The New Face of Cybersecurity

How digital technology is transforming cybersecurity in healthcare

In recent years the healthcare industry has undergone a digital revolution. The replacement of paper files with electronic medical records is just one aspect. Many medical procedures and devices now rely on digital technology.

While this digital evolution has resulted in significant improvements in the efficiency and effectiveness of treatment, there continues to be pressure to actively manage costs as provider profit margins are forecast to fall by as much as 2% in 2019. As such, hospital executives are increasingly considering partnerships with medical technology companies to curtail costs and drive efficiency.[1]

On the other side of the coin, the use of websites and mobile applications has also made healthcare providers increasingly vulnerable to hackers. Data breaches, data manipulation and systems control are three of the biggest cyberthreats the healthcare industry is facing today.

Secure your data

As technology evolves, the healthcare industry, like so many industries, is at risk for data breaches. But because of the sensitive nature of their data, healthcare organizations need to be especially vigilant in their cybersecurity efforts.

The majority of data breaches are caused by malicious or criminal attacks. They are increasing in frequency, there were 503 domestic healthcare breaches in 2018 impacting 15 million patient records, triple the 2017 count.[2] They're also costly. In 2018, the average cost incurred for each stolen record in the healthcare industry was $408, nearly three times the cross-industry average of $148.[3] But the biggest consequence to healthcare organizations that experience a data breach is the loss of customer trust, which may never be recovered.

The healthcare industry is an attractive target for hackers, who can seize large batches of personal data for medical fraud. Stolen patient data—names, birth dates, policy numbers, diagnosis codes and billing information—can all be easily sold. Fraudsters use the data to create fake IDs with which they can purchase medical equipment or drugs to resell for cash. Or they can combine a patient number with a false provider number and file fraudulent claims with insurers.

Apply multiple layers of protection

As in most things, prevention is far better than the cure. Employee training can be incrementally helpful toward reducing the probability of data theft. Policies and procedures need to be put in place to eliminate vulnerabilities and verify patient identities. However, technology and automation are necessary to have a more meaningful widespread impact on data theft.

For example, the intelligence currently exists to assess the devices used to access data. This can be extremely effective as an initial layer of defense, since, when implemented properly, it's frictionless and undetectable from a user perspective. Once a device has been successfully assessed, additional authentication layers can be applied.

A good next step might be two-factor authentication, which is an industry standard for verifying patient identity such as name and date of birth. Using three or four factors such as adding home address is even more effective.[4]

The right technology must be employed to deter hackers. A data technology partner can help healthcare providers establish and maintain the highest level of cybersecurity.

In 2018, the average cost incurred for each stolen record in the healthcare industry was $408, nearly three times the cross-industry average of $148.[3]

Prevent data manipulation

To date, cybersecurity for the healthcare industry has revolved around safeguarding data. But the possibility for an even more malicious type of cyberthreat exists—data manipulation.

Imagine the possible consequences if a hacker gains access to a hospital system and changes patient data, such as lab results. Doctors reading false information could make an incorrect diagnosis or prescribe the wrong medication.

Data manipulation can also happen to any connected medical device with embedded web services including pacemakers, defibrillators, insulin pumps and neuro-stimulators. Those devices, which feed digital data directly to patient medical records, are vulnerable to hackers and could also provide an access point to systems at large.

No one can dispute the value of technological innovations that improve the quality of patient care. But often security of that technology is an afterthought. That needs to change. Existing medical equipment must be better protected and security must become part of the design and development of future healthcare technology.

