Spring 4-5-2022

# Ransomware Incident Preparations With Ethical Considerations and Command System Framework Proposal

Stanley Mierzwa
*Kean University*, smierzwa@kean.edu

James Drylie
*Kean University*, jdrylie@kean.edu

Dennis Bogdan
*Kean University*, dbogdan@kean.edu

# Ransomware Incident Preparations With Ethical Considerations and Command System Framework Proposal

**Stanley J. Mierzwa**
**Kean University Center for Cybersecurity**

**James J. Drylie**
**Kean University**

**Cochi Ho**
**NJ InfraGard Board Member**

**Dennis Bogdan**
**Kean University**

**Kenneth Watson**
**Montclair State University**

*Concerns with cyber-attacks in the form of ransomware are on the mind of many executives and leadership staff in all industries. Inaction is not an option, and approaching the topic with real, honest, and hard discussions will be valuable ahead of such a possible devastating experience. This research note aims to bring thoughtfulness to the topics of ethics in the role of cybersecurity when dealing with ransomware events. Additionally, a proposed set of non-technical recovery preparation tasks are outlined to help organizations bring about cohesiveness and planning for dealing with the real potential of a ransomware event. Constraints from many factors come into focus during preparations for ransomware, and a method to categorize them is detailed. Finally, the use of Incident Command Systems is well known and documented in emergency management, and a proposed model for integrating this process for ransomware episodes is sketched.*

*Keywords: incident command, ransomware, cybersecurity, ethical response, framework*

## INTRODUCTION

The technical cybersecurity incident of ransomware is an issue that continues to plague our information technology systems and solutions employed by businesses and organizations of almost any type. Despite the point that not every organization may report if they have been infected or breached with ransomware, there are those individuals and organizations that will. One formidable area to capture this data is with the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3). In viewing the number of

reported ransomware events over the past three years in 2018, 2019, and 2020, there is an increase of over 65% (IC3.GOV, 2021). Because of the increased incidents of ransomware, it is no surprise that ransom payments are also on the increase. The United States Treasury Department has reported that in the first six months of 2021, over $600 million in transactions were linked to ransomware payments, culminating with an increase of 40% as compared to 2020 (Talley, 2021).

With the increasing impetus for organizations to consider and possibly pay the ransom when inflicted with debilitating ransomware, this article will outline several critical components to plan and prepare for the real possibility of ransomware breaches. Content related to the background and history of ransomware, along with the role and responsibility of ethics in helping guide organizations through the incident, as well as recommendations, is provided. Additionally, steps organizations can take to help put themselves in a best-prepared manner for the potential of ransomware will be detailed, and a proposed customized Incident Command System for ransomware will be outlined.

## GLOBAL CYBERCRIME AND CYBERSECURITY INCIDENTS INCREASE DURING THE PANDEMIC

For those teams and individuals tasked with defending against cybercrime and cybersecurity attacks, it should come as no surprise that the pandemic has brought about an increase in breach attempts. If organizations compare their numbers of attacks via their logging systems year over year, there is a strong possibility that the increases will present themselves. The United Nations has reported that during the first quarter of 2020, as the COVID-19 pandemic was in full swing, there was a 350% increase in phishing websites, which can lead to such malware infections as ransomware (Lederer, 2020). Cybercrime, threat actors, organized criminal groups, and those who saw an opportunity to strike with cyber-attacks took the advantage presented by the pandemic, due to the flood of personally identified and vaccine information, that was now readily available with little to no protection.

