*Journal of the American Medical Informatics Association*, 26(1), 2019, 81–90
doi: 10.1093/jamia/ocy148
Advance Access Publication Date: 28 November 2018
Review

Review

# EARS to cyber incidents in health care

**Mohammad S Jalali,[1] Bethany Russell,[1] Sabina Razak,[1] and William J Gordon[2,3,4]**

[1]MIT Sloan School of Management, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA, [2]Division of General Internal Medicine, Department of Medicine, Brigham & Women's Hospital, Boston, Massachusetts, USA, [3]Partners Healthcare, Boston, Massachusetts, USA, and [4]Harvard Medical School, Harvard University, Boston, Massachusetts, USA

Corresponding Author: Mohammad S. Jalali, PhD, MIT Sloan School of Management, Massachusetts Institute of Technology, 245 1st St, E94-1567, Cambridge, MA 02142, USA (jalali@mit.edu)

Received 23 July 2018; Revised 15 October 2018; Editorial Decision 18 October 2018; Accepted 18 October 2018

**ABSTRACT**

**Background:** Connected medical devices and electronic health records have added important functionality to patient care, but have also introduced a range of cybersecurity concerns. When a healthcare organization suffers from a cybersecurity incident, its incident response strategies are critical to the success of its recovery.
**Objective:** In this article, we identify gaps in research concerning cybersecurity response plans in healthcare. Through a systematic literature review, we develop aggregated strategies that professionals can use to construct better response strategies in their organizations.
**Methods:** We reviewed journal articles on cyber incident response plans in healthcare published in PubMed and Web of Science. We sought to collect articles on the intersection of cybersecurity and healthcare that focused on incident response strategies.
**Results:** We identified and reviewed 13 articles for cybersecurity response recommendations. We then extracted information such as research methods, findings, and implications. Finally, we synthesized the recommendations into a framework of eight aggregated response strategies (EARS) that fall under managerial and technological categories.
**Conclusions:** We conducted a systematic review of the literature on cybersecurity response plans in healthcare and developed a novel framework for response strategies that could be deployed by healthcare organizations. More work is needed to evaluate incident response strategies in healthcare.

**Key words**: incident response strategies, cyber incidents, healthcare organizations, cybersecurity, systematic review

## INTRODUCTION

Healthcare organizations are increasingly affected by cybersecurity attacks. These incidents can have numerous deleterious effects on healthcare organizations, from the inadvertent release of protected health information to disruptions in clinical care.[1,2] Healthcare organizations must establish effective responses to new cybersecurity threats in order to avoid long periods during which they are unable to access essential health records and provide safe clinical care.[3,4] In the current climate of advanced cyber threats, successful attacks are all but inevitable, and healthcare organizations must be able to respond appropriately. Healthcare systems can no longer focus their resources on medical purposes alone.[5]

Many organizations focus their cybersecurity management on prevention and detection capabilities. Incident handling or incident response, which the U.S. National Institute of Standards and Technology defines as the mitigation of violations of security policies and recommended practices,[6] is an essential component of organizational cybersecurity hygiene, and should be established prior to an actual cyberattack.[4] Response plans can attenuate the impact of attacks and ultimately minimize the negative consequences. Unfortunately, incident response is often ignored as a cybersecurity management strategy.[7] A 2018 study of 2800 respondents from various industries found that 77% do not consistently apply formal incident response plans across their organizations. About half also reported

that their incident response plans were either completely nonexistent or informal/ad hoc.[8] We suspect that this discrepancy is even more pronounced in healthcare organizations, given that healthcare is falling behind other industries when it comes to cybersecurity preparedness in general.[9]

In this article, we aim to identify gaps in research concerning cybersecurity response plans for healthcare delivery organizations. Through a systematic review, we developed 8 aggregated strategies that can be used by cybersecurity professionals to construct response strategies in their organizations.

## METHODS

### Search strategy

A systematic review was conducted to look at research on incident response strategies in healthcare organizations. This process was carried out in 2 parts. First, we conducted a broad search to locate articles relevant to both cybersecurity and healthcare. We identified search keywords by adopting terminologies in The National Initiative for Cybersecurity Careers and Studies[10] and The British Standards Institution glossaries[11]—see Supplementary Figure S1 in the supplementary document for search terms. A second search was done within those articles to identify studies with a focus on incident response strategies.

### Inclusion and exclusion criteria

We reviewed journal articles published from the inceptions of PubMed (1966) and Web of Science (1900) to September 2017. The inclusion and exclusion criteria were defined prior to the review of articles. In order to be included, articles had to be research papers written in English that demonstrated a clear application to cybersecurity, healthcare, and response. This study excluded conference and review articles.

Each selected article was reviewed by 2 researchers. If there was a disagreement between the reviewers regarding the inclusion or exclusion of an article, discussion and further review of the article was conducted until a final decision was reached.

