Ponemon INSTITUTE

Executive Summary: The Impact of Ransomware on Healthcare During COVID-19 and Beyond

Sponsored by Censinet

Independently conducted by Ponemon Institute LLC

Publication Date: September 2021

Full, 43-page report available for free at: censinet.com/ponemon-report-covid-impact-ransomware

Ponemon INSTITUTE

The Impact of Ransomware on Healthcare During COVID-19 and Beyond

Prepared by Ponemon Institute, September 2021

Executive Summary

The purpose of this research is to understand how COVID-19 has impacted how healthcare delivery organizations protect patient care and patient information from increasing virulent cyberattacks, especially ransomware. Prior to COVID-19, 55 percent of respondents say they were **not** confident they could mitigate the risks of ransomware. In the age of COVID-19, 61 percent of respondents are **not** confident or have no confidence.

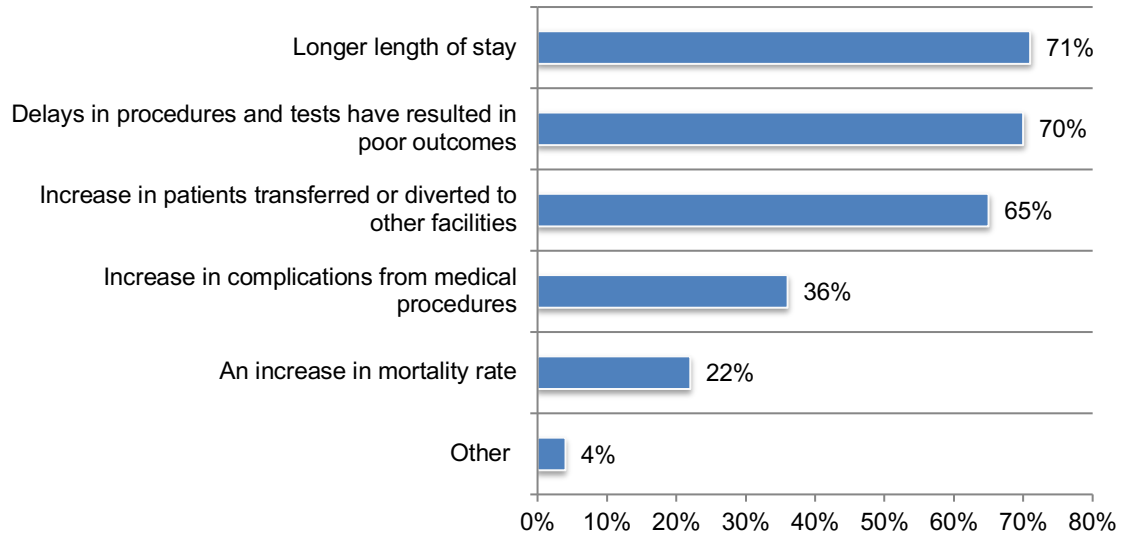
Sponsored by Censinet, Ponemon Institute surveyed 597 IT and IT security professionals in Healthcare Delivery Organizations (HDOs). In the context of this research, HDOs are entities that deliver clinical care and rely upon the security of third parties with whom they contract services and products. These include integrated delivery networks, regional health systems, community hospitals, physician groups, and payers.

Ransomware attacks on healthcare organizations can be a life-or-death situation.
The onset of COVID-19 introduced new risk factors to HDOs, including remote work, new systems to support it, staffing challenges, and elevated patient care requirements. There's been a great deal of media coverage on the rise of cyberattacks such as ransomware both within the healthcare industry and beyond. This research focuses on the healthcare industry to understand the extent to which HDOs are being targeted and ascertain the impact of those attacks. Both are covered in-depth in the key findings section of the report.

Over the last two years, 43 percent of respondents say their HDOs experienced a ransomware attack. Of these respondents, 67 percent of respondents say their HDO had one and 33 percent of respondents say they experienced two or more.

As shown in Figure 1, these attacks risk patient safety, data, and overall care availability. Respondents report that ransomware attacks had a significant impact on patient care, reporting longer length of stay (71 percent of respondents), delays in procedures and tests (70 percent of respondents), increase in patient transfers or facility diversions (65 percent of respondents) and an increase in complications from medical procedures (36%) and mortality rates (22%).

