The Role of Stress in Incident Response

Mark L Davis III

Davenport University

CAPS795

Dr. Decker

November 3, 2025

Table of Contents

Table of Contents **2**

Abstract **4**

Introduction **5**

Literature Review **7**

Role of Stress and Pressure in Decision Making **10**

Consequences of Stress and Burnout **13**

Associated Risks of Incident Response Burnout **16**

Recommended Improvements **20**

Final Thoughts **22**

Methods **23**

Design **23**

Data Collection and Analysis **24**

Other Considerations **27**

Results **29**

Presence of an Impact **29**

Decision Making **30**

Attention from Management and Research **31**

Perceived Effects on Associates **32**

Perceived Effects on Organizations **34**

Discussion **35**

Impact of Stress on Incident Response **35**

Limitations **39**

Opportunities for Future Research **40**

Conclusion **42**

References **45**

Abstract

The incident response sector of the cybersecurity industry contains some of the most stressful and time-sensitive work across the information technology industry. However, the impact that this level of stress presents remains undetermined, understudied, and unaddressed. Such high levels of stress hold significant consequences for all parties involved including the individual workers, their organizations, and the entire cybersecurity industry. Furthermore, no current research directly addresses the impact that high levels of stress hold on these parties and the exact consequences that follow it in incident response. This paper focuses on identifying the existence of an impact presented by stress in incident response as well as the lack of attention given to this problem by research and industry leadership. To accomplish this objective, interviews were conducted with industry experts to uncover this impact and to gain inside knowledge as to how the problem is addressed by leadership and academia. To summarize, the participants declared that the presence of an impact in incident response is real and is unaddressed by the relevant parties. These findings prove that the issue is real, and it has massive consequences on all of those involved in incident response. Also, they prove that the issue is going unaddressed by leadership and research alike.

Introduction

Incident response is the most critical element of the information security field. It is the very aspect of data protection that requires accurate and rapid solutions to not only restore systems back into working order, but also to protect critical organizational and personal information. One wrong decision may lead to catastrophic damage to an organization. Therefore, the individuals working within these environments must remain persistent as they manage cyber-attacks on a weekly to daily basis. However, the required level of persistence is often not achievable. This begs the question that has been asked so little in this field, what impact may stress and pressure have on these individuals and their work?

Furthermore, the primary concern behind this issue is that stress has an impact on incident response teams and associates alike. This issue leads to other problems in these time-sensitive environments when decision making processes are impacted by stressful situations. The justification for this research stems from the lack thereof in current literature. There is a plethora of studies on incident response procedures and the role of stress in decision making processes, but very minimal research conducted on how these two areas intersect. Moreover, the impact that stress and pressure have on incident response decision making is an area that has obtained little attention while it remains a critical area to understand. Therefore, the subject that is in need of further understanding is exactly how this impact has influenced incident response environments based on real events. Furthermore, this research will hopefully be used to help information security teams identify this as an issue and therefore motivate them to develop methods to alleviate stress in these environments as well as the impact it creates. Also, understanding how stress has impacted real-time incident response situations will provide an understanding and path towards alleviating this impact for associates and teams overall.

While stress and pressure play a significant role in decision making, it also carries a major impact on incident response associates and teams that influences both the mental health of associates as well as incident response procedures. This study also provided an idea as to what this impact's effects may look like and how it presents an issue among incident response workers. Similarly, this study provided a glimpse of how organizations may also suffer from the impact that stress may have within their incident response environment.

There were a number of research questions to address in this study. Many of these questions were a direct result of the lack of literature on the subject that may have been able to answer them previously. First, does there exist an impact presented by stress and pressure in the incident response profession? Next, what effects does this impact of stress and pressure have on incident response procedures? As the research addresses how exactly stress and pressure take effect, there more than one impact may be present. Next, what impact does stress and pressure have on associates within incident response teams? This question pertains to individual employees and how stress can affect them in their professional and personal lives. Also, this question pertains to both the short-term and long-term effects that stress may have on an individual worker. Next, what consequences may organizations experience from the impact of stress experienced by their incident response teams? Furthermore, how can stress and pressure influence decision making processes among these individuals? This is a very important question to address as this subject has the most literature to support it, albeit not focusing on information security or incident response. Many studies were found to be available that highlight how stress can affect decision making. Also, it provides important insight as to what exactly may occur in stressful situations inside an incident response scenario. Lastly, can this impact be alleviated without negatively influencing critical processes? This question focuses more on if incident

responder well-being can be maintained while refraining from negatively impacting incident response procedures.

Overall, the information security industry has failed to properly acknowledge that stress and pressure have an impact on associates in times of incident response. Moreover, this impact needs to be understood and identified before action can be taken to alleviate it. This impact that stress and pressure hold serve as a threat to both individual employees and their organizations alike.

