ARTICLE

New Year's Resolutions:
Cybersecurity Preparedness for the Healthcare and Life Sciences Sector

Perhaps no sector has more at stake, or is more targeted, when it comes to cybersecurity than healthcare and life sciences. From health systems that care for thousands of patients a day and store protected health information, to biotech and pharma companies that have valuable IP and supply critical medicines around the globe, cyber attacks in the healthcare and life sciences industry are wreaking havoc on an already fatigued workforce and field under regulatory scrutiny.

In the third annual FTI Consulting Survey: U.S. Healthcare & Life Sciences Industry Outlook 2023, we asked more than 250 leaders of healthcare and life sciences companies in the U.S. about their expectations for the sector in 2023. And among their top expectations is the continued cybersecurity threat looming over the industry.

According to the survey, 70% of respondents experienced a cybersecurity incident in the last 12 months, and 42% continue to think their company is vulnerable to a potential cyber attack or incident. Particular areas of vulnerability listed include malware and ransomware (47%), incidents that involve privacy violations (i.e., Health Insurance Portability and Accountability Act (HIPAA), Personally Identifiable Information (PII)) (46%), and phishing (43%). Further, healthcare and life sciences leaders acknowledge that the potential operational, financial, legal and reputational impacts of a cybersecurity event can be wide-ranging and severe. Data access/exposure (60%), financial costs (52%), patient care (44%), operational disruptions (44%) and reputation impact (38%) were cited in the study as the biggest risks facing the industry.

Against this backdrop, healthcare and life sciences organizations – from health systems to biotech startups and established pharma companies – should consider the following New Year's resolutions to enhance their cybersecurity preparedness in 2023.

Resolution #1: Establish Workstreams and Assign Executive Leadership Accountability

The potential operational disruption in a cybersecurity incident, especially ransomware attacks involving encryption, often forces leaders of healthcare and life sciences organizations to "divide and conquer" across a number of different workstreams. It is important to identify accountabilities to be better prepared to handle post breach recovery activities. Clear ownership is recommended across critical workstreams, including:

— Containment

— Restoration and recovery

— Forensics investigation

— Legal/regulatory response

— Internal and external communications

Knowing who has decision making authority in critical aspects of the incident response process, and who is leading corresponding workstreams, will enable the swift and decisive action that is required to effectively manage an incident.

Resolution #2: Develop Clear Communications Processes And Tools

In ransomware attacks especially, healthcare and life sciences organizations will be pressed to communicate quickly in order to provide guidance to staff regarding operational workarounds and to establish confidence in customers, partners and patients regarding restoration progress and the availability of critical services. At the same time, ransomware attacks often render typical methods of communications – including corporate e-mail – inaccessible, at least until the initial threat has been contained. In advance of a serious issue, healthcare and life sciences organizations should establish out-of-band communications solutions for reaching stakeholders; and streamline internal processes for developing, approving, and disseminating messages to facilitate responsive communications and updates.

Resolution #3: Scenario Plan Ahead Of Threat Actor Escalations

Threat actors continue to evolve their ransomware extortion tactics to impose maximum pain on an organization to elicit payment. And they will not let up on healthcare and life sciences organizations. Extortion tactics can include "naming and shaming" victim organizations on leak sites, directly contacting executive leaders and staff, disseminating ransom notes through organizations' on-site printers, and leaking organizations' sensitive data – all of which are likely to lead to an influx of questions and scrutiny from stakeholders and potential media attention. It is important for healthcare and life sciences leaders to stay ahead of the curve and determine, in advance, their communications posture and messaging approach for these and other likely scenarios.

Resolution #4: Test And Practice Incident Response Procedures

According to FTI Strategic Communications' survey, while 58% of healthcare and life sciences leaders said their organizations have a cybersecurity crisis plan in place, only a little more than one-third of respondents (36%) are considering participating in a crisis simulation or table-top exercise in the next year. **This is a missed opportunity**. Even if a cybersecurity incident response procedure is documented, it is only as effective as leadership's understanding of the protocol and their ability to act on it. Cybersecurity table-top exercises offer controlled environments for leadership teams to pressure test existing response plans and build muscle memory for effective incident response. Further, testing extended downtime procedures is also a critical exercise for healthcare and life sciences organizations to enhance their operational preparedness.

Resolution #5: Ensure Staff Are Up To Date On Cybersecurity Policies And Have An Early Detection System In Place For Threats Of All Kinds

The prevalence of cybersecurity incidents presents an opportunity to refresh staff on organization's existing data retention, cybersecurity and social media policies, especially those that are healthcare or HIPAA specific. Reinforcing policies and the importance of data security and privacy through periodic training exercises and awareness programs is an effective way to consistently build cybersecurity hygiene across all organization levels and among third party vendors or contractors. The effectiveness of keeping individuals diligent can be multiplied by having a dedicated team in place to monitor for early signs of incidents of all kinds, including insider threats and misinformation campaigns.

Resolution #6: Assess Cyber Risks Introduced By Third Parties

It is common for healthcare and life sciences organizations to rely on vendors, suppliers, and contractors to assist with their day-to-day operations, and these third parties are often granted access to the organization's network or data as part of that working relationship. While outsourcing can create efficiencies, healthcare and life sciences organizations need to understand and plan for potential impacts if a connected entity suffers a cybersecurity incident. This can be accomplished by determining what vulnerabilities the organization has limited control over and identifying actions to mitigate these risks pre-incident. This assessment should also include implementing a plan for what to do post-incident, should a third party be hit with a cyber attack.

Resolution #7: Understand Your Organization's Cybersecurity Maturity And Be Prepared For Recovery

As a result of cyber incidents, healthcare and life sciences organizations have experienced data privacy and regulatory investigations, had significant issues with employee morale and turnover, and suffered impacts to their reputation, especially among patients and providers. Conducting a cybersecurity maturity assessment to identify critical gaps and risks in your organization's existing infrastructure can lead to the development of an effective roadmap to guide organizational cybersecurity investment decisions. An effective roadmap can also minimize the likelihood of an incident and the impact to reputation in the event of one. Following a cyber incident, it can be challenging to rebuild trust with key stakeholders as the tail on these incidents can be elongated. Having experts in place that know your organization, stakeholders and values is critical to quickly navigating the immediate and long-term aftermath of a cyber incident. Instantaneous access to data and insights allows leaders to uncover emerging stakeholder needs, concerns and expectations. These insights can inform compelling strategies around what organizations should focus on to build confidence among key stakeholders.

In 2023, the healthcare and life sciences industry will continue to be a prime target of cyber criminals[1]. There is no time like the present for the sector to take some of its own preventative medicine and make proactive investments now to prepare for the inevitable.

[1] Jill McKeon, Easterly Reaffirms CISA's Focus On Healthcare Cybersecurity at mWISE, HealthITSecurity.com (October 20, 2022), https://healthitsecurity.com/news/easterly-reaffirms-cisas-focus-on-healthcare-cybersecurity-at-mwise.

JAMIE SINGER
Managing Director, Co-Head of Cybersecurity & Data Privacy Communications

ROBERT STANISLARO
Senior Managing Director, Head of Healthcare & Life Sciences Corporate Reputation

MATT CHEVRAUX
Managing Director, Cybersecurity

ERIN WILLIAMS
Director, Healthcare & Life Science Corporate Reputation