EXECUTIVE SPOTLIGHT: RESPONDING TO RANSOMWARE

PREPARED BY

EHI EXECUTIVES FOR HEALTH INNOVATION

Booz | Allen | Hamilton

INTRODUCTION

Preparing for the inevitable cyberattack takes time, money and increased workforce burden. There is no one right way to prepare, nor is there a single solution to picking up the pieces after the attack.

Recently, Executives for Health Innovation (EHI) held an expert roundtable, *Responding to Ransomware Attacks, Practical Advice and Experiences*. During the session, executives and cybersecurity experts discussed why attacks occur, how hospitals and health systems can better prepare, and the pros and cons of paying the ransom.

KEY TAKEAWAYS

Ransomware attacks are costly and time consuming. Organizations should expect to spend months, or sometimes years recovering from an attack. Organizations rarely get all of their data back. An average of 65-70% of patient data is returned to its original state.

Ransomware is a business. Attackers primary goal is to make money from its victims. This is organized crime and they work systematically. Their prime objective is money which they then put back into their work and continue to gain monetary success.

COVID-19 increased vulnerability. The COVID-19 pandemic has made hospitals, who are already seen as easy targets, more vulnerable to attacks. Staff is being burned out, and the organization is stressed to their limits financially.

Instant reponse plans (IRP) are the bare minimum preparation required by organizations. Having a plan does not ensure a successful, well-controlled event. Even with the best IRP in place, risks cannot be eliminated, only mitigated. There are many reasons healthcare organizations will abandon a plan designed for the moment they are attacked, including lack of professional advice in the IRP's creation, inefficient preparation exercises, untested backups that fail.

Most experts recommend NOT paying ransoms. While experts may agree that paying a ransom is not the correct choice, the decision is never simply ‘pay or not pay.’ While ransomware is often seen as a financial decision, factors such as patient and community trust, leadership’s ability to decrypt patient records with a dependable backup, and current risks to patient’s safety should be considered.

Organizations are required to report breaches both to federal and state agencies. The current federal regulatory requirement is that all breaches must be reported within 60 days of discovery. State rules vary.

Understand what your cyberinsurance does and does NOT cover. Cyberinsurance is expensive but crucial to have in the event of a cyberattack. Often your plan does not pay for everything that happens. Being prepared involves a lot of planning and budgeting .

Speakers Bridget Quinn Choi, Director, Booz Allen Hamilton, and John Riggi, Senior Advisor, Cybersecurity and Risk, American Hospital Association brought unique insight from their real-world experience with ransomware attacks. They, along with roundtable attendees, flesh out the intricacies to truly protecting a hospital or health system and their patients from a cyber-attack, what to do when it inevitably happens to your organization, and how to recover and learn from mistakes.

Bridget Quinn Choi
Director
Booz Allen Hamilton

John Riggi
Senior Advisor, Cybersecurity
and Risk Advisory
American Hospital Association

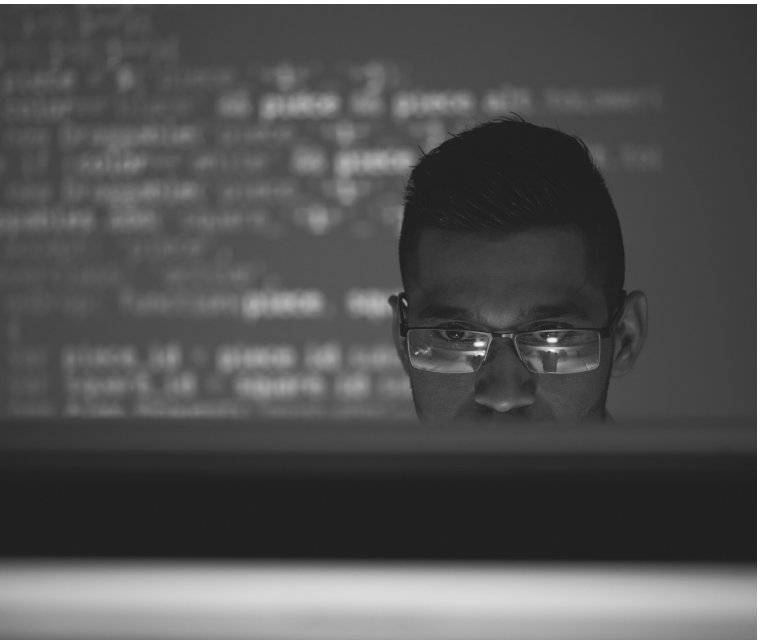
UNDERSTANDING THE ATTACKERS

Who is attacking American hospitals and health systems?