As far as literature is concerned, there is a wide variety of literature that pertains to the ways stress influences decision making. However, there is not much available literature on how it may affect decision making in an information security setting and what the consequences may be if decision making is affected. The research was conducted to identify the existence of this impact, its perceived effects, and the potential consequences it may have on associates and organizations alike.

This study was conducted in hopes that it would influence policy makers and executives of organizations to take action to alleviate the stress and pressures that incident response associates experience when working in incident response situations. Not only will this alleviation assist their associates, but also their organization as better decision-making efforts are made to protect their organization's data. Also, it would hopefully inspire a call to action amongst researchers to further study this issue.

Literature Review

To reiterate, the problems identified prior to this study are that there may exist an impact presented by stress and pressure in incident response and the information security industry has failed to effectively address the problems presented by this impact as they pertain to incident

response procedures and employees. Specifically, the impact it presents is simply not understood to its entirety as it pertains to individuals and organizations alike. Moreover, solutions must be identified and employed in order to mitigate the risks associated with the impact of stress and pressure in such a sensitive profession.

Many studies such as Van der Kleij et al (2017) describe the factors of success for incident response teams as the inclusion of the required tools and procedures as well as the knowledge and skills to handle the incidents. These studies make no mention of how stress and burnout may serve as negative factors in this profession. While they highlight important elements of success in the profession from an individual and managerial standpoint, there is a serious lack of attention towards negative elements such as stress and burnout. By leaving this element undiscussed and understudied, the issue continues to remain prevalent with no solution or controls.

Stress, pressure, and burnout are common subjects of research among psychology literature as they pertain to various professions such as the medical and business fields. Oddly enough, the literature available as for how these elements impact cybersecurity and, more importantly, incident response, is very limited as acknowledged by works such as Paul and Dykstra (2017) and Arora and Hastings (2024). Similarly, Singh et al (2023) also recognizes that there is a significant lack of stress research for the cybersecurity profession. Also, Singh et al (2023) highlights that the existing research on this subject ultimately lacks context, clarity, and understanding in terms of how it directly applies to cybersecurity professionals and their work. This is problematic as the overall effectiveness of research up to this point is mostly questionable or incomplete. Singh et al (2023) also emphasizes that while the current stress research in cybersecurity is lacking, it is still progressing and has much room and opportunities for

improvement. Arora and Hastings (2024) stresses that this lack of research and attention introduces risk to the well-being of professionals as well as the security of their organizations. Moreover, this is a significant limitation within the subject as there are very limited studies for exiting literature to compare results to. Likewise, many studies such as Nepal et al (2024) experience issues with establishing baselines among subjects as many are introduced to the study having currently experiencing burnout from their profession.

Despite the limitations identified by the existing literature, the existing studies already provide significant contributions to the overall topic. For instance, the existing literature sheds light on a little-addressed issue that has the potential to be catastrophic to either an individual or entire organization. Also, many available studies provide recommended actionable improvements for organizations to take in order to address potential impacts caused by burnout among their incident response teams.

The identified literature was found using casual research methods. For instance, using two primary sources in the form of Davenport University's online database and Google Scholar exclusively for journal articles. Using these sources, keywords such as "burnout", "stress", "incident response", and "decision-making" were employed to identify not only journal articles, but also systematic reviews containing more resources to analyze.

Furthermore, the selected method of reviewing literature for this topic was the simple method of employing the thematic approach. Moreover, identified literature will was reviewed in groups based on common themes. Specifically, the review begins with a more psychological approach by examining the impact that stress and pressure have on the decision-making processes of associates. The second theme will consist of the general consequences that these impacts may have on individual employees and their organizations. Most importantly, the

following theme will focus on the associated risks of burnout and stress among incident response associates. Finally, the last theme regarding literature will pertain to recommended improvements to address these impacts.

Role of Stress and Pressure in Decision Making

The first topic of discussion pertaining to the role of stress and pressure among incident response associates is how exactly these elements impact decision making. For instance, there are many examples of literature that focus on this subject and, specifically, the negative impacts that the elements of stress and pressure play on decision making. While there is very limited literature on this impact as it pertains to incident response procedures specifically, there are plentiful studies to reference that pertain to other various high-stress professions.

First, Groombridge et al (2019) reviews research on the impact that stress has on decision making in first responder professions. Moreover, this systematic review aims to describe and discuss stress factors in decision making during critical first aid scenarios. This systematic review identifies that specific stressors such as noise, fatigue, and critical moments negatively impair decision-making and situational awareness in emergency medical situations (Groombridge et al, 2019). While these findings do not pertain to the field of information security, they have significance as the results show that specific and universal factors can negatively impair performance among individuals in stressful situations.