## RANSOMWARE AND ITS HISTORY

The prospect of using an information technology asset or solution to install or infect a system with ransomware seems exceptionally modern. Historically, one of the first forms of technology ransomware was inflicted and distributed with the use of 20,000 floppy disks being circulated to HIV and AIDS researchers in 1989 across 90 countries (Tuttle, 2017). This initial ransomware was able to spread without the use of the Internet and was coined the *PC Cyborg* virus. In this initial ransomware incident, Joseph Popp, a biologist involved in conducting HIV and AIDS resource, is often credited with inventing ransomware (O'Kane et al., 2018). In similar fashion to current and modern ransomware incidents, the original *PC Cyborg* ransomware encrypted files and folders on the infected computers. The program was designed to sit dormant and ultimately encrypt the files after the computer was rebooted 90 times, and in order for the victim to attempt to regain access to their files and folders, they would need to send $189.00 to a P.O. box at an address located in Panama (KnowBe4, 2021). Although current forms of ransomware use more modern approaches for encrypting and requesting payment, most namely through cryptocurrency technologies, the same basic principles apply after the original ransomware incident over thirty-two years ago.

## ROLE OF ETHICS IN RANSOMWARE RESPONSE

When confronted with difficult and trying situations where it is critical to make decisions in the interest of affected parties, the role of ethics can be reflected to help provide guidance. With greater accountability and decision-making, the role of ethics can add value as a reminder, but also to demonstrate the *cybersecurity social responsibility* events like a ransomware attack (Mierzwa et al., 2021). Those members at the leadership and board levels, tasked with guiding a business, organization, or agency, could be

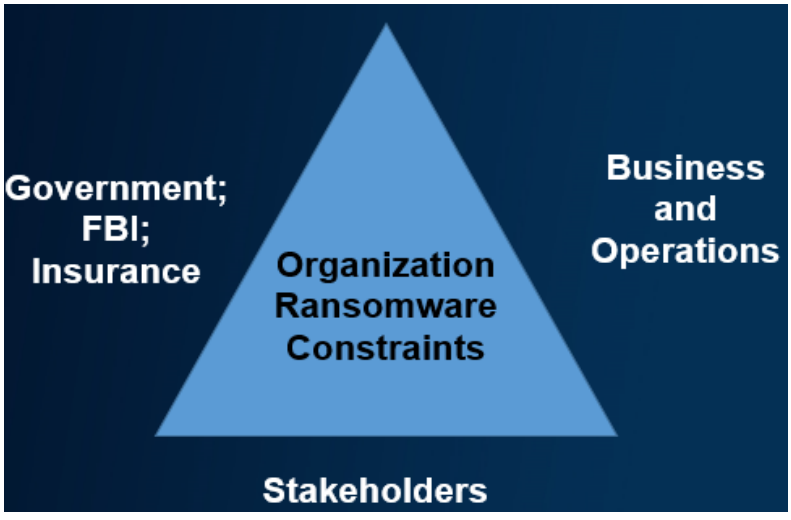
considered negligent if not assessing serious issues or concerns brought forward to them. In essence, there is an ethical norm and responsibility to deal with or tactic when warnings of ransomware potential arise.

## RANSOMWARE RESPONSE CONSTRAINTS

Cyber-attacks and crime do not occur in a vacuum. A number of pre-existing constraints in addition to unanticipated variables as a result of the incident, will be clear markers to assist and guide in the response and mitigation process. Constraints from a business perspective, includes the identification of the most critical limiting factors that can prevent achieving a goal, in essence addressing the bottlenecks (Lean Production, 2021). In one arena, the premise is that if the ransom is not paid, something bad or damaging will happen (Bennett & Genung, 2021). Unfortunately, responses for the most part are highly reactive, ill conceived, and impulsive. The idea of putting a ransomware event behind you, by simply paying the ransom can be tempting but shortsighted. However, there are concerns about the validity of getting your systems or technology back online. In the realm of a business or operation, this is one of the first constraints to appear – how to get back to functioning. A second constraint is those resulting from the organization or business key stakeholders. Stakeholders exist at all levels in the organization and can be in the form of customers, employees, the general public, critical facilities such as healthcare or energy, stock shareholders if applicable, and also an organization's leadership. Another yet third possible constraint will be in the form of law enforcement, such as the FBI, the government and insurance companies. The constraints from law enforcement may come in the form of requiring an initial announcement and reporting of your ransom attack and results, and by this notification, obtain assistance. Additionally, the payment of ransomware to countries that are listed by the US Treasury Department for economic embargo would be a violation of multiple US Statute and subject the company for legal liabilities. The role of government constraints could be difficult to monitor and maintain. It was reported that the Biden Administration is placing greater emphasis on combatting ransomware, and even putting in place guidance for organizations to follow, and if not done so, may risk penalties and other punitive measures (Talley, 2021). Insurance companies providing cyber-liability insurance may cover expenses through a policy, but in order to obtain coverage, a review of an organization's best practices and cybersecurity posture will be required (Shea & Flinton, 2021).

