Why Unplanned Downtime Occurs and How to Mitigate Potential Risks in Healthcare's Growing Dependance on Computer Technology

Eric Ching,

Dr. April Rogers

Department of Health Care Systems, St. John's Lesley H. and William L. Collins College of Professional Studies, Queens, NY, USA

Date of Completion: May 4, 2021

Table of Content

Abstract

Everyday thousands of people use healthcare services, for treating physical injury, a fever or for prescription medication. This makes hospitals, pharmacies, and private practices critical infrastructure in any country. Whenever a patient walks into any of these healthcare services their personal data is logged into a computer database. These computer systems are interconnected with all healthcare services to instantly give specific and important information when needed, saving time, money and even potentially a patient's life. However, if these systems are compromised there could be huge repercussions risking thousands of lives. When computer systems become inaccessible this occurrence is called downtime. Downtime can happen to any computer for a number of reasons and can cause astronomical damages in any industry if not managed properly. Downtime in the healthcare sector can be especially bad as interruption to a computer system could lead to a negative chain of events, especially in places like the Emergency Room. Unlike other industries, healthcare services are responsible for the wellbeing of their patients, any interruption in a patient's health care can endanger their life. This paper investigates the effect of unplanned downtime on computer systems in healthcare and how to mitigate it. By mitigating unplanned downtime, we can save both millions of dollars in losses and in patient fatalities. While system downtime is not new, there is limited research based on the subject, despite the growing importance of computer technology. By gathering research papers from the last two decades, we can find a trend on how we can mitigate losses in healthcare services. The paper will also be looking at more modern causes of downtime to reflect the new "normal" caused by the COVID-19 virus. The new normal is in reference to how society is depending on computers for everyday tasks during the pandemic, such as telemedicine, and

working from home. Through this paper you will be able to see how properly training and educating personnel can reduce loss from unplanned downtime and the growing importance Health Information Technology (HIT) will play in the role of Healthcare.

Keywords: Downtime, unplanned downtime, healthcare, HIT, EHR, cyber security

Introduction

In the past decade, the use of Electronic Health Records (EHRs) has replaced healthcare's original and outdated manual filing systems. The enactment of Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009 along with the American Reinvestment and Recovery Act (ARRA) and Obamacare would be a landmark change in the history of healthcare. The HITECH and ARRA acts, through incentives would help "promote the adoption and meaningful use of health information technology" and making them a standard in the industry by 2015 (Department of Health and Human Services, and Office for Civil Rights, 2017). The presence of computer technology in healthcare was always growing even before the enactment of the HITECH act, however as computers became more sophisticated and readily available to the public even becoming convenient enough to fit in our pockets, relying on computers also reveals many drawbacks.

From information systems such as EHRs, data analysis and medical imaging, computers are just as essential as physicians and nurses in providing health care to patients. However, this dependance on technology also makes health care volatile when computer systems stop working. When users are not able to properly access or use specific applications this unavailability is called downtime. There are two types of downtime, planned and unplanned and can also be referred to as scheduled or unscheduled downtime. Unplanned downtime is when systems

unexpectedly stop working due to many different possible errors and can produce huge loses for companies. Planned downtime is a preventative measure used to conduct maintenance and to update computer systems to minimize unplanned downtime and occurs usually in low impact times. During this period, systems are in an environment which can be controlled to be fully or partially unavailable, employees are then notified so preparations can be made to continue business as per usual. Due to the lack of coverage on unplanned downtime in research, this paper aims to inform readers the growing risks of unplanned downtime and mitigation techniques.

In healthcare, EHRs are the most widely talked about system for unplanned downtime. Due to the important role EHRs plays in delivering and storing patient health data, a sudden disruption could create a safety hazard and put countless patients at risk. The worst part of unplanned downtime is its unpredictability. Disruptions could last for just a single minute or could last for hours and in worse case days. When Hurricane Sandy devastated both the New York and New Jersey areas in 2012 creating power outages and lost in network connectivity, few hospital staffs were able to even perform downtime contingency procedures. To make it worse, downtime procedure was only available in a digital format which meant that it was inaccessible during the power outage (Larsen et al, 2016). While this is an extreme case, it shows that more needs to be done to make sure hospital functionality does not completely fall through the moment disaster strikes.

Another more common event that might happen is documented in a large US northeastern medical center, where the hospital's Computerized Physician Order Entry (CPOE) lost connectivity. When this occurred, physicians had to use paper prescription pads, however junior physicians had never received any sort of training prior to the CPOE's sudden unscheduled

downtime. This resulted in several prescriptions that were included in patient discharge packets being improperly filled out. Furthermore, nurses began to devise their own unofficial downtime procedures resulting in poor clinical decision which caused high-risk incidents in medication overdoses and misadministration (Larsen et al, 2020).

The cost of unplanned downtime does not stop at endangering lives of patients, but also devastating financial loss. A 2017 article titled "The Price of EHR Downtime" based on a study by the AC Group, a Health Information Technology Consultation Company, saw the cost of unplanned downtime rise an "estimated 30% in the past seven years to more than $634 per physician per hour" (Goar, 2017). This is compared to 2011's estimated cost of $488 per physician per hour. Steps to calculate cost of EHR downtime based on the article are as followed:

1. Compute the average of annual salary costs (including benefits).
2. Multiply the value of step 1 by 2.15 (the calculated cost in dollars/minute of system unavailability).
3. Divide the value of step 2 by 2,080 (the average number as of 2017 of hours paid per staff member annually or 52 weeks x 40 hours per week).
4. Determine the number of hours which the EHR system needs to be available to staff including before and after operational hours.
5. Multiply the value of step 4 by 52 (weeks/year) and again by 1% or the expected percentage of downtime given by your server platform. The product of the equation represents the expected hours/year of downtime.

6. Multiply the value of step 3 (the value of the cost of staff per hour) by the value of step 5 (the estimated downtime per year). This results in the estimated cost per year of unplanned EHR downtime.

Unfortunately, despite the awareness system vendors have in aiming to create programs that result in zero downtime, a recent 2020 study suggests that downtime events are actually a growing issue in healthcare (Larsen et al, 2020). According to Larsen, there have been 43 reported instances of EHR-related downtime in US hospitals since HITECH act from 2009-2020. This however only accounts for available information. We can reduce the possibility of unplanned downtime through the system itself in several ways, such as the EHR or other program vendors regularly strengthening their system, facilitating working hardware and regularly updating software, strengthen healthcare facility's cybersecurity to prevent malware and always have a back-up system to fall onto.

Origin	Frequency	Definition	Exemplar
EHR provider	2	The provider as the host of the data loses connectivity; all subscriber hospitals experience downtime.	Temporary power outage affects dozens of hospitals' access to medical records.[16]
Nature	2	Downtime triggered by external "act of God" such as a destructive storm.	The impact of hurricanes.[17]
Internal IT	7	Failure of hardware or software within hospital IT system.	Coping with prolonged EHR downtime.[18]
Facility	8	Failure of a non-IT related service or system within the hospital such as accidental activation of a fire suppression system.	System-wide epic EHR downtime affects 24 sutter health hospitals.[19]
Cyber-attack	21	Any form of virus infection, deliberate hack, ransomware, or other malicious data access attempt.	Ransomware leads to EHR downtime in DC-area health system.[20]
Unknown	3	The event reached notice for publication in a news story, but the cause was not indicated in the news release.	All in a health recovers from system-wide stint of EHR downtime.[21]

Table 1. Reported EHR Downtime Events (Larsen et al, 2020)