### Data extraction, synthesis, and quality assessment

Articles meeting the inclusion criteria were reviewed to determine recommended response strategies. Each article was reviewed individually, and the recommendations were noted. A second review was conducted to aggregate these recommendations.

To evaluate the quality of the articles, we assessed the scientific methods in each study using tools from the National Heart, Lung, and Blood Institute.[12,13] These tools provided concise criteria for assessing the quality of the research methods. The full list of quality assessment tools and individual scores can be found in Supplementary Table S1 in the supplementary document. Most assessment questions, except for 1, required a binary answer to determine whether a method satisfied the requirement. It should be noted that none of the articles in the review process was excluded based on the quality assessment results.

## RESULTS

Figure 1 outlines the search method and inclusion process for the selected articles. Out of the 1980 papers initially searched concerning cybersecurity and healthcare, 472 had a primary focus on the intersection of the 2 topics. Within that 472, only 33 referenced response, and 4 other articles were added through the citations of the 33 articles. Upon further full-text review, 13 of those potential 37 articles fulfilled the inclusion criteria with a significant focus on incident response plans in healthcare.

### Study characteristics

The characteristics of the studies included in this review are presented in Table 1. There were 8 studies from the United States, 2 from the United Kingdom, 1 from Lebanon, 1 from the Netherlands, and 1 from Singapore. The papers used different methods to generate results. Four studies were based on the author's perspective, 3 involved a case analysis, 2 were achieved through modeling, 1 was done using experimental analysis, 1 involved interviews, 1 conducted a needs assessment, and 1 conducted a survey followed by a correlational analysis.

### Aggregation of recommendations

The 13 articles that met the inclusion criteria for this review produced significant recommendations for handling incident responses in healthcare. Throughout the review of these articles, it became clear that some articles shared the same response recommendations. To avoid repetition, these recommendations were aggregated into 8 strategies, creating the eight aggregated response strategies (EARS) framework. A comprehensive list of the strategies can be found in Table 2. The most common overlapping recommendation included in the EARS framework was the involvement of key personnel within the organization. For a visual presentation of the EARS framework, see Figure 2. We sorted each of the 8 response recommendations into managerial and technological categories, based on the nature of their implementation. We then divided the elements of the 8 strategies (R1-R8) into pre- and post-incident actions.

### Pre-incident actions

**R1 - construction of an incident response plan**

An incident response plan (IRP) should be established to guide a healthcare organization through a cyber incident. Regardless of preventive efforts, organizations can still fall victim to attacks. A healthcare organization needs an IRP to specify how to document and react to incidents when they occur. Incident containment and remediation is already stressful, and creating a response strategy while simultaneously trying to handle an incident only exacerbates the issue.[15] An IRP should include steps for detection, investigation, containment, eradication, and recovery.[15] The first step of the IRP should be notification of key personnel about the breach.[17] The IRP should also include the contact information for legal counsel (for assistance in determining whether the applicable local requirements for cybersecurity are being met) and for the relevant law enforcement agencies.

Investigating the incident is a crucial step in the plan. A digital forensics expert needs to be contacted for this process. Once incident investigation is completed, the organization must implement a corrective action plan and address public breach notification methods. All vulnerabilities involved with this incident should be patched. This section of the IRP can also include employee disciplinary actions. The IRP should thoroughly document all mitigating steps. All evidence must also be secured and documented, including a chain of custody to trace each person who came in contact with the evidence in case any post-incident alterations are found later.[16] The organization can construct a contingency plan alongside the IRP to ensure the functionality of healthcare systems during an incident.

