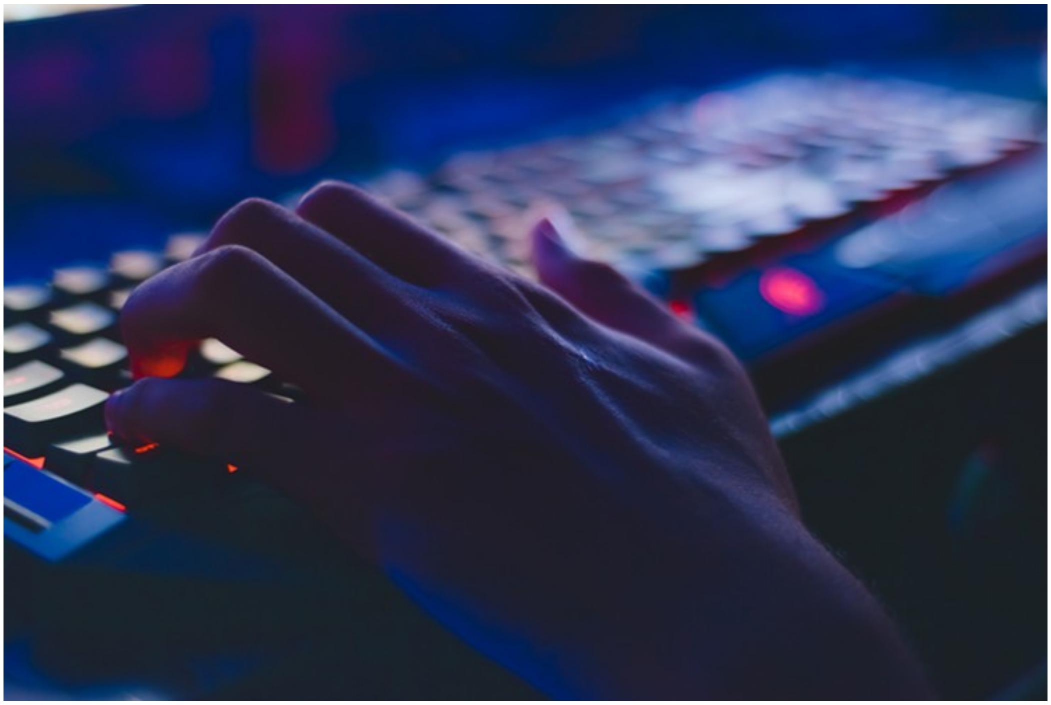
MIAMI New Times®



Miami healthcare providers could be at risk of cyber attacks. / **Photo by Soumil Kumar/Pexels**

Cyber Attacks Are Just Another Problem for Miami Hospitals to Worry About Right Now

ALEXI C. CARDONA | MAY 7, 2020 | 8:00AM

Healthcare systems across the United States are overwhelmed by a lot of things right now – sick and dying patients, equipment shortages, overworked medical staff, and more.

If that's not enough, the FBI and Interpol have warned that hospitals are at increased risk of experiencing a range of cyber attacks, including hacks of medical records and attacks involving ransomware – software designed to lock a computer system until a ransom is paid to restore access.

Miami cybersecurity experts say it's imperative for health systems to double down on their security efforts, especially because medical equipment can be particularly vulnerable to cyber attacks and patient records are among the most lucrative documents on the dark web.

"Healthcare organizations have always been at risk," says Franklin Mesa, lead instructor at Miami Dade College's Cybersecurity Center of the Americas. "But now because of COVID-19, everyone is vulnerable because they're so busy. They can get caught with their pants down, so to speak."

Medical information is worth much more than Social Security or credit card numbers alone. Such records contain a treasure trove of personal information that can be used to commit medical identity theft, allowing the wrong person to seek medical care or prescription medication under someone else's name, fabricate insurance claims, or fraudulently apply for Medicare or Medicaid.

When health records are encrypted, cyber attackers might not be able to see all the contents, Mesa says. In that case, ransomware attacks could prove more profitable.

