.

[7] https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/.

[8] https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[9] https://www.justice.gov/criminal-ccips/file/872771/download.

[10] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.

[11] https://us-cert.cisa.gov/ncas/tips/ST19-001.