The complex constraints placed on an organization concerning ransomware can be demonstrated in varied methods. Given the three main categories of constraints outlined, the proposed constrain triad can be considered and viewed in Figure 1.

**FIGURE 1**
**RANSOMWARE CONSTRAINTS TO AN ORGANIZATION OR ENTERPRISE**



## ORGANIZATION RANSOMWARE RECOVERY PREPARATIONS

### Creation of a Ransomware Policy Brief

The function of an organizational and operational policy brief can be beneficial in making an introduction to an important or emerging challenge topic idea to those at the decision-making or executive level. They will often be found as a unique standalone document or report and designed to be extraordinarily succinct and understandable to the reader (Kobzar, 2013). For the authors, the activity of creating a policy brief is approached in an undergraduate Criminal Justice course by students. The activity often proves difficult for students in this course, because although the policy brief may be short in stature, it needs to include many of the key elements, including an executive summary, the outline of the approached problems and challenges, as well as the recommended steps or considerations for discussion and decision on the difficult encounter. When faced with a ransomware incident, employing a spontaneous response may not be adequate, because not all possible recovery options may have been environed or prepared.

Organizational and personality differences clearly have an impact on the factors or qualities to be included in a cyber-policy brief on the topic of ransomware. However, some essential items that can be considered include: a) When to contact law enforcement and the insurance company; b) A determination of timeframe before committing to paying a ransom; c) Commitment to verify and test a business continuity and disaster recovery plan; d) Reaffirming an obligation to be ethical in decisions regarding ransomware payments, these would include the key stakeholders of the said organization.

### Budgeting for Ransomware

During the course of discussions and approaches to dealing with technology risks brought about by such items as malware and ransomware, the use of technology tools will often be discussed in order to create layered defenses for organizations. In the case of ransomware, the considerations should also include other factors not related to technology, as the idea of paying a ransom may not end the associated funding costs (Tuttle, 2021). In planning for a budget to contend with ransomware, it would be prudent to contemplate initiatives such as the need for more intensive employee training, the potential for a full forensic investigation and identifying the forensics team, and the myriad issues related to legal counsel (Tuttle, 2017). Additionally, costs related to the loss of work product or productivity will need to be addressed. During the crisis, staff will need to be available and possibly work extra hours to solve the issue and get the company and organization back in operation.

### Contacting Law Enforcement

An important area for preparations to make in the event of a serious ransomware event is to determine when and whom to contact in law enforcement. Reflexively, many may be inclined to call the local police department, but that may not be the best course of action in the event of a ransomware incident. Most local law enforcement is not equipped or trained to handle a ransomware incident, and those agencies would recommend contacting state or federal authorities. Logically, the recommended course of action is to contact the Federal Bureau of Investigation (FBI). The FBI does not, and continues to not advocate that companies or organizations inflicted with ransomware pay the ransom (IC3.GOV, 2019). The reasons for not paying the ransom are well known, including the realization that one may not get their data or systems back in order, as well as the act of payment will empower and embolden the threat actor. Because the FBI does maintain and keep data to be reported in such services as the Internet Crime Complaint Center's yearly Internet Crime Report, reporting the incident will help to provide a more accurate account of such attacks. Furthermore, by reporting the incident to the FBI, the information will add value to law enforcement in their attempts of tracking and holding accountable, under United States law, those bad actors engaged in cybercrime to continue to try and prevent future such attacks (IC3.GOV, 2019).

An important discussion and subsequent effort of who and when to contact law enforcement should take place in an organization in their ransomware preparations. The information should be kept confidential, but held closely within an organization's business continuity or disaster recovery plans with personnel.