Similarly, Nobles (2022) also notes that fatigue plays a significant role in information security burnout. This is significant as, like Groombridge et al (2019), fatigue remains a common factor towards stress and, ultimately, employee burnout. Moreover, Nobles (2022) expresses that fatigue in cybersecurity has directly led to higher numbers of data breaches and similar security incidents. This study, in particular, focuses on surveys of information security workers as well as

reviewing the elements of security fatigue and stress. Nobles (2022) emphasizes the universal lack of organizational acknowledgement of prolonged exposure to stress that employees commonly experience in the workplace. Notably, this is stated to lead to other issues such as noncompliance and low production amongst employees.

Furthermore, it is also critical to understand the underlying impact that stress has on an individual's decision-making processes. Starcke and Brand (2012) discuss this subject as it pertains to the idea that decision making and stress are intricately connected to each other. This study was established to fill a hole in the research gap regarding this connection. Starcke and Brand (2012) provide a review to summarize identified studies that pertain to stress and decision making that were conducted between 1985 and 2011. To summarize, Starcke and Brand (2012) resulted in consistent findings across all studies that stress affects decision making in a positive or negative manner depending on the situation at hand. This remains a significant limitation of this study as most studies regarding decision-making under stress generally result in primarily negative effects being identified. However, the fact that effects are being identified regardless makes the findings of this study significant.

Similarly, Wemm and Wulfert (2017) conducts a quantitative study involving an experiment on decision making under the influence of stress among college students. While employing convenient sampling methods by gathering subjects from the university's psychology classes, Wemm and Wulfert (2017) used a two-group experimental design to expose participants to a stress group or non-stress group while reading heart rates. The study shows notable results as they suggest that present stressors may negatively affect decision making processes. However, this study has various limitations such as employing the convenience sampling method and small sample size (Wemm and Wulfert, 2017). Ultimately, various literature exists to back the

understanding that stress and pressure have a negative impact on the decision making of individuals.

Moreover, the element of stress certainly presents risk in the context of incident response. According to Paton (2003), stressors that are present during an incident or disaster have the potential to impact a worker's ability to interpret information that is presented to them and understand it. Also, the workers can struggle or fail to make decisions based on the information presented to them (Paton, 2003). In the context of cybersecurity, the ability to be presented information and understand it in a timely manner is a critical component of responding to incidents and disasters.

Lastly, Young et al (2012) examines decision making of subjects under time constraints. In other words, the element of time pressure is investigated for its effects on decision making among subjects over the course of three experiments. In summary, Young et al (2012) concludes that subjects under time pressure express increased risk-seeking behaviors to meet demands. This conclusion relates to the findings of Nobles (2022) where noncompliance becomes a concern among employees experiencing burnout. Also, these results relate to those of Wemm and Wulfert (2017) as both studies show negative effects of stress on an individual's decision-making processes. This is relevant to the current study as incident response employees who experience time pressure would express increased risky behavior as referenced by the results of Young et al (2012). Furthermore, this risky behavior can lead to further consequences for the employee's organization.

Furthermore, these pieces of literature offer a great glimpse of the overall presence of an effect that stress has on an individual. Overall, the key point made by these studies is that there

exists an underlying effect on decision making from high levels of stress. The next important step is to identify the consequences that come with this underlying effect.

Consequences of Stress and Burnout

Furthermore, this presence can then be applied to information security environments where the stakes are not so much the consequences of medical practice or other timely situations, but rather critical information and systems for an organization. Trope (2019) backs this claim as their study states that stresses from cyber threats can alter data officers' decisions on responding. Moreover, this study relates to one of the main problems at hand in that not only are individual associates at risk from these effects, but also their organizations just as much. Trope (2019) explains this stance using real-life examples of cyber-attacks that took place at Uber and Equifax. These are significant examples of the shortcomings of incident response teams that are caused by poor decision making of associates. Moreover, this can be expected to occur when employees are experiencing burnout.

Similarly, the major consequences that organizations face in the event of a major cyber-attack are well known throughout the information security industry and academia. One example, in particular, is the cyber-attack on the NHS in the United Kingdom in 2017 resulted in massive delays and constrains for the agency. O'Dowd (2017) describes this incident as an attack involving a virus that put a halt to the information systems of dozens of organizations. Ultimately, this attack went on to last for multiple days and delayed critical health procedures (O'Dowd, 2017). This serves as only one of many examples of the seriousness behind some of the consequences that organizations face regarding failed incident response. Moreover, events such as this could result from one incorrect or delayed decision made by one individual employee under the influence of stress. Schlackl et al (2022) adds further emphasis as they

explain that the average breach of information systems in 2006 averaged $3.5 million in damages to the organization and those associated with it. With this degree of potential damage to the organization, the security analyst trusted with securing its systems and resolving security matters will seemingly face pressure from the weight of the potential consequences that they will ultimately be responsible for.

Additionally, the events where these high-profile cyber-attacks take place also serve as stressors for cybersecurity professionals. In other words, cybersecurity professionals are