ManageEngine
Log360

IT security hardening at **healthcare organizations:**

A 1-page strategy plan

www.manageengine.com/log-management

Table of **Contents**

The current state of the **global healthcare** and **healthcare IT market**

Global healthcare spending is expected to reach $8.7 trillion in 2019 and is expected to grow to $10.1 trillion by 2022.[1] This increase can be primarily attributed to a growing and aging population, and rising rates of chronic disease. Another reason for increased spending is the rapid adoption of new, advanced technologies to aid in providing care. In fact, the healthcare IT market is expected to climb from $67 billion in 2019 to $80 billion in 2022.[2]

Some of the technologies the healthcare sector is adopting are electronic medical records, telehealth, health wearables, robotic surgery, and connected medical devices. In addition to this, healthcare organizations are also investing heavily in interconnectivity with suppliers, insurance companies, and doctors. All of this is going to enable healthcare organizations to provide better care for patients, but it will also open up numerous vulnerable endpoints that cybercriminals can compromise. Once an attacker gains entry into any of these components, they could gradually escalate their privileges and get their hands on sensitive information. Even worse, they could cause a life-and-death situation.

Unsurprisingly, healthcare data breach costs are the highest among all industries.[3] A recent study found that healthcare data breaches costs $408 per record on average.[4] Assuming that spending on IT security is 10 percent of the overall IT budget, we can estimate that the healthcare IT security market is worth $7 billion in 2019 and will grow to $8 billion in 2022.[5] But a large budget set aside for IT security won't guarantee safety.

The trend of the last few years is apparent — there's always a new data breach or cyberattack making the news. This is because cyberattackers need only one small oversight to cash in big. For most healthcare organizations, investing in expensive security solutions may not even be necessary. One study says that organizations should spend no more than 37 percent of the expected loss due to a cyberattack on security solutions.[6] IT security professionals must take a holistic and structured approach to security.

In this e-book, we'll examine some of the new technologies in healthcare and how attackers could compromise them. We will also look at the security-productivity conundrum in the healthcare sector, and how to arrive at a happy medium. And finally, we'll develop a framework using which IT security professionals in the healthcare sector can build a holistic IT security strategy for their organizations. This framework will be a 1-page toolkit that is more practical than academic. We'll provide insights about developing your own 1-page toolkit throughout this e-book. We've gathered all of these toolkit components together, for your convenience, in the appendix.

New technologies in the healthcare sector, and the dangers they pose

IT security professionals should take care when adopting the following technologies in healthcare

1. Electronic health records

As the name suggests, an electronic health record (EHR) or electronic medical record (EMR) is a digital version of a patient's medical history. It can contain information such as name, age, gender, medical conditions, diagnoses, prescription details, treatment history, scan reports, test results, and more. In the US, 99 percent of hospitals use EHRs in 2019, compared to only 31 percent in 2003.[7] Moreover, 86 percent of office-based physicians used some form of EHR in 2017 alone.[8] EHRs have seen similar adoption rates in much of Europe. While adoption rates may currently lag in some of the emerging economies, they're expected to demonstrate strong growth in the next five years.

Benefits: There are several benefits of EHRs. They can be a repository of the most recent health information about a patient. They can also enable doctors with different specialties to collaborate efficiently, and provide the best care. They can reduce human errors, and improve the quality of diagnoses. The benefits are not for the patients alone—healthcare organizations can also operate more effectively, and meet their business and financial goals.

Risks: Data security is a huge concern. Numerous healthcare organizations have become victims of cyberattacks that have compromised the EHR database. In 2018, SingHealth, Singapore's largest group of healthcare institutions, was hit by an attack in which details of 1.5 million people were stolen. Since personally identifiable information (PII) is contained in EHRs, criminals can sell this information on the dark web for as much as $1,000 per record.[9] Adding to this, they could commit identity theft or fraud.

