COSMOS
Navigate the Compliance Universe

Compliance Today - April 2022
Ransomware response thoughts for the board

By Jan Elezian, MS, RHIA, CHC, CHPS


Jan Elezian

Jan Elezian (jan.elezian@sunhawkconsulting.com) is a consultant and Director at SunHawk Consulting LLC.

- linkedin.com/in/jan-elezian-30821011/

As your organization's HIPAA privacy and security officer, you cited a report by Cybersecurity Ventures stating a business is expected to fall victim to a ransomware attack every 11 seconds.[1] Cyberattacks occurs when malicious software is used to restrict access to a computer system or data until the victim pays ransom requested by the criminal. You have provided the board with the Office for Civil Rights (OCR) cybersecurity ransomware guidance material published July 11, 2016,[2] and have discussed how to lower risks of a cyberattack.

Most corporate boards have discussed hacking and its aftermath as part of meeting agendas according to the Q2 2021 CNBC Global CFO Council survey.[3]

The recent OCR Privacy List letter[4] reminds organizations to promptly report any cybersecurity incidents to the Federal Bureau of Investigation (FBI). The FBI officially recommends that organizations not give in to ransom demands[5] but off the record may tell you to pay the ransom if you cannot go without the data. However, there is no guarantee that criminals will restore the data after receiving payment or that they won't come back for more.

Cyber insurance also isn't a guarantee that organizations will get their money back. Restrictions in policies may restrict reimbursement, particularly if negligence is determined. Ransomware cyber insurance is typically an add-on to a cyber liability policy. It is important to notify your insurer before paying a ransom; otherwise it may not be covered.

Hackers like being paid in Bitcoin. Since 2013, criminals have assumed that Bitcoin was anonymous and untraceable.[6] Bitcoin is the cryptocurrency most popular and accessible, but it is not completely untraceable. Even though identities can be hidden, at some point Bitcoin will be exchanged for real money. This can only be done with proof of identity.

Criminals tend to keep the demands low and at an amount an organization is willing to pay quickly. In the second quarter of 2021, the average ransom payment reported was $136,576.[7] Yet, "seven-figure demands are not uncommon. Security experts say that even these numbers underestimate the true cost of ransomware attacks, which have disrupted factories and basic infrastructure and forced businesses to shut down."[8]

Bitcoin can be purchased through cryptocurrency exchanges, stockbrokers, or even Bitcoin ATMs. Beware of risk: Bitcoin is speculative and much more unpredictable than traditional investments like stocks, bonds, or mutual funds.

Be prepared for all circumstances, but in the end, it's a business decision on whether to pay the ransom.

1 "2022 Must Know Cyber Attack Statistics and Trends," Business Advice & Research, Embroker, January 31, 2022, https://bit.ly/34L4m96.
2 U.S. Department of Health & Human Services, Office for Civil Rights, "Ransomware and HIPAA," fact sheet, July 11, 2016, https://bit.ly/30yclh9.
3 Eric Rosenbaum, "What do companies think when hacker's demand ransom? Time to pay," CNBC CFO Council, last updated July 1, 2021, https://cnb.cx/3JaMXpt.
4 Xavier Becerra, "On the Urgent Need to Remain Vigilant Against Cybersecurity Threats," letter to the HPH Sector, December 30, 2021, https://bit.ly/3BfrR6p.
5 "Ransomware," Common Scams and Crimes, Scams and Safety, Federal Bureau of Investigation, accessed February 9, 2022, https://bit.ly/3HJHdTp.
6 Nicolas Martin, "Why hackers rely on Bitcoin for ransom payments," Deutsche Welle, July 9, 2021, https://bit.ly/34NFhuA.
7 Steve Alder, "The Average Ransomware Payment Fell by 38% in Q2, 2021," *HIPAA Journal*, July 27, 2021, https://bit.ly/3ozlR3s.
8 Scott Ferber and Phyllis Sumner, "Ransomware: To Pay or Not to Pay?" JD Supra, October 15, 2020, https://bit.ly/3gzfFUA.