Bridget Quinn Choi (BQC), Booz Allen Hamilton (BAH): [Organized crime.] These are not nice people, it is organized crime which feeds into a broad criminal network. It has become big business, and can no longer be consider a nuisance or some opportunistic crime. It is systemic...The important thing to understand is their primary objective of the ransomware attacker is to obtain money. As long as attacks continue to render profit, the criminal will continue to build in sophistication and scale to grow the profit.

> "AS LONG AS ATTACKS CONTINUE TO RENDER PROFIT, THE CRIMINAL WILL CONTINUE TO BUILD IN SOPHISTICATION AND SCALE TO GROW THE PROFIT. " (BRIDGET QUINN CHOI, BOOZ ALLEN HAMILTON)

You should liken it to [an] American franchise model. These ransomware groups…the top ones make a lot of money so they are investing in themselves for further success…they are building a brand much like a franchisor. These ransomware groups have affiliates or outsourced specialized teams that carry out the attacks. The affiliates operate like franchisees. They are given tools and playbooks allowing them to repeat their attacks across multiple victims. The afilliates are given a large portion of the proceeds from the attack and the ransomware group takes a smaller percentage. The ability to use affilates and build repeatable methods for carrying out these attack allows them to attack at scale. It is also the reason ransomware attacks are seemly ubiquitous and growing in sophistication...They are looking for continued monetary success, and they are flush with capital to continue.



What is the objective of attackers?
Many of [the attackers] don't necessarily know exactly whose network they've accessed right away. Attackers may not look for a particular entity to attack. Rather, they have simply gained accesss to an entity with easily exploitable security vulnerabilities. Once they gain access, they research their victims often using public available information and decide the size of the ransom based upon the perceived value or wealth of the victim. Their primary objective, remember, is to get money. Many do not necessarily care about healthcare services and they do not care about your data. They really just care about creating the most pressure on a victim to gain an entity's money.

There are exceptions as threat landscape continues to shift. After the major public attacks on critical infrastructure, we have seen **some** threat actors willing to provide decyption keys without payment and cease their attack when they learn it's a healthcare entity. However, other ransomware groups are more ruthless.

Why are hospitals targeted?
The fact that healthcare organizations are regularly successfully attacked demonstrates and broadcasts that healthcare institutions have exploitable vulnerabilities. Hospitals are attacked with frequency because the barrier of entry is low due to their security posture making them a prime target for an attack.

This is particularly concerning because if a foreign adversary or nation state wanted to weaponize cyber attacks on healthcare systems, they could with relative ease, particularly because hospitals are vulnerable when at capacity and stress tested due to COVID.

"GENERALLY AND HISTORICALLY, NO HEALTHCARE ORGANIZATIONS HAVE PREPARED AN INCIDENT RESPONSE PLAN AND PRACTICED DOWNTIME PROCEDURES FOR AN INCIDENT EXTENDING BEYOND THE REQUIRED 72 TO 96 HOURS." (JOHN RIGGI, AMERICAN HOSPITAL ASSOCIATION)

INCIDENT RESPONSE PLANS

Should all hospitals design an incident response plan?
BQC: Yes – it is an imperative. A hospital should have a plan to test the plan and design the plan to fit the particular purpose of a response to a ransomware attack and/ or cyber incident. The plan should be to sized to the things that are drivers in a well-planned attack…and that should include processes, roles for people within the organization, and technical solutions focused on the ability to recover, respond, and restore with speed and intent.

John Riggi (JR), American Hospital Association (AHA): [It is extremely important to have a cross functional] cyber incident response plan, which is fully integrated into the healthcare incident command structure for your organization. It is also very important to participate in a regional cyber incident response plan which includes surrounding organizations that will also feel the secondary impact of a disruptive ransomware attack targeting one hospital or health sytem in their region. I call [this] “the ransomware blast radius”…One victim organization may be hit, but there are reverberations throughout region’s health care delivery systems as patients and ambulances may be diverted from the victim hospital to surrounding facilities.