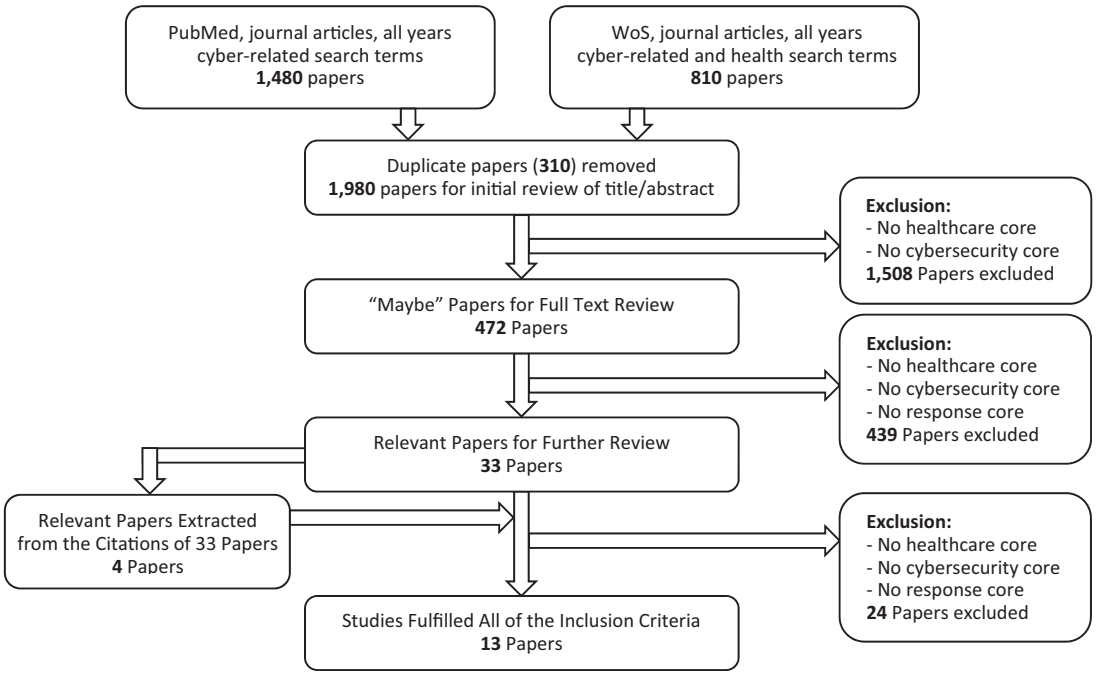


**Figure 1.** Search method and inclusion process.

This can include methods of alternative communication, alternative facilities to use, and utilization of loaned or backup equipment from other hospitals. The safety of patients always comes first in the healthcare industry, so it is essential to identify these temporary communication channels and infrastructure in addition to technological responses.[15]

**R2 - construction of an information security policy to act as a deterrent**

There are many benefits to having a good information security policy in place. Most importantly, clearly defined security measures deter computer abuse and establish compliance. These policies need significant backing to be successful; this means support from management and the allocation of necessary funding. Once the policy is created, it must be regularly followed, maintained, and updated. In a survey study conducted in hospitals in central Kentucky, researchers found a positive correlation between the existence of an information security policy and the reporting of incidents within healthcare institutions. The study also demonstrated a strong relationship between the existence of an information security policy and the reporting of the *seriousness* of the incidents. However, information security policies alone are not sufficient to protect a healthcare organization. They should be accompanied by additional measures, such as security awareness training sessions and distributed policy statements.[18,19]

**R3 - involvement of key personnel within the organization**

Regardless of the size of a healthcare organization, all key personnel must be educated on the importance of information security, with an emphasis on response. Physicians may believe a certified electronic health record system provides the necessary security infrastructure. Leaders begin to emphasize information security only once the healthcare organization falls victim to an attack or must prepare for an upcoming audit. These are not appropriate practices; information security systems, especially information breach response strategies, deserve adequate attention. Small-practice physicians tend to be unaware of the pervasiveness of cyber threats and often hold the misconception that their practices are not large enough targets to attract hackers. There is no healthcare organization too small to be targeted for an attack.[14] All organizations should invest in information security.

The support of managers within a healthcare organization can determine the success of a response strategy.[17] An organization should have a group of key personnel responsible for dealing with high-level cyber incidents. This group can range from department managers to doctors and physicians.[16,20] Key personnel do not need to be experts on the technical aspects of the incident response strategy, but they are responsible for understanding the effect an incident will have on the organization. In fact, it is often the front-line workers, as opposed to executives, who are the first to be exposed to the signs of a cybersecurity breach. For this reason, it is imperative that key personnel be able to detect and respond to such an incident. If the key personnel are fully aware of the criticality of an attack, they are more involved in response plans. To understand response strategies, these leaders must identify the potential effects of an attack in their daily work processes and on their organization's reputation.[15] One strategy is for organizations to develop multidisciplinary healthcare organization teams. Members of these teams can provide different perspectives on incidents and aid in developing and improving response plans, and should engage in timely and effective communication.[23] It is essential for the team members to understand the importance of shared team knowledge.[21]

**R4 - regular mock testing of recovery plans**

Regular testing of recovery plans can improve response strategies within a healthcare organization. Performing response strategies prior to the occurrence of an actual incident trains employees to practice proper response protocol. If a healthcare organization waits until the incident occurs to test its response plan, the organization

