Cyber Risks in the Healthcare Sector and the Antidote for Them

Summary: As in most other industries, data is a valuable asset for healthcare companies. These organisations are increasingly adopting cloud solutions and BYOD trend for quick access to electronically stored patient records. Unauthorised access to such data, its loss or manipulation can not only impact the brand image of an organisation but also endanger lives. For effective management of the growing number of network endpoints, the industry needs a scalable endpoint protection platform that can protect each device in the complex cyber threat landscape.

The healthcare sector has been adopting digitalisation to serve patients better, but it is also plagued by several online threats. While there are benefits of storing patient data in easily accessible electronic health records (EHRs), the abundance and availability of information have increased security concerns.

From malware compromising the integrity of computers and data breaches stealing critical data to distributed denial of service (DDoS) attacks disrupting organisations’ abilities for patient care, these attacks pose unique challenges for the healthcare industry.

Failure of conventional security measures

When they plan and implement measures against such issues, the focus of these organisations is primarily on external threats. However, some genuine and strong risks to the integrity of systems are internal.

Employees can pose a threat with the authorised access that they have (or had) to proprietary IT systems of the organisation. Some may be exempt from security measures such as intrusion detection and content filtering. And they may be aware of network setups and vulnerabilities.

Issues that originate from internal sources can be due to carelessness or malice. At times, workers can unknowingly click on a harmful link that compromises the organisation’s network, or they may lose a device storing sensitive data. In another case, someone may give away passwords or access codes in return for money.

While they also affect other industries, the ramifications of cyber threats in the healthcare segment can go beyond privacy breach and financial loss – they can endanger the very lives of people being treated by an organisation.

Areas that need attention: BYOD, shadow IT, information in third-party data centres

The growing BYOD trend in the healthcare industry has added to the convenience of workers but is also a top concern in managing cybersecurity. Since the bulky desktop computers containing patient records stay confined to specific rooms, the medical fraternity has started using personal laptops, tablets and smartphones to check medical histories and make notes. These mobile devices help physicians make quicker decisions on diagnosis, medication and treatment. However, most of them use only basic antivirus programs, making the device susceptible to malware and phishing attacks.

Another issue related to both personal and company-owned devices is that of shadow IT – the use of hardware, software, applications and services without the IT department’s direct approval. It has increased in recent years due to the ubiquitous availability and adoption of cloud-based services.

To improve productivity and drive innovation at work, employees in a healthcare organisation may download potentially harmful applications on their devices. Most of these apps refuse to function unless the users grant them access to different kinds of data stored on their device. If the organisation is not
aware of the diverse apps and software used by its employees, it will not be able to take quick remedial measures when a device or the network gets compromised.

Data stored by healthcare companies in third-party data centres can also become a cybersecurity issue if it is not encrypted using the right tools.

**Obstacles to IT security in the healthcare sector**

The prime operations in hospitals and healthcare organisations revolve around medical diagnosis, treatments, patient care, consultations with physicians and pharmacy sales. Even though they use a variety of digital tools to store records of such activities, many lack a full-time IT team to monitor the usage of devices. Unlike IT and ITES companies, senior management at healthcare organisations is not deeply involved in the management of technology.

Employees are expected to take care of their devices on their own. However, their routine duties keep them too busy to look into complex computer issues. Amidst the recent outbreak of COVID-19, healthcare teams are working for extended hours to support patients. When security patches and updates are not applied proactively, unauthorised access to systems through ‘backdoor vulnerabilities’ cannot be ruled out.

**Deploying an endpoint security platform for better risk management**

To mitigate IT risks in their strenuous work environments, medical and healthcare organisations need endpoint security solutions. Instead of using a siloed approach to cybersecurity by trusting antivirus software on individual devices, they must have a comprehensive, one-stop solution for connectivity and applications.

Endpoint security safeguards a company's data as also the workflows associated with personal devices that connect to its IT network. Once an endpoint security platform is deployed, it examines all the files entering the concerned network.

By harnessing the power of the cloud, it can hold on to an ever-expanding database of risks and threats. With this action, it frees the endpoints of the bloat that comes with the local storage of such information and the maintenance needed to keep the databases updated. The evaluation of this data in the cloud also offers better speed and scalability.

The cloud-based endpoint security platform tailored by Tata Tele Business Services (TTBS) is called DoBig Endpoint Security. Our solutions under this tool provide a robust first line of defence against the sophisticated cybersecurity threats that plague several verticals, including the healthcare industry. They safeguard a variety of IT equipment used for work – laptops, tablets, smartphones and other wireless devices. They work seamlessly on Windows, iOS and Android operating systems.

Beyond the security offered by a run-of-mill antivirus software package, the DoBig Endpoint Security Solutions help an organisation at network access control, application whitelisting, managed threat detection & response and indicators of compromise (IOC) security.
The features include:

- Antivirus
- Anti-Spyware
- Anti-Ransomware
- Application Control
- Component Updates
- Data Loss Prevention
- Device Control
- Firewall
- HTTPS Web Protection
- Predictive Machine Learning
- Role-Based Administration
- Unauthorised Change Prevention Service
- URL Filtering
- Web Reputation
- Full Disk Encryption

With this endpoint security service, one system administrator can easily manage security for a variety of devices, irrespective of the location the employees use them from. There is a centralised console deployed on a network gateway that gives a complete view of the devices’ integrity status. The facility greatly simplifies policy and exception management.

DoBig Endpoint Security protects the endpoints for healthcare application control and blocks the usage of shadow IT apps that can harm a device. By offering end-to-end encryption, it reduces the possibilities of data loss from laptops and desktop computers, tablets and smartphones.

The rapid detection and elimination of any existing malware begin as soon as the cloud-hosted DoBig Endpoint Security is configured to a machine. It also safeguards the device from phishing attempts, zero-day attacks and fileless malware.

Thanks to the scalability and cloud orientation of DoBig Endpoint Security Solutions, the real-time discovery of threats and instant patch management become feasible.

In addition to such benefits, users get value-for-money subscription packages that come with the multi-tenant architecture of all TTBS products and services. A single bill covers all the devices that are protected with our endpoint security solution. We also have a 24*7 contact centre to provide telephonic support to clients.

To know more about DoBig Endpoint Security for healthcare companies, please call Tata Tele Business Services at 1800-266-1800.