Key contacts

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Abhijit Katkar
Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Kamaljit Chawla
Leader – Cyber Operate
Risk Advisory, Deloitte India
kamaljitc@deloitte.com

Tarun Kaura
Leader – Cyber Advisory
Risk Advisory, Deloitte India
tkaura@deloitte.com

Anand Tiwari
Partner, Risk Advisory
Deloitte India
anandtiwari@deloitte.com

Anand Venkatraman
Partner, Risk Advisory
Deloitte India
anandv@deloitte.com

Chintan Matalia
Partner, Risk Advisory
Deloitte India
chmatalia@deloitte.com

Deepa Seshadri
Partner, Risk Advisory
Deloitte India
deseshadri@deloitte.com

Manish Sehgal
Partner, Risk Advisory
Deloitte India
masehgal@deloitte.com

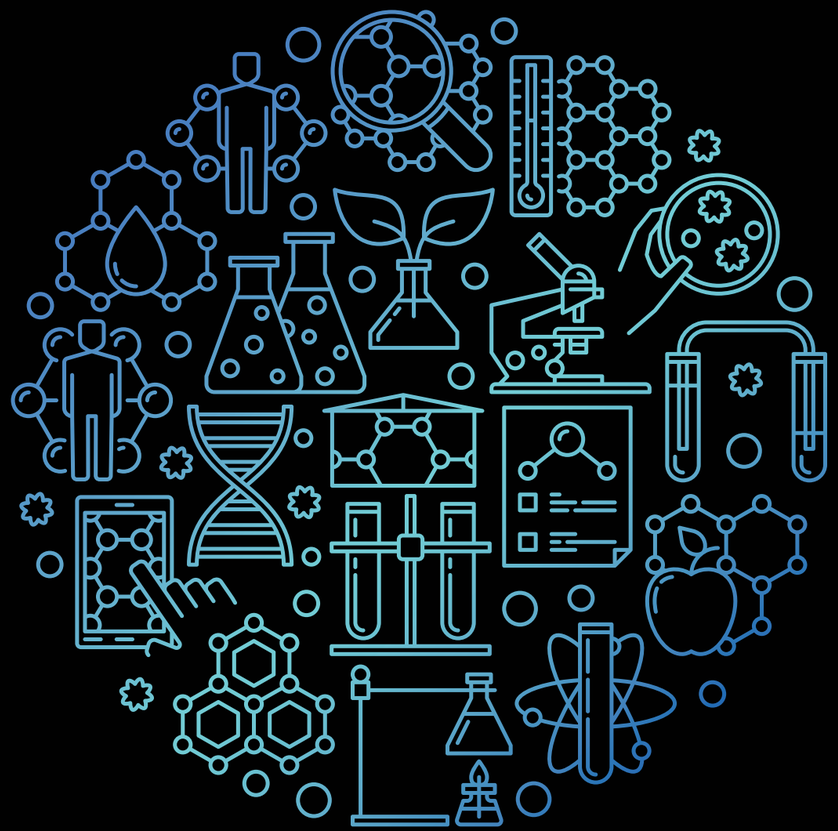
Muthukumar Karuppiah
Partner, Risk Advisory
Deloitte India
mkaruppiah@deloitte.com

Praveen Sasidharan
Partner, Risk Advisory
Deloitte India
psasidharan@deloitte.com

Vikas Garg
Partner, Risk Advisory
Deloitte India
vikasgarg@deloitte.com

Deloitte.

Deloitte.



The future of the healthcare industry

Cyber everywhere. Breakthrough anywhere.

2020

Introduction

Digitisation has a massive impact on the operation of the healthcare and diagnostic industry as it has played an instrumental role in enabling healthcare service providers to create a robust and critical digital infrastructure. Embracing emerging technologies such as artificial intelligence (AI), blockchain, predictive analytics, big data, machine learning (ML) and the internet of things (IoT) has accelerated the rate of digital innovation within healthcare segments i.e. hospitals, drug manufacturing, diagnostics, medical equipment and supplies, and medical insurance providers within the healthcare industry. From providing personalised care options, gathering insights to addressing new care formats such as telemedicine and outpatient care, these digital disruptors continue to rapidly transform the way healthcare is delivered by life sciences, healthcare and medical service providers.

Key trends

Personalised medicine
Technological advances for biological profiling at molecular levels is leading tailor-made medicines that are suited to individual needs. The future of health will be in scaling personalised care for different patient segments.

Artificial Intelligence (AI)
AI has the computing power to improve diagnosis and treatment plans. It cuts down the time for research and development drastically, making decision-driving data available with accuracy and speed.

