

# Organizational Tensions: Learning from Cybersecurity Incidents

*Full Paper*

**Hwee-Joo Kam**

University of Tampa

[hkam@ut.edu](mailto:hkam@ut.edu)

**Wael Soliman**

University of Agder

[wael.soliman@uia.no](mailto:wael.soliman@uia.no)

**Alaa Nehme**

Mississippi State University

[a.nehme@msstate.edu](mailto:a.nehme@msstate.edu)

**Merrill Warkentin**

Mississippi State University

[m.warkentin@msstate.edu](mailto:m.warkentin@msstate.edu)

## Abstract

Ransomware attacks and similar threats have become increasingly prevalent, often involving demands for ransom payments, sometimes repeated. This underscores the critical importance of organizational learning (OL) in protecting information assets. However, OL alone may not suffice to prevent cyberattacks exploiting zero-day capabilities. Thus, this research explores OL challenges and outcomes, examining notable past cybersecurity incidents in the United States. Through a timeline analysis, initial findings reveal two primary categories of OL challenges: pre-incident factors such as zero-day capabilities, and post-incident factors such as information asymmetry and an uneven playing field that favors cyber offense over defense. These challenges are identified as organizational tensions that serve as a negative force to OL. Building on these insights, the study proposes strategies to mitigate these tensions. In summary, this study contributes valuable insights into OL dynamics within a complex organizational context marked by intricate system dependencies.

**Keywords:** cybersecurity incidents, organizational learning, tensions

## Introduction

Cybersecurity incidents pervade various contexts, posing a significant threat to organizational information security (InfoSec). The National Institute of Standards and Technology (NIST) defines a cybersecurity incident as an event that imposes an adverse impact on the organization, requiring a response and recovery (NIST 2018). Learning from cybersecurity incidents empowers organizations to build cyber resilience (Patterson et al., 2024) through practicing what they have learned (Orlikowski, 2002). However, many organizations fail to learn after suffering from massive cybersecurity incidents. A global survey reported that 84% of surveyed victims who had already paid an initial ransom were targeted again, and among these victims, 78% faced repeated ransom demands, with 63% asked to pay the second ransom (Cybereason, 2024). This suggests that organizational learning (OL) is critical to information asset protection. OL is defined as a process in which “*organizations build, supplement, and organize knowledge and routines around their activities within their cultures and adopt and develop organizational efficiency by improving the use of the broad skills of their workforces*” (Dodgson, 1993, p. 377).

OL in information security (InfoSec) is challenging. Despite implementing advanced security mechanisms, organizations experience cyberattacks targeting zero-day vulnerabilities. Moreover, an organization’s IT infrastructure is often interlinked with external entities and stakeholders for collaboration. This creates difficulties in sensemaking (i.e., understanding current incidents) (Weick, 1988) and renders OL difficult. For example, it was difficult to trace the cyberattack against SolarWinds’ supply chain system that distributes data to over 18,000 organizations (Williams, 2020). Such challenges may instigate misfits ascribed to tensions,

provoking a negating force manifested as tensions (Putnam et al., 2016). In this vein, we examine tensions emerged during learning from cybersecurity incident. Our research question (RQ) is:

*RQ: How would tensions emerged when organizations try to learn from cybersecurity incidents?*

Addressing tensions during OL from cybersecurity incidents would help organizations resolve some of their challenges that might have prevented them from learning. In this context, we adapted a content analysis approach (Weber, 1990) to analyze secondary data collected from the United States (U.S.) congressional hearings and various sources. Through the lens of contradictory management approach (Hargrave & Van de Ven, 2017), we investigated the emerging tensions or contradictions during OL from cybersecurity incidents. Overall, this study contributes to the IS literature in several ways. First, in terms of OL from cybersecurity incidents, numerous studies explained how organizations learned (Rezazade Mehrizi et al., 2022), and shared what motivated organizations to learn as well as prevented organizations from learning (Patterson et al., 2024). These studies discussed the approaches, antecedents, and consequences of OL in a cybersecurity incident context. However, our research delves deeply into the intricacies of organizational complexities and shares the intrinsic factors impeding organizations from effectively “*learning their lessons*”, wherein a failure in organizational learning perpetuates the recurrence of cybersecurity incidents. Second, our research presents some suggestions on how to avoid the failure of learning from cybersecurity incidents, thus enhancing organizational InfoSec.

## Literature Review

### Cybersecurity Incidents

NIST defines a cybersecurity incident as an event “*that has been determined to have an impact on the organization prompting the need for response and recovery*” (NIST 2018, p. 45).

Cybersecurity incidents exert adverse effects on an organization's IT infrastructure, and these effects can be alleviated through incident response (IR). The occurrences of cybersecurity incidents involve the threat actors who instigated a cyberattack and the IR teams that run responses and recovery (Aoyama et al., 2015). IS studies related to cybersecurity incidents are usually linked to IR. Naseer et al. (2021) ran a multiple case study to examine the role of business analytics in IR management, and Naseer et al. (2021) proposed that real-time analytics of IT infrastructure offers agility for organizations' IR strategy. Lee & Kim (2020) empirically established that citizens from wealthier European nations displayed a higher level of cybersecurity preparedness, whereas Kim & Lee (2021) revealed that attributes of IR such as apologies and excuses differed between American and Korean organizations due to cultural differences. In recent studies, Rezazade Mehrizi et al. (2022) outlined conceptual models of OL, and Patterson et al. (2024) discussed OL from the Neo-Institutional perspective (DiMaggio & Powell, 1983; Meyer & Rowan, 1977).

## **Organizational Learning**

Previous studies have studied InfoSec OL by drawing upon the theoretical framework of single-loop (i.e., identifying a problem) and double-loop (i.e., examining the underlying problem) learning (Ahmad et al., 2020; Argyris & Schön, 1997). Such studies have indicated that cybersecurity incidents offer opportunities for single-loop learning, such as identify the problems through detecting new attack vectors, and double-loop learning, such as, question the underlying assumptions through investigating the existing InfoSec policies (Ahmad et al., 2020). On the other hand, Ghahramani et al (2022) proposed that, through organizations' adaptability to cyber threats, OL fosters continuous improvement of InfoSec management. Also, Kwon & Johnson (2014) suggested that proactive InfoSec investment offers ample rooms for OL.