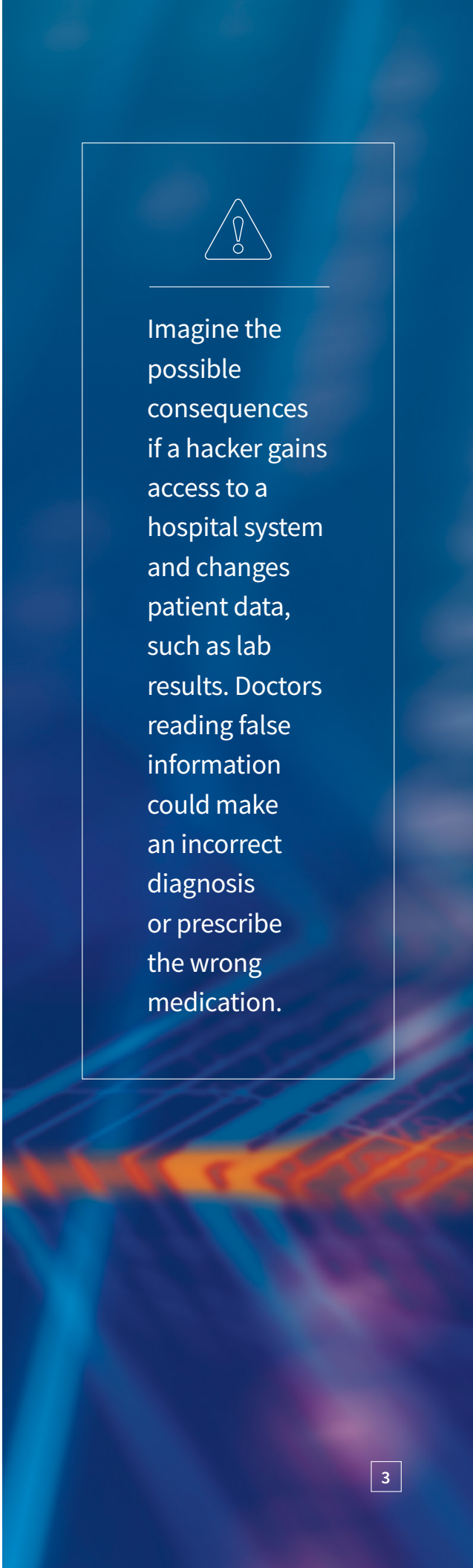
Combat the rise of ransomware

The latest cyberthreat to healthcare organizations is ransomware. A form of malware, it doesn't steal data. Rather it encrypts it so that users are essentially locked out of their own system. What's most concerning is that the attack can be initiated from something as simple as an employee clicking on an infected email link or opening an attachment in a seemingly legitimate email.

For healthcare providers, unavailable data poses serious risks. It disrupts their ability to treat patients. Business operations grind to a halt until the system is restored or replaced.

According to recent research, 78% of providers reported that they experienced a healthcare ransomware or malware attack in 2017.[5]

Typically, the hacker demands monetary compensation to provide the decryption key. Whether the victimized organization is at the mercy of the hacker and must pay up largely depends on what precautions were taken prior to the attack.



Imagine the possible consequences if a hacker gains access to a hospital system and changes patient data, such as lab results. Doctors reading false information could make an incorrect diagnosis or prescribe the wrong medication.

Changing the cybersecurity culture

Most healthcare organizations are reactive. Only if a cybersecurity event occurs do they take action. Unfortunately, by that time the damage may already be done.

Instead, healthcare organizations need to become proactive in safeguarding their data and protecting company resources. Patch and pray is not an effective strategy!

Management must change the corporate culture from "if we get hacked" to "when we get hacked" and take all possible measures of protection.

An experienced, trusted data partner can provide an array of technology solutions that help organizations reduce costs and improve efficiency with frictionless account origination and login processes. The right data partner can also concurrently identify vulnerabilities, fend off hacking and adequately respond to a successful cybersecurity attack.

For more information, call 866.396.7703 or visit
risk.lexisnexis.com/healthcare/provider

LexisNexis® RISK SOLUTIONS | Health Care

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

Our healthcare solutions combine proprietary analytics, science and technology with the industry's leading sources of provider, member, claims and public records information to improve cost savings, health outcomes, data quality and compliance and minimize exposure to fraud, waste and abuse.

[1] https://www.mckinsey.com/business-functions/operations/our-insights/creating-beyond-the-product-partnerships-between-providers-and-medtech-players
[2] https://digitalguardian.com/blog/breached-healthcare-records-tripled-2018
[3] https://healthitsecurity.com/news/healthcare-data-breach-costs-remain-highest-among-industries
[4] https://www.healthleadersmedia.com/clinical-care/6-best-practices-patient-identification
[5] https://healthitsecurity.com/news/78-of-providers-report-healthcare-ransomware-malware-attacks