2. Telehealth

Telehealth enables healthcare organizations to provide care using telecommunication technologies. According to a 2017 report by the American Hospital Association, 65 percent of hospitals have implemented telehealth in at least one care unit.[10] It has also caught steam in India, with several healthcare organizations offering this service. One of the most popular examples of telemedicine is two-way video conferences between patients and physicians. The main driver for the growth of telehealth is the need to reduce cost of care. The global market for telehealth is expected to reach $40 billion in 2019.[11]

Benefits: Telehealth services makes physical barriers a non-issue. No matter the geographical location of a medical professional and a patient, they can easily connect. It also offers access to medical specialists at any time of the day or night. In case of serious ailments, patients don't have to leave their homes for an initial consultation. Doctors can also work from remote locations, thus improving their productivity and the quality of care they give to patients.

Risks: Communication between patients and doctors over the internet is fraught with risks. It's as risky as any other online communication. Cyberattackers may intercept the communication, and listen in. Even worse, an attacker could intersperse legitimate conversation between doctors and patients using forged clips. "Deepfakes", or AI-generated video forgeries, could pose a big risk in the days to come. This is why encrypting this type of communication is extremely important. Furthermore, an attacker may attempt to assume the identity of a patient, and use the consultation with the doctor for sinister motives. This is why multi-factor authentication becomes critical. A criminal could also initiate a DDoS attack, thus harming a patient who relies on telehealth.

3. Health wearables

In the last few years, wearable technology in healthcare has grown by leaps and bounds—they are not just used as fitness trackers anymore, but are increasingly used as real-time health monitors. Patients wear these smart, electronic devices either on their person or on clothing; these devices will continuously monitor their vitals, and relay this information to medical professionals. The growing shift of healthcare providers relying on wireless connectivity, coupled with an increase in diseases including obesity and diabetes, is expected to stimulate market growth.[12] The market size of health wearables was estimated at $7.01 billion in 2018, and is expected to grow to $27.5 billion in 2026.[13] Another related instance of the technology is the "smart pill." These pills are actually swallowed by the patient, and they relay information that's otherwise difficult to get. Abilify MyCite, the first smart pill in the US, was approved by the FDA in 2017.

Benefits: As wearables proliferate in healthcare, physicians can quickly diagnose ailments even from remote locations. This will be especially beneficial to patients who suffer from ailments that require early detection for effective treatment. Doctors can also monitor if the patients are taking their medications on time and at the right dosage. Since information is continuously recorded, doctors can also analyze how a patient's condition has changed over time. This will enable them to personalize the treatment program based on individual needs. Patients with chronic conditions will benefit substantially from such personalized care.

Risks: Privacy and data security issues can arise from the use of healthcare wearables. Since real-time information is continuously transmitted, an attacker could attempt to intercept this information. They could also compromise the database where all of this information is stored, and delete or modify it. This can have adverse consequences on the type of treatment rendered by the doctor, and can negatively affect patient safety.

4. Robotic surgery

In a robotic surgery, a surgeon uses either a telemanipulator or a computer to move the robotic arms that perform the actual surgical operations. A robotic surgery using a telemanipulator requires that the surgeon be in the operation room. However, with computer control, a surgeon can perform a surgery from a remote location. For example, the world's first telerobotic intervention study was conducted on a patient from a remote location in India in December 2018.[14] In 2018, the global surgical robotics market was worth $5.4 billion, and it's expected to rise to $24 billion by 2025.[15] Robotic surgery has successfully been used in specialties including cardiology, general surgery, and urology.

Benefits: Robotic surgery provides many benefits compared to traditional open surgery. The incisions are smaller, which leads to less scarring and reduced blood loss. Robotic surgeries are also known to reduce the time of hospitalization and recovery time of patients. For doctors, it can eliminate or reduce fatigue, improve precision, and increase dexterity.

Risks: An attacker could compromise either endpoint (the surgeon's computer-control console or the robot). They could also attack the network over which communication is taking place. It could either be a denial-of-service attack (DoS) or distributed denial-of-service (DDoS) attack in which the surgeon is unable to access the network due to substantial illegitimate traffic. In a worst-case scenario, the attacker could even give malicious instructions to the robot performing the surgery. This technology could also have privacy repercussions for surgeons. Since it is performed by a robotic arm, each and every move by the surgeon could leave behind a log trail, and this could be used by an attacker to create a surgeon's profile. It could then be used in a myriad of malicious ways.