Moreover, several studies presented barriers of OL. Madsen & Desai (2010) concluded that the major obstacles of learning from failure are caused by the difficulty in knowledge acquisition (e.g., difficulty in collecting relevant data). In a cybersecurity context, the obstacles may be even more convoluted, because cybersecurity incidents involve IT complexity in that IT interconnectedness makes it hard to detect where an attack started. Even if organizations are able to identify the starting point of an attack, organizations may not be able to acquire knowledge of when and how that attack occurred, especially in an external component administered by their business associates. For example, the SolarWinds attack exemplified this difficulty. The attack against SolarWinds supply chain systems began by injecting arbitrary codes into a library that was digitally signed as legitimate and then executed during system updates (Williams, 2020). The malicious codes were spread to various system components, installing backdoors to create system resources for exploiting the active directory. Understanding such sophisticated attacks requires significant cognitive effort and preventing them in the future presents a formidable challenge.

## **Contradiction Management**

Broadly speaking, IS researchers adopt one of two explanation logics to motivate their research endeavors: the *logic of determination*<sup>1</sup>, and the *logic of opposition*<sup>2</sup> (Robey & Boudreau, 1999). According to the deterministic logic, the more prevalent approach, researchers seek to explain the phenomenon under study by developing “a single prediction equation” (Weinstein et al., 1998, p. 291) that combines a set of static dependent and independent variables (Siponen, 2024;

---

<sup>1</sup> The *logic of determination* “explains change as the consequence of variation in a set of predictor variables” (Robey & Boudreau, 1999, p. 168).

<sup>2</sup> The *logic of opposition* “explains organizational change by focusing on opposing forces that respectively promote and oppose social change” (Robey & Boudreau, 1999, p. 168).

Soliman & Tuunainen, 2022). Research adopting such logic is best described as a consistency-seeking research, and when faced with empirical inconsistencies, as Robey and Boudreau (1999) point out, “studies often motivate revisions of theory so that observations might be explained more satisfactorily.” (p. 170). From this predominantly rational view of the organization, contradictions are often seen “a barrier to productivity and a sign of organizational weakness” (Tracy, 2004, p. 120). As such, deterministic research provides excellent insights especially into research problems that are stable or not affected by the passage of time. On the other hand, deterministic research is also less suitable for phenomena that are dynamic, complex, and fraught with contradictions. In contrast to deterministic research, the logic of opposition thrives on contradictions and the reader may recognize them in IS writings referring to them as “*paradox, irony, hypocrisy, oxymoron, conflict, inconsistency, double bind, and dilemma*” (Robey & Boudreau, 1999, p. 169).

Rooted in the logic of opposition, contradiction management (sometimes referred to as ‘tension-centered approach’; see, Gibbs 2009) provides a broad theoretical framework to capture, analyze and explore ways to deal with tensions or contradictions (Gibbs, 2009; Jarvenpaa & Wernick, 2011; Karjalainen et al., 2019; Smith & Lewis, 2011; Soliman & Ojalainen, 2023; Tracy, 2004). Trethewey and Ashcraft (2004) note that the “*tension-centered approach begins with the premise that organizations are conflicted sites of human activity; accordingly, foregrounding tension can lead to richer understandings of actual practice and thereby aid in theory building.*” (p. 82). While some may view contradictions in negative light; others argue that contradictions are “*inevitable, even beneficial to organizations*” (Gibbs, 2009, p. 907). Typically, contradiction management is concerned with reaching a resolution to conflicts between opposing pairs, such as: *thesis and antithesis* (Karjalainen et al., 2019); *exploration and exploitation* (He & Wong, 2004;

March, 1991; O'Reilly & Tushman, 2004), *cooperation and competition* (Wiener & Saunders, 2014), and *short-term and long-term orientation* (Drummond, 2008), to name a few.

Specifically, this study examines contradictions or tensions emerged during learning from cybersecurity incidents to better understand the obstacles of OL. As noted earlier, addressing tensions or contradictions during organizational learning would help organizations resolve some of their challenges that might have prevented them from learning.

## **Research Methodology**

### **Data Collection**

We gathered secondary data from U.S. congressional hearings, comprising over 1000 pages of documents concerning cyber incidents such as the UnitedHealth ransomware attack, SolarWinds hack, Colonial Pipeline ransomware attack, and data breaches involving the Office of Personnel Management (OPM), Yahoo!, and Equifax. These incidents occurred between 2014 and 2024. The collected documents contain exchanges of questions and answers among Chief Executive Officers (CEOs), IR experts hired by affected organizations, and members of Congress. This approach allowed us to examine the narrative of IR management. Additionally, we collected data from reputable entities like the National Conference of State Legislatures (NCSL), the Center for Strategic and International Studies (CSIS), and the SANS Institute. To ensure a diverse perspective, we also captured insights from online panel discussions featuring Chief Information Security Officers (CISOs) discussing the aforementioned cyber incidents. Specifically, we downloaded these panels and transcribed their content using software tools.

## Data Analysis

This study adopts a qualitative research method, using an interpretative approach for inductive reasoning (Walsham, 1995). This approach enables an in-depth investigation of OL in a cybersecurity context by understanding human's thoughts and actions taken (Klein & Myers, 1999) during incident handlings. To analyze the data, we adopted a content analysis (Weber, 1990) approach. Content analysis is a method that allows researchers to draw inferences about psychological behaviors and communication styles in a group (Weber, 1990). It involves categorizing words within the text into fewer categories (Kleinheksel et al., 2020), facilitating the construction of concepts based on data rather than preconceived notions or biases (Agar, 1980). When categorizing words into categories, researchers need to make decisions about the mutual exclusivity and the breadth of these categories (Weber, 1990). We discovered that there were some overlaps among the emergent categories. For example, the following narrative (The US House Energy and Commerce, 2017) could be classified into the category of prevention that prevented further systems damages through attack containment. On the other hand, it could also point to systems interruptions, thus falling into the category of interruptions.