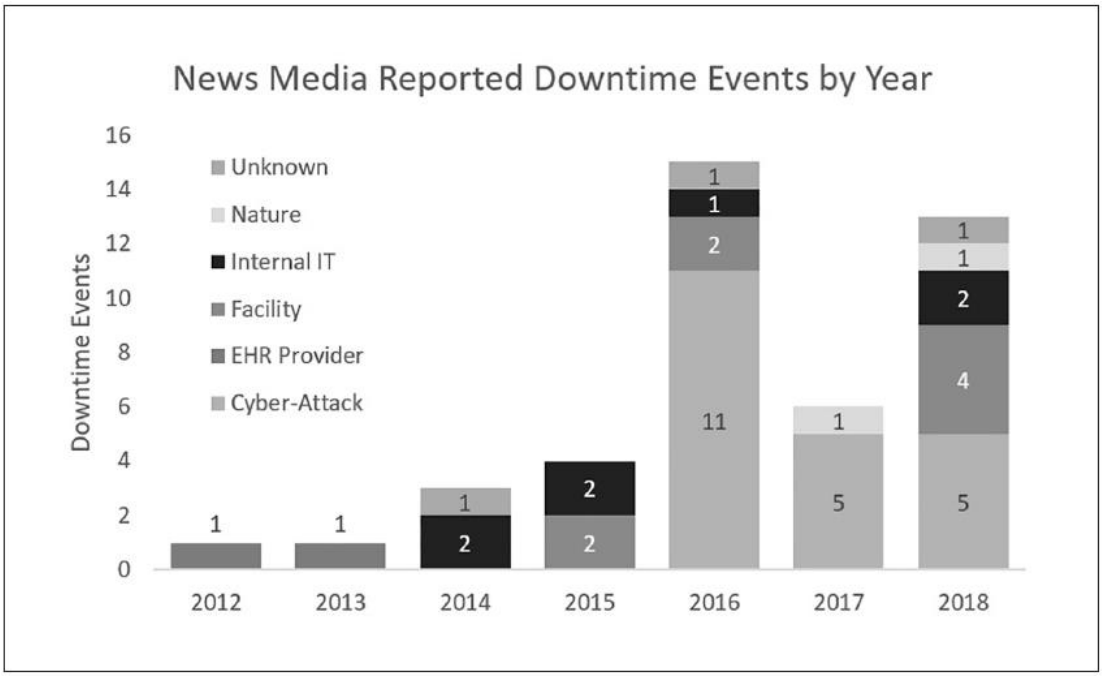

Figure 1. Reported Downtime Events by Year (Larsen et al, 2020)

Through Larson's data we can see that facility errors and internal IT errors account for about 19% and 16% respectively of all reported downtime events that were reported from 2012-2018. We can manage facility errors by making sure that non-IT related services are properly managed, secure, and not tampered with. Internal IT problems can be solved through maintenance of hardware and software. This means regularly updating system firmware, and security protocols and making sure computer hardware such as cables, and personal computers (PCs) are functional and are up to standard. However, the greatest cause for unplanned downtime are cyber-attacks making almost 50% of all reported cases. While facility and internal IT errors can be solved internally through trusted employees providing maintenance and management, cyber-attacks are a little bit more complicated. Preventing cyber-attacks not only require experienced personnel who can tests the hospital's digital infrastructure for vulnerabilities and monitor for unusual activities, but also training for all staff members who use the hospital's

network and computers. This need for training by all members of an organization whether they work in IT or not is due to the factor that connects almost all computers, the Internet of Things (IoT).

IoT is a simple term which describes a system in which devices are internet-connected and are able to share data using a wireless connection such as the internet or Bluetooth. IoT has now integrated into almost all forms of technology, our phones, and even medical devices, its sole purpose of making our lives easier, but also making it easier for hackers to infiltrate. In a documented case, Dr. Marie Moe a security researcher found these vulnerabilities in her own pacemaker by hacking her own device (Moe, 2020). Due to Dr. Moe's pacemaker which has built-in wireless capabilities it can be referred to as an IoMT or Internet of Medical things which refers to medical devices with IoT qualities. The pacemaker had a "near-field interface to facilitate adjusting the configuration settings and another wireless interface for remote monitoring purposes," allowing it to connect to its vendor's server (Moe, 2020). The connected device transmits the device's log and patient data for easy access to monitor. Dr. Moe's story not only revels how IoMT devices work, but her work shines light onto the ethical issues and dangers of IoMT devices which goes beyond the scope of this study. As of today, hacking pacemakers via the internet is not yet known to be possible, but studies show that we are not far off from it happening. A 2008 study confirms that sensitive patient data can be stolen and similar IoMT devices can be manipulated (Halperin et al, 2008). IoMT devices must remain up to date in security protocols, weak security could leave hospitals prey to black hat hackers, potentially causing a shutdown in hospital operations.

Black hat hackers are malicious hackers who deploys tactics to gain unauthorized access of computer systems. Looking at figure 1, we can see a growing trend in cyberattacks starting in 2016 and while numbers of incidents have dropped in 2017 and 2018, they still make up a majority downtime events. A 2020 healthcare cybersecurity report by Cybersecurity Ventures noted several alarming predictions and statistics (Cybersecurity Ventures, 2020):

- It is believed that healthcare saw more than 2-3 times more cyberattacks than any industry in 2019.
- Between 2017 and 2020 ransomware attacks quadrupled and by 2021 we will see more attacks.
- With Emails being a common point of information compromise, healthcare email frauds have increased by 473% in the last two years.
- It is believed that by 2020, more than 25% of cyberattacks in healthcare organization will involve IoT.
- In the last three years 93% of healthcare organizations have experienced a data breach with more than 57% experiencing more than five data breaches in the same timeframe.
- Only 4% to 7% of healthcare organizations' budget is spent on cybersecurity while other sectors have 15%
- While 91% of hospital administrators see security of data as a top focus 62% feel inadequately trained or unprepared to mitigate risks.

Cybersecurity issues can complicate mitigation of unplanned downtime as cyberattacks are always evolving. Cyberattacks are commonly done through malware or any software that is

installed without user's consent and alters the behavior of a computer. While there are different types of malware, healthcare facilities are commonly attacked by ransomware. Ransomware is a type of malware which encrypts the attacked computer's files locking and disabling the user from accessing any important documents. For users to reclaim their computers they must pay a ransom fee usually in the form of bitcoin, if the ransom is not paid, files are then threatened to be deleted (Langer, 2017). Paying the ransom would result in getting a decryption key, but it is not guaranteed that paying would result in the user's files returning to them. However, depending on the age of the malware, opensource solutions could be available to decrypt the attack, saving precious documents from being lost without having to pay the ransom. In 2017, the ransomware WannaCry severely struck hospitals in several different countries. The United Kingdom's National Audit Office (NAO) reported that 81 National Health System hospitals, 603 primary care and 595 medical practices were attacked. This caused more than 19,000 appointments to be cancelled. The attack was discovered to have originated from an unlikely country, North Korea and sponsored by the North Korean government (Riggi, 2020). Despite North Korea's lack of resources, they were still able to launch an organized attack which took out thousands of hospitals. The NAO reports that no UK healthcare organizations paid the $300 ransom, but the attack still caused millions in damages (National Audit Office, 2018). Damages included cancelled appointments, additional IT support, restoring data and systems affected by WannaCry and Staff overtime. WannaCry exploited a vulnerability in the Windows computer systems. Once discovered, Windows would immediately create a patch update for the operation system (OS) and alert all windows users of the update to protect themselves from the ransomware months prior to the big attack. This unplanned downtime event could have been easily averted if

healthcare organizations had properly updated their computer's outdated OS. The WannaCry attack in 2017 is a prime example on how vulnerable computer systems can be, easily infecting not one healthcare organization but literally thousands in a single day.

