RSA

WHITE PAPER

DIGITAL RISK IN HEALTHCARE TODAY

Digital transformation is a top priority across every sector of the dramatically changing healthcare industry. Rapidly emerging digital technologies are being used by healthcare organizations and healthcare-related businesses to improve patient care, compete more effectively, comply with regulations, protect sensitive electronic patient data and manage costs. As a result, healthcare providers (doctors and hospitals), insurance companies, pharmaceutical companies, medical device manufacturers, ambulatory services providers, biotech companies, health informatics companies and third parties are all examining how best to apply these technologies in their own operations. In addition, merger and acquisition (M&A) activity has also grown over the last ten years, complicating digital transformation as similar and dissimilar organizations merge and adopt new technologies.

Today, increasing complexity is a hallmark of healthcare organizations and their delivery models, external networks of partners and patient providers, insurance reimbursement models and regulatory requirements. This complexity is creating new and often unexpected risks, especially when coupled with the technology advancements and explosion of personal health information (PHI) and electronic health records (EHR).

The results of the RSA Digital Risk Study, included in the 2019 RSA Digital Risk Report, highlight three key risks emerging from digital transformation, all of which are critical in healthcare: the risk of a cyber attack, risks associated with a dynamic workforce and data privacy risk.

Increasing complexity of healthcare organizations is creating new and often unexpected risks, especially when coupled with the technology advancements and explosion of personal health information (PHI) and electronic health records (EHR).

CYBER ATTACK RISK

Cyber threats are the number one risk for healthcare organizations. Healthcare is one of the top two industries most targeted by cyber threats.[1] In 2019, ransomware increased 118%,[2] while over the last two years 90% of healthcare organizations suffered some sort of cyber attack.[3]

Cyber attack risk is a rising concern because of the incredible growth in number and types of medical devices that make up the internet of medical things (IoMT). These smart medical products include wearables, mobile devices, apps, sensors, robotics, monitors, medical equipment, implants and many more, and they comprise a global market that is predicted to top $410 billion by 2020.[4] IoMT devices and systems often lack security controls, which means they create exponentially more opportunities that cybercriminals can exploit. A related reason cyber attack

risk is becoming so prevalent is the availability and amount of healthcare data, especially electronic PHI (ePHI) and EHR, being proliferated and exchanged. In fact, healthcare data has grown an astounding 878% over the last two years.[5] PHI is a particularly high-value target to cybercriminals.

Another factor in cyber attack risk is that healthcare organizations are changing their care delivery models and adopting new technologies in ways that increase their risk. For example, many organizations are in the process of moving from segmented care to value-based or community care, which results in a constant flow of interconnected data throughout the patient life cycle via interoperability between devices and data, increasing ecosystem complexity. As a result, the attack surface is much more expansive and difficult to protect because the security perimeter includes a vastly expanded digital footprint, including multiple organizations, IoMT devices and third parties. And, despite more regulatory oversight and increased security investments, breaches continue to happen because of lax security hygiene in many organizations. This is consistent with the RSA Digital Risk Study finding that even though organizations have digital transformation efforts underway, their risk management practices don't always keep pace.[6]

Many organizations are in the process of moving from segmented care to value-based or community care, which results in a constant flow of interconnected data throughout the patient life cycle via interoperability between devices and data, increasing ecosystem complexity.

DYNAMIC WORKFORCE RISK

The healthcare workforce is changing dramatically. Improving patient care is the primary driver of digital transformation for doctors, hospitals and other providers, and digital technology provides more options for how and where they provide care. Large organizations are putting employees' wellness into their own hands through programs, access and data that allow them to control their own healthcare. As a result, patients are seeking access to information and personal attention around the clock. To support them, physicians and other providers require secure and rapid access to information via mobile and web-based applications and data (including ePHI) stored across multiple online systems. Healthcare workers who serve patients in multiple locations require access to devices and data as they travel, work from home, visit patients or work across healthcare facilities.