**Table 1.** Study characteristics (sorted based on publication year)

| Article Title | Year of publication | Journal | Journal category; ranking quartile* | Citations** | Country of publication | Research method | Keywords |
|---|---|---|---|---|---|---|---|
| Computer security incident response team effectiveness: a needs assessment | 2017 | *Frontiers in Psychology* | Psychology (multidisciplinary)-Q2 | 0 | Netherlands | Needs assessment | Incident handling; team performance; CSIRT; collaborative sensemaking; internal communication; CERT; team cognition |
| Challenges of information security incident learning: an industrial case study in a Chinese healthcare organization | 2017 | *Informatics for Health & Social Care* | Health care sciences and services-Q4; medical informatics-Q4 | 4 | UK (case study in China) | Case analysis | Information security; incident response; incident learning; healthcare; security assurance modelling |
| Using agility to combat cyber attacks | 2017 | *Journal of Business Continuity & Emergency Planning* | N/A | 0 | USA | Author's perspective | Agile; incident; cyber; BCR; DR; teams |
| Data damage assessment and recovery algorithm from malicious attacks in healthcare data sharing systems | 2016 | *Peer-to-Peer Networking and Applications* | Computer science (information systems)-Q3; telecommunications- Q3 | 5 | Lebanon | Experimental analysis | Data security; data exchange; healthcare data protection; healthcare data tampering |
| The rise of ransomware | 2016 | *Texas Medicine* | N/A | 0 | USA | Interview | N/A |
| A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks | 2016 | *Applied Clinical Informatics* | Medical informatics-Q3 | 24 | USA | Modeling | Health information technology; electronic health record; sociotechnical; cybersecurity; ransomware |
| An academic medical center's response to widespread computer failure | 2013 | *American Journal of Disaster Medicine* | N/A | 2 | USA | Case analysis | Electronic health record; computer security; medical informatics; disaster planning; hospital administration |
| Security breaches: tips for assessing and limiting your risks | 2011 | *Journal of Medical Practice Management* | N/A | 0 | USA | Author's perspective | HIPAA; compliance; security; privacy; risk assessment; breach |
| Organizational repertoires and rites in health information security | 2008 | *Cambridge Quarterly of Healthcare Ethics* | Healthcare sciences and services-Q4 | 9 | USA | Case analysis | N/A |
| IT security in biomedical imaging informatics: the hidden vulnerability | 2007 | *Journal of Mechanics in Medicine and Biology* | Biophysics-Q4; Engineering, Biomedical-Q4 | 1 | Singapore | Author's perspective | Biomedical engineering; computing; medical informatics; security. |
| Information security policy's impact on reporting security incidents | 2005 | *Computers & Security* | Computer science (information systems)-Q2 | 83 | USA | Survey, correlational analysis | Computer abuse; deterrence; medical records; policy; incidents; seriousness; security |
| What to do before disaster strikes | 2001 | *Nursing Management* | N/A | 4 | USA | Author's perspective | N/A |
| Methods of responding to healthcare security incidents | 1998 | *Studies in Health Technology and Informatics* | N/A | 5 | UK | Reference modeling | Healthcare security; incident reporting; security guidelines; awareness |

*Categories and rankings were extracted from Journal Citation Reports by Thomson Reuters.

**The number of citations was extracted from Google Scholar (on 29 May 2018).

**Table 2.** Eight aggregated response strategies (EARS) framework for cyber incidents in healthcare organizations

| Timing in relation to incident | Recommendation (R) | Category of response | Details | Relevant article(s) |
|---|---|---|---|---|
| Pre-incident | R1. Construction of an incident response plan[a] | Managerial and technological | An incident response plan should be constructed prior to an incident and include the following:<br>• Securing all evidence<br>• Detection mechanisms<br>• Investigative methods such as forensic analysis<br>• Corrective methods for incident damage mitigation<br>• Containment process<br>• Incident eradication<br>• Recovery plans<br>• Alternative communication channels<br>• Alternative facilities<br>• Backup or loaned equipment | 14–17 |
| | R2. Construction of an information security policy to act as a deterrent | Managerial | Information security policies are shown to have the following effects if implemented prior to an incident:<br>• Encourage the reporting of the incidents<br>• Encourage the reporting of the severity of the incidents | 18,19 |
| | R3. Involvement of key personnel within the organization | Managerial | Key personnel and teams should have a solid understanding of the following prior to the incident:<br>• The critical nature of an incident<br>• The effects of an incident on daily work<br>• Reputational damage in relation to an incident<br>• Possible scenarios to consider the effects of downtime on their systems<br>• The importance of multi-disciplinary cooperation and teamwork in an incident<br>• The importance of shared team knowledge<br>• The importance of effective and timely communication within and across teams | 14–17,20–23 |
| | R4. Regular mock testing of recovery plans | Technological | Regular testing prior to an incident should be conducted on:<br>• Backups<br>• Restorative tools and processes | 14,17,20 |
| | R5a. Containment of the incident | Technological | Contain the incident and prevent further spreading through the following actions:<br>• Separation of the medical and hospital network via VLAN and air gapping<br>• Inspection of devices prior to connection to the medical network | 15,20,24 |
| Post-Incident | R5b. Containment of the incident | Technological | Contain the incident and prevent further spread through the following actions:<br>• Turn off all infected devices<br>• Disconnect any infected devices from the network<br>• Disable wireless network functionalities of infected devices<br>• Shut down the entire network if under a widespread attack | 15,20,24 |
| | R6. Embedded ethics and involvement of others beyond the organization | Managerial | Response to an incident must be able to sustain the following ethical values:<br>• Concern for member well-being<br>• Aggressive internal organizational communication<br>• Notification of all members affected by the breach<br>• Open business practices<br>Contact and involvement of the following personnel external to the organization:<br>• The organization's insurance provider<br>• Computer forensics experts<br>• Local law enforcement agencies | 14,17,20,25 |
| | R7. Investigation and documentation of the incident | Managerial and Technological | Investigative measures for an incident include:<br>• Securing any evidence<br>• Forensic analysis of the incident by an expert | 15,16,17,22 |