2020 has been a chaotic year especially in healthcare due to COVID-19 with hospitals overwhelmed by the epidemic. During the chaos hospitals could have been easily attacked by black hats, but surprisingly were not. During the early period of the epidemic hackers had developed an honor code to not attack hospitals. Some infamous groups going as far as declaring of their ceasefire until the COVID-19 epidemic was solved and even providing solutions for hospitals if they were inadvertently attacked by ransomware (Beshar, 2020). Unfortunately, the ceasefire between healthcare organizations and hackers ended recently as the pandemic has begun to stabilize with the introduction of several vaccines. Universal Health Services, a Pennsylvania-based healthcare service which operates about 400 facilities was attacked in late September of 2020. The attack left the healthcare giant's system down for several days (Jerchich, 2020). The resurgence of cyberattacks has also returned more viciously than before by deploying a new tactics called "double extortion". Instead of just encrypting the data to hold hostage, attackers are now threatening victims to release sensitive data to the public, which has increased leverage for the attackers (Beshar, 2020). Due to fact that cyberattacks are predicted to rise in 2021 and are a major cause of unplanned downtime, hospital should also be prepared to see a similar increase in both issues. However, by properly educating staff in cybersecurity literacy and properly implementing contingency plans, hospitals should be able to significantly reduce both cyberattacks and unplanned downtime. This paper will investigate how to mitigate the issues discussed through detailed staff training procedures and preventative methods.

Methodology

Due to the nature of this paper which investigates hospital security infrastructure, only secondary data could be gathered. This is due to two factors: one, conducting a survey or interview for this paper would require a decent sample size, this sample size would also require specific individuals in the IT and cybersecurity department of several hospitals; two, being able to successfully gather data would take an extensive amount of time and should gain approval by a hospital's Chief Information Officer (CIO) (or proper authority) to conduct this study as unplanned downtime will discuss possible security breaches detected by the hospital. Therefore, for this study it was best to conduct a systematic review. Databases such as Pubmed, ResearchGate, Association for Computer Machinery Digital Library and ScienceDirect were used to find most of the research material. Keywords used were downtime in healthcare or hospitals, reducing downtime, hospital cybersecurity, and cybersecurity issues in healthcare. Since unplanned downtime is a rare occurrence there were limited amount of research papers on unplanned downtime in healthcare especially within the last five years. It is important to note that three research papers that were written in the last five years were also written by the same person, Ethan Larsen. While gathering material, Larsen is currently the only known researcher whose research has been consistently been about unplanned downtime in healthcare. His research appears across several databases when searching for the keywords downtime in healthcare.

Figure 2 below shows search results based on keywords using Pubmed. Pubmed was selected since its library contained mostly healthcare related studies and provided users the number of papers published based on years. The chart looks at the number of published articles

on keywords relating to downtime within a 10-year period. Total search results of each key phrases are denoted in parentheses. Healthcare downtime and EHR downtime provided the best results in obtaining research published specifically on downtime in healthcare organizations. However, selecting research papers were still difficult in all keyword searches as many did not actually pertained to the subject or were too subject specific such as, "Managing a Multisite Academic-Private Radiology Practice Reading Environment: Impact of IT Downtimes on Enterprise Efficiency". While this paper itself discusses about downtime it investigates radiology whereas this paper tries to investigate management issues and infrastructure requirements. While there are more than 400 results combined, we must take into account redundancy of papers through other search queries and unrelated articles which lowers the actual number of qualified papers to include in this study. Of those papers that could be used, many were not free to access making it difficult to obtain information on downtime management. Lastly, research conducted in the last 10 years are the most optimal as it is up to date with most standard technology, however studies done in the last 20 years were included in the research process due to the lack of overall papers published. There is a total of 6 articles included from research libraries into this study out of the 20 sources referenced. This shows the difficulty of finding relevant and thorough articles on the topic.

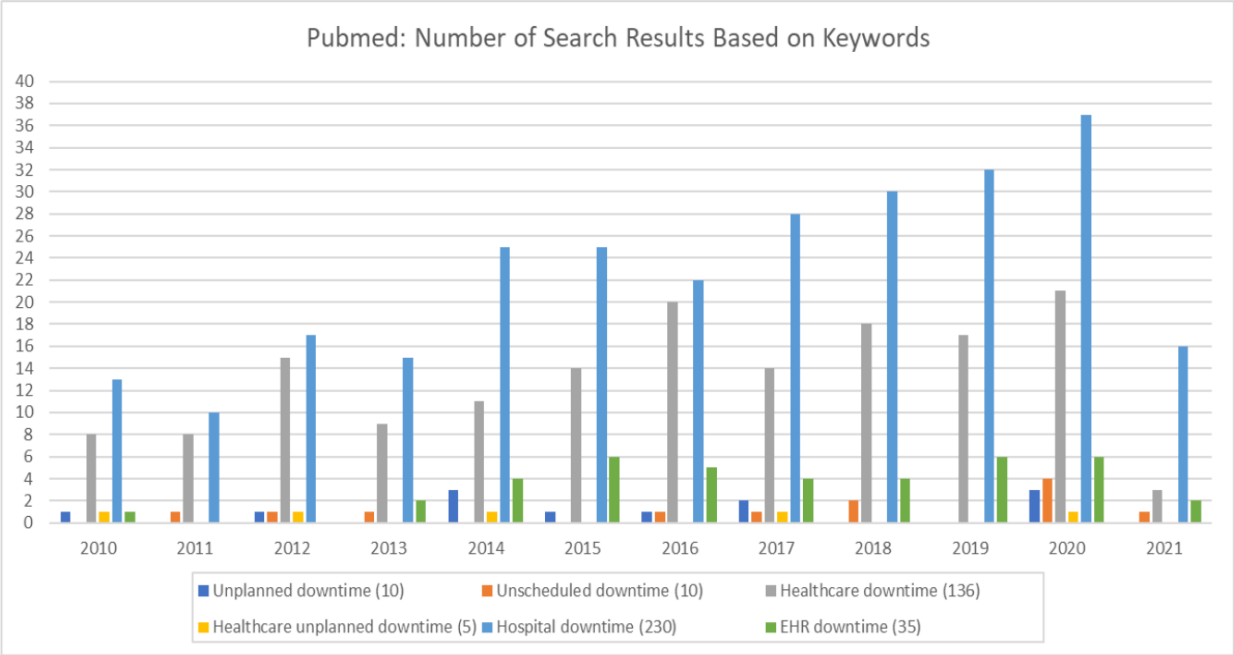

Figure 2. Number of Search Results Based on Keywords

Another issue of unplanned downtime not being widely researched is that many of articles found are based on word of mouth from personal experience of HIT professionals. Usually, the article would use examples from the author's own experience rather than from a study or recent news event. A quick google search of unplanned downtime would result in many articles on what it is and how to mitigate it. However, these articles are from magazines usually for health information technology professionals but have no credibility on the legitimacy of said magazine. Many of these articles are anecdotal written by professionals in the field, but because the magazines themselves are not known to be trustworthy this makes the authors' credibility to be hard to validate and use them in this paper. To supplement the lack of research articles, government articles and guidelines were used to establish a standard procedure. Requirements for including magazine articles in this study were to be affiliated with an established organization such as a healthcare or cyber security organization or the author's credentials are checkable, or

article is mentioned from a reputable source such as another study or report from a reputable organization. Several articles about cyber security news and statistics were used in this study as they were included in a report from a reputable cyber security agency as well as the reports being sponsored by larger organizations.

Results

Several independent studies indicated that the lack of training in unplanned downtime events results in subpar performance by healthcare personnel. Results in one experiment saw delays in 11 out of 15 different laboratories during downtimes. By conducting a Kruskal-Wallis test, researchers saw that 9 of those laboratories had significant delays compared to their normal operations (Larsen et al, 2019). In order to test downtime in a laboratory setting, any activities that is done such as operating analyzers during an off-network state and manually transcribing information would count as downtime as long as the network was unavailable. Hospital data collected was based on a 300-bed suburban acute care facility with a 24-hour emergency department located on the East Coast adjacent to a major metropolitan area. All data in this study was gather within the same period matching seasonality of the data. Researchers conducted interviews with 17 participants from both the hospital and laboratory. Of these participants 44% voiced concerns on how downtime training and preparation is handled. Interviewees were also concerned about colleagues being unaware of the limitations placed on laboratory operations during downtime. Nursing participants indicated that there was no formal training for downtime procedures and most of the weight fell onto senior nurses who experienced “pre-EHR” days. This heavy reliance on senior staff also resulted in heavy workload making it difficult for senior

staff to keep up with their own tasks while providing support to those inexperienced. Results from the interview saw that there were communication issues between and within departments, indicating a need to include effective communication plans to mitigate downtime. Several recommendations by participants made to improve downtime management are as follows:

- Have designated communication plans to alert all areas when one or more department experiences downtime.
- Reduce workload for services that are highly EHR dependent and automated and requires high levels of manual interventions.
- Train and drill all staff on downtime procedures.
- Have designated staff and support roles to handle nonclinical but necessary tasks to reduce workload. This includes communication and paperwork.