*“On July 30, Equifax identified several ACIS code vulnerabilities. Equifax noticed additional suspicious traffic from a second IP address...These red flags caused Equifax to shut down the ACIS web portal for emergency maintenance.”*

To enable multi-perspective (Karjalainen et al., 2019), two of the authors ran open coding in face-to-face manner via multiple Zoom meetings. This allowed us to resolve any disagreements during the coding procedure. As a result, we did not compute the inter-rater reliability (Sarker et al., 2001). Overall, we produced 436 codes during open coding. These codes were then analyzed and placed into subcategories based on common shared patterns. After that, we further classified



these subcategories into core categories by examining common shared patterns among subcategories. The following depicts the core categories emerged from our coding procedures.

### **Category: Interruption**

When under attack, organizations experienced *interruptions* that instigated their sensemaking (Weick et al., 2005). The CEO of United Healthcare, Andrew Witty, mentioned when testifying in congress (CBS News, 2024),

*“We immediately severed connectivity with Change’s data centers to eliminate the potential for further infection. While shutting down many Change environments was extremely disruptive, it was the right thing to do.”*

### **Category: Incident Response Management**

After identifying a cyber incident, organizations engaged in IR management incorporating IR activities such as decision-making, forensic investigations, and systems restoration. In a testimony of SolarWinds hack (The US Select Committee on Intelligence, 2021), Brad Smith, the President of Microsoft, mentioned,

*“We also continued investigating our own network to see if Microsoft was a target, and we confirmed that as a SolarWinds customer we had also been attacked. We began an intensive operation to find, isolate, contain, and expel the attacker, and to understand what the Russian actor was able to do while in our network.”*

IR Management also involved decision-making of paying ransom. The former CEO of Colonial Pipeline, Joseph Blout, mentioned (The Committee on Homeland Security, 2021b),

*“When you are there in the early hours of having your system and your servers and computers encrypted, you don't know what you have in front of you...What I have learned over the course of the last month is a lot of companies have back-up systems that don't help them at the end of the day. So, again, not knowing what the answer to that was for days, whether we could use our back-up systems to restore the Colonial Pipeline system back to service or not, we had to avail ourselves of any and every*

*option that we had, one of which was the de-encryption tool. So, therefore, the ransom payment was made in order to get the tool.*”

### **Category: Prevention**

Our data also revealed that organizations engaged in cybersecurity incident prevention (Baskerville et al., 2014). During the congressional hearing of OPM hack (The US House of Representatives Committee on Oversight and Government Reform, 2015), Dr. Andy Ozment, a former Assistant Secretary in the Office of Cybersecurity and Communications, was trying to implement a better security countermeasure across the federal agencies,

*“EINSTEIN 3A will be a step forward. It uses classified information and is modeled on a similar Department of Defense program. It is still a signature-based program, but it will rely upon classified information obtained from the intelligence community to help us detect adversaries and block them.”*

Additionally, Richard T. Smith, the former CEO of Equifax, stated the following in a congressional hearing of Equifax data breach (The US House Energy and Commerce, 2017),

*“In the last 3 years alone, we have invested approaching a quarter billion dollars in security. There is an IBM benchmark. It says financial service companies who tend to be best in class spend somewhere between 10 and 14 percent of their IT budget in security.”*

### **Category: Organizational Constraints**

Organizations faced some limitations to detect malicious traffic masquerading as legitimate. In a congressional testimony regarding SolarWinds hack (The US Select Committee on Intelligence, 2021), the CEO of CrowdStrike, George Kurtz, supervised the forensic investigation. He stated,

*“Because when you look at this particular attack, why did they use U.S. infrastructure? Because they just wanted to blend in. Right?...So, if you can use infrastructure that looks legitimate no matter who’s infrastructure it is, you’re going to blend in and make it harder [to detect]. And this particular attack*

*was insidious just the way it communicated and the protocols it used. It looked like legitimate traffic going to infrastructure that you know is normal.”*

### **Category: Organizational Misconduct**

Some cyberattacks were caused by organizational misconduct, which is defined by organizations’ irresponsible, unethical, and even illegal behaviors stemmed from organizational power structure and political climate (Greve et al., 2010). According to a report prepared by the US Government Accountability Office (GAO) (U.S. Government Accountability, 2018), the political climate in Equifax was problematic.

*“The working relationship between CIO Robert Webb and his subordinate CSO Tony Payne devolved due to “fundamental disagreements,” so the significant decision was made to move the security function out of IT and into the legal office...The functional result of the CIO/CSO structure meant IT operational and security responsibilities were split, creating an accountability gap.”*

As a result, such misconduct might have engendered IS errors contributed to data breach in Equifax. The former CEO of Equifax stated (The US House Energy and Commerce, 2017),

*“We know now that this criminal attack was made possible because of a combination of human error and technological error. The human error involved the failure to apply a software patch to our dispute portal in March of 2017. The technological error involved a scanner which failed to detect that vulnerability on that particular portal. Both errors have since been addressed.”*

When sharing his views about the OPM hack in a panel discussion (Chertoff Group LLC, 2015), Gregory Touhill, the Deputy Assistant Secretary of Cybersecurity and Communication in the Department of Homeland Security (DHS), mentioned the political climate in the federal agencies. We further argue that, given the political climate, it would be hard to implement changes for information asset protection.