**Training Considerations**

Training is invaluable to the overall success of any organization. The depth and level of training vary at given points within the organizational structure. However, in order for training to be worthwhile, it should be ground in industry *best practices*, and be approached in a unidirectional format, both top-down, and bottom-up. The top-down approach allows for the operational elements to learn and reinforce positive behavior based on the overall needs of the organization. Additionally, the bottom-up approach allows for management and leadership to respond to the output of the operational element. the actions and reactions of leadership does not occur in a vacuum. The actions of those tasked with the day-to-day operations of the organization can and will have consequences. Training in this regard may seem foreign and counterintuitive, particularly in the cybersecurity arena, but the interconnectedness between operations and leadership cannot be overstated.

The Federal Emergency Management Agency (FEMA) uses the approach of *best practices* with the Incident Command System (ICS) as a model for local, state, federal agencies, and organizations to plan, prepare, and respond to myriad crisis. The key to ICS and the related planning and managerial functions used under the FEMA umbrella is training. Training can be broken down into three levels; Basic, Intermediate, and Advanced. Private sector organizations looking to implement an ICS type function should probably consider a formalized initial training program and continuing education for all employees. This would not only provide the obvious education and skill for staff, but would also help the organization to identify its leaders during these type of crisis situations and more easily establish the roles that they would play in during such an event. ICS stresses the use of common language. Training would also help to reinforce this for an organization (National Safety Inc. 2009). These types of ransomware situations are probably not an everyday event. Without regular training, the skills learned in an initial class may erode over time and make the response less effective for the organization. During training of the ICS, inclusion of tasks outlined to help attain such goals will include following the 14 key management characteristics (National Safety Inc. 2009). As an example, such content will contain ensuring that agency-specific codes and jargon be banned and replaced with more common terminology. Additionally, content related to ensuring proper meetings and management facilities is considered ahead of such ransomware events for dealing with the response to the incidents.

**Board and Executive Leadership**

It is common practice to ensure that the enterprise risk management programs and teams working to minimize risks to organizations keep their board of directors and executive teams informed of risk register repositories and minimizing risk status. As part of these enterprise risk efforts, the board may be briefed or be involved in an education activity surrounding current threats to an organization. Simply put, the board of directors or advisors has a strong ventured interest in the success and sustainability of the organizations they serve, and also a personal interest, having their names publically associated with the outfits. Given the ethical considerations the board of directors will have to entertain related to stakeholders such as shareholders, customers, employees, and the general public, it will be important to educate them on the topic and potential of ransomware. Included in these discussions will be the difficult questions about when to pay or not pay a threat actor for a ransomware event. Outlining the steps and approaches the organization will take when dealing with a ransomware event will keep the content transparent, and minimize surprises. The board of directors can also determine the best methods for integrating the enterprise risk management teams with the information technology and, particularly, the individual tasked as the Chief Information Security Officer (CISO).

**Insurance Concerns**

The role of insurance in organizations exists for many varied reasons. Corporate insurance can be in place to protect the business, its employees, customers, and even its board members. The role of cybersecurity insurance is also a component that needs to be considered and depending on the group that manages or owns the process of updating and maintaining the insurance policy; they may need to be briefed on performing a policy assessment for ransomware inclusion. With regard to ransomware, it will be

important to understand and be attentive to the ransomware notice clause that may exist under a policy. Additionally, suppose a company or organization has decided it will pay a ransom. In that case, the insurance company providing the cyber-liability faculties may actually cover the expenses, and thus this should be known upfront on the price point limits (Tuttle, 2017).

**Operational Concerns**

In a ransomware event, there will be operational tasks and projects related to technology and other procedural elements that will benefit the results of such an attack. Reviewing all available knowledge and information gathered of a ransomware incident, and performing a post-incident debrief or review will be valuable in order to try to prevent such a future event. The tasks could include items related to data storage recovery, the technology used to protect the environment, such as endpoint solution adjustments and backup strategies. The backup strategies may warrant greater investment in fault-tolerant methods to minimize ransomware damage. Additional education to both staff, partners, customers, and the like may be warranted. The topic of an incident command strategy, which will be discussed in a future section of this paper, along with greater self-assessments and table-top exercises, can be added to an operational core of tasks for ransomware preparations. Other operational factors to consider are what additional communication outreach may be necessary and through which media channels to help manage the reputational damage that may occur to an organization.