5. Connected machines

The Internet of Things (IoT) and connected machines have started to make a mark in the healthcare sector. While wearable technology is comprised of smart devices that patients wear on their person, connected machines are smart machines that exist within the hospital premises and are traditionally standalone devices. Today machines such as X-ray machines, magnetic resonance imaging (MRI) machines, pacemakers, defibrillators, computed tomography (CT) scanners, and wheelchairs have become "smart." Gartner predicts that we will soon enter a world of smart hospitals.[16]

Benefits: Connected machines can improve the quality of engagement and care that medical professionals provide to patients. Test results and scan reports can be shared with both the patient and the doctor in real time. It saves substantial amounts of time, and enhances productivity.

Risks: Connected machines can become another vulnerable endpoint that cyberattackers can strike. For example, all that a cyberattacker might need to do is compromise one connected machine. Once they achieve this initial foothold into the network, they can start moving laterally. Connected machines are also subject to DoS and DDos attacks, and this can have an adverse effect on patients who are waiting for treatment. Furthermore, attackers can steal sensitive information from these machines.

6. Chatbots

Chatbots conduct conversations via auditory or textual methods. They mimic human conversations and can interpret what a patient says. They are on their way to becoming reliable assistants for healthcare providers. The healthcare chatbots market was worth $122 million in 2018 and is expected to grow to $314 million by 2023.[17] As of now, Europe is leading the market, closely followed by North America.[18]

Benefits: They can be used for repetitive and mundane tasks such as setting up doctors' appointments, providing information about treatment, and checking symptoms, nutrition, and location of clinics. As chatbots become more sophisticated, they could also reduce the number of visits that a patient needs to make to the doctor. Doctors also benefit, as they can focus on doing work that actually requires their expertise. Healthcare organizations that use chatbots can therefore become more productive.

Risks: Chatbots are vulnerable to attacks such as spoofing, DoS, DDoS, and data theft. For example, substantial amounts of PII could be shared in a conversation with a chatbot, and these could be stored in a file server along with a patient's history. A cyberattacker who obtains access to this file server can wreck some real havoc. Not only can they attempt to read files and extract data; but they can also attempt to modify or delete files with malicious intent. This can have adverse effects on the treatment plan of the patient. Moreover, for the healthcare provider, this could have serious compliance-related ramifications.

7. Virtual reality

Virtual reality (VR) is a simulated experience that closely mimics the real world. The size of the virtual reality market in healthcare was $1.8 billion in 2018.[19] It is estimated to grow to $6.9 billion by 2026, at a compound annual growth rate (CAGR) of 16.2 percent.[20] The main drivers of demand are increased disease awareness, the need for innovative diagnostic techniques, the higher prevalence of neurological disorders, and better network connectivity.

Benefits: One of the biggest benefits of VR in healthcare is its application for educational purposes. For example, doctors and nurses can be trained in a 3D virtual surgical environment. This makes them better prepared to face challenges in the real world. Apart from the classroom, VR can also be used for counseling patients, treatment of mental illnesses, and pain management.

Risks: The use of VR in healthcare can lead to both privacy and security concerns. Cyberattackers could place malware on VR applications. Data that patients share on VR can then be exposed, leading to privacy issues. Attackers can use this data to commit fraud. A criminal with a far more malicious intent could interfere in the actual therapy or treatment that a patient receives. Since everything looks very real, the patient will likely have no way of knowing that they're a victim until it is too late.

We have looked at only seven emerging technologies in healthcare, and this is not an exhaustive list. There can also be innovations that use the integration of several technologies. For example, VR can be used in robotic surgery, wearables can be used with connected machines, and chatbots can be used in telehealth. Bringing in the right technology can be a sustainable competitive advantage for healthcare organizations. Adoption of technology has benefits for both patients and healthcare organizations, but it has security pitfalls as well. Healthcare, just like any other industry, is wrestling with the productivity vs. security conundrum.

The productivity vs. **security conundrum**

It is commonly thought that tighter IT security controls decrease business productivity. The primary misconception is that tighter security controls and the restrictive processes they set in place will negatively impact the efficiency of the business. However, this is only true for organizations that treat security as a separate entity from the business. A good security strategy is interwoven with the business and will actually improve the productivity of healthcare organizations in the long term. There are three main reasons for this: 1) non-disruption of healthcare services, 2) streamlined business security processes, and 3) better compliance with regulations and increased brand reputation.