(continued)

**Table 2.** continued

| Timing in relation to incident | Recommendation (R) | Category of response | Details | Relevant article(s) |
|---|---|---|---|---|
| | | | The following should be documented throughout the response to an incident:<br>• The date the breach was identified, and the nature and scope of the breach<br>• Steps taken for mitigation of risk<br>• Individuals impacted by the incident<br>• Chain of custody for the evidence under review<br>• Lessons learned about the incident | |
| | R8. Construction of a damage assessment and recovery algorithm | Technological | Damage assessment algorithm, including the ability to:<br>• Use a dependency matrix and complementary array<br>• Perform sequential ordering<br>• Receive a set of malicious transactions from an IDS<br>• Select the minimum transaction ID<br>• Traverse through the transactions to find altered data<br>• Find out if the transaction is found to have altered data and if so, add the transaction to the set of affected transactions<br>• Search the complementary array for affected or malicious transactions and if found, add them to the list of affected transactions<br>Recovery algorithm, including the ability to:<br>• Receive the set of malicious and affected transactions<br>• Delete malicious transactions<br>• Read the affected transactions into an array<br>• Retrieve the log file for each transaction in that array<br>• Update the database accordingly with the affected transactions | [26] |

[a]Reviewed articles suggested technological recommendations for this component, but the creation of the plan should be managerial too.

will likely encounter serious issues and suffer unnecessary losses.[17] The incident response team should fully understand all the tools and processes involved in the restorative process and test them regularly. This shift from reactive measures to proactive measures will help the healthcare organization identify any issues with its response strategy and fix them before an actual incident occurs.[14] Mock system recovery exercises (eg, tabletop or scenario-based simulations) can help organizations to identify backups and to test restorative capabilities.[20]

**R5a - containment of the incident part A: proactive measures**

It is much easier for the response team to contain an incident if the network for patient equipment and systems is segmented away from other networks in the hospital. Segmenting the network stops an attacker's actions from impacting all devices at once. This can also prevent the spread of malware, which can consume copious amounts of network resources and eventually bring down an entire network. The separation of networks can be achieved via air gapping or a virtual LAN (VLAN). All devices must be inspected prior to connection to the medical network to ensure they are clean of malware such as ransomware, worms, and viruses[1]. This inspection should include service vendors' laptops and modality equipment. Healthcare organizations can even go as far as making vendors sign a declaration form making them liable for downtime costs due to their negligence.[15] Hospitals are unique environments in the information security field; their need for constant availability leaves virtually no room for downtime.[24]

## Post-incident actions

**R5b - containment of the incident – part B: reactive measures**

If the infected system is not business critical, immediately disconnect it from the network. Even if the infected system is business critical, this option should still be considered in order to prevent further damage.[15] In the event of an extreme case of malware such as ransomware on a healthcare network, an infected device should be reported to the organization's IT team immediately. The IT team can then disconnect the infected device from the network and disable its wireless network functionality. If the attack is severe enough, the IT team may choose to shut down the entire network to prevent the spread of the infection to more devices in the organization.[20] However, it is important to note that these drastic measures are often infeasible due to the reliance of most hospitals on technological systems. Furthermore, it is important to investigate the issue and its potential impacts, which cannot be done if the entire network is shut down. We suggest that the infected device be disconnected from the system, but left on to allow for analysis.

1 It should be noted that systems left online and connected "outside" the firewall may yet provide command-and-control (C2) traffic as part of the analysis while limiting exposure of the rest of the network. The C2 traffic may aid the organization in detecting additionally infected systems on the internal network.


**Figure 2.** Eight aggregated response strategies (EARS) framework for cyber incidents. *This component is both managerial and technological. **This component is both pre- and post-incidental.