**Jurisdictional Concerns**

Along with the possibility of contacting law enforcement, at the same time, it is important to recognize the complexities that may arise when doing so. Law enforcement will want to be able to utilize all resources available to them, if warranted in a ransomware event, and this can mean granting them further or exclusive control of the incident. When considering jurisdiction as it pertains to an emergency response to a situation, ICS often uses to term Unity of Command. This refers to shared responsibility for the way in which a situation is managed when multiple entities or agencies respond to the incident. It also helps to address any potential situations when objectives conflict among those entities when resources are limited. It encourages a clear line of authority for decision-making (FEMA Incident Command System. (2020).

A potentially significant concern may evolve as this may become an issue for a private organization that is responding to a crisis situation involving ransomware, and does partner with law enforcement in the response. Within an organization, there might need to be a clear table of organization that specifically addresses this type of situation regarding a cyber-ransomware event. It could be that the CEO is in charge as might be during normal day to day operations. However, the Incident Commander, according to ICS protocol, can be anyone in the hierarchy and may simply be the first person to respond to the incident. This person might be relieved of that duty by a higher authority or could be left in charge regardless off rank.

As part of an organizations preparations for dealing with ransomware, forethought should be given to the involvement of government entities working with a private company. Legal considerations and a willingness/legal ability to work within a private sector organization may get complicated. Law Enforcement (Federal, State, County & Municipal) may work under different laws and guidelines. There may also be an issue with the lawful gathering of evidence and how that can differ from private organizations to Law Enforcement (ex. Search warrants, subpoenas, willing consent, etc.). Practically speaking, there may also be a reluctance on the part of one side to concede authority to the other.

## PROPOSED CUSTOMIZED RANSOMWARE INCIDENT COMMAND SYSTEM FRAMEWORK

In the event of a serious incident that may cripple an organization, such as in the case of a severe ransomware action, it may be prudent to have available an incident command framework to be followed and practiced ahead of time. Organizations may be able to utilize the Incident Command System (ICS) and the National Incident Management System (NIMS) utilities and practices, which are provided by and maintained by the Federal Emergency Management Agency (Chen et al., 2021; Federal Emergency

Management Institute. 2021). The ICS has endured the test of time and is adaptable to evolving and a variety of crisis. The ICS has been available since the early 1970s, when it was introduced in the State of California and utilized in responses to varying events and disasters (Auf der Heide, 1989; Jensen, & Thompson, 2006). Depending on the severity of the ransomware event, the proper groups with the ability and responsibility to enable or activate the use of an Incident Command System could do so with greater confidence and practice.

In reviewing the existing Incident Command Systems available through FEMA, it was discovered that there are modules, pamphlets and specialties of the system available for various sectors and disciplines. These areas include Public Works, Schools, and Utilities, but there is not a particular element focused on the very specific type of serious incident such as ransomware. The authors are proposing that because of the significant challenges posed to organizations of a variety of type, having a module or topical focus presented precisely on ransomware, there would be value-added to those end-users of the ICS-100 course materials.