*“Yeah, and I've got over 30 plus years of experience in the federal government on the [military] as well as the [government] side of the house. I think the answer to your question can be summed up with the size and heft of the federal acquisition [regulations]. I double dog dare you to bench press them.”*

### **Category: Offense Advantages**

Our data suggested that organizations were unable to prevent attacks on zero-day vulnerabilities, which inadvertently created some advantages for cyber offense. In a congressional testimony (The US Select Committee on Intelligence, 2021), the CEO of FireEye, Kevin Mandi, who was in charge of SolarWinds' IR noted,

*“And here's the reality: this group has zero-day capability... I haven't seen anything larger...”*

Additionally, threat actors' attack technique would always evolve, making it difficult for organizations to defend. In the same testimony, the CEO of CrowdStrike, George Kurtz, stated,

*“To me, the attacker did the SolarWinds implant. They've already moved on to whatever's next. We've got to go find it. This attacker, you know, maybe their pencil's down for a few months. But the reality is, they're going to come back. They're going to be an ever-present offense that we have to play defense against, and how they break in will always evolve.”*

In the same token, when commenting about the OPM hack in a discussion panel (American Security Project, 2015), Logan Brown, the President of Exodus Intelligence, shared that attackers tended to have more flexibilities.

*“Don't challenge the attacker. Because the attacker is, I don't want to say more advanced than us, but they're more agile.”*

### **Category: Cyber Environment**

Additionally, organizations realized that the cyber environment has always been fraught with ubiquitous cyberattack even before they were hit by cyberattacks. In a follow-up congressional testimony of Colonial Pipeline's ransomware attack (The Committee on Homeland

Security, 2021a), Eric Goldstein, the Executive Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency (CISA) mentioned,

*“In fact, it is estimated that over 100 Federal, State, and municipal agencies, over 500 medical centers, and 1,680 educational institutions in the United States were hit by ransomware in 2020 and ransom demands exceeded \$1 billion dollar”*

### **Category: Institutional Pressure**

The institutional environment includes external pressures prompting organizations to conform for legitimacy (Meyer & Rowan, 1977). Our findings indicate organizational conformance to federal regulations in reporting cybersecurity incidents, reflecting regulatory compliance to meet regulatory pressures (Meyer & Rowan, 1977; Patterson et al., 2024). The former CEO of Colonial Pipeline, Joseph Blount, stated during a testimony (The Committee on Homeland Security, 2021b),

*“We have an incident response process that follows the same framework used by some Federal agencies.... On the morning of the attack, we proactively reached out to the FBI to inform them...”*

Organizations also adhere to industry norms, known as normative pressures (Meyer & Rowan, 1977; Patterson et al., 2024), by recruiting external help for IR. Recruiting external help is a standard practice. In the same testimony, the former CEO of Colonial Pipeline stated,

*“I already explained that we, not only in addition to Mandiant, have also brought in Dragos to take a very close look at our OT system.”*

Moreover, the CEO of CrowdStrike, George Kurtz, mentioned in a testimony (The US Select Committee on Intelligence, 2021),

*“In mid-December, following public disclosures by multiple victims, SolarWinds engaged our professional services team to perform incident response.”*

### Category: Sensemaking

By interacting with employees, organizations exercised discursive engagement to socially construct an incident's meanings (Rezazade Mehrizi et al., 2022). This suggests that organizations made sense of an incident through communication (Weick et al., 2005) to attain a better understanding of an incident, gaining knowledge about a given incident. The former CEO of Equifax, Richard T. Smtih, noted,

*"I had the full debrief from Mandiant, our forensic auditors, from outside counsel, and my team."*

Similarly, in a written testimony of SolarWinds hack, the president of Microsoft, Brad Smtih, stated,

*"After several days of intense research and collaboration, the story of what occurred started to come into focus. FireEye discovered that an attacker had successfully breached its on-premises network (its private data center housed in their own facility). FireEye had installed an update to software it used from SolarWinds, and when they did, they unknowingly also installed the attacker's malware, opening a back door into FireEye's private system."*

### Category: Improved Prevention

Our data suggested post-incident analysis that empowered cybersecurity professionals to discover lessons learned and best practices that would prevent future attack (Rezazade Mehrizi et al., 2022). Eventually, this would engender improved security countermeasures or preventions to stop future attack. In a panel discussion about the recent United Healthcare's ransomware attack (CareTalk: Healthcare, 2024), Gregory T. Garcia, a cybersecurity expert in the healthcare industry, suggested ways to address third-party risks.

*"And one of the areas I think that is telling here there, the issue with the Change Healthcare attack, it was essentially a third party. Yes. UnitedHealth Group owns them, but it was a third party resource... We don't have in the healthcare industry very rigorous standards or regulations about how, for example, a hospital can assess and attest to the security of their third party providers... We are an interdependence*

*interconnected ecosystem in healthcare with plans and payers and health IT and medical devices, pharmaceuticals, and the providers. And every hop along the way introduces a vulnerability. So, we need to look at this in a holistic, comprehensive way, the way that the financial system has matured, in 30 years ago...”*

### **Category: Information Asymmetry**

When an incident occurred, there was information asymmetry wherein organizations might not obtain all the information that would help them fully understand how an attack transpired, but attackers had full information of what was going on (Bergh et al., 2019). In a congressional testimony of the Colonial Pipeline’s ransomware attack (The Committee on Homeland Security, 2021b), Charles Carmakal, the Senior Vice President and Chief Technology Officer of FireEye, oversaw the IR. When asked about the reused password that might have caused the hacking incident, he answered,

*“We do not know the exact source of the website that it was used, but presumably it was used on at least one other website because there are passwords that are readily available on the internet, and we did find that it was one of the passwords that was stolen from another website. But we don't know exactly where it came from.”*

Information asymmetry may result from complex learning, which involves connecting various knowledge structures (Van Merriënboer & Sweller, 2005). Our data reveals that IT complexity, arising from multiple system components, causes complex learning, making it difficult to grasp incident occurrences. In the same testimony, the former CEO of Colonial Pipeline stated,

*“It is an extraordinarily intricate and complex system...That investigation is ongoing, and while we may not have all of the answers today to the questions that you have, we are working hard to get them.”*

## Preliminary Findings

We contextualize our findings using a timeline that illustrates events occurring before incidents (left of incident) and after incidents (right of incident) (Willison & Warkentin, 2013). This approach is consistent with a cybersecurity framework that presents the prevention and response “paradigms”, in which to the left, there were indications and warnings for deterrence, while to the right, there were incident responses consisting of detection, recovery, and systems hardening (Baskerville et al., 2014).