Many of these recommendations also share similarities to the general theme of SAFER guides. Safety Assurance Factors for EHR Resilience (SAFER) is a public guide made by the Office of the National Coordinator for Health Information Technology in order to "develop and validate proactive, self-assessment tools to ensure EHR-clinical work systems are safe and effective" (The office of the National Coordinator for Health Information technology, 2018). The SAFER guide is based on 3 phases:

- Phase 1 looks at safe HIT by addressing safety concerns unique to EHR technology and emphasizes data availability, data integrity and data confidentiality, the basic principles of EHR usage.
- Phase 2 is about using health IT safely by optimizing the safe use of EHRs. This can be done through complete and correct EHR usage and the overall EHR system's usability.

- Phase 3 focuses on monitoring safety where EHRs are used to monitor and improve patient safety through surveillance, optimization, and reporting.

There are a total of 9 SAFER guides which can help healthcare staff asses EHR downtime issues. (More information on the guide can be found on https://www.healthit.gov/topic/safety/safer-guides.) While SAFER was designed as a preventative method to mitigate and diagnose EHR downtime issues in a quick manner, it would be completely useless on large scale issues which could render the institution's computer useless like a ransomware attack where files become encrypted. Researchers also suggest that while the SAFER guide can provide a solid foundation on understanding EHR downtime it can use further development on the actual specification of how downtime procedures should be developed.

A 2017 article from the American Academy of Pediatrics discusses how many institutions have developed toolkits to mitigate risks of downtime (Cain, 2017). Toolkits contain paper copies of clinical documents and procedures when downtime occurs. These toolkits contain instructions on using analog paper documentation allowing inexperienced physicians to continue their work when computer systems only have access to read-only files. Other than paper documents, toolkits can benefit having items such as digital cameras, batteries, portable chargers and storage cards (Walsh et al, 2020). Conducting downtime training drills and usage of these toolkits will allow smooth transition in the event that downtime actually occurs. Thus, reducing heavy workload on experienced nurses and physicians who are relied on by younger and inexperienced staff members during downtime.

There are several strategies performed by HIT personnel which can reduce unplanned downtime. Providing redundancy and backups to systems are key mitigation concepts allowing

minimal interruption to clinical users when downtime occurs. Having generators, and uninterruptible power supplies are crucial when hospitals lose power. Archiving systems allow hospitals to retrieve data when there is a compromise in data integrity (Walsh et al, 2020). Lastly, regularly scheduled maintenance is necessary to keep computer systems up to date from vulnerabilities.

In 2014 a researcher conducted a survey on hospital infrastructure and downtime readiness. Representatives in the study were from 50 of the 59 (84%) institutional members of the Scottsdale Institute, over 80% being affiliated with large hospital systems (Sittig et al, 2014). All respondents to the study were CIOs or personnel directly responsible in maintaining their organization's HIT infrastructure. Participants were surveyed on if their hospital had the necessary infrastructure and practices to deal with unplanned downtime events. The tabulated results from this study shown below not only display the strengths and weaknesses of the 50 hospitals but are great reference points on what healthcare organizations need to focus on in order to mitigate downtime. Positive response in the survey were calculated based on the percent of participants responding positively to each item listed.

Dimension	Item	Positive response
Hardware/software	*Have an uninterruptable power supply (UPS)*	100%
Workflow	Test UPS at least monthly	50%
Hardware/software	*Have a back-up generator dedicated to HIT infrastructure*	96%
Workflow	Test generator at least monthly	79%
Hardware/software	Greater than 2 days of fuel	79%
Hardware/software	Greater than 75% of power replaced by generator	68%
Hardware/software	*Have a warm site*[a] *back up*	80%
Workflow	Warm-site available in 8 h or less	78%
Workflow	Test warm site at least quarterly	31%
Workflow	Warm-site has come online	70%
Workflow	Warm-site has come online because of an emergency	33%
Workflow	Switched over to warm site before 4 h	50%
Hardware/software	*Redundant path to the internet at organizational level*	92%
Internal policy/procedure	Different internet provider as their redundant path	68%
Hardware/software	*Have an EHRs interface transaction error log*	60%
Internal policy/procedure	Greater than 75% errors investigated and fixed	50%

[a] Remote site with pre-configured hardware and network connectivity on which an organization's application software and data can be quickly loaded.

Table 2. Overview of infrastructure for backup systems (Sittig et al, 2014)

Dimension	Item	Positive response
	Practices related to downtime, read-only EHR	
Hardware/software	*Have a network-accessible, hospital-wide read-only back-up*	77%
Workflow	Backup data updated at least every hour	85%
Workflow	Test central read-only back-up system at least monthly	33%
User interface	Downtime, read-only version of EHRs is clearly marked	62%
User interface	Downtime, read-only EHRs disabled during normal operation	45%
Hardware/software	*Have a local, clinic-level read-only back-up system*	75%
Workflow	Update data in clinic-level read-only back-up system at least hourly	90%
Internal policy/procedure	Clinicians activate clinic-level read only back-up system	50%
External rules and regulations	Read only clinic-level back-up system generic password protected	52%
Workflow	Test clinic-level read-only back-up system at least monthly	33%
Hardware/software	Clinic-level read-only back-up system connected to UPS	94%
	Practices related to data backup	
Content	*Back up patient data in a secure, off-site location*	100%
Content	Data at off-site location is complete and encrypted	48%
Workflow	Back-up their data to an off-site location daily	100%
Workflow	Organization conducts at least quarterly tests to ensure data can be reloaded	15%
Content	Back-up includes complete, up to date copy of all data used to configure system	96%
Workflow	Organization backs up data before every upgrade	100%
Personnel	*Organization trains staff on what to do in planned and unplanned downtime*	100%
Workflow	*Have a yearly unannounced downtime drill*	28%
Monitoring and surveillance	Follow up on drills looking for opportunities for improvement	100%
Internal policy/procedure	*Have a written downtime policy and procedure*	94%
Workflow	Review and update downtime policy at least every 2 years	41%
Workflow	Planned downtime communication strategy via email	81%
Workflow	Unplanned downtime communication strategy via email	59%
Workflow	Out of band downtime communication strategy (pager, overhead, people)	92%
	Availability of paper forms before downtime	
User interface	Order and document medications	88%
User interface	Order and document laboratory tests and results	92%
User interface	Order and document radiology tests and results	92%
User interface	Document RN observations and care delivered	83%
User interface	Document MD observations and plans	79%
Workflow	Enough paper on hand to last >48 h	43%
Personnel	Staff trained in use of paper forms	92%

Table 2. Overview of point-of-care components during downtimes (Sittig et al, 2014)

While it is acknowledged by both HIT and cyber security professionals that healthcare organizations are heavily at risk from cyber-attacks, many studies on the topic of downtime do not seem to include any mitigation strategies on preventing cyber-attacks. However, it is to be noted that cyber security in healthcare is already a prevalent topic outside of the idea of downtime, but more can be done. It is reported that 24% of U.S. healthcare employees have never received cybersecurity awareness training which could potentially cause vulnerabilities

within a healthcare organization's system. A 2019 survey reported nearly 60% of U.S. hospital representatives and HIT professionals agreed that email is the most common point of information compromise such as phishing scams and other types of email fraud (Cybersecurity Ventures, 2020). With emails being an essential tool for communication, not only is it easy to use, but also easy to create vulnerabilities for a healthcare organization's network. Users can get viruses when opening their emails usually when an unknown attachment or link is opened (Cybersecurity and Infrastructure Security Agency, n.d.). If the email client allows scripting, users can easily be infected with a virus just by opening up an email. The Cybersecurity and Infrastructure Security Agency (CISA), a department in Homeland Security says that the safest way to open email messages is simply as plain text without the use of HTML. Other recommended practices in mitigating cyberattacks include:

- Installing anti-virus software from a reputable vendor as well as regularly updating and using it to scan for viruses.
- Install an "on access" scanner which should be configured to check for viruses every time the computer is booted up. This is normally included in most anti-virus software packages.
- Before opening any new programs or executable programs use a virus scan. Normally computer systems belonging to an organization will lock the user's ability to download unauthorized programs to prevent potential vulnerabilities.
- Be cautious of accepting files or clicking links especially from an online community or chat room.