Non-disruption of healthcare services: Organizations with good security strategies will preempt all possible causes of service disruption. If an attacker attempts to enter the network to sabotage it or a malicious insider tries to take down any critical systems, these organizations will have processes in place to alert security personnel in real time. Security personnel can then take action to avert the attack before it even takes place.

Streamlined business security processes: A good security strategy will ensure that security processes only complement the business processes. No security process should come in the way of delivering high quality care to patients. The main goal of the business is identified first, and business processes are developed around that main goal. Security processes are then brought in to fortify these business processes.

Better compliance with regulation, and increased brand reputation: Over time, people will start to value healthcare organizations with good security strategies. These organizations will be able to comply with regulations more effectively. People will also realize that their data is safer with such organizations.

A good security strategy will be proactive, minimize risk, have the right level of coverage, consider the current threat landscape, and complement business.

Building a healthcare **IT security strategy**

In the Appendix, you'll find a 1-page toolkit that healthcare IT professionals can follow as they build their IT security strategy. IT security professionals can follow these nine steps to build an effective IT security strategy:

Understand the business' vision and objectives: To manage the security posture of a healthcare organization, IT security professionals first need to understand the vision and objectives of the business. This is how the IT team can see the big picture, and recommend the right technologies to invest in for tangible business outcomes. Moreover, security teams can integrate security initiatives to empower the business. This will, in turn, lead to higher rates of security initiative implementation in other teams.

Develop a successful technology investment plan: Relate your technology investment plan to the individual goals of your organization. You will need to develop a functional requirement analysis, develop a vendor list, evaluate shortlisted vendors based on an objective rating criteria, and finally choose the best vendor. Table 1 provides guidance for developing your technology investment plan.

Vision:	Technolgy needs
Goal 1:	Technology 1:
Goal 2:	Technology 2:
Goal 3:	Technology 3:
...	...

Table 1: Identifying your business' vision, goals, and technology needs

Take a comprehensive inventory of all network access points: Technology that's used by the organization could have several network access points. IT security professionals must list these out carefully. They should also have a process to update this inventory on a regular basis. Table 2 shows how this can be done. Any of these network access points has the potential to become a vulnerability.

A vulnerability is a weakness or gap in a company's network, systems, applications, or even processes which can be exploited to negatively impact the business. Vulnerabilities can be physical in nature (such as old and outdated equipment), they can involve weak system configurations (such as leaving a system unpatched or not following the principle of least privilege), or they can result from awareness issues (such as untrained staff). Security teams may find it helpful to use scanning tools to perform a thorough systems analysis. Penetration testing or ethical hacking techniques could also be used to delve deeper and find vulnerabilities that regular scanning might miss.

Vision:	Technolgy needs	Network access points
Goal 1: Improve ease of insurance claims, and payment processes	Technology 1: Blockchain	Access point 1: Billing systems Access point 2: Access point 3:
Goal 2:	Technology 2:	Access point 1: Smart X-ra machine Access point 2: Smart pacemaker
Goal 3:	Technology 3:	
...	...	

Table 2: Taking stock of all the vulnerable access points

Identify all valuable data assets: Companies should also identify the data that is critical to their day-to-day operations. Most healthcare organizations would consider patient health records their most important assets. It's vital to understand how all of this critical data moves through a network and identify which computers and servers are used to store this data. This can reveal even more vulnerable access points than was identified before in step 3. Healthcare organizations must also have solid identity and access management processes in place so that only authorized users are able to access this data.

Estimate business impact due to loss: Risk and impact assessment have to go hand in hand. For each valuable data asset, the corresponding negative financial impact of a compromise or loss should be estimated. Apart from direct costs, loss estimates should also include intangible costs such as damage to reputation and legal ramifications.

Determine threats to the business: A threat is anything that has the potential to cause harm to the valuable data assets of an organization. The threats companies face include natural disasters, power failure, system failure, accidental insider actions (such as accidental deletion of an important file), malicious insider actions (such as a rogue agent gaining membership to a privileged security group), and malicious outsider actions (such as phishing attacks, malware, spoofing, and more). Each company should determine the threats that it will likely face, and plan accordingly.