Referring to Figure 1,  $T_0$  indicates that an incident occurs, causing systems interruptions or a halt in organizational operation. The CEO of Equifax noted in a testimony (The US House Energy and Commerce, 2017),

*“On July 29<sup>th</sup>...suspicious activity was detected ...the team immediately shut down the portal.”*

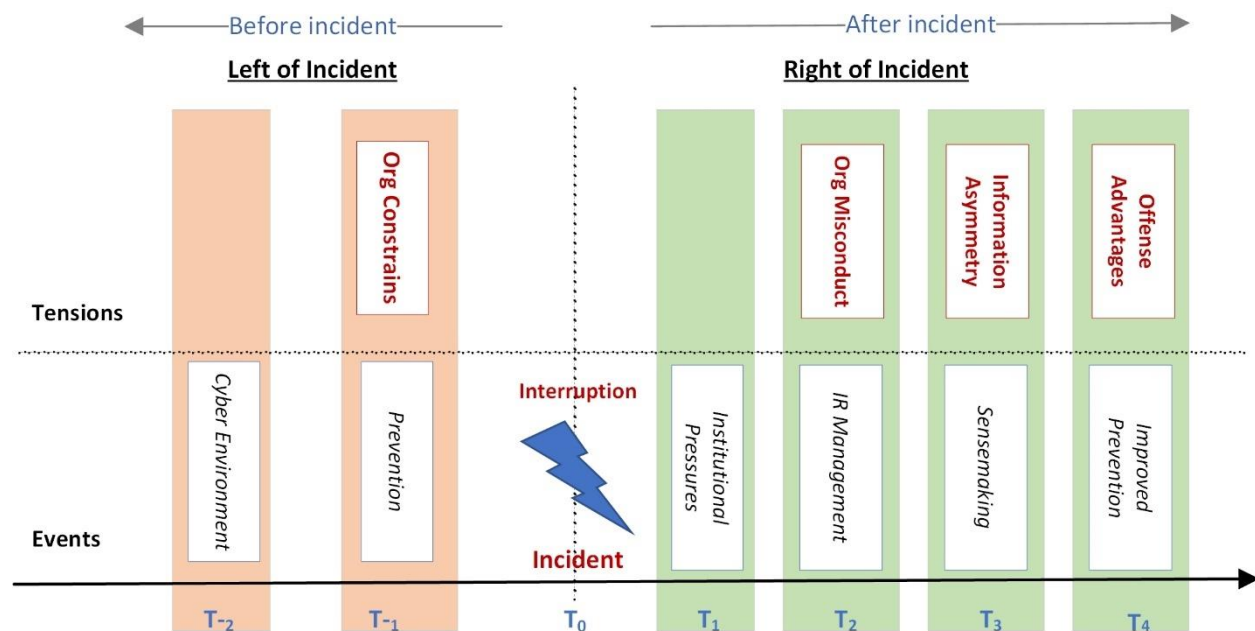


Figure 1: Timeline

The left of  $T_0$  shows a time series of before-incidents. Given the cyber threats in cyber environments ( $T_{-2}$ ), organizations executed preventive actions ( $T_{-1}$ ). Yet, organizations failed to



stop attackers due to organizational constraints. For example, a former CEO of Yahoo, Marrison Mayer, noted in a senate hearing (The US Committee on Commerce, Science, and Transportation, 2017) that it was hard to prevent sophisticated attack.

*“Yahoo! had in place multiple layers of sophisticated protection...Unfortunately...Russian agents intruded on our systems...Even robust defenses and processes are not sufficient to protect against a state-sponsored attack, especially when it’s extremely sophisticated and persistent.”*

The narrative above suggested zero-day capabilities. We assert that there are no resolutions to such challenges. Organizations struggle to learn about the “unknown” (i.e., zero-day capabilities) when they lack clarity of what exactly constitutes the “unknown”. In essence, it is challenging to learn about something that has not been identified. However, some organizations failed to prevent “non-zero day” cyberattacks even with implementation of cybersecurity countermeasures. This is due to organizational constraints in handling complex systems. In a panel discussion about Colonial Pipeline’s ransomware attack (Cyber Houston, 2021), George Crawford, the CISO of Partner of Catapult Energy Service, mentioned that,

*“More and more differentiation that we have between OT and IT and with what companies are doing it's getting to be a big problem, especially in oil and gas and obviously [with] Colonial [Pipeline]... a lot of the concepts that apply in IT don't apply in OT and vice versa.”*

Consequently, we argue that these narratives reflect tensions against prevention or cybersecurity countermeasures. Because it would be very hard to predict zero-day capabilities and manage a highly complex systems, the resolution for these tensions is placing a comprehensive IR plan that would facilitate effective IR and mitigate attack impact.

Once organizations fail to stop an attack, they will suffer from systems interruption that instigates sensemaking (Weick et al., 2005). The right of  $T_0$  shows a time series of after-incidents. Triggered by interruptions ( $T_0$ ), organizations started the sensemaking process (Weick et al.,

2005). Organization immediately reported to the authorities to conform to regulatory pressure and recruited external help for IR to comply with industry norms (i.e., normative pressure) (T<sub>1</sub>). This reflected upon complying with institutional pressure (Meyer & Rowan, 1977) during incident handling (Patterson et al., 2024).

Consequently, organizations participated in IR management to collect forensic evidence and restore systems (T<sub>2</sub>). However, organizational misconduct, caused by organizational political climate (Greve et al., 2010), might emerge as tensions that undermine IR management. When discussing about the OPM hack (American Security Project, 2015), Scott Applegate, the Chief Operation of US Army Cyber Command mentioned,

*“The government in and of itself, whether you're talking about the military or the civilian side of the government, is just a huge bureaucratic beast and it takes time to do anything. It takes time to implement new policies, it takes time to put new tools in, and especially when you're talking about networks that are as vast as these networks are.”*

The narrative above implies that the climate of bureaucracy can lead to organizational misconduct (e.g., slow forensic discoveries and decision-making), thereby undermining IR management characterized by quick actions. We propose that resolving these tensions would require new leadership (Sims, 2000).