- Back up data such as documents, bookmarks, and important email messages in the event of the user's computer being compromised.

User accounts (like email, bank, and computer system) can be compromised without even having the user's computer infected with malware. This is usually done through phishing techniques where the user is tricked into giving personal information. Phishing scams can take the form of anything from an email, a fake webpage, a paper letter, and even a simple text message. Due to the creative nature of phishing scams, the best way to avoid them is by keeping up to date with the latest news on scams and be suspicious of messages from unknown senders even if they claim to be a legitimate organization.

Figure 3. Example of a phishing scam mimicking an urgent Netflix email (Federal Trade Commission, 2019)

Phishing scams can be hard to discern when there is no context such as the senders name or URL link sent, especially when webpages and emails can look legitimate. Falling for phishing scams can give the scammer enough personal information to hack into the victim's email which is a vulnerable point for healthcare personnel. Emails usually contain personal information and if a healthcare's personnel's email is compromised private emails and health records could be exposed. Phishing scams usually share several similar qualities that tricks users into clicking or opening attachments:

- Say they have noticed suspicious activity or log-in attempts to get users to log into a fake website and steal username and password.
- Claim there is a problem with account or payment information to potentially steal credit card information.
- Say that the user must confirm some personal information such as birthday date and answers to potential security questions.
- Sends user a fake invoice.
- Click on a link to make a payment.
- Tells user they are eligible to register for a government refund.
- Offer coupon for free stuff.

Similarly, with malware, updating computer, phone, and security software, and backing up data can mitigate security vulnerabilities from phishing scams. Users should also be changing passwords regularly as well as setting up a multi-factor authentication to deter hackers. While phishing scams might not directly cause unplanned downtime events, it does pose huge security

risks to healthcare organizations. Malicious hackers who use phishing can potentially hack into an organization's computer and infect the organization's network which could induce downtime.

Overall, mitigating unplanned downtime takes several different approaches. These approaches look at hospital infrastructure, personnel workflow and lastly computer and cybersecurity literacy. By following the mitigation techniques above, healthcare organizations should see an overall decrease in unplanned downtime due to vulnerabilities that can be controlled by personnel errors.

Discussion

There is no definitive solution to get rid of unplanned downtime. In order to fight downtime, the best way to mitigate damage caused by it is to simply be prepared as much as possible. Healthcare organizations should have the necessary infrastructure to provide support to their organization in the case of any situation such as a blackout or loss of data. Organizations should also have a properly funded HIT team and cybersecurity team to deal with increasing cyber threats. It is reported that health systems only allocate about 4-7% of their IT budget to cybersecurity while most sectors receive about 15% (Cybersecurity Ventures, 2020). Lastly, training for downtime procedures ensure that while healthcare organizations might be under more tension, staff should be able to continue following procedures without being unsure what to do. While these three factors play a big role in mitigating unplanned downtime, organizations should be constantly aware of new potential threats that can cause downtime. A great example of a threat healthcare organization should have known was the WannaCry attack. Now with COVID-19 we see unprecedented new potential causes for downtime. COVID-19 has forced

society to change habits making many recluses at home rather than going out. This societal change has put strain on the healthcare system tremendously especially in the beginning of 2020. The need for healthcare workers has risen but crowded areas are no longer acceptable due to fear of spreading the virus further. With hospitals overwhelmed, many healthcare organizations worldwide were blessed by the fact that many black hat hackers would not target hospitals during the chaos. Since the rollout of several COVID-19 vaccines, hackers have now continued their usual activities. In this section we will discuss several growing and current issues that threaten healthcare security and can potentially be new factors for downtime.

Evolving Threat

While many hospitals that experienced the first wave of COVID-19 patients are now able to handle more added stress like a cyberattack, vulnerabilities now lie elsewhere in the healthcare system that we have not seen before. One such new issue is network overload, where there are too many users on the internet at one time causing systems to be slower. With millions at home at the same time, doing strenuous online activities such as streaming videos, video conferences like Webex, Skype and Zoom and online video games can slow down the surrounding area's internet capabilities. This new push for working at home has also affected healthcare workers eligible for remote work. New initiatives like telemedicine uses the internet to communicate with patients who cannot physically come to see physicians. However, telemedicine would essentially be impossible if internet providers are unable to handle the load of users due to internet traffic. According to Moritz, "Typically businesses allocate enough network capacity to accommodate the everyday needs of a small number of employees working remotely, but

a large-scale shift could cause temporary trouble. If internet providers are unable to expand capacity and control traffic, users would essentially be unable to do any online activity. This includes physicians being unable to meet with their patients just because the internet is too slow. This is of course almost no different from downtime if healthcare providers are unable to do their job due to low bandwidth.

Another issue which can arise is the security vulnerabilities in remote work. It is reported that over 29% of the U.S workforce are able to work from home (Moritz, 2020). While working at home is safer during a pandemic, remote workers are less likely to have a secure internet network at home compared to at work. Organizations usually lend their workers a secured computer for their remote work needs, which is monitored and restricted to prevent malware and leakage of private information. If healthcare organization allow for remote access using an unsecured computer there could be consequences. With technology evolving we are beginning to see it take on more important tasks. From EHR system to IoMT devices and remote-controlled surgeries, everything has a connection to the internet. With a massive shift in work culture to move to remote work, hackers can take advantage of individuals with weak network security. An example of this during the COVID-19 pandemic was a cyberattack of a Florida water treatment plant on February 5, 2021. The incident entailed that the treatment plant was remotely hacked into and almost poisoned the state's water supply with a deadly level of sodium hydroxide (Levenson, 2021). Facilities with critical infrastructures are not meant for remote access work and are intentionally closed off from the internet. Vulnerabilities from the incident were simply a combination of the facility having remote access and multiple facility computers running an outdated version of Windows. Healthcare facilities are filled with devices that are critical

infrastructure like EHR systems or IoMT devices, having these devices connected to a remote computer could be an accident waiting to happen. The National Institute of Standard Technology (NIST) identified several vulnerabilities (Scarfone, n.d.):

- Remote access devices generally have weaker protection than standard client devices such as not being managed by an organization, not having firewalls or antivirus or lack of physical security controls.
- Remote access devices can be used in hostile environments but are not configured for them.
- Remote access communications use untrusted networks.

These vulnerabilities can then lead to:

- Hackers monitoring or manipulating communication such as deploying rogue wireless access points.
- Exploiting remote access client devices and users through phishing and keyloggers to collect credentials and other sensitive data or gain unauthorized access to an organization's resources.
- Loss or theft of remote access devices.

While remote access can create new vulnerabilities and threats, it does not mean it cannot be done securely. It is recommended that when allowing remote access, users should not have shared accounts, users should have multi-factor authentication and lastly use a Virtual Private Network (VPN). A VPN allows users to not directly expose their systems to the internet by encrypting the user's data and hiding their IP address or the user's physical location by routing connection requests through a VPN server. If someone tries to track the user the tracker will only

see the VPN's IP address and instead of the user's IP address (Levenson, 2021). The recommended advice on cybersecurity in the results section can also be used as a method to use remote access devices securely. Lastly, even though remote work has become more common due to COVID-19, it is likely that remote work will remain an option even after the pandemic ends. We will see more technology advancement on conference applications as well as more secured remote access devices as the professional work environment shifts to a combination of office and remote work.

