COSMOS
Navigate the Compliance Universe

# Report on Patient Privacy Volume 20, Number 8. August 06, 2020 Ransomware Incident Security Tips

By Jane Anderson

To manage a ransomware incident, Sanjay Deo, 24By7Security Inc. president and founder, recommended the following to health care entities.

- Understand the process and your organization's role in it. The first call to make following a breach or a ransomware notification is to the insurance company, Deo said. "This is very akin to a property casualty incident," he said. "Then from there, the adjuster basically takes over," and attorneys, forensics, analysts, Bitcoin experts and restoration experts all may become involved. Insurance should pay for all of that, assuming the organization has proper coverage. From there, experts will advise the organization on what to do next, particularly whether or not to pay the ransom.

- Have reserves to spend on ransomware expenses, particularly if your organization does not have breach insurance. "You still have to negotiate with the hackers that perpetrated the crime," Deo said. "The only thing is, you don't have a fallback for all of the expenses, including the ransom. So the company needs to have reserves to spend in all of this."

- Assume payment must be made in Bitcoin, and be prepared for that if you decide to pay the ransom. Bitcoin is an untraceable payment method, which makes it impossible to see where the money is going.

- Realize that hackers may act reasonably, despite their criminality. Deo described one situation where a company had been hacked and paid the ransom. A few months later, they were hacked again, but by a different bad actor. They called the insurance company, and the insurance company contacted the hackers with screenshotted proof of the previous ransom payment, and the hackers apologized for the hack, saying they hadn't known about the prior ransom payment and that they would leave the company alone for a while, Deo said.

- Decide whether to negotiate with the hackers and whether to pay the ransom. The answers to these questions will depend on whether the organization has good backups or not, Deo said. "This is why you need the CEO, the chief financial officer and the board all engaged in this negotiation," Deo said. "If you have good backups, then the answer is very clear: You basically don't pay and you restore from backup." However, if the hackers realize you're planning to do this, they may get more aggressive, he said. For example, in one situation on which Deo consulted, hackers saw that the organization was trying to restore via its backups and increased the ransom demand by 50%, he said.