Mitigating Risk and Impact of Ransomware Attacks in the Healthcare Sector

How do you get ahead of a ransomware attack in the healthcare delivery environment? By acting, now. A quick way to organize? Look at the 405(d) group's work, including its recently released ransomware infographic.

The Context

The news is full of headlines concerning ransomware – malware that attacks an information system and holds its data contents for 'ransom' until an attacker's (typically monetary) demands are satisfied. Just ask the leaders of cities like Atlanta and Baltimore. An organization's data has significant value, particularly when malicious actors place their focus on them. New threats to those data arise with remarkable frequency: take, for instance, the log4j vulnerability – a potentially devastating gap just discovered this month that affects a core coding foundational block used across systems globally. Indeed, just last month President Biden issued broad policy goals to combat ransomware attacks on the global stage, including state-sponsored activities.

The Healthcare Ecosystem

Through its reliance on digital information exchange, our nation's healthcare delivery system is not excepted. It began shifting, well before the pandemic, to more data in more places – whether through the complex management of electronic medical records, the deep dive into telemedicine or the use of mobile devices and the cloud to access patient data. As the pandemic has accelerated the pace of this change, it likewise has amplified opportunities for mischief. With the pandemic showing no sign of slowing, healthcare's digital footprint remains a key point of vulnerability. A nonprofit organization (NGO), the Cyber Peace Institute, documented scores of attacks – often in multiples by the same actors – against healthcare institutions in 27 countries during an 18-month span of 2020-2021. The consequences of inaction, particularly among healthcare institutions charged with protecting information under the Health Insurance Portability and Accountability Act (HIPAA), can be financially (let alone, reputationally) onerous and devastating.

The 405(d) Group

Recognizing the growing cybersecurity risks in the healthcare environment, in its 2015 Federal Cybersecurity Act, Congress included language mandating a strengthened approach to cybersecurity in the healthcare and public health sectors (*see, e.g.,* Section 405(d) of the Act). This spurred formation of the 405(d) Task Group, convened by the Federal Department of Health and Human Services and that brings together numerous Federal government leaders alongside hundreds of private-sector healthcare and cybersecurity contributors. Together the Task Group has developed publicly facing resources, including its seminal "Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients," a wide-ranging document touching on areas such as protections against phishing attacks, data loss and medical device protections to ensure patient safety.

405 (d) Infographic

Recently the 405(d) group went live with a publicly facing portal, and in complement published a how-to infographic on ransomware defense. The guidance – geared toward healthcare practitioners as a key audience – affords practical tips to build defenses and think through policies. Elements include:

1. Before an attack:
    A. Practicing operations without digital access (pen and paper) to maintain hard copies of patient data as circumstances may require;
    B. Reviewing organizational incident response plans; and
    C. Identifying internal security points of contact now, so you're ready when a cyberattack occurs, rather than resolving the issue amid a response. (As the aphorism among incident response experts goes, a crisis is not the time to be exchanging business cards.)
2. During an attack:
    A. Quickly moving to response once an incursion is recognized, including to incident command structure; and
    B. Limiting home or remote access to EMRs or email systems to control an attack's spread.
3. Recovering:
    A. Cautiously returning compromised systems online to prevent extension of an attack; and
    B. Documenting lessons learned.

More Tips to Stay Ahead of Ransomware – and Practice Good 'Cyber Hygiene'

With its quick sheet the 405(d) Task Group offers a good foundation to build ransomware knowledge and response nimbleness. More tips to limit exploitable gaps include:

1. **Operational**
    A. Applying patching software to mitigate vulnerabilities as soon as they are discovered and solutions identified;
    B. Examining an organization's **legacy devices** and decommissioning any that no longer can be protected – if left unattended, they can be the domino that tips forward a ransomware event;
    C. Implementing **multifactor authentication** widely across your network;
    D. Training employees thoroughly, including through 'secret shopper' styled exercises that expose data protection habits and highlight areas for improvement; and
    E. Conducting **penetration testing** – testing data controls to find points of weakness that can be hardened.
2. **Technical**
    A. Ensuring network access is issued in a '**least privileged**' position – meaning that no one should have access beyond the elements necessary to complete one's role and responsibilities – this can limit how widely a ransomware event might spread; and

B. Using strong passwords and changing them regularly.

3. **Compliance**

A. Regularly **reviewing obligations** around cybersecurity to government actors – including **notification requirements** – in this fast-changing area of the law;

B. Ensuring contracts incorporate clear language concerning data governance and protocols affecting data compromise; and

C. Updating policies on a regular basis to adapt to a changing technologic environment where ransomware is real and not abating, soon.

Other areas to think about in the ransomware arena include:

- Deciding as a policy consideration whether to pay ransom – particularly as federal leaders debate whether paying ransomware is tantamount to insufficient risk management;
- **Obtaining** a ransomware insurance policy;
- Carefully examining such a **policy's exclusions** to ensure the policy affords the coverage you want;
- Developing plans for **business continuity** (which may bridge from your incident response plans); and
- Adopting clear **operational pathways** – again, before any attack commences – concerning who holds the authority in your organization both to pay ransom and to streamline, wherever possible, preceding approvals.

These are not exhaustive tips, but a place to start.

Information Exchange – the New York Healthcare Cyber Alliance (NYHCA)

For New York State healthcare institutions strengthening their ransomware protocols and their cybersecurity posture more broadly, there is another resource to consider: the New York Healthcare Cyber Alliance. NYHCA focuses on cybersecurity at small to mid-size healthcare delivery organizations – particularly those that have been historically under-resourced around their cybersecurity readiness – to mitigate healthcare continuum cybersecurity risks and build trust in preparing for and in responding to cyber incursions. (Gabriel Oberfield is a co-chair of NYHCA.) NYHCA branches from the New York State Cyber Security Advisory Board – which has a multidisciplinary composition akin to the 405(d) Task Group providing cross-sectoral cybersecurity guidance to New York State's executive branch.

During NYHCA's first operational year – just coming to a close – the body convened several educational sessions, including:

- A presentation by New York County District Attorney Cyrus Vance Jr., who was instrumental in founding the Global Cyber Alliance;
- A presentation from R. S. Richard Jr., Chief of Cybersecurity for Region II with the Cybersecurity and Infrastructure Security Agency (CISA); and
- A presentation from Geoff Brown of the New York Cyber Command.

During 2022, NYCHA is expected to publish a compendium of 'quick-dial' governmental resources (finalization pending); facilitate cybersecurity readiness assessment activity, in partnership with CISA;

and build capacity for town halls and exercises to test capacities (as well, with CISA). Completing these exercises has the ancillary effect of helping healthcare institutions satisfy Conditions of Participation concerning emergency preparedness, requisite for Medicare and Medicaid providers. We encourage Bond clients to get involved and learn, both from their healthcare sector peers and from governmental leaders involved in the work.

Bond Resources

Your Bond attorney can direct you to further resources concerning data privacy and cybersecurity – whether at its intersection with healthcare or beyond. Please reach out to Gabriel S. Oberfield or Jessica L. Copeland with any question you may have about any content contained in this information memo.

BOND SCHOENECK & KING ATTORNEYS