"[Cyber attackers] know the documents are so sensitive to organizations, that they're pretty sure they're going to pay for them," Mesa says. "So they may not have access to the information, but they could hold it hostage and say, 'Pay me to get this back.'"

Even if a hospital or doctor's office takes steps to prohibit unauthorized access to its systems, a cyber attacker could encrypt the records and lock out administrators.

"[The health system] has a lockbox. And the attackers lock the lockbox inside their own lockbox," Mesa says.

Being locked out of patient records could give a hospital no choice but to use pen and paper to make important medical notes until – or if – access is restored. A hospital could be forced to pay a ransom or risk losing its patients' medical histories.

The FBI doesn't recommend paying a ransom in response to a cyber attack because payment doesn't guarantee restoration of access. Nevertheless, ransomware victims paid more than $140 million to cyber attackers between 2013 and 2019.

According to the U.S. Department of Health and Human Services' Office for Civil Rights, this year more than 75,000 Floridians have been affected by healthcare data breaches that are still under investigation. Most cases stemmed from one breach at NCH Healthcare System based in Naples – a hacking incident that impacted 63,581 patients.

Michael Garcia, Jackson Health System's chief information officer, says that while the hospitals are on high alert for increased hacking or fraudulent activity related to the pandemic, Jackson has always been proactive about strengthening and optimizing its security. And he says Jackson's IT team has tools that analyze the activities and behaviors of all the devices on its networks.

"I know the traffic every device should have based on historical trends and patterns," Garcia says. "So when I notice something different – if a device is doing something at 2 in the morning that it's never done before – we can determine whether that machine might be vulnerable or exploited and take it off our network."

Jackson also sends phishing emails internally and uses other forms of social engineering to determine if employees are likely to fall for a scheme and give up their work credentials or other information.

"The key is education," Garcia says. "If they fall for it, we let the person know they've compromised the organization."

Garcia says one of the reasons vigilance in healthcare settings is particularly important is because there's a lot of biomedical equipment that doesn't get updated as frequently or easily as, say, a smartphone. A few years ago, a portable x-ray machine at Jackson that wasn't kept up to date became infected by a ransomware-type virus, Garcia says.

When IT looked into what happened, it turned out to be a WannaCry ransomware attack, which spread swiftly across hundreds of thousands of computer networks worldwide in 2017.

The x-ray machine was never at risk of being accessed for information, Garcia says, but the incident shows how some pieces of medical equipment are vulnerable to viruses because they're not updated constantly. Even life-saving equipment like ventilators could be vulnerable if they're not kept up to date, Garcia says. And cyber attackers targeting healthcare providers know that medical equipment and software can't be constantly updated.

"Hackers realize that," Garcia says. "The reason they'll encrypt anything vulnerable is to hold it for ransom hoping it contained something of value which an organization is willing to pay the ransom to have it decrypted."

Still, Garcia says Jackson has long been preparing for what could come in the way of cyber attacks and feels confident in its security measures.

Jorge Rey, chief information security officer for the accounting and consulting firm Kaufman Rossin, says his concerns lie more with smaller healthcare providers than large hospital systems.

"Smaller healthcare providers are the ones that don't necessarily have the budget to have a more dedicated security function in their environment," Rey says.

He says the possibility of hospitals experiencing some kind of cyber attack or data breach is absolute. The question is what extent and impact such a breach will have. Larger healthcare systems likely have the necessary tools and investment in security to quickly recover from an attack.

"Smaller organizations can be devastated," Rey says.

Paying a ransom for locked medical records could ruin a smaller healthcare provider. While many organizations are forced to make tough financial decisions at the moment, Rey says now isn't the time for any healthcare provider to roll back its security budget. And if security wasn't high on the list of priorities, it should be now.

"I think it's time to assess what your exposure is," Rey says. "If something bad happens, the impacts would be catastrophic, and right now companies can't afford to handle catastrophic incidents. Invest in security. If you haven't looked into it, I think it’s a good time to start."

RELATED TOPICS: NEWS NEWS HEALTH TECHNOLOGY