Establish a risk management framework: Risk is a business construct, but it can be represented by the following formula: Risk = threat x vulnerability x business impact.

To reduce risk, IT teams in companies need to minimize the threats they're exposed to, the vulnerabilities that exist in their environments, or a combination of both.

From the business side of things, management may also decide to evaluate the business impact of each data asset and take measures to reduce it.

The risk team will need to assign risk values of high, medium, or low for the potential loss of each valuable data asset. Using this process, a company can also prioritize which data asset risks it needs to address. This is a highly-involved process and should be done carefully. Table 3 shows how a healthcare organization can do this. After this is done, a company should come up with solutions for each identified risk and the associated cost for each solution.

Data asset	Threats	Vulnerabilities	Business impact	Risk
Electronic health records	- Insider attacks - Malware (High)	- Patient database server in cloud (High)	Very high	Very high
Financial information	- Insider attacks - Malware - ...	- Payment gateway - Billing system	High	High

Table 3: Estimating the risk of data assets

Develop a risk appetite: Companies should gauge themselves on what level of risk they're comfortable taking. Do they want to address all the risks or do they only want to address risks identified as high? The answer to this question will vary from company to company, and the estimated total cost of the solutions will have a huge bearing on the risk appetite. At the end of the day, it doesn't make sense to spend $10,000 on a solution to safeguard a risk of $5,000. The right risk appetite must be developed after looking at the projected return on investment of a solution.

Start mitigating risks: Finally, healthcare organizations should invest in the right solutions and start mitigating risks of a cyberattack. Below is a sample framework for evaluating security vendors. IT professionals can use several criteria including completeness of the product, ease of installation, extent of technical support, scalability, and more to rate each vendor.

It might be a good idea to rate each vendor on a scale of 1 to 10 on each of these criteria. The final score is a sum of the scores received for each criteria. Table 4 shows a sample vendor evaluation template.

Vendor name	Vendor 1	Vendor 2	Vendor 3	Vendor 4
Completeness	7			
Ease of installation	7			
Ease of use	7			
Technical support	4			
Training	4			
Scalability	5			
Credible customer success stories	3			
Recognition by industry analysts	1			
Size of the customer base	2			
Value for money	5			
Final score	**45**			

Table 4: Evaluating and choosing the right IT security vendor

Securing your organization with **ManageEngine Log360**

Log360 is a comprehensive SIEM solution that helps enterprises detect data breaches, ensure the security of stored personal data, and track each and every access to personal data. It also tracks critical changes to the files and folders where personal data is stored.

Let's take a closer look at some of Log360's features that can help healthcare organizations tighten their security:

Real-time Active Directory (AD) auditing: Log360 aggregates security log data from different domain controllers to centralize AD audit information, placing it all in a single location. Administrators can track important changes made to AD objects, including users, computers, groups, organizational units (OUs), and Group Policy Objects (GPOs), and get real-time alerts about critical changes. If access permissions are changed and privileges are escalated in AD, administrators will receive real-time notifications and can investigate if it's a threat.

Real-time network device auditing: Log360 can analyze syslogs generated by your network perimeter devices, including routers, switches, firewalls, intrusion detection systems and intrusion prevention systems (IDS/IPS) in real-time. Administrators can track configuration changes—such as rule modifications, links that are up or down, denied and accepted firewall connections, and IDS/IPS alerts—all from a single console. This helps with mitigating data breach risks that originate outside the business' network.

Discover data: With Log360, administrators can find, analyze, and track sensitive personal data—also known as personally identifiable information (PII)—stored in files, folders, or shares. This will prove beneficial when dealing with requests from consumers on data deletion and data access.

Audit file servers: Companies can monitor, report on, and receive real-time alerts for changes made to files and folders in file servers. This is how Log360 maintains the integrity of data and ensures it's not being misused. In addition to this, Log360 can thoroughly audit activities on your files and folders in Windows and Linux devices. Every access, creation, deletion, modification, and permission change made to files and folders can be tracked to ensure the security of confidential data. Figure 1 shows the file integrity monitoring report available in Log360. Using this report, administrators can quickly investigate if sensitive data has leaked.