The healthcare workforce is also being augmented by technology to help meet the needs of a changing patient population. More patients are seeking care under the Affordable Care Act; at the same time, there is a shortage of physicians and medical workers. A growing number of healthcare facilities have expanded their use of telemedicine to deliver services to patients in hospitals as well as in remote locations.

These are just a few examples of the dramatic disruption to the traditional model in which a patient visits their doctor's office or a hospital to seek medical treatment. The necessary shift to a dynamic, mobile workforce exposes healthcare organizations to the risk of improper worker access and authentication. This is especially concerning when it is also difficult or impossible to effectively monitor the online activities of healthcare providers, third parties, gig workers and others across dozens of IoMT devices.

DATA PRIVACY RISK

There are many different users of data across today's healthcare ecosystem. For example, patients want and have more control over their data and healthcare decisions; by 2020, it's estimated that 25% of all healthcare data will be collected by patients themselves.[7] Health practitioners and medical researchers also leverage data to improve the quality of medical decisions and patient care, such as using artificial intelligence and cognitive solutions in areas ranging from delivery of care to continuous health monitoring. Collaborative care is a delivery model that involves patient data being available across large, complex healthcare environments and accessible to many users from multiple devices and locations.

Healthcare organizations are mandated to protect highly sensitive PHI and EHR, meet HIPAA security and privacy obligations, satisfy ARRA/HITECH "meaningful use" provisions, and comply with DEA Electronic Prescriptions for Controlled Substances (EPCS) authentication and security requirements, among other demands. However, because of the myriad ways and means PHI can be collected, stored and used, it has become infinitely more difficult to protect. And because PHI exists across so many applications, systems and endpoints, it may seem unclear who is responsible for protecting it. Ultimately, it is every healthcare organization's duty to protect that data, and patients are right to demand the confidentiality and integrity of their personal health and medical records.

Without adequate security controls the risk is more than someone's personal data being lost; a patient's well-being can be put at risk if, for example, an attending physician makes a bad treatment decision based on compromised patient data.

Collaborative care is a delivery model that involves patient data being available across large, complex healthcare environments and accessible to many users from multiple devices and locations.

CONCLUSION

The healthcare industry faces other risks besides the three discussed here—including regulatory, operational, third-party risks and more. As healthcare organizations embrace the positive benefits of digital transformation, they must equally embrace security and risk management practices that enable them to successfully address the volatile, hyper-connected nature of these risks. In the increasingly connected world of digital healthcare, systems and data, each organization has a responsibility not only to shore up their own security and risk management practices, but also to contribute to the greater good of the expanded healthcare ecosystem.

DIGITAL RISK IS EVERYONE'S BUSINESS
HELPING YOU MANAGE IT IS OURS

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection and integrated risk management, RSA customers can thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk world at rsa.com

1 "Number of data breaches in the United States from 2013 to 2018, by industry," Statista, https://www.statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business (August 5, 2019)

2 "Ransomware Attacks Double in 2019, Brute-Force Attempts Increase," HealthITSecurity.com, https://healthitsecurity.com/news/ransomware-attacks-double-in-2019-brute-force-attempts-increase (September 3, 2019)

3 Security Transformation in Healthcare, Dell EMC, https://www.dell.com/html/global/healthcare/mobile/index.html#p=2 (September 2017)

4 "What's at Stake with Healthcare IoT and Cloud? Unnecessary Risk," HealthITSecurity.com, https://healthitsecurity.com/news/whats-at-stake-with-healthcare-iot-and-cloud-unnecessary-risk (February 14, 2019)

5 "Organizations See 878% Health Data Growth Rate Since 2016," HIT Infrastructure, https://hitinfrastructure.com/news/organizations-see-878-health-data-growth-rate-since-2016 (May 8, 2019)

6 "RSA Digital Risk Study," RSA Digital Risk Report, 1st Edition, https://www.rsa.com/content/dam/en/white-paper/rsa-digital-risk-report-2019.pdf (September 2019)

7 IDC FutureScape: Worldwide Health Industry 2018 Predictions, IDC, https://www.idc.com/research/viewtoc.jsp?containerId=US41114417 (October 2017)

RSA