**R6 - embedded ethics and involvement of others beyond the organization**

Embedded ethics refers to a commitment to member well-being. When a healthcare organization falls victim to an incident, it is important to remember that all of its stakeholders are potentially affected as well. When the California-based integrated managed healthcare consortium Kaiser Permanente's Internet portal service (KP Online) experienced an incident, they ensured that their response strategy would uphold their cultural values. Their three main stated values were concern for member well-being, aggressive internal communication, and commitment to open business practices. KP Online made it a point to contact all the members affected by the incident within 24 hours to establish an open communication line. Even senior staff members made these notification calls. Frequent and consistent internal communication informed all members of the organization of the state of affairs and what they could do to help remediate the issue. KP Online also had open business practices. They kept their members, regulatory agencies, and media all informed with regular updates. All of their notifications were prompt, organized, and accurate.[17]

External resources also provide assistance for an organization under attack.[25] The organization should notify its legal counsel and all relevant regulatory agencies about the incident in a prompt manner—the legal counsel can provide guidance throughout the incident.[17] Once the incident has been contained, the IT department should contact its insurance provider and the FBI Internet Crime Complaint Center, if the organization is located within the United States.[14,20]

**R7 - investigation and documentation of the incident**

The investigation of an incident needs to be prompt and thorough. Every step of this process should be documented, and all evidence should be secured during this stage. A digital forensic analysis expert should be contacted to analyze the key system components, configurations, policies, and procedures.[16] The investigation should seek to identify the root technical cause of the issue. A thorough investigation of vulnerabilities can also aid in identifying other vulnerabilities unrelated to the incident that, if caught early on, can prevent future incidents.[17]

Healthcare organizations should document all actions so that they are able to withstand any future legal issues. This documentation can also act as a guide for future incident response measures. Documentation should include the date the incident was identified, the nature and scope of the breach, steps taken to mitigate the risk, and the individuals impacted by the incident. A chain of custody can

**Table 3.** Comparing EARS with other frameworks

| EARS | NIST | ISO 27001 | CIS | HITRUST | COBIT | HITECH |
|---|---|---|---|---|---|---|
| Construction of an incident response plan | PR.IP-9 | 4.2.2; 5.1; A.13.2.1 | 19.x | PR.IP-9 | PO9.6; DS4.2 | 3003; 3004 |
| Construction of an information security policy | ID.GV-1 | 4.2x; 4.5x | 7.x; 19.4 | ID.GV-1 | DS5 | 3001.3.A |
| Involvement of key personnel within an organization | RS.CO-1; RS.AN-2 | 5.2.2 | 17.x | ID.AM-6; RS.CO-1 | PO7; DS4.6; PO4.13 | EHR |
| Mock testing of recovery plans | PR.IP-10 | A.10.3.2; A.10.4.1 | 20.x | RC.IM-2 | DS4.1; DS4.5 | 13.201; 3003.1.c |
| Containment of the incident | RS.MI-1 | – | 1.6; 15.4 | RS.MI | PO9; PO9.5;DS5; A16; DS12 | 13402[a] |
| Embedded ethics/ involvement of others beyond the organization | RS.CO-4; RS.CO-5 | 4.2.1; 4.2.5; 4.2.3.d | – | ID.RM-1; RS.CO-4; RS.CO-5 | PO1.4; PO5; PO8 | 3001.b.5; 13101.c.5; 3001.7; 13408; 13113.c; 13401.a |
| Investigation and documentation of the incident | RS.AN-1; RS.AN-3 | 4.3; A.13.2.3 | 19.2 | ID.RA-3; RS.MI-3 | ME1; DS9; DS10 | – |
| Construction of a damage assessment and recovery algorithm | – | – | – | – | – | – |

NIST: National Institute of Standards and Technology.
ISO: International Organization for Standardization.
CIS: Center for Internet Security.
HITRUST: The Health Information Trust Alliance.
COBIT: Control Objectives for Information and Related Technologies.
HITECH: Health Information Technology for Economic and Clinical Health Act.
[a]Requires notification of what is being done to mitigate losses, but does not detail how this should be done.

document the individuals who have come in contact with the evidence.[15,16] In addition to gathering incident information, it is essential to disseminate lessons learned and incident knowledge.[22]

**R8 - construction of a damage assessment and recovery algorithm**

Researchers have proposed a damage assessment and recovery algorithm for malicious transactions in a healthcare data source. The purpose of the algorithm is to delete all malicious transactions and recover transactions affected by malicious activity. The algorithm is triggered by an intrusion detection system (IDS). The IDS analyzes transactions and determines whether they are clean or malicious. When it detects a set of malicious transactions, it sends these transactions to the damage assessment and recovery algorithm. A sequential log file is maintained in which only committed transactions are saved. A dependency matrix and complementary array are both used to find the relationships between current and previous transactions. Transactions in the log file and dependency matrix are stored according to their commitment, and they are organized in ascending order by transaction ID. The damage assessment algorithm will search through all the transactions until it finds a transaction that may have been affected. Once the assessment algorithm establishes that the transaction has been altered, it will find the corresponding transaction from the complementary array. The recovery algorithm will trigger when it receives the malicious and affected transactions from the damage assessment algorithm. The malicious transactions will be deleted, and the affected transactions will be restored to their original state. This algorithm has proven effective for healthcare organizations when the IDS provides an accurate list of malicious transactions.[26] Many organizations may believe that damage assessment is the responsibility of a third party, such as a cybersecurity insurance company. However, it is advantageous for organizations to have their own means of assessment.