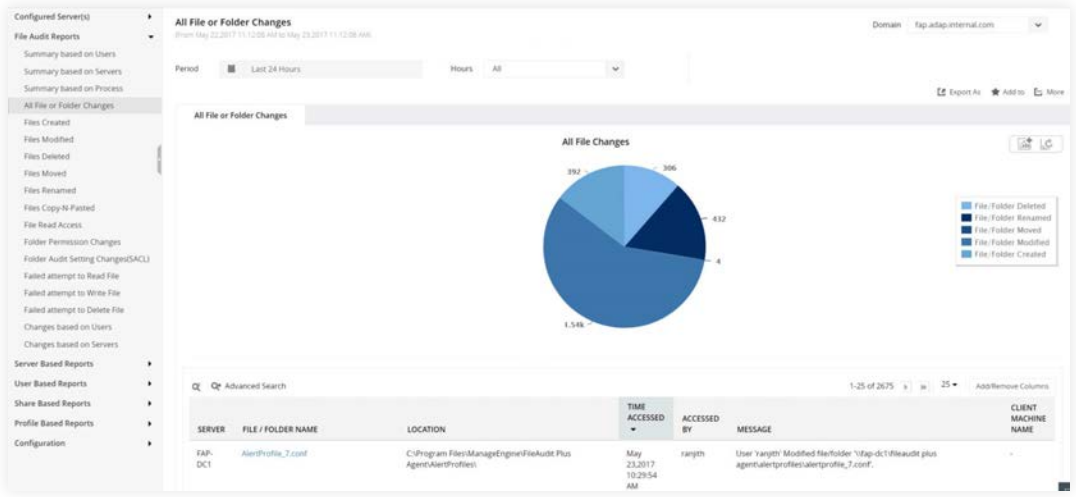

Figure 1: File integrity monitoring in Log360

Conduct audit trails: Log360's log search capability makes forensic analysis easy (Figure 2 shows the ElasticSearch module of Log360). One of the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is to quickly stop a breach or a breach attempt. This can be accomplished by finding the root cause of any security issue. Log360 can help find the root cause of a data breach by searching terabytes of log data within minutes. The solution also provides an option to export the search results as a forensic report.