Next, IR results were communicated through interactions or discursive engagement that socially construct the meanings of an incident (Rezazade Mehrizi et al., 2022) (T<sub>3</sub>). This indicates sensemaking by communications (Weick et al., 2005) in that organizations make sense of an incident through conversations. However, organizations were confronted with learning barriers consisting of information asymmetric, which was stemmed from complex learning ascribed to complex IT systems. As a result, this tension posed challenges to sensemaking. In a testimony of SolarWinds hack (The US Select Committee on Intelligence, 2021), the president of Microsoft stated,

*“...The attacker is the only one that knows everything they did. We have pieces...we all have slices.”*

We propose that resolving this challenge involves sensemaking through plausibility. While organizations may lack the complete narrative, they can refine a story through further investigations, providing plausible explanations for sensemaking (Weick et al., 2005).

Next, in T<sub>4</sub>, with lessons learned, organizations try to implement better, improved prevention or security countermeasure. However, the emergent tension, namely, offense advantages, may thwart their efforts. In a testimony about Yahoo! data breach (The US Committee on Commerce, Science, and Transportation, 2017), Karen Zacharia, the Chief Privacy Officer of Verizon Communication, stated,

*“In addition, though, all of our security teams need to understand that security isn’t static, it’s always changing. The attackers are getting better; the tools are getting better.”*

This narrative reflects an uneven playing field, indicating that cyber offense may hold an advantage over defense (Lieberthal & Singer, 2012). In essence, cyber offenders only need to succeed once, whereas cyber defenders must succeed consistently. We contend that addressing this challenge entails implement the best defense and embracing risk acceptance, given the difficulty in thwarting a sophisticated, novel attack. The following table summarizes our findings.

Time Series	Events	Event Descriptions	Challenges	Solutions
T <sub>2</sub>	Cyber Environment	The cyberspace is fraught with threats.	N/A	N/A
T <sub>1</sub>	Prevention	Organizations take actions to blocks some malicious attacks.	Organizational Constraints of stopping zero-day capabilities and detecting attacks in complex systems	Implement a comprehensive IR plan to mitigate attack impacts.
T <sub>0</sub>	Interruption	A cybersecurity incident takes place that instigates systems interruptions	N/A	N/A

T <sub>1</sub>	Institutional Pressures	Conform to regulations and industry norms in IR.	N/A	N/A
T <sub>2</sub>	IR Management	Executed IR	Organizational misconduct stemmed from political climate	New leadership
T <sub>3</sub>	Sensemaking	Understand incidents via conversations	Information asymmetry	Sensemaking by plausibility – refining the “story”.
T <sub>4</sub>	Improved preventions	Implement better preventive measures	Offense advantages	Put the best defense and accept the risk of cyberattacks.
Table 1. Summary of Research Findings				

## Conclusion, Future Research, and Limitations

In conclusion, this study examined challenges emerged during OL from cybersecurity incidents. Using a time series to contextualize findings (Willison & Warkentin, 2013), we identified OL challenges of both preceding and following incidents. Specifically, prior to incidents, the challenges are pertained to organizational constraints in detecting zero-day capabilities and identifying attacks in complex systems, whereas during post-incident, there are challenges related to information asymmetry, organizational misconduct that disrupts IR, and cyber offense advantages. These challenges act as tensions to OL and thus require attention. In the future, this study intends to explore better approaches for resolving these challenges by running a second study involving interviews with IR experts and CISO. Finally, this study is not without limitations. Using secondary data restricted our analysis to Fortune-500 organizations, which typically hold abundant resources for safeguarding information assets. We did not study small- and medium-sized businesses (SMBs), which may face financial constraints. In future research, we aim to address this limitation by including SMBs in a second study.

## References

- Agar, M. H. (1980). *The professional stranger: An informal introduction to ethnography*. Academic Press.
- Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., and Baskerville, R. L. 2020. “How Integration of Cyber Security Management and Incident Response Enables Organizational Learning,” *Journal of the Association for Information Science and Technology* (71:8), pp. 939–953.
- American Security Project (Director). (2015, September 17). *Cyber Security: Lessons from the OPM Hack (Panel 1)*. <https://www.youtube.com/watch?v=PIEYb4qUGI4>
- Aoyama, T., Naruoka, H., Koshijima, I., & Watanabe, K. (2015). How Management Goes Wrong? – The Human Factor Lessons Learned from a Cyber Incident Handling Exercise. *Procedia Manufacturing*, 3, 1082–1087. <https://doi.org/10.1016/j.promfg.2015.07.178>
- Argyris, Ch., and Schön, D. A. 1997. “Organizational Learning: A Theory of Action Perspective,” *Monográfico Sobre La Formación y Las Organizaciones* (77:78), p. 345.
- Baskerville, R., Spagnoletti, P., and Kim, J. 2014. “Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response,” *Information & Management* (51:1), pp. 138–151.
- Bergh, D. D., Ketchen, D. J., Orlandi, I., Heugens, P. P. M. A. R., and Boyd, B. K. 2019. “Information Asymmetry in Management Research: Past Accomplishments and Future Opportunities,” *Journal of Management* (45:1), SAGE Publications Inc, pp. 122–158.
- CareTalk: Healthcare (Director). (2024, March 15). *Change Breach & Healthcare’s Cyber Threats*. <https://www.youtube.com/watch?v=j85GYsKi1gs>
- CBS News (Director). (2024, May 1). *CBS News*. [https://www.youtube.com/watch?v=vjQAcWy1\\_dQ](https://www.youtube.com/watch?v=vjQAcWy1_dQ)
- Chertoff Group LLC (Director). (2015, November 11). *After the OPM Breach: What’s Needed Next*. [https://www.youtube.com/watch?v=hGOcLhZt\\_eY](https://www.youtube.com/watch?v=hGOcLhZt_eY)
- Cyber Houston (Director). (2021, May 25). *Power Panel—Colonial Pipeline Ransomware Attack*. <https://www.youtube.com/watch?v=VIQ734jBQPY>
- Cybereason. 2024. “Ransomware: True Cost to Business 2024,” Annual Global Study on Ransomware Business Impact. (<https://www.cybereason.com/ransomware-the-true-cost-to-business-2024>).
- DiMaggio, P. J., and Powell, W. W. 1983. “The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields,” *American Sociological Review* (48:2), pp. 147–160.
- Dodgson, M. (1993). Organizational Learning: A Review of Some Literatures. *Organization Studies*, 14(3), 375–394. <https://doi.org/10.1177/017084069301400303>
- Drummond, H. (2008). The Icarus paradox: An analysis of a totally destructive system. *Journal of Information Technology*, 23(3), 176–184. <https://doi.org/10.1057/palgrave.jit.2000119>