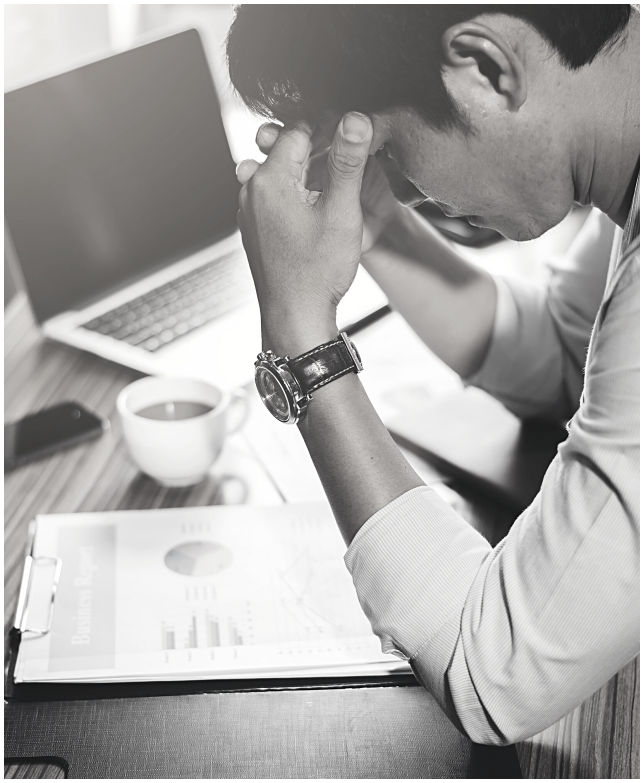
How effective are these incident response plans?
BCQ: A well designed and tested plan is very effective, however, a BAH study found that 60% of victims of a ransomware attack, abandoned their incident response plan. Interestingly, those who followed their plan were able to recover faster and were less likely to have paid the attacker...Having a plan in itself does not ensure a well-controlled event but having a plan that is well designed and tested certainly reduces the risks.

JR: Generally and historically, no healthcare organizations have prepared an incident response plan and practiced downtime procedures for an incident extending beyond the required 72 to 96 hours. Beyond that time frame, especially for incidents lasting up to 4 weeks, most organizations are unprepared. In addition, when it comes to restoring systems from, hopefully, uncorrupted backups, no one can say with precision how long it will take to restore the entire network and how much data will be recovered or lost.

The reason for that is, no hospital or health system has practiced shutting down their entire network soley to attempt restoration from backup. An intentional enterprise wide network shutdown could be dangerous as it would take an extended time to restore systems and would thereby disrupt patient care and risk patient safety.

Why are some plans ineffective during actual incidents?
BCQ: What most victims found is that they never tested the backups [of their data], and they never tested the recovery plan. So, the guidance built to respond to the incident, they thought they had it in place, [but] it wasn't useful. No one knew how to carry out the response. Many companies didn't have a retainer for incident response services prior to an attack. Or an understanding of the ability of their own staff to respond. Devoloping that muscle memory is crucial.

JR: Based upon what I have seen across the nation while assisting hospital and health system victims of ransomware attacks, it appears that many do not anticipate nor factor in their incident response plans the disruptive impact that the simultaneous loss of all medical, information, and operational technology will have on the organization. A loss of email and phone communications also adds to the disruption, confusion and delay in an effective response by the organization. Incident response plans and preparedness may also be lacking because they have succumbed to human nature - they just don't believe they will become victim of a high impact ransomware attack. They believe that's something that happens to "someone else." They may not recognize their organization's level of risk and understand that, no matter how much human, financial, technical resources you devote to cybersecurity, cyber risk can never be eliminated it can only be mitigated.



TO PAY OR NOT TO PAY

The debate of 'should we or should we not pay the ransom' is incredibly controversial. There doesn't seem to be a right or wrong answer. What are your thoughts on hospital leadership choosing to pay, or choosing not to pay the ransom attackers are demanding?
JR: First we hope that no organization finds themselves in such a position. But if they do, we at the AHA follow the reasonable and responsible policy of the FBI which I had a direct hand in writing when there. [We] strongly discourage the payment of ransom as it emboldens the adversary. It incentivizes [ransomware attacks and] the proceeds may also fund more serious crimes, including violent crimes.

That being said, we and the FBI also understand that ultimately it is a business decision that must be made by the victim organization, based upon their individual circumstances. They must weigh their ability to independently restore systems, provide continuity of care, impact to patient safety, and other business considerations. It is important to note that payment of the ransom does not guarantee recovery of all the data nor that the organization will not be attacked again.

BCQ: Some organizations decide to pay a ransom in order to suppress the leaking of the stolen information to some attacker public shaming site. However, in that scenario, you're going to have to assume that any information that has been extracted is in the criminal community forever. The attacker might give some assurances that the stolen information is deleted. They might provide all sorts of assurances and proofs to make you believe that it's no longer in their possession and control, but there is nothing that confirms and proves that they didn't make a copy.