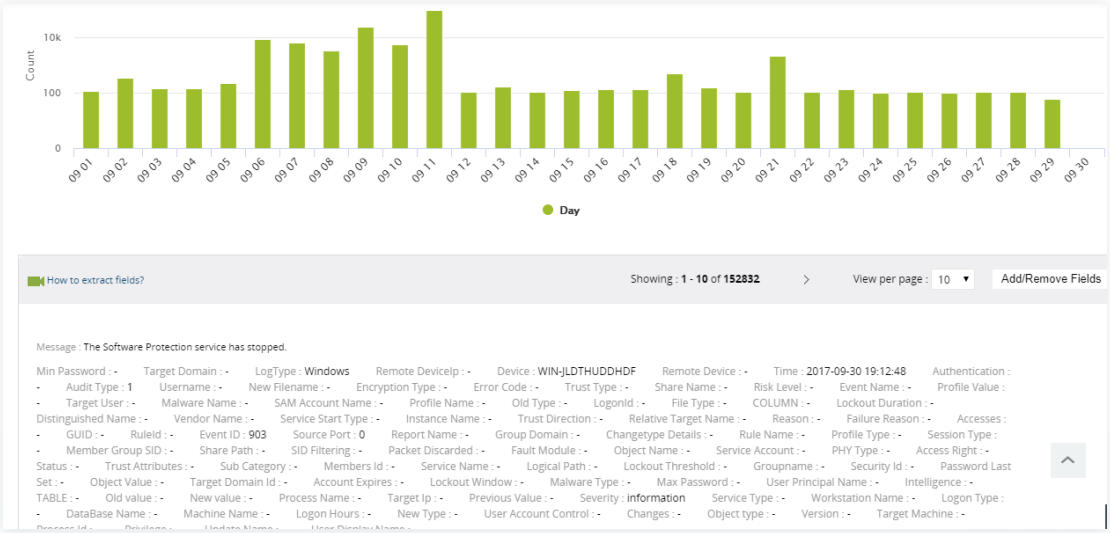

Figure 2: ElasticSearch in Log360

User and entity behavior analytics (UEBA): UEBA learns about each user and creates a baseline of regular activities for each user and entity. Any activity that deviates from this baseline gets flagged as an anomaly. The IT administrator can then investigate the issue and take the necessary steps to mitigate the risk. Powered by machine learning, Log360's UEBA module grows more effective the more experience it gains. A risk score is calculated for each user and entity in the organization after comparing their actions to their baseline of regular activities. The risk score can range from 0 to 100, indicating no risk to maximum risk, respectively. If the IT administrator feels an entity or user's risk score is too high, they can investigate it further and quickly stop any potential catastrophes.

For example, the chief of medicine of a hospital may usually log on to the network between 9am and 6pm, and the system would learn that this is their “normal” behavior. If this user logs on to the network at 12:30am, it would then be treated as an anomaly and their risk score would be increased. You may wish to refer to the article, "Combating threats with UEBA: Health is Wealth" for some interesting, real-world examples.[21]

Appendix: 1-page toolkit for building a **healthcare IT security strategy**

You can use the toolkit below to build your IT security strategy:

Assessing vulnerabilities in your healthcare organization

Vision:	Technolgy needs	Network access points
Goal 1:	Technology 1:	Access point 1: Access point 2:
Goal 2:	Technology 2:	Access point 1: Access point 2:
Goal 3:	Technology 3:	
...	...	

Risk assessment in your healthcare organization

Data asset	Threats	Vulnerabilities	Business impact	Risk

Evaluating IT security solution vendors

Vendor name	Vendor 1	Vendor 2	Vendor 3	Vendor 4
Completeness				
Ease of installation				
Ease of use				
Technical support				
Training				
Scalability				
Credible customer success stories				
Recognition by industry analysts				
Size of the customer base				
Value for money				
Final score				

References

1. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-hc-outlook-2019.pdf

2. https://www.imarcgroup.com/healthcare-it-market

3. https://healthitsecurity.com/news/healthcare-data-breach-costs-remain-highest-among-industries

4. Ibid.

5. https://www.spiceworks.com/marketing/state-of-it/report/

6. https://en.wikipedia.org/wiki/Gordon%E2%80%93Loeb_model

7. https://www.hcinnovationgroup.com/clinical-it/news/13029134/survey-nearly-all-us-hospitals-use-ehrs-cpoe-systems

8. https://dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php

9. https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#6ba60c3250cf

10. https://www.aha.org/system/files/content/17/telehealth-case-examples.pdf

11. https://intouchhealth.com/whats-driving-telehealth-growth-in-2019/

12. https://www.globenewswire.com/news-release/2019/02/27/1743565/0/en/Wearable-Healthcare-Medical-Devices-Market-To-Reach-USD-27-49-Billion-By-2026-CAGR-18-5-Reports-And-Data.html

13. Ibid.

14. https://www.businesswire.com/news/home/20181206005067/en/Corindus%E2%80%99-Technology-Successfully-World%E2%80%99s-First-in-Human-Telerobotic-Coronary

15. https://undark.org/2019/08/15/surgical-robots-are-suring-in-popularity/

16. https://www.gartner.com/doc/3887670

17. https://www.marketsandmarkets.com/PressReleases/healthcare-chatbots.asp

18. Ibid.

19. https://www.globenewswire.com/news-release/2019/03/25/1760469/0/en/Virtual-Reality-in-Healthcare-Market-to-Reach-USD-6-91-Billion-By-2026.html

20. Ibid.

21. https://www.manageengine.com/log-management/ueba/resources/combating-threats-with-ueba-health-is-wealth.html

Further reading

Here are some more sites and resources that you can benefit from as you harden the security at your healthcare organization.

General information about healthcare security and compliance
https://www.manageengine.com/log-management/healthcare-security-compliance.html

Establishing least privilege in healthcare organizations: The right access control policies to thwart security breaches
https://download.manageengine.com/log-management/healthcare-security-compliance/least-privilege-healthcare-security.pdf

Real world use cases in healthcare security: Scenario-based depiction of common attacks
https://www.manageengine.com/log-management/healthcare-security-compliance/attacks-in-hospital-network-use-cases.html