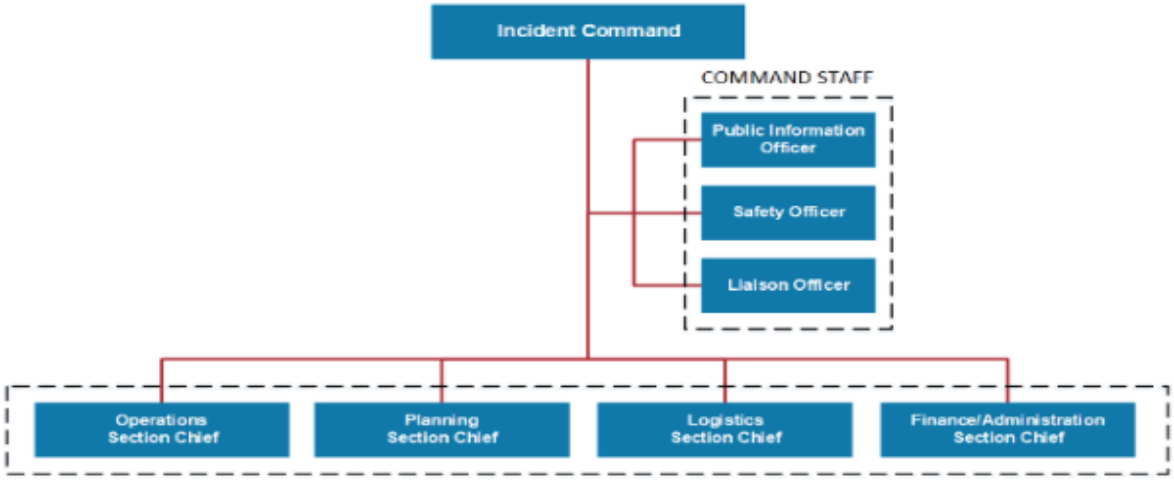
**Background on FEMA Incident Command Systems Training**

The Federal Emergency Management Agency makes available a variety of training modules related to Incident Command System, ranging from introductory to more advanced topics. The training is made available in a variety of delivery models including interactive web-based versions, ability to download materials, materials for train-the-trainer roles, that also permits for independent study. A list of available independent study guidelines and procedures are easily available to provide a step-by-step introduction into using the available learning materials that can result in certificates, Continuing Education Credits, and even college credit (Emergency Management Institute – Independent Study Course Brochure, 2021). The training program provided can be a valuable asset in training staff that are responsible for handling emergency management situations, which in the case of ransomware, can be seen as a true emergency condition.

**Envisioned or Proposed Ransomware Incident Command System Framework**

The standard Incident Command organizational structure to be utilized in the event of a general incident requiring focused attention and coordination can be found in Figure 2. The structure is well suited for general incidents regardless of the type and size (FEMA IS-100.c. 2021). The categories and groups are well served, but may benefit from minor complements to further coordinate in the event of an organizational ransomware event.

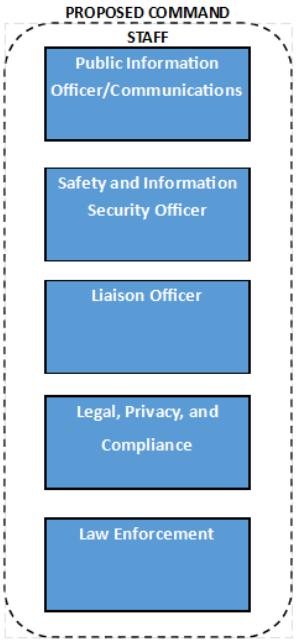
**FIGURE 2**
**STANDARD INCIDENT COMMAND SYSTEM (ICS) ORGANIZATION STRUCTURE**




Source: FEMA: IS-0110.C: An Introduction to the Incident Command System

A proposed modified structure or components of the Command Staff is outlined in Figure 3, which outlines several very important categories and functions that will be critical in addressing a ransomware event. The minor tweaks of incorporating Command Staff from IT Services, External Forensic Services, Legal and Compliance, and Law Enforcement amend the standard ICS organization structure to help streamline the specific tasks that may evolve from serious ransomware events. Additionally, it would be beneficial to update or include the updated serious technical incident types, such as ransomware or cryptocurrency that have emerged into the ICS terminology used or definitions.

**FIGURE 3**
**PROPOSED AMENDMENT OR INCLUSION OF COMMAND STAFF GROUPS FOR ICS**




An addendum and complementary set of tasks will benefit the Incident Command in the event of a serious and disruptive ransomware event. A predetermined set of tasks are outlined in Table 1, which can be amended, but provide a foundational start and platform.