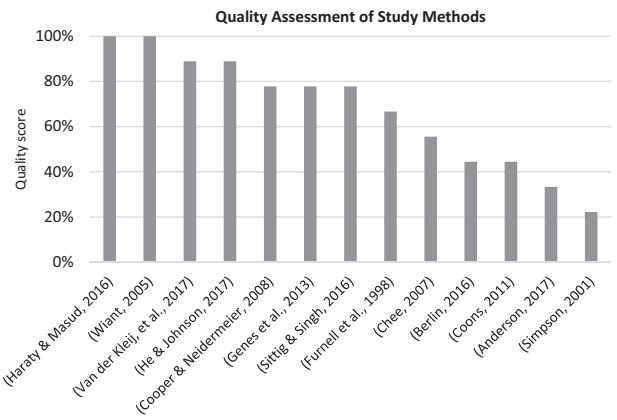


**Figure 3.** Quality assessment of study methods.

## Comparing EARS with major existing cybersecurity frameworks

We compared our framework with existing cybersecurity frameworks such as NIST, ISO, CIS, HITRUST, COBIT, and HITECH, which are based largely on practice. The aim of this comparison is only to review how these 6 frameworks cover the 8 areas of EARS. See Table 3 for the results of the comparisons and the full names of the 6 frameworks.

## Quality assessment

Each method used in the articles we reviewed was given a quality assessment score, as shown in Supplementary Table S1 of the supplementary document. Figure 3 presents a summary of the assessment results. This critical assessment of the study methods shows that there is a great need for more studies with scientifically sound design and implementation.

## DISCUSSION

In this systematic review, we identified and aggregated 8response strategies for cybersecurity incidents for healthcare organizations.

There have been numerous recent cybersecurity-related events that have significantly impacted healthcare organizations worldwide. Ransomware attacks have taken components of many healthcare organizations offline, including Britain's National Health Service and several hospitals in the United States[27]. We can only expect such attacks to continue. Understanding how healthcare organizations respond to attacks, and how this can be improved, is of the utmost importance for the continued safe and effective delivery of healthcare worldwide. In this context, we have created a framework (EARS), based on a systematic review of the available literature, to guide this conversation.

EARS is designed to be used by cybersecurity professionals and managers in healthcare organizations. This framework provides strategies that will aid in pre-incident and post-incident response methods. As each organization is different, the recommendations should be tailored to the organization. It should be noted that an organization needs to continuously develop and modify its response plan to match the pace of evolving cyber threats. These plans need to ensure minimum delay, maximum confidentiality, and definitive integrity, and they should be carefully tested and practiced (eg, through tabletop exercises or simulation games).

EARS is by no means a comprehensive framework in and of itself. We suggest that EARS be used cooperatively with another comprehensive framework in order to optimize cybersecurity response capabilities.

A prominent shortcoming was discovered throughout our review process: There is an overall lack of research in cybersecurity response. Given the importance of incident response strategies, this topic merits more attention.

### Limitations and suggestions for future research

Retrieval was limited to articles that included the exact terms used in the search strategy in their titles or abstracts. Any articles that used different terminology, eg, "computer security" or "risk management," would not have been retrieved. In addition, the exclusion criteria limited article selection for the review. If the article was not written in the English language or published as a journal article, it was excluded.

Overall, the lack of research on this topic has been limiting. The 8 strategies were aggregated from a limited set of materials and have not been fully tested by researchers to prove their efficacy. However, several of these strategies are already considered best practices outside of the healthcare industry, and researchers can further test the validity of these strategies to observe their accuracy, feasibility, and effectiveness in healthcare organizations. Moreover, these strategies can be expanded upon, tested, and tailored to environments outside of healthcare.

## CONCLUSION

It is essential that healthcare organizations invest in cybersecurity response plans to ensure the provision of reliable, secure operations. The combination of response, prevention, and detection capabilities has the potential to minimize operational disruption and monetary loss from cyber incidents. The implementation of EARS for cyber incidents in a healthcare organization can provide structure for cybersecurity response strategies.

The dearth of research in this area is an opportunity for researchers to close this gap by further exploring this topic. Although this review focused on healthcare, the recommendations found could be applicable to other organizations and industries.

## FUNDING

Financial support for this study was provided by Cybersecurity at MIT Sloan (CAMS).

## CONTRIBUTORS

MSJ conceived, designed, and supervised the study. BR and SR conducted the search, data collection, and data analysis. MSJ and BR wrote the first draft of the manuscript, and WG and SR contributed to the following drafts. All authors interpreted the data and critically revised the manuscript for important intellectual content.

## SUPPLEMENTARY MATERIAL

Supplementary material is available at *Journal of the American Medical Informatics Association* online.

*Conflict of interest statement*. None declared.

## REFERENCES

1. Gordon WJ, Fairhall A, Landman A. Threats to information security—public health implications. *N Engl J Med* 2017; 377 (8): 707–9.
2. Perakslis ED. Cybersecurity in health care. *N Engl J Med* 2014; 371 (5): 395–7.
3. Larsen E, Fong A, Wernz C, *et al*. Implications of electronic health record downtime: an analysis of patient safety event reports. *J Am Med Inform Assoc* 2018; 25 (2): 187–91.
4. Jalali MS, Razak S, Gordon W. Health care and cybersecurity: a bibliometric analysis of the literature. JMIR Preprints. 31/10/2018:12644 DOI: 10.2196/preprints.12644. https://preprints.jmir.org/preprint/12644
5. Werlinger R, Muldner K, Hawkey K, *et al*. Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Inform Manag Comp Security* 2010; 18 (1): 26–42.
6. Cichonski P, Millar T, Grance T, Scarfone K. Computer Security Incident Handling Guide. *NIST Special Publication*. Gaithersburg, Maryland, USA; 2012: 1–147.
7. Jalali M, Siegel M, Madnick S. Decision-making and biases in cybersecurity capability development: evidence from a simulation game experiment. *J Strateg Inf Syst* 2018. https://doi.org/10.1016/j.jsis.2018.09.003. (http://www.sciencedirect.com/science/article/pii/S0963868717304353)
8. The Ponemon Institute. *The Third Annual Study on the Cyber Resilient Organization*. Ponemon Institute Research Report; Traverse City, Michigan, USA. 2018.
9. Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. *J Med Internet Res* 2018; 20 (5): e10059.
10. National Initiative for Cybersecurity Careers and Studies. *Glossary of Common Cybersecurity Terminology*. 2017. https://niccs.us-cert.gov/glossaryAccessed November 27, 2017.
11. BSI. *Glossary of cyber security terms*. 2018.
12. Long AF, Godfrey M. An evaluation tool to assess the quality of qualitative research studies. *Int J Soc Res Methodol* 2004; 7 (2): 181–96.
13. Akazawa S, Igarashi M, Sawa H, Tamashiro H. Strategic approach to information security and assurance in health research. *Environ Health Prev Med* 2005; 10 (5): 282–5.
14. Berlin J. The rise of ransomware. *Tex Med* 2016; 112 (8): 53–8.
15. Chee WSA. It security in biomedical imaging informatics: the hidden vulnerability. *J Mech Med Biol* 2007; 07 (01): 101–6.

16. Coons LR. Security breaches: tips for assessing and limiting your risks. *J Med Pract Manage* 2011; 26 (6): 385–8.
17. Cooper T, Collmann J, Neidermeier H. Organizational repertoires and rites in health information security. *Camb Q Healthc Ethics* 2008; 17 (4): 441–52.
18. Wiant TL. Information security policy's impact on reporting security incidents. *Comput Secur* 2005; 24 (6): 448–59.
19. Genes N, Chary M, Chason KW. An academic medical center's response to widespread computer failure. *Am J Disaster Med* 2013; 8 (2): 145–50.
20. Sittig DF, Singh H. A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Appl Clin Inform* 2016; 7 (2): 624–32.
21. Van der Kleij R, Kleinhuis G, Young H. Computer security incident response team effectiveness: a needs assessment. *Front Psychol* 2017; 8: 2179.
22. He Y, Johnson C. Challenges of information security incident learning: an industrial case study in a Chinese healthcare organization. *Inform Health Soc Care* 2017; 42 (4): 393–408.
23. Anderson K. Using agility to combat cyber attacks. *J Bus Contin Emer Plan* 2017; 10 (4): 298–307.
24. Simpson RL. What to do before disaster strikes. *Nurs Manage* 2001; 32 (11): 13–4.
25. Furnell S, Gritzalis D, Katsikas S, Mavroudakis K, Sanders P, Warren M. Methods of responding to healthcare security incidents. *Stud Health Technol Inform* 1998; 52: 1138–42.
26. Haraty RA, Zbib M, Masud M. Data damage assessment and recovery algorithm from malicious attacks in healthcare data sharing systems. *Peer Peer Netw Appl* 2016; 9 (5): 812–23.
27. Clarke R, Youngstein T. Cyberattack on Britain's National Health Service—a wake-up call for modern medicine. *N Engl J Med* 2017; 377 (5): 409–11.