September 28, 2022

TLP White

This week, Hacking Healthcare begins by examining an SEC enforcement action taken against Morgan Stanley for serious and extensive failures to protect consumer data. We break down what happened and what healthcare organizations can learn from the incident. Next, we break down a new report on healthcare cybersecurity that has some surprising and distressing findings on how malicious cyber activity impacts patient care. Finally, we provide another brief reminder of the resourcefulness and adaptability of malicious cyber actors, and why it's important to always remain vigilant. Welcome back to *Hacking Healthcare*.

1. **SEC Penalty Against Morgan Stanley Highlights the Importance of Proper Data Disposal**

   The Securities and Exchange Commission (SEC) recently levied a penalty of $35 million against Morgan Stanley for "extensive failures" to safeguard customer data over a prolonged period.[1] While Morgan Stanley may be a financial sector entity, the SEC's purview extends to the healthcare sector, and this regulatory action highlights the importance of not just securing but also disposing of sensitive information.

   While the SEC cited multiple elements, one of the more egregious appears to be the "improper disposal of thousands of hard drives" that ended up being auctioned off with Morgan Stanley customer data still intact.[2] In many cases the data on these hard drives was unencrypted, despite the fact that encryption was a feasible option. In total, the SEC alleges that roughly 15 million customers had their data exposed.[3]

   Ars Technica reports that the improper disposal of hard drives appears to have been due to Morgan Stanley trusting a "moving company" with little or no expertise in IT or proper data disposal to "decommission" roughly 1,000 hard drives and thousands of backup tapes from a Morgan Stanley data center.[4] This moving company apparently contracted out that work for a time before eventually just selling them off to be auctioned. Morgan Stanley was apparently not made aware and did not approve any of these contractor/subcontractor involvements.[5] Morgan Stanley was made aware of the incident after a consultant who had purchased some of the hard drives found the data and reported it.

   ### *Action & Analysis*

   Included with H-ISAC Membership

2. **New Report Underscores Cyberattack Risk to Patient Care**
   A new report that surveyed over 600 IT and IT Security practitioners in the healthcare sector has produced some alarming facts and figures on the healthcare cyber threat landscape and the various costs cyberattacks have levied on the sector. In particular, the study's findings on the impact cyberattacks have had on patient care are a continuing cause for concern.

   The Ponemon Institute report *Cyber Insecurity in Healthcare: The Cost of and Impact on Patient Safety and Care* was sponsored by enterprise security company Proofpoint, and its broad scope assesses the cyber threat landscape and the impacts of malicious cyber activity in the healthcare sector. While its 50 pages contain many useful insights and data points, the report's section on how cyberattacks have impacted patient care paints a bleaker picture than many might assume.

   While ransomware may regularly steal the headlines, and 67% of respondents agreed that ransomware attacks had disrupted patient care, the number of respondents who cited supply chain attacks (70%), BEC/spoofing attacks (67%), and cloud compromises (64%) is noteworthy.[6] The disruptions caused included "delays in procedures and tests that have resulted in poor outcomes, longer length of stay, increase in patients transferred or diverted to other facilities, increase in complications from medical procedures and an increase in mortality rate."[7]

   Action & Analysis
   Included with H-ISAC Membership

3. **HHS Warns of Widespread Monkeypox ... Phishing Attacks**
   Monkeypox may not be quite the headline grabber it was a few months ago, but a recent sector alert from the U.S. Health and Human Services (HHS) Health Sector Cybersecurity Coordination Center (HC3) is warning that Monkeypox is being weaponized by malicious actors much in the same way that COVID-19 has been.[8]

   The September 19th alert details a malspam campaign that is currently targeting healthcare providers and relies on curiosity or anxiety over the disease to drive recipients to open PDFs with malicious links.[9] The alert contains screenshots of the fraudulent emails, known IOCs, and patches, mitigations, and workarounds.

   Action & Analysis
   Included with H-ISAC Membership

Congress -

Tuesday, September 27th:
- No relevant hearings

Wednesday, September 28th:
- No relevant hearings

Thursday, September 29th:
- No relevant hearings

International Hearings/Meetings -

- No relevant meetings

EU –

Monday, October 10th:

- 7th eHealth Security Conference (ENISA)

Conferences, Webinars, and Summits

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

About the Author

Hacking Healthcare is written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, and as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST) and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

---

[1] https://arstechnica.com/information-technology/2022/09/morgan-stanley-pays-35m-penalty-for-extensive-failure-to-safeguard-customer-data/

[2] https://arstechnica.com/information-technology/2022/09/morgan-stanley-pays-35m-penalty-for-extensive-failure-to-safeguard-customer-data/

[3] https://arstechnica.com/information-technology/2022/09/morgan-stanley-pays-35m-penalty-for-extensive-failure-to-safeguard-customer-data/

[4] https://arstechnica.com/information-technology/2022/09/morgan-stanley-pays-35m-penalty-for-extensive-failure-to-safeguard-customer-data/

[5] https://arstechnica.com/information-technology/2022/09/morgan-stanley-pays-35m-penalty-for-extensive-failure-to-safeguard-customer-data/

[6] https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf

[7] https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf

[8] https://www.hhs.gov/sites/default/files/monkeypox-themed-phishing-campaign-sector-alert.pdf

[9] https://www.hhs.gov/sites/default/files/monkeypox-themed-phishing-campaign-sector-alert.pdf