Cyber Attacks Threaten Health and Safety

By Sai Huda, author, Next Level Cybersecurity

The healthcare care sector has become a key target for cyber attackers. Take the recent case of a U.S. hospital that suffered a ransomware attack that froze all computer systems. All systems, schedules, documents and patient data became unavailable. Patients requiring urgent care had to be transferred to another hospital.

As the hours went by, the hospital realized it could not be down for much longer, otherwise patients could die. So the hospital decided to pay the ransom to avoid loss of patient life and regain operations.

It is not only the patient data that the attackers are after, it is also extracting a ransom because the bad actors have realized that with ransomware they can instead disrupt operations and hold hostage patient health and safety until money is paid.

Take the case of NHS England in the U.K., a few years ago, that fell victim to the WannaCry ransomware attack. In my book, Next Level Cybersecurity: Detect The Signals, Stop The Hack, I cover this case in detail, along with several other healthcare cases, such as Anthem in the U.S. and SingHealth in Singapore.

In the book, I show how the ransomware disrupted NHS England, impacting patient health and safety. Had a security researcher not discovered a "kill switch" the same day the ransomware propagated, the ransomware could have caused further damage, leading to possible deaths.

The book shows what a cyber attack chain is and reveals the common signals to look for to detect the attacker or the ransomware itself in a timely manner, regardless of whether you are a healthcare organization or other type of entity.

Bad actors such as organized crime groups and rogue nation-states are going after the healthcare sector with more cyberattacks than ever before.

Here are some metrics for the healthcare sector:

- According to Health IT Security, the average cost of a data breach per organization is $2.2 million.
- Per IBM Security and Ponemon Institute, the cost of a data breach per record rose to $408 in 2018 from $380 in 2017. This is the highest cost per record among all sectors.

And now, ransomware has become a key threat to the healthcare sector, in addition to theft of patient data for sale in the dark web or for espionage or blackmail purposes by a rogue nation-state.

The U.S. Department of Health and Human Services (HHS) in partnership with the healthcare sector and the Health Sector Coordinating Council in December 2018 issued the publication ***"Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients."***

This publication sets the bar for the healthcare sector by providing practical, understandable, industry-led, cybersecurity best practices to manage cyber risk for small, medium and large healthcare organizations:

- Small: 1 -10 physicians for a practice or 1-50 beds for a hospital.
- Medium: 11-50 physicians for a practice or 51-299 beds for a hospital.
- Large: Over 50 physicians for a practice or over 300 beds for a hospital.

It is a model based on the NIST Cybersecurity Framework, comprised of risk mitigation best practices mapped to five key threats and vulnerabilities specific to the healthcare sector, broken out by small medium and large entity. The five key threats are:

- E-mail phishing attack
- Ransomware attack
- Loss or theft of equipment or data
- Insider, accidental or intentional data loss
- Attacks against connected medical devices

There are 5,000 hospitals in the U.S. alone, and all healthcare organizations must be proactive and not get caught by surprise by either a cyberattack or a HHS audit or patient class-action lawsuit. The stakes are too high.

A regulatory audit or patient class-action lawsuit discovering non-compliance can be costly, but a cyberattack will be even more costly. So what can healthcare organizations do now? Take the below five minute, five question risk assessment. If you answer No to any of the questions, you have unmitigated risk and must take action immediately.

Healthcare Organization Five Minute Risk Assessment

1. Have you performed a self-assessment, comparing the cybersecurity best practices relevant for your size organization and risk profile, to your current practices, to identify gaps and blind spots, and implemented an action plan to adopt missing practices and mitigate exposures? Yes No

2. Have you trained your entire organization on the cybersecurity best practices you have adopted for your particular organization, beyond basic security awareness, so that the training is relevant and effective? Yes No

3. Are you performing ongoing Crown Jewels Threats and Vulnerabilities Risk Assessment, to make sure you have captured all mission-critical cyber assets and systems, but also you have mapped to threats, vulnerabilities and risk mitigation, including monitoring for signals of cyber attackers trying to get to the Crown Jewels, and reporting results to the board for ongoing oversight? Yes No

4. Are you performing ongoing Medical Devices Threats and Vulnerabilities Risk Assessment, to make sure you have captured all connected medical devices, but also mapped to threats, vulnerabilities and risk mitigation, including monitoring for signals of cyber attackers trying to exploit the devices, and reporting to the board for ongoing oversight? Yes No

5. Have you performed a ransomware simulation and table top exercise, including involving your board, to identify vulnerabilities, gaps and blind spots and developed a risk mitigation plan to plug holes and mitigate the threat and risk from a ransomware attack and an effective response plan to prevent any adverse impact? Yes No

About the Author

Sai Huda is a globally recognized risk and cybersecurity expert, technology visionary and business leader, with more than 20 years of hands-on experience.

He is the best-selling author of the game-changing book, ***Next Level Cybersecurity: Detect The Signals, Stop The Hack***. It is a book like no other. It is based on intensive reviews of the world's largest data breaches and ransomware attacks and reveals the secret to cybersecurity success – detect cyber attackers' signals early.

The book shows what those signals are and how to detect them in time to prevent loss or damage.

He served seven years as General Manager, Risk, Information Security and Compliance Solutions at Fidelity National Information Services, Inc. (FIS), a Fortune 500 company serving more than 20,000 clients globally. Under his leadership, FIS attained number 1 ranking in Chartis RiskTech100®.

Prior to FIS, he was the founder and CEO of Compliance Coach, Inc., an innovative company providing risk management software and consulting services to more than 1,500 clients in financial services, healthcare and government sectors. Compliance Coach helped clients manage Information Security, Operational and Compliance risks. Compliance Coach was acquired by FIS.

He serves as an expert consultant to boards and executives on risk and cybersecurity best practices. He is also a frequent keynote speaker at industry conferences. To find out more, visit the author's website at www.saihuda.com. To obtain his book, ***Next Level Cybersecurity***, please visit Amazon.