Extended Look into Cyber Security

While we know about cyber-attacks and basic malware and ransomware tactics, cyber security is an extensive field and requires deeper understanding. This part of the discussion looks into a more in-depth view of cyber security and common terminology. This section was made to help individuals that want to understand more about downtime caused by cyberattacks but are not well versed in the topic of cyberspace. Around 94% of healthcare organizations have experienced a cyber-attack so it is important for organizations to understand what cyber security professionals look at when attacks happen (Bhuyan et al, 2019). Cyber-attacks happen in healthcare usually for extortion purposes, where hackers try to hold information ransom until said hacked organization pays a specified amount usually in hundreds of thousands. Later, in the discussion on the topic of, "The War on Big Data", we will also discuss the value of stolen healthcare data beyond monetary purposes and how foreign powers can exploit it.

A breach is defined as an event in which information is lost, stolen or displaced, hacked or communicated to unofficial recipients. Oddly enough however, around 70% of data frauds in organizations are done by insiders (Bhuyan et al, 2019). Patient records store all sorts of

sensitive data such as names, date of birth, social security numbers, addresses and credit card information, all which are valuable in the black market. Compared to value of credit card information on the black market, healthcare patient data can be worth 10 to 100 times more. Beyond ransomware and phishing, there are many other different types of cyber threats.

Denial-of-Services or commonly known as a DoS attack is a commonly known cyberattack where a network is flooded with traffic that disrupts services and can even shut down an entire network depending on the intensity of the traffic. DoS attacks can prevent healthcare providers in accessing or transmitting vital data.

Privilege Escalation is a type of attack which exploits vulnerabilities in a program or network. The primary goal is to gain higher level access in a program or network through those vulnerabilities. By gaining a higher level of access hackers can change patient information. Malware that has infected an organization's system can inflict even more damage by escalating privileges of access to their system.

A Cryptographic attack is simply decrypting encrypted information. Organizations usually encrypt sensitive data and files on their network computers as to hide data from those that do not have privilege or access to view them. If those files were somehow transferred to another computer, it would simply be gibberish. A ransomware attack can be seen as the opposite where the hacker would encrypt data making files unreadable to the victim until a ransom is paid to receive a key to decrypt. Hackers that initiate a cryptographic attack on the other hand try to decrypt an organization's encrypted data to use for malicious purpose such as selling personal information on the black market.

Man in the Middle or sometimes known as Eavesdropping unlike the previous cyberattacks focus on reconnaissance where the attacker intercepts communication between two parties. The attacker then could use the intercepted information to blackmail both parties.

Structured Query Language Injections Exploit is a more sophisticated cyber-attacks compared to the above discussed attacks. Structured Query Language (SQL) is a commonly used programming language to manage databases and is practically the lynchpin that holds systems like EHRs and patient register systems together that uses it. Attackers could exploit the vulnerabilities in SQL and execute detrimental commands to the system such as altering important information in the database.

Many cyberattacks utilize malicious software to execute an attack. Like cyberattacks, there are several different kinds of malware. Other than ransomware which we have gone over Trojans are commonly known malware which can give hackers a “backdoor” and allow access into infected computers (Bhuyan et al, 2019). Trojans can be unknowingly installed into an infected computer by appearing as a useful and legitimate software. This backdoor in infected computers can put patient information at risk. In 2017, the Alaska Department of Health and Social Services were hit by Trojan attacks on two separate computers (Davis, 2017). Through the Trojan virus, the attackers were potentially able to access confidential data from the Office of Children’s Services, which contained family case files, diagnoses, medical observations, and other personal information.

Spyware is the form of malware which is used in Eavesdropping attacks and can sometimes take the form of Trojans. Like most malware, it is unknowingly installed and transmits the victim’s activities over the internet. A common form of spyware is a keylogger

which logs down all of the victim's keystrokes and sends them to the attacker, which is an easy way to find out information such as usernames, passwords and banking information.

While sometimes used interchangeably with malware, a virus is actually the most common type of malware. Viruses are simple malware that usually insert themselves as executable files to host files and then delete files, data, or code or add useless code to corrupt programs until it stops working. While viruses are known as the most common form of malware, today we see less virus attacks making headlines compared to the more complex alternatives. A worm is a type of virus as it self-replicates and propagates independently. The key difference is that unlike a virus which is triggered by the activation of the host, worms are not held back by that limitation. Worms are considered more dangerous than a virus as it can spread rapidly. A well-known worm attack is the 2017 WannaCry attack which quickly infected thousands of healthcare organizations' computer systems worldwide and especially wreaking havoc in the UK.

The importance of computer and cyber security literacy will begin to increase as future generations are exposed to growing technology. EHR systems were created in the 1960s but were made mandatory fairly recently. Today all hospitals rely on computer technology to assist with all aspect of work. Not having literacy in computer and cyber security is the same thing as driving a car without a license. Because there is such a reliance on technology, personnel should be able to understand the basics of using a computer like connecting to the internet, printing documents and virtual conferencing applications. Along with computer basics, is computer safety as users who do not understand computer basics are the most at risk of exposing their healthcare organization's network system to danger. Usually, the lack of knowledge in

technology comes from older personnel who were not exposed to the same level of technology as younger generation are. It is recommended for older personnel who might not understand technology as much learn basic up-to-date computer terminology as to close the gap in computer literacy. However, while older personnel might be more likely to not have a comprehensive understanding of computer and cyber security, anyone can be susceptible to malicious cyberattacks if they are not careful.

Bring Your Own Devices (BYOD)

Historically, computers were gigantic machines that had no interface, and complex functionality. It is only recently within the last two decades that computers are user friendly for casual usage and portability. The portability and advancement of phones are basically minicomputers that can be brought and used almost anywhere. Smart phones have made daily tasks easier and are in the hands of most people, however just like remote access work, its wide usage creates possible issues that healthcare organizations will have to face. Personal devices like a smart phone are considered as BYOD in a work setting. Due to the lack of security and lack of the organization's control on a device, BYODs are security risks for leaking sensitive healthcare data (Wani et al, 2019). BYOD is considered a phenomenon where organizations allow their employees to use their personal devices in the workplace for professional duties. Traditionally, employers would provide devices in the workplace as a way to control and secure the surrounding network. However, most BYODs lack the same security configurations as workplace provided devices since they are personal devices not controlled by the employer. BYODs are extremely helpful as they are multifunctional such as communication, photos, and

documentation or for clinical references through online resources. While extremely helpful, due to the lack of control employers have over BYODs every new added device becomes an added risk. A survey showed that 28% of US healthcare doctors stored patient information in their own mobile devices, 14% of these devices contained no form of authentication to protect patient information, furthermore 11% of devices were highly vulnerable to security breaches (Wani et al, 2019). While healthcare organizations' IT departments can enforce compulsory use of long and complex passwords, automatic log-off after a period of inactivity, using a preferred and secure application and connecting to a VPN to create a safer environment, researchers found that these methods to be ineffective. Research suggests that hospital employees would neglect tedious security protocols for better user experience. An example would be physicians consistently using a non-recommended application like Whatsapp which lack the necessary security to send sensitive messages and photos about patients, even when said application is banned. Employees would also forget to logoff of medical applications possibly giving access to unauthorized users if their devices are compromised or stolen. In order to use BYOD safely in healthcare, employees must agree to have strict guidelines to use their devices in a safe manner. It is recommended that BYODs must be registered and follow their IT department's safety standards. All registered devices must grant permission to install necessary security configurations or certificates, lastly if a BYOD causes or is a threat for a security breach the organization's IT department has the ability and permission to remotely wipe personal data off the user's device.