- Ghahramani, F., Yazdanmehr, A., Chen, D., & Wang, J. (2022). Continuous improvement of information security management: An organisational learning perspective. *European Journal of Information Systems*, 1–22. <https://doi.org/10.1080/0960085X.2022.2096491>
- Gibbs, J. (2009). Dialectics in a global software team: Negotiating tensions across time, space, and culture. *Human Relations*, 62(6), 905–935. <https://doi.org/10.1177/0018726709104547>
- Greve, H. R., Palmer, D., & Pozner, J. (2010). Organizations Gone Wild: The Causes, Processes, and Consequences of Organizational Misconduct. *Academy of Management Annals*, 4(1), 53–107. <https://doi.org/10.5465/19416521003654186>
- Hargrave, T. J., & Van de Ven, A. H. (2017). Integrating Dialectical and Paradox Perspectives on Managing Contradictions in Organizations. *Organization Studies*, 38(3–4), 319–339. <https://doi.org/10.1177/0170840616640843>
- He, Z.-L., & Wong, P.-K. (2004). Exploration vs. Exploitation: An empirical test of the ambidexterity hypothesis. *Organization Science*, 15(4), 481–494. <https://doi.org/10.1287/orsc.1040.0078>
- Jarvenpaa, S. L., & Wernick, A. (2011). Paradoxical tensions in open innovation networks. *European Journal of Innovation Management*, 14(4), 521–548.
- Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Information Systems Research*, 30(2), 687–704. <https://doi.org/10.1287/isre.2018.0827>
- Kim, N., & Lee, S. (2021). Cybersecurity Breach and Crisis Response: An Analysis of Organizations' Official Statements in the United States and South Korea. *International Journal of Business Communication*, 58(4), 560–581. <https://doi.org/10.1177/2329488418777037>
- Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, 23(1), 67–93. <https://doi.org/10.2307/249410>
- Kleinheksel, A. J., Rockich-Winston, N., Tawfik, H., & Wyatt, T. R. (2020). Demystifying Content Analysis. *American Journal of Pharmaceutical Education*, 84(1), 7113. <https://doi.org/10.5688/ajpe7113>
- Kwon, J., and Johnson, M. E. 2014. “Proactive Versus Reactive Security Investments in the Healthcare Sector,” *MIS Quarterly* (38:2), pp. 451-A3.
- Lee, C. S., and Kim, J. H. 2020. “Latent Groups of Cybersecurity Preparedness in Europe: Sociodemographic Factors and Country-Level Contexts,” *Computers & Security* (97), p. 101995.
- Lieberthal, K., & Singer, P. W. (2012). *Cybersecurity and US-China relations*. Brookings.

- Madsen, P. M., and Desai, V. 2010. "Failing to Learn? The Effects of Failure and Success on Organizational Learning in the Global Orbital Launch Vehicle Industry," *Academy of Management Journal* (53:3), pp. 451–476. (<https://doi.org/10.5465/amj.2010.51467631>).
- March, J. G. (1991). Exploration and exploitation in organizational learning. *Organization Science*, 2(1), 71–87.
- Meyer, J. W., and Rowan, B. 1977. "Institutionalized Organizations: Formal Structure as Myth and Ceremony," *American Journal of Sociology* (83:2), The University of Chicago Press, pp. 340–363.
- Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., and Masood Siddiqui, A. 2021. "Real-Time Analytics, Incident Response Process Agility and Enterprise Cybersecurity Performance: A Contingent Resource-Based Analysis," *International Journal of Information Management* (59), p. 102334.
- Naseer, H., Maynard, S. B., and Desouza, K. C. 2021. "Demystifying Analytical Information Processing Capability: The Case of Cybersecurity Incident Response," *Decision Support Systems* (143), p. 113476.
- NIST. 2018. "Framework for Improving Critical Infrastructure Cybersecurity," No. 1.1, National Institute of Standards and Technology (NIST), April 16. (<https://doi.org/10.6028/NIST.CSWP.04162018>).
- O'Reilly, C. a, & Tushman, M. L. (2004). The ambidextrous organization. *Harvard Business Review*, 82(4), 74–81.
- Orlikowski, W. J. (2002). Knowing in Practice: Enacting a Collective Capability in Distributed Organizing. *Organization Science*, 13(3), 249–273. <https://doi.org/10.1287/orsc.13.3.249.2776>
- Patterson, C. M., Nurse, J. R. C., and Franqueira, V. N. L. 2024. "'I Don't Think We're There yet': The Practices and Challenges of Organisational Learning from Cyber Security Incidents," *Computers & Security*, p. 103699.
- Putnam, L. L., Fairhurst, G. T., and Banghart, S. 2016. "Contradictions, Dialectics, and Paradoxes in Organizations: A Constitutive Approach," *Academy of Management Annals* (10:1), pp. 65–171.
- Rezazade Mehrizi, M. H., Nicolini, D., and Rodon, J. 2022. "How Do Organizations Learn from Information System Incidents? A Synthesis of the Past, Present, and Future," *MIS Quarterly* (46:1), pp. 531–590.
- Robey, D., & Boudreau, M. C. (1999). Accounting for the contradictory organizational consequences of information technology: Theoretical directions and methodological implications. *Information Systems Research*, 10(2), 167–185. <https://doi.org/10.1287/isre.10.2.167>
- Sarker, S., Lau, F., & Sahay, S. (2001). Using an adapted grounded theory approach for inductive theory building about virtual team development. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, 32(1), 38–56. <https://doi.org/10.1145/506740.506745>