**TABLE 1**
**COMPLEMENTARY RANSOMWARE RESPONSE CHECKLIST FOR THE INCIDENT COMMAND SYSTEM**

| Item | Category | Detailed Task | Status (X) |
|---|---|---|---|
| 1 | Initial Event | Evidence of encrypted files found on users accounts. | |
| 2 | Initial Event | Receiving ransom demand. | |
| 3 | Initial Event | Incident Commander notified, timeline and Security Operations Manager to begin event actions response. | |
| 4 | Engage IT Services | Start recovery of services, if possible. | |
| 5 | Engage IT Services | Removal of infected systems and isolation for Forensic Analysis. Begin recovery from backup. If backup is infected, initiate clean install. | |
| 6 | Engage IT Services | Ascertain method of entry or compromise and disrupt or sever the connection(s). | |

| | | | |
|---|---|---|---|
| 6 | Engage IT Services | Initiate retrieval of log files for analysis. If logs are unavailable, enable logs retention of 3 to 6 months moving forward. | |
| 7 | External Forensic Response | Engage outside incident forensic response under contract to investigate compromised systems to ascertain level of compromise. All requests to be routed through Incident Commander. | |
| 8 | Legal, Privacy, and Compliance | Initiate briefing for collaboration, request timeline for legal and regulatory notification requirements to avoid non-compliance. | |
| 9 | Legal, Privacy, and Compliance | Initiate notification to insurance carrier of ransomware incident. | |
| 10 | Legal, Privacy, and Compliance | Designate member of team to maintain strict timeline and coordinate tasks. | |
| 11 | Communications | Designate member to work alongside coordinator for formal communications. | |
| 12 | Communications | Initiate Senior Staff level meeting, including Board members for updates and decisions. Preferred to include Director or VP as liaison. | |
| 13 | Payment | Engage with external firm to handle negotiations and payment if authorized by Legal Department. Must ensure no laws are broken when payments are made due to legal liabilities. | |
| 14 | Law Enforcement | Consideration for contacting the local Federal Bureau of Investigations in the area of responsibility. | |
| 15 | Law Enforcement | Consideration for contacting the National White Collar Crime Center (NW3C) and report incident to IC3.GOV. | |
| 16 | Law Enforcement | Considerations for contacting other federal agencies such as: US Secret Service, US Customs and Immigration, Federal Trade Commission. | |

## CONCLUSION

The restrictions for an organization that emerges from a serious cybersecurity ransomware incident can bring about enormous challenges, stress, and chaos to an organization's leadership. These incidents will negatively impact the overall health and operations of most organizations, regardless of the size and scope of the organization. In the proposed formalized preparedness actions report, content related to ethical responsibilities to consider, as well as a checklist framework for dealing and contending with ransomware have been provided. With clear-headed and planned response plans, there will be provided advantages, when compared with those organizations that do not entertain the difficult task of preliminary table-top and forethought decisions. Organizations have a great deal of ethical responsibilities to their multi-functional and varied internal and external stakeholders, to make the best ethical decisions related to responding to a ransomware event. This commentary report, with a proposed checklist, is one step towards greater ransomware situational awareness, and complementing the already well-designed FEMA Incident Command System. With the increasing number of cybersecurity attacks and incidents with large scale implications, it is envisioned that a further training course and detailed content for incident responders may be considered related to ransomware. In addition, further formal updating of the Incident Command System can be considered for having to deal with more specific details related to ransomware incidents.

## ACKNOWLEDGMENTS

This proposal report and commentary study were supported by the Kean University Center for Cybersecurity, a multidisciplinary collaboration between the School of Criminal Justice and Public Administration and School of Computer Science and Technology. The authors are genuinely grateful to Dennis Letts, from the Board of Advisors for the College of Business and Public Management, and the New Jersey InfraGard leadership, for their support and vision of a first in-person InfraGard event post the COVID-19 pandemic, which lead to the presentation on the researched topic and ensuing publication.

## REFERENCES

Aud der Heide, E. (1989). *Disaster Response: Principles of Preparation and Coordination*. Mosby, Baltimore, MD.

