STRATEGIC MANAGEMENT SERVICES

Health Care Sector is the Top Target of Cybercriminals

Richard P. Kusserow | April 2024

10 Cybersecurity Tips

Authorities report increasing ransomware attacks aimed at the healthcare sector, and the FBI's Internet Crime Complaint Center (IC3) issued an Internet Crime Report that describes the level of ransomware attacks that target critical infrastructure in the United States. All sectors of the economy are targets, including healthcare, financial, banking, transportation, manufacturing, agriculture, trade, retail, construction, mining, insurance, education, utilities, energy, technology, food services, and real estate. However, the healthcare sector is at the top of the list for ransomware attacks. The FBI reported receiving more reports in 2023 of ransomware attacks targeting the healthcare sector than any other area, with over 20% of the ransomware directed in this area. The FBI noted that this statistic underscores the growing threat cybercriminals pose to the nation's healthcare infrastructure and the safety and security of vital medical systems and patient data. It has been reported that nearly half of health care IT professionals have experienced a ransomware attack in the past two years.

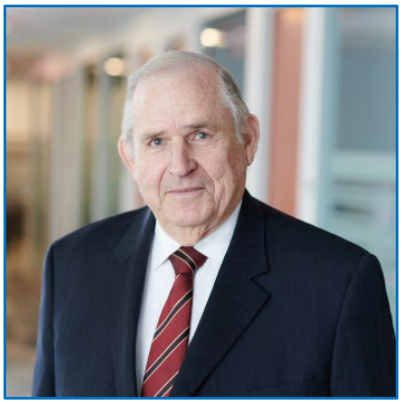
The simple reality is that health care providers, especially those involved in acute care, are attractive to cybercriminals because their data is critical to patient care. Without that information, decisions about needed actions and patient care are put at immediate risk. In short, cybercriminals view hospitals as good targets because they know that many will pay to restore their systems, and patient records are valuable on the dark web. Another factor making healthcare vulnerable, and a prime target is that many in the sector lack sound controls to prevent attacks, unlike other areas, such as the banking and financial sectors. When cybercriminals take control of their data and systems, it creates desperate conditions ideal for extortion. As a result, victims commonly succumb and pay enormous ransom demands to regain control of vital data.

Mitigating Risks of Cyber Attacks

This is a reminder of the need for enhanced cybersecurity measures and greater vigilance in safeguarding sensitive medical data and essential healthcare services from malicious cyber threats. To attack systems, cybercriminals need to access them. Therefore, healthcare entities must bolster their defenses and implement robust cybersecurity protocols to mitigate the risks of ransomware attacks. The following are steps that healthcare organizations should ensure are in place to mitigate risks of attacks on their organization's systems:

1. Enable multi-factor authentication for all email accounts;
2. Verify all payment changes and transactions in person or via a known telephone number;
3. Educate employees about identifying phishing emails and responding to suspected messages;
4. Prohibit the automatic forwarding of emails to external addresses;
5. Add an email banner to messages coming from outside your organization;
6. Prohibit legacy email protocols that circumvent authentication;
7. Ensure changes to mailbox login and settings are logged and retained for at least 90 days;
8. Enable alerts for suspicious activity, such as foreign logins;
9. Enable security features that block malicious emails; and
10. Implement anti-phishing and anti-spoofing policies.

You can also keep up-to-date with Strategic Management Services by following us on **LinkedIn**.



About the Author

Richard P. Kusserow established Strategic Management Services, LLC, after retiring from being the DHHS Inspector General, and has assisted over 2,000 health care organizations and entities in developing, implementing and assessing compliance programs.