Figure 1. What impact does ransomware have on patient care?
More than one response from the 43 percent of respondents in HDOs that had a ransomware attack.



HDOs forecast that the number of contracted third parties will increase by 30 percent over the next 12 months

Driven by cost containment, regulatory directives and the demand for accessible, higher-quality patient care, HDOs have shifted to the digitization and distribution of health information. Moreover, medical devices, whether in patient rooms or labs, rely on network connectivity for operations and maintenance.

Nearly all of the technology components described are not developed by the HDO. These include software, services, and hardware development from organizations known as **third parties**. This study revealed that the average number of third parties that organizations contract with is 1,950, and this will increase to an average of 2,541 in the next 12 months.

Third-party products and services are a necessary and critical part of the HDO IT blueprint, but each brings another set of risk factors to the table. Some risks are inherent to the third party such as secure operating systems and other software in medical devices. Other risks involve how the HDOs deploy and use third parties, including storing protected health information (PHI) on cloud-based systems that weren't meant to support it. In either case, the risk created by the third party or the HDO use of the third party needs to be managed. The burden is on the HDO to perform assessments throughout their relationship with the third party (e.g., procurement, implementation, usage, updates, termination, etc.).

Third-Party Risk Management is Hard, and COVID-19 Made it Worse

This research also looks at the capabilities and maturity of HDOs to manage third-party risk, both before and during COVID-19. According to only 44 percent of respondents, controls critical to assessing third-party risks are only partially accomplished in HDOs. Only 40 percent of respondents say their organization always completes a risk assessment of its third parties prior to contracting with them. However, 38 percent of respondents state the assessment findings are ignored by leaders.

Re-assessments are another critical part of third-party risk management and are not conducted as often as required. More than half (53 percent) of respondents say re-assessments are conducted only on-demand or on no regular schedule.

Recommendations for Mitigating Ransomware and Third-Party Risks

According to the findings, healthcare organizations are less prepared to deal with third-party risks. Following are recommended steps for HDOs to take to protect patient safety, data, and care operations.

- Invest in workflow automation, resources, and processes to establish a digital inventory of all third parties and PHI records. An HDO must know the number and location of PHI records that are accessed, transmitted or stored by third-party products or services.

- Increase overall risk coverage of third parties by leveraging automation to conduct more assessments. The average number of third parties that organizations contract with is expected to increase from 1,950 to 2,541 over the next 12 months. However, only 40 percent of respondents say their organizations always complete a risk assessment prior to engaging with a third party. If their organizations conduct an assessment, only 38 percent of respondents say their leaders always accept their recommendation not to contract with them.

- Allocate resources and funding to re-assess high-risk third parties. Currently, only an average of 32 percent of critical and high-risk third parties are assessed annually, and only an average of 27 percent of these third parties are re-assessed annually.

- Increase efforts to secure medical devices. Only 36 percent of respondents say their organizations know where all medical devices are. Only 35 percent of respondents say they know when a medical device vendor's operating device is end-of-life or out-of-date. Only 29 percent of respondents say they know the non-planned expense of medical device operating system patches.

- Ensure critical steps for identifying and mitigating third-party risks are in place. Sixty percent of organizations represented in this research had a data breach in the past two years, resulting in an average of 28,505 records containing sensitive and confidential information compromised. According to the research, organizations can only partially evaluate the various threats targeting their assets and IT vulnerabilities. They also lack the capability to continuously monitor vendor risks.

- Assign risk accountability and ownership to one role. The ability to execute an enterprise-wide risk management strategy is affected by not assigning accountability and ownership to one role.

To receive a free copy of the entire, 43-page report, please send an email to info@censinet.com or visit censinet.com/ponemon-report-covid-impact-ransomware.

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or call at 1.800.887.3118.

Ponemon Institute
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

About the Sponsor

Censinet, based in Boston, MA, enables healthcare organizations to take the risk out of their business with Censinet RiskOps™, the first and only cloud-based exchange that integrates and consolidates enterprise risk management and operations capabilities across critical clinical and business areas.

RiskOps builds upon the Company's foundational success with third-party risk management (TPRM) for healthcare. Censinet transforms healthcare risk by increasing productivity and operational effectiveness while eliminating risks to care delivery, data privacy, and patient safety.

Find out more about Censinet and its RiskOps platform at censinet.com or email us at info@censinet.com.