- Sims, R. R. (2000). Changing an Organization's Culture Under New Leadership. *Journal of Business Ethics*, 25(1), 65–78. <https://doi.org/10.1023/A:1006093713658>
- Siponen, M. (2024). Stage theorizing in behavioral information systems security research. *Proceedings of the 57th Hawaii International Conference on System Sciences*, 1, 4724–4733.
- Smith, W. K., & Lewis, M. W. (2011). Toward a theory of paradox: A dynamic equilibrium model of organizing. *Academy of Management Review*, 36(2), 381–403. <https://doi.org/10.5465/AMR.2011.59330958>
- Soliman, W., & Ojalainen, A. (2023). Conflict resolution in an ISO/IEC 27001 standard implementation: A contradiction management perspective. *56th Hawaii International Conference on Systems Sciences*, 4839–4848.
- Soliman, W., & Tuunainen, V. K. (2022). A tale of two frames: Exploring the role of framing in the use discontinuance of volitionally adopted technology. *Information Systems Journal*, 32(3), 473–519. <https://doi.org/10.1111/isj.12355>
- The Committee on Homeland Security. (2021a). *CYBER THREATS IN THE PIPELINE: LESSONS FROM THE FEDERAL RESPONSE TO THE COLONIAL PIPELINE RANSOMWARE ATTACK* (117-18) [Legislation]. U.S. Government. <https://www.congress.gov/event/117th-congress/house-event/LC67088/text>
- The Committee on Homeland Security. (2021b). *CYBER THREATS IN THE PIPELINE: USING LESSONS FROM THE COLONIAL RANSOMWARE ATTACK TO DEFEND CRITICAL INFRASTRUCTURE* (117-15) [House Hearing]. U.S. Government. <https://www.govinfo.gov/content/pkg/CHRG-117hrg45085/html/CHRG-117hrg45085.htm>
- The US Committee on Commerce, Science, and Transportation. (2017). *PROTECTING CONSUMERS IN THE ERA OF MAJOR DATA BREACHES* (115-401) [Senate Hearing]. The US Government. <https://www.govinfo.gov/content/pkg/CHRG-115shrg33395/html/CHRG-115shrg33395.htm>
- The US House Energy and Commerce. (2017). *Oversight of the Equifax Data Breach: Answers for Consumers* (115-59) [House Hearing]. The US Government. <https://www.congress.gov/event/115th-congress/house-event/106455>
- The US House of Representatives Committee on Oversight and Government Reform. (2015). *OPM: DATA BREACH* (114) [House Hearing]. Full Committee on Oversight and Accountability. <https://www.hsdl.org/c/view?docid=793071>
- The US Select Committee on Intelligence. (2021). *OPEN HEARING: HACK OF U.S. NETWORKS BY A FOREIGN ADVERSARY* (117-79) [Intelligence Hearing]. U.S. Government Publishing Office.



- <https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary>
- Tracy, S. J. (2004). Dialectic, contradiction, or double bind? Analyzing and theorizing employee reactions to organizational tension. *Journal of Applied Communication Research*, 32(2), 119–146. <https://doi.org/10.1080/0090988042000210025>
- Trethewey, A., & Ashcraft, K. L. (2004). Special issue introduction—Practicing disorganization: The development of applied perspectives on living with tension. *Journal of Applied Communication Research*, 32(2), 81–88. <https://doi.org/10.1080/0090988042000210007>
- U.S. Government Accountability. (2018). *The Equifax Data Breach* [Majority Staff Report]. U.S. House of Representatives Committee on Oversight and Government Reform.
- Van Merriënboer, J. J. G., and Sweller, J. 2005. “Cognitive Load Theory and Complex Learning: Recent Developments and Future Directions,” *Educational Psychology Review* (17:2), pp. 147–177.
- Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems*, 4(2), 74–81. <https://doi.org/10.1057/ejis.1995.9>
- Weber, R. P. (1990). *Basic Content Analysis*. SAGE. <https://dx.doi.org/10.4135/9781412983488>
- Weick, K. E. (1988). Enacted Sensemaking in Crisis Situations. *Journal of Management Studies*, 25(4), 305–317. <https://doi.org/10.1111/j.1467-6486.1988.tb00039.x>
- Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the Process of Sensemaking. *Organization Science*, 16(4), 409–421. <https://doi.org/10.1287/orsc.1050.0133>
- Weinstein, N. D., Lyon, J. E., Sandman, P. M., & Cuite, C. L. (1998). Experimental evidence for stages of health behavior change: The precaution adoption process model applied to home radon testing. *Health Psychology: Official Journal of the Division of Health Psychology, American Psychological Association*, 17(5), 445–453.
- Wiener, M., & Saunders, C. (2014). Forced coopetition in IT multi-sourcing. *Journal of Strategic Information Systems*, 23(3), 210–225. <https://doi.org/10.1016/j.jsis.2014.08.001>
- Williams, J. (Director). (2020). *SANS Emergency Webcast: What you need to know about the SolarWinds Supply-Chain Attack* - SANS Institute. <https://www.sans.org/webcasts/emergency-webcast-about-solarwinds-supply-chain-attack-118015>
- Willison, R., and Warkentin, M. 2013. “Beyond Deterrence: An Expanded View of Employee Computer Abuse,” *MIS Quarterly* (37:1), pp. 1–20.