Wearable digital devices
Using sensor-based technology in wearable medical devices ensures accurate reading of the health vitals of an individual, and helps in real-time data collection. Wearable digital devices will prove to be a powerful tool to not only help medical practitioners deliver personalised care, but also encourage individuals to proactively manage their health.

Telemedicine
With the increasing popularity of telemedicine, doctors are now able to treat patients living in remote villages and monitor their patients' health and well-being. This is enabled by data exchange platforms.

The Internet of medical Things
Combining IoT with health services has given rise to the Internet of Medical Things. For example, even in operation theatres, devices connected to a network through the use of IoT are installed to keep track of the patient's vitals and facilitate a seamless real-time analysis, manage long-term conditions and medications, and to support basic procedures.

Cloud computing in healthcare
Digital health records and medical history data are now stored on the cloud, thus, offering a chronological history of medical visits, tests, and medications. This has proved to be extremely handy, especially in cases of medical emergencies. Cloud computing, along with big data and predictive analytics, can provide a real-time analysis of the conditions of a disease, and help address various health disparities.

Threat landscape

While these technological innovations are transforming the healthcare industry for the better, by improving accessibility to diagnosis and care for the patients and automating routine tasks of managing patients' health records for the doctors, they are also increasing the threat surface. In recent years, the cybersecurity world has experienced a multitude of data breaches and the healthcare industry has been, and still is, a major target.

- According to the Irdeto Global Connected Industries Cybersecurity Survey 2019, 82% of organisations in the healthcare sector, globally, have faced cyberattacks on IoT devices in the past twelve months.
- In a recent study, nearly 90% of healthcare organisations surveyed had a data breach in the last two years, and 45% had more than five breaches in the same time period.
- It is estimated that medical information is worth 10 to 20 times more on the black market than credit card data because of its potential for fraud, identity theft and abuse.

TYPES OF ATTACKS

Attacks	Impact
Data breaches	The core processes and support functions of the life sciences and healthcare sector are to collect and process personal and sensitive personal data of individuals, giving rise to security and privacy related concerns.
Social engineering	Phishing is the most common way by which healthcare staff and professionals could be tricked into disclosing personal data. Education and awareness is the only way to combat this tactic.
IoT vulnerabilities	Medical devices connected through IoT capabilities may be left open to an online attack. The severity of such an attack is visible when critical medical equipment such as anaesthesia devices, medication infusion systems, pacemakers, etc. are left vulnerable, which might lead to situations of life and death.
Distributed-Denial-of-Service (DDoS)	Attackers use DDoS attacks as distractions. This is a coordinated assault on several connected systems on a network or server. It is used by hackers to disrupt medical care facilities.
Ransomware	During this attack, hijackers make data inaccessible to its owner unless a fee is paid. As hospitals use IT systems to provide critical healthcare, the denied access may even be life-threatening for patients.

Our solutions

Cybersecurity in healthcare has become a board-level priority over the past several years, as the industry recognises that cyber risk can create massive liabilities. With such evident security risks, it becomes pertinent to safeguard patients' medical records and personal information, lest they become a target of information theft, placing them in a vulnerable position that could even endanger lives. We, at Deloitte, understand the risks brought forth by digital transformation, and can help life science and healthcare organisations secure their digital perimeter, so that they can better defend themselves against such attacks and leverage digital opportunities.

BUSINESS VALUE
- Growth/Innovation
- Operational efficiency
- Risk Management
- Regulatory compliance

GOVERNANCE

Identify top risk, align investments, develop an executive-led cyber risk program and adapt to changes in business strategies and threat
- Strategy and operating model
- Policies standards and architecture
- Cyber Risk culture and behavior
- cyber risk management metrics and reporting

RESILIENT CAPABILITIES

Have the ability to recover from and minimize the impact of cyber incidents
- Incident readiness
- Incident response
- Business continuity management and recovery

VIGILANT CAPABILITIES

Develop situational awareness and threat intelligence to identify harmful behavior
- Penetration testing and vulnerability scanning
- Cyber security and threat response framework

SECURE CAPABILITIES

A measured risk-prioritized approach to defend against know/ emerging threats
- Cloud security
- Third party risk management
- Human resources security
- Physical security
- GDPR Assessment
- Access control
- Project Monitoring
- Application security
- Asses Management
- Malware Protection
- Infrastructure Security
- Network Security
- Data loss prevention
- Emerging technology
- Risk Assessment
- IoT Security
- Data Protection and Privacy

Sources:
https://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924
https://www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data
Thousands of Critical Medical Devices Open to Attack," by Katie Dvorak, Fierce Healthcare (Sept. 30, 2015)
https://mobidev.biz/blog/technology-trends-healthcare-digital-transformation
https://www.weforum.org/agenda/2018/01/this-is-what-the-future-of-healthcare-looks-like/