Bennett, S., & Genung, J. (2021). *All in One: Certified Chief Information Security Officer Exam Guide* (pp. 167–168). McGraw Hill. New York.

Chen, P-H., Bodak, R., & Gandhi, N.S. (2021). Ransomware Recovery and Imaging Operations: Lessons Learned and Planning Considerations. *Journal of Digital Imaging, 34*, 731–740.

Federal Emergency Management Institute. (2021a). Emergency Management Institute – National Incident Management System (NIMS). Retrieved from https://training.fema.gov/is/courseoverview.aspx?code=IS-200.c

Federal Emergency Management Institute. (2021b). Emergency Management Institute – Independent Study Course Brochure. Retrieved from https://training.fema.gov/is/docs/fema_emi_independent-study-brochure_10-01-2021.pdf

FEMA Incident Command System. (2020). Unit Seven Incident Command System. *FEMA Training*. Retrieved from https://training.fema.gov/emiweb/downloads/301unt07.pdf

FEMA IS-100.c. (2021). *An Introduction to the Incident Command System, ICS 100*. Retrieved from https://emilms.fema.gov/is_0100c/curriculum/1.html

IC3.GOV. (2016). *Ransomware Victims Urged to Report Infections to Federal Law Enforcement*. Public Service Announcement I-091516-PSA. Federal Bureau of Investigation. Retrieved from https://www.ic3.gov/Media/Y2016/PSA160915

IC3.GOV. (2019*). High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*. Public Service Announcement I-100219-PSA. Federal Bureau of Investigation. Retrieved from https://www.ic3.gov/Media/Y2019/PSA191002

IC3.GOV. (2021). *Internet Crime Report 2020*. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Jensen, J., & Thompson, S. (2006). The Incident Command System: A Literature Review. *Disasters, 40*(I). 158–182.

KnowBe4. (2021). *AIDS Trojan or PC Cyborg Ransomware*. Retrieved from https://www.knowbe4.com/aids-trojan

Kobzar, S. (2013). *Transforming research into an engaging policy story: How to write a policy brief*. Migration Policy Centre, CARIM-East. Retrieved from http://diana-n.iue.it:8080/handle/1814/62781

Lean Production. (2021). *Theory of Constraints (TOC)*. Retrieved from https://www.leanproduction.com/theory-of-constraints/

Lederer, E.M. (2020). UN Reports Sharp Increase in Cybercrime during the Pandemic. *AP News.*

Mierzwa, S., RamaRao, S., & Jackson, T. (2021). Global Ethical and Societal Issues and Considerations with Cybersecurity in Digital Health: A rapid review. *Northeast Decision Sciences Institute Conference Proceedings*. Retrieved from https://nedsi.decisionsciences.org/wp-content/uploads/2021/06/NEDSI-2021-Proceedings.pdf

Mierzwa, S., Spath-Caviglia, L., & Christov, I. (2021). Commentary or Perspective: Opportunities to Leverage Global Public Health Innovative Research Technology in Combatting Cybercrime. *Journal of Leadership, Accountability and Ethics, 18*(4). https://doi.org/10.33423/jlae.v18i4.4608

National Safety Inc. (2009). *The Basics of Incident Command. National Safety Inc*. Retrieved from https://www.nationalsafetyinc.com/Assets/Downloadables/The%20Basics%20of%20Incident%20Command.pdf

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of Ransomware. *The Institution of Engineering and Technology Journals.* DOI: 10.1049/iet-net.2017.0207

Shea, J., & Flinton, B. (2021). Preparing for Ransomware. *The Business Journal – Central New York, 35*(27).

Talley, I. (2021, October 17). Suspected Ransomware Payments Have Doubled This Year. *Wall Street Journal*.

Tuttle, H. (2017). Ransomware Ready: How to Prepare for the Day You Get Locked Out. *Risk Management, 64*(7).

Tuttle, H., & Jacobson, A. (2019). Enemy of the State: Ransomware Surges Against State and Local Governments in 2019. *Risk Management*, *66*(11), 30–35.