The War on Big Data

Much of recent technology is built with artificial intelligence (AI) capabilities. AI is expected to make the world easier in all form of industries including Healthcare. EHR and

Clinical Decision Support Systems (CDSS) are common examples of healthcare technology with AI built in. Particularly in CDSS where AI is used to help assist physicians to make decisions in diagnosing a patient. The advent of AI technology is driven by big data which refers to datasets containing large volumes of gathered structured or semi-structured data to train AI programs. Big data is also referred to as the new gold due to its limitless potential in various industries. On January 31, 2021 CBS released an episode of 60 Minutes reporting on the Chinese Communist Party's (CCP) push on controlling America's healthcare (CBS news, 2021). According to FBI investigator Edward You, that by gathering large datasets on DNA the CCP can potentially create a personalized and effective healthcare plan at a low cost. While the interview looks at the CCP's goal of monopolizing healthcare, the major issue lies in how they are getting their data. Former top counterintelligence official, Bill Evanina says in the interview, "Current estimates are that 80% of American adults have had all of their personally identifiable information stolen by the Communist Party of China" (CBS news, 2021). China's interest in private health information is dangerous for healthcare organizations and HIPPA laws and can be considered a national security threat. Not only are healthcare infrastructure vulnerable from a cyber-attack from China, but patient privacy is at risk of being stolen and sold on the black market. A 2019 security report from Trustwave says that a health care record data can be valued up to $250 on the black market (Trustwave, 2019). It has already been reported that China is using gathered DNA datasets on the Chinese Uyghur population. By using their DNA, facial recognition and surveillance software can recognize if a person is Uyghur or not. DNA becomes more relevant on the individual level as it can be seen as a person's unique biomarker that identifies them, just like a Social Security Number or driver's license. While the idea of using a large number of genetic data can bring

about good, stricter laws on usage of patient information must be passed, not just on a national level but globally. As data become more valuable healthcare organizations will most likely face more cyberattacks seeking patient health information.

Minimizing Planned Downtime

Planned downtime normally occurs for infrastructure maintenance and usually refers to scanning for malware or getting updates done on computer systems to minimize potential vulnerabilities. While updating software can be a mundane task which can take hours, software engineers create updates in order to improve user experience and strengthen software. Updating can help fix version issues such as a function in the program not responding as designed or to protect volatile users from malicious actors trying to get access into the system. It also allows for better compatibility with newer computer systems. Software compatibility with a computer's OS can become an issue if software is not maintained by the vendor. Overtime, software programs can become outdated and while the version of the program being used could be perfect on the end-user side, it might eventually lose compatible with newer updated computer systems internally. Software updates are beneficial, but this also means system usability might be down when they occur. While schedule maintenance is usually done during low impact hours, planned downtime can still hinder users when systems are not available. A recent study published by collaborating researchers at Facebook and Brown University, looked into possible ways for eliminating downtime in order to update applications, researchers referred to this as Zero Downtime Release (Naseer et al, 2020). The study came into fruition by looking into how big companies like Facebook whose whole business model is reliant on users constantly being on their application and cannot afford to shut down to do maintenance. Zero Downtime Release is a

mechanism used to shield end-user from disruptions and to preserve robust infrastructure of digital businesses. The ability of being able to send updates to programs without any physical disruption will be able to further push all businesses. Beside the concept of zero disruptions during updates, Zero Downtime Release allows for the use of pre-existing kernels. The use of pre-existing kernels or the central module of an OS, allows for older systems to use Zero Downtime Release without any physical changes to hardware. However, there will be limitations in implementing this design in other systems such as EHRs and computer OS as they are fundamentally different compared to companies like Facebook which delivers their updates for their mobile application and web-based services. EHRs and Operating Systems are local stored on a computer and while EHRs might access databases that are online or stored in a separate server, delivering non-disrupting updates might prove challenging. Vendors will have to look at most likely a different type of architecture to introduce Zero Downtime Release for local computer applications. In the future we will most likely see the actual implementation of Zero Downtime Release as it will not only save on manhours in computer maintenance, but money in many industries including healthcare.

COVID-19

As discussed in the beginning of the section, COVID-19 has put healthcare organizations at risk for downtime. On April 2020, the International Criminal Police Organization released a report warning about a global increase in cyber-attacks relating to COVID-19 virus. A study published by International Journal for Quality in Health Care documented the most recent attacks from the start of the pandemic to end of July 2020.

Date of Cyber-Attack	Country/ Institution	Reported Details
13 March 2020	Brno University Hospital, Czech Republic	Shut down of the IT network that caused postponement of urgent surgeries and compromised emergency medical care (https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attackwhile-in-the-midst-of-a-covid-19-outbreak/).
13 March 2020	World Health Organization (WHO)	Creation of a malicious site mimicking the WHO internal email system which aimed to steal employee passwords (https://tech.newstatesman.com/security/who-cyber-attackcovid19).
14 March 2020	Hammersmith Medicines Research Group, UK (COVID-19 Vaccine Trial Group)	Ransomware attack resulting in the publication of personal details of former patients, and a failed attempt to disable the network (https://www.computerweekly.com/news/252480425/Cybergangsters-hit-UK-medical-research-lorganisation-poised-for-workon-Coronavirus).
16 March 2020	United States Health and Human Services (HHS) Department	Unspecified attack on the HHS servers (https://tech.newstatesman.com/security/us-health-humanservices-department-cyber-attack).
22 March 2020	Paris Hospital Authority (APHP), France	Unspecified attack on AP-HP servers (https://www.bloomberg.com/news/articles/2020-03-23/parishospitals-target-of-failed-cyber-attack-authority-says).
4 April 2020	UK and Spanish Healthcare Workers	Ransomware attack attempting to deactivate anti-virus software (https://www.computing.co.uk/news/4012969/hospitalscoronavirus-ransomware; https://www.digitalhealth.net/2020/04/neither-covid-19-norcyber-criminals-care-who-gets-infected-and-suffers/).
13 May 2020	UK's ARCHER Academic High-Performance Computing (HPC) network	Exploitation of login nodes forcing rewriting on all user passwords (https://www.theregister.com/2020/05/13/uk_archer_supercomputer_cyberattack/).
13 May 2020	Bam Construct and Interserve (Companies who helped construct temporary COVID-19 hospitals for the UK's National Health Service)	Unspecified attack (https://www.constructionnews.co.uk/contractors/bamconstruct/bam-construct-hit-by-cyber-attack-13-05-2020/).
10 June 2020	Babylon Health (Appointment and video-conferencing software for NHS doctors)	Data breach due to software error (https://www.mobihealthnews.com/news/europe/babylon-healthadmits-gp-hand-app-data-breach-caused-software-issue).
16 July 2020	US, UK and Canadian authorities	Alleged unspecified state-sponsored cyber-attacks on institutions working on COVID-19 vaccines (https://www.theguardian.com/world/2020/jul/16/russian-statesponsored-hackers-target-covid-19-vaccine-researchers).

Table 3. Summary of reported cyber-attacks/data breaches in healthcare and academic organizations during the COVID-19 outbreak (Stevenson et al, 2020).

While the study is slightly outdated with multiple new cases appearing after the paper published, this study provides great insight on cyberattacks during the height of the pandemic. Attacks on WHO and institutions in the US, UK and Canada that were working on a vaccine for COVID-19 are most notable in the study. While the pandemic distracted many, hackers were already looking for a way to steal the cure to the pandemic itself. Institutions that are treating COVID-19 patients or are researching for a more effective cure or are currently distributing vaccinations should be on alert as hackers might want to hamper on operations for ransom.

Conclusion

Unplanned downtime is a dangerous phenomenon especially during a pandemic. Downtime is most dangerous when there is a large number of patients in a healthcare facility as it can overwork clinicians. Since there is no one definitive solution, healthcare institutions must implement downtime toolkits and contingency plans. However, having a contingency plan and actually implementing it is easier said than done. Staff should have thorough training on the process in order for smooth transition when downtime occurs. Strengthening communications between departments is crucial as so staff members can understand issues between departments that might affect them. Infrastructure is also critical in preventing downtime and should not only have the necessary tools to sustain an organization if downtime were to occurs but also have regular maintenance. Malicious actors who use cyberattacks, malware and phishing scams are one of the biggest causes for unplanned downtime and can put thousands if not millions of lives in danger. These cyber-criminals can disrupt patient-records, imaging and surgical services,

medical devices, appointment systems and even pacemakers. If healthcare organizations under-invest in their IT and cyber security departments it can leave them vulnerable to attacks that can shutdown devices, servers or even networks and ultimately causing downtime. Covid-19 is not only causing strain in hospitals globally but is changing how healthcare institutions will be vulnerable to unplanned downtime. Prior to the pandemic, many institutions already lacked adequate mitigation strategies in dealing with unplanned downtime. While unplanned downtime is well known, little research has actually been published and more research should be conducted in the future to accommodate recent change in society due to the pandemic such as risk of working at home and new mitigation strategies that better accommodate the situation. Organizations currently working with COVID-19 related matters should be cautious as it can mark them as a target for cyberattacks. Overall, mitigating downtime means looking at hospital infrastructure, personnel workflow and computer and cybersecurity literacy. By applying downtime mitigation strategies in these perspectives, we can better protect our healthcare institutions, personnel, and patients.

References

1. Beshar, P. J. (2020, December 9). *The hacker 'ceasefire' with hospitals is over—and that should terrify us*. Fortune. https://fortune.com/2020/12/09/covid-hospitals-hackers-ransomware/
2. Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D., & Dobalian, A. (2020). Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. *Journal of Medical Systems*, *44*(5), 97–99. https://doi.org/10.1007/s10916-019-1507-y
3. Cain, M. (2017, November 8). *When not if: How to prepare for EHR downtime*. American Academy of Pediatrics. https://www.aappublications.org/news/2017/11/08/HIT110817
4. Centers for Disease Control and Prevention. "Public Health and Promoting Interoperability Programs." *Centers for Disease Control and Prevention*, Centers for Disease Control and Prevention, 17 Sept. 2020, www.cdc.gov/ehrmeaningfuluse/introduction.html.
5. Cybersecurity and Infrastructure Security Agency. (n.d.). *Virus Basics | CISA*. Https://Us-Cert.Cisa.Gov/. Retrieved April 1, 2021, from https://us-cert.cisa.gov/publications/virus-basics#:%7E:text=Most%20viruses%2C%20Trojan%20horses%2C%20and,by%20simply%20opening%20a%20message.&text=The%20safest%20way%20to%20view%20email%20messages%20is%20in%20plain%20text.
6. Cybersecurity Ventures. (2020). *The 2020 Healthcare Cybersecurity Report*. Herjavec Group. https://www.herjavecgroup.com/wp-content/uploads/2019/12/Healthcare-Cybersecurity-Report-2020.pdf

7. Davis, J. (2017, September 7). *Alaska DHSS facing potential breach after two Trojan malware attacks*. Healthcare IT News. https://www.healthcareitnews.com/news/alaska-dhss-facing-potential-breach-after-two-trojan-malware-attacks

8. Federal Trade Commission. (2019, May). *How to Recognize and Avoid Phishing Scams*. https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

9. Department of Health and Human Services, and Office for Civil Rights. "HITECH Act Enforcement Interim Final Rule." *HHS.gov*, US Department of Health and Human Services, 16 June 2017, www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.

10. D. Halperin *et al.*, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," *2008 IEEE Symposium on Security and Privacy (sp 2008)*, Oakland, CA, USA, 2008, pp. 129-142, doi: 10.1109/SP.2008.31

11. Goar, E. (2017, November). *The Price of EHR Downtime - For The Record Magazine*. The Price of EHR Downtime. https://www.fortherecordmag.com/archives/1117p24.shtml

12. Jercich, K. (2020, September 29). *UHS hospital chain hit with apparent ransomware attack*. Healthcare IT News. https://www.healthcareitnews.com/news/uhs-hospital-chain-hit-massive-ransomware-attack

13. Langer, S. G. (2016). Cyber-Security Issues in Healthcare Information Technology. *Journal of Digital Imaging*, *30*(1), 117–125. https://doi.org/10.1007/s10278-016-9913-x

14. Larsen, E., Haubitz, C., Wernz, C., & Rat., R. (2016). Improving Electronic Health Record Downtime Contingency Plans with Discrete-Event Simulation. *2016 49th Hawaii*

International Conference on System Sciences (HICSS), 1–11. https://doi.org/10.1109/hicss.2016.399

15. Larsen, E., Hoffman, D., Rivera, C., Kleiner, B. M., Wernz, C., & Rat., R. M. (2019). Continuing Patient Care during Electronic Health Record Downtime. *Applied Clinical Informatics*, *10*(03), 495–504. https://doi.org/10.1055/s-0039-1692678
16. Larsen, E. P., Rao, A. H., & Sasangohar, F. (2020). Understanding the scope of downtime threats: A scoping review of downtime-focused literature and news media. *Health Informatics Journal*, *26*(4), 2660–2672. https://doi.org/10.1177/1460458220918539
17. Levenson, E. C. (2021, February 13). *Florida water hack highlights risks of remote access work without proper security*. CNN. https://edition.cnn.com/2021/02/13/us/florida-hack-remote-access/index.html
18. Moe, M. (2017, June 3). *Go Ahead, Hackers. Break My Heart*. Wired. https://www.wired.com/2016/03/go-ahead-hackers-break-heart/
19. Moritz, S. (2020, March 8). *Empty offices, full homes: Coronavirus might strain the internet*. Fortune. https://fortune.com/2020/03/08/coronavirus-internet-remote-work-from-home/
20. Naseer, U., Niccolini, L., Pant, U., Frindell, A., Dasineni, R., & Benson, T. A. (2020). Zero Downtime Release. *Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication*, 1–13. https://doi.org/10.1145/3387514.3405885
21. National Audit Office. (2018, April). *Investigation: WannaCry cyber attack and the NHS*. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

22. Riggi, J. (2020). *Ransomware Attacks on Hospitals Have Changed | Cybersecurity | Center | AHA*. American Hospital Association. https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed

23. Scarfone, K. (n.d.). *Security Concerns with Remote Access*. NIST. https://csrc.nist.gov/CSRC/media/Events/HIPAA-Security-Rule-Implementation-and-Assurance/documents/NIST_Remote_Access.pdf

24. Sittig, D. F., Gonzalez, D., & Singh, H. (2014). Contingency planning for electronic health record-based care continuity: A survey of recommended practices. *International Journal of Medical Informatics*, *83*(11), 797–804. https://doi.org/10.1016/j.ijmedinf.2014.07.007

25. Stevenson, K., & Muthuppalaniappan, M. (2020). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, *33*(1), https://doi.org/10.1093/intqhc/mzaa117

26. The office of the National Coordinator for Health Information technology. (2018, November 28). *SAFER Guides* HealthIT.Gov. https://www.healthit.gov/topic/safety/safer-guides

27. Trustwave. (2019). *2019 Trustwave Global Security Report*. https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/

28. Walsh, J. M., Borycki, E. M., & Kushniruk, A. W. (2020). Effects of Electronic Medical Record Downtime on Patient Safety, Downtime Mitigation, and Downtime Plans. *International Journal of Extreme Automation and Connectivity in Healthcare*, *2*(1), 161–186. https://doi.org/10.4018/ijeach.2020010110

29. Wani, T., Mendoza, A., & Gray, K. (2019). BYOD in Hospitals-Security Issues and Mitigation Strategies. *ACSW 2019: Proceedings of the Australasian Computer Science Week Multiconference*, 1–10. https://doi.org/10.1145/3290688.3290729

30. Wertheim, J. (2021, February 1). *China's push to control Americans' health care future - 60 Minutes*. CBS News. https://www.cbsnews.com/news/biodata-dna-china-collection-60-minutes-2021-01-31/