So, paying for data suppression is something that [BAH] typically advises against unless it's information for which secrecy is so critical to the business that availability to the public would be devastating. An example may be some guarded and unique trade secret or some research and development.

> "HOWEVER, FOR MOST OF THE VICTIMS IN THE STUDY, THE DECISION TO PAY ATTACKERS RESTED LARGELY ON THE ABILITY TO PROPERLY ACCESS DATA AND ITS FUNCTIONALITY, [IN ORDER TO] RECOVER FROM BACKUP." (BRIDGET QUINN CHOI, BOOZ ALLEN HAMILTON)

Does it ever make sense to pay the ransom?

BQC: In the Booz Allen study [some organizations thought that they] would not survive the business disruption at the scale [of] this attack; they didn't think they could survive the monetary losses or losses of productivity, as a result of the attack. They want minimization of financial losses, and disruption to the business operations. These organization believe that the attacker supplied decryption tool is a means to ensure a swift recovery. [Other] victims paid for data suppression...They didn't want the data that was taken or purportedly taken to be leaked on the Dark Web. Some victims [studied] said the timeline for recovery was too long with backups. [This] goes back to the data recovery plan. Having confidence in the ability to recover and confidence in the validity of backup is a common factors in those victims who did not have to pay a ransom. However, for most of the victims in the study, the decision to pay attackers rested largely on the ability to properly access data and its functionality, [in order to] recover from backup.

JR: Speaking strictly from the hospital and health system perspective, I will never say that it makes sense to pay the ransom - for a number of reasons, the first being, that statement alone, coming from me as the national representative for hospitals and health systems on cyber issues, could actually encourage ransomware attacks against hospitals and health systems. The second being that, as we have seen, whether the victim pays the ransom or not, the percentage of data recovered and data lost is about the same.We know it's a very, very difficult decision whether to pay the ransom or not when faced with intense pressure, including when confronted with the now common triple extortion threat victims face in ransomware attacks - encryption of data, threat of publication of stolen data, and now we have the third layer of extortion…The attackers are actually calling patients, executives and staff directly and demanding that the organization pay the ransom. This creates enormous public pressure on the organization to pay the ransom.

BQC: What we found from the study is that 50% of those who paid wouldn't choose to do it again. There are many reasons for this including understanding after the fact that attacker supplied decryption tools may not lead to faster recovery, that for many victims data could not be restored to the pre attack state or that paying for data suppression did not prevent any follow-on regulatory activity. In the study, victims who paid the attacker experience greater reputational harm and greater regulatory challenges.

In contrast, the victims in the study who chose not to pay the attackers, 74% would make the same decision again.

TRANSPARENCY ABOUT THE ATTACK

How transparent do organizations need to be about attacks?

JR: [To give an example], when one well known health system went down, they lost all their medical technology, not just the Electronic Medical Record (EMR) – but all network connected medical technology, including telemetry systems, radiology, imaging, labs, and oncology systems.

This disrupted the timely and efficient delivery of care and created a risk to public health and safety. Outside counsel in this case advised the organization to make very general public statements indicating everything was under control and being properly handled. [An] issue I've seen is that…outside counsel will recommend, for proper reasons, to be very opaque with the public and to be very cautious in [public] statements, which may be good legal advice. However, the community will know exactly what is going on through social media channels and word of mouth from patients and staff. The public will view inconsistent or vague statements from the victim organization as a potential betrayal of trust and a lack of transparency, potentially leading to lasting reputational harm.

The other issue to keep in mind is that, insurance company breach response assets don't work for the victim organization. They work for the insurance company. Yes, they have the victim's interests in mind, but ultimately, they work for the insurance company and their motivations may differ from the victim in terms of reducing the expense of the claim, even if it means paying the ransom when other alternatives exist or they may advise against cooperation with law enforcement. This may conflict with the institutional values of the victim organization. After the incident, the insurance company team will pack up and leave, and the victim organization will be left to deal with the community and the decisions they made on ransom payment and transparency with the government and the community.

"THE PUBLIC WILL VIEW INCONSISTENT OR VAGUE STATEMENTS FROM THE VICTIM ORGANIZATION AS A POTENTIAL BETRAYAL OF TRUST AND A LACK OF TRANSPARENCY, POTENTIALLY LEADING TO LASTING REPUTATIONAL HARM." (JOHN RIGGI, AMERICAN HOSPITAL ASSOCIATION)

Does a hospital have to report to the federal government?

JR: [Hospitals are required to report breaches to the federal and their state's government.] There is a regulatory requirement that all breaches be reported within 60 days.

At the federal level, Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to report data breaches to impacted individuals without unreasonable delay, and in no cases less than 60 days.[1] Breach notification requirements implemented by the Health Information Technology for Economic and Clinical Health (HITECH) Act states that the HIPAA covered entity must notify the affected individuals of a breach, as well as the HHS secretary and the media where a breach affects more than 300 people.[2]

[1] https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
[2] https://www.hhs.gov/hipaa/for-professionals/breach-notification/laws-regulations/final-rule-update/hitech/index.htmlt

In both the House and the Senate, there are efforts to develop federal mandates for critical infrastructure, including hospitals and healthcare organizations, around breach notifications.

RECOVERING FROM THE ATTACK

When a ransom is paid, do organizations get their data back?

JR: Not necessarily. For a variety of reasons, including technical issues related to the slow decryption and restoration processes, it can take three to four weeks, minimum, to recover just the mission critical systems – whether the ransom is paid or not. In addition, whether a victim pays or does not pay, they generally only recover about 65-70% of their data due to technical data recovery and restoration issues.

[In a study, it was found that] most companies who paid the ransom did not get their data fully restored at the same level. 40-44% got everything back in the manner that they expected when they paid for the decryption tool. Victims often paid the attackers because [they thought] it was the fastest or cheapest road…to recovery. [Study victims often, given the limited satisfaction, paid because] they thought it was less expensive than any other recovery means; it's not necessarily [true].

How long does it take to recover fully from an attack?

BQC: The key things to consider is how badly it affected the network, what the extent of the damage was, how old the network is… There's a lot of variables. It could take a year because you're going to have to rebuild your entire infrastructure. There are so many components [that] go into rebuilding a better and mature network. It may have to be phased over time. In the BAH, study to regain operability of business critical assets, on average took only a week. But, that is the beginning of the journey for many victims.

[3] https://www.hhs.gov/hipaa/for-professionals/breach-notification/laws-regulations/final-rule-update/hitech/index.html

JR: In high impact healthcare ransomware attacks, we have seen that it takes a minimum of three to four weeks for mission critical medical technology to come back online. Many systems just cannot be rebuilt, the interfaces may be wiped out for example and cannot be rebuilt, I want to stress that, pay or not, you will never make a full recovery even months after the attack. Many hospitals have certain legacy systems and medical devices that, …even if you paid for the key, the decryption process just may not work.

BQC: Some victims thought they would literally get back everything and get it back in a week, mostly when you see [that] they [got their] critical systems [back up], not everything. When the malware gets into the system and the encryption process happens, it impacts data integrity, so you may get a decryption key and the decryption key may in fact work but it won't work on everything. It's so difficult to understand at the get-go, when you're making your value decisions on what will be impacted. Is it worth it to pay? Will it be able to recover? What [is] the recovery time? Aging infrastructure within healthcare networks is [a] huge [problem].

"IT'S SO DIFFICULT TO UNDERSTAND AT THE GET-GO, WHEN YOU'RE MAKING YOUR VALUE DECISIONS ON WHAT WILL BE IMPACTED. IS IT WORTH IT TO PAY? WILL IT BE ABLE TO RECOVER? WHAT [IS] THE RECOVERY TIME? (BRIDGET QUINN CHOI, BOOZ ALLEN HAMILTON)

A BETTER WAY TO PREPARE FOR AN ATTACK

What are some important things hospital and healthcare system leaders should be doing to prepare?

BQC: After doing an incident response plan, please print out your cyber insurance policy and print out your incident response plan because…if systems are down, and your information technology is affected, how are you going to find it? If it's encrypted, you can't. So, you've done all this work, made all these plans, and then you can't locate the plan.

Before [an] incident, do an accounting of the assets within the network and identify…who your technical staff is, what their skill sets are, and if those skillsets are appropriate for their response role during the incident.

The same should be made for the organization, decisions must be made quickly, it is important to identify how and who is going to respond to the crisis from not just for technical workstreams but also for a operational, legal, communications and crisis management workstream that must happen in parallel.

Additionally, identifying the needed outside legal and technical vendors is imperative. Building a relationship through a retainer before the incident with the incident response consultants has enormous benefits. With a retainer relationship, the incident response firm will learn the people, processes, and technology of the healthcare entity prior to the incident. If an incident occurs, the outside incident response team does not have to spend time learning the environment or negotiating a contract. They can act with intent and speed to respond, contain, and remediate the attack.

Another thing to consider…is cyber insurance. [Cyber insurance provides a crucial service and a substantial risk transfer for an event that can have an incredible financial impact on an organization. For example, in the recovery process, staff augmentation as far as rebuilding the system may be something that is so important, and an insurance policy does pay for that.] [However,] cyber insurance does not pay for a new network, or betterment which might be needed in order to fully recover, to get back to operational. [Many businesses overlook this point when purchasing cyber insurance. If your old systems are rendered unusable, you need to buy new hardware, maybe new software, too. [This] takes capital and your insurance policy likely does not cover that expense. Budgeting for that financial need is so important.

[My recommendation] is before buying cyber insurance, make sure basic security measures like multifactor authentication, offline offsite secured backups are in place, and then go to your broker and negotiate the broadest, most expansive policy for the least amount of money. In this market, the only way to do that is to show the insurance carriers that you have plans and a mature security posture so that you are a good risk.

Are there specific things you think those who have been hacked need to do to prepare for 'next time'?
BQC: You can expect counter strike or subsequent attack activity, even if the ransom was paid. [The attackers] are competing [with one another] in the criminal ecosystem so there might be one attacker in your system today and another attacker at the back door knocking.

It is important to take steps to prevent another attack immediately and ensure that all attackers have been eradicated from the network or that the present group of attackers no longer have a foothold in the systems.

Additionally, having a post incident “lessons learned” meeting with key stakeholders in the organization and the incident response provider, and gaining an understanding of what vulnerabilities were exploited during the attack, what common vulnerabilities are exploited generally by the different ransomware groups, and then building a plan to remediate those vulnerabilities based on your new understanding will be extremely important.

The silver lining of this is that you are not going to have a better opportunity or the attention of the key decision makers in the organization more than the day after the attack. So, my recommendation is to ask for everything that may be needed and map out the plan. The incident has created a very important proof of concept as to the importance of investing in a mature security posture. The decision makers in the organization will fully realize the gravity of the threat. So, get what you need now and then build toward a better future.

Jessica Wilkerson, Cyber Policy Advisor
Food and Drug Administration

With all the medical devices connected to the hospitals system, who should be involved?
Jessica Wilkerson, Food & Drug Association (FDA): There are organizations, like FDA, that would be interested in ‘Are medical devices impacted?’ ‘Are there patient safety impacts, and if so, what kind?’ The first and foremost thing that [the FDA] is worried about within a ransomware incident is whether or not public safety has been protected.

When making decisions about paying ransom, beyond financial implications, what should be considered?
Nina Alli, Executive Director, Biohacking Village: Revenue is one of the last issues that people should be focusing on when there is an [attack]. You're dealing with [the potential for] loss of life, this risk is higher than the fiscal loss.

Nina Alli, Executive Director
Biohacking Village

Lynn Sessions, Partner
BakerHostetler

Does Attorney-Client privilege apply when the systems legal team is called in for a ransomware attack?

Lynn Sessions, Partner, BakerHostetler**:** We're facing these types of issues with our healthcare clients on a daily basis. What we tell our clients is "I can't guarantee you it's going to be privilege, because the various jurisdictions are [looking at privilege] in a variety of ways." We come in, put together a statement of work for the incident that is at issue and privilege has been upheld [in some jurisdictions]. We've [also] done exactly the same thing in a different jurisdiction and it wasn't upheld. Some of it is driven very jurisdictionally. It's gotten trickier in the last few years…but your outside counsel can be creative. We can't guarantee anything but there is a way to put together relationships via contract that are more helpful to clients in being able to preserve that privilege.

EXPERT ANALYSIS

Kelly Rozumalski, Vice President, Booz Allen Hamilton: "After listening to this roundtable, it's clear that ransom attacks are becoming top of mind for influential executives in the healthcare industry. While no one is under the impression that preventing cyberattacks has an easy solution, leadership inside the healthcare industry is learning just how much it takes to be prepared and are willing to learn from past mistakes and fight for a safer future."

Andy Speirs, Principal, Booz Allen Hamilton: "Ransomware events are another reminder to us that context, insights, and diverse perspectives showcased during this webinar do matter in sustained planning for how health delivery organizations (HDOs) remain resilient to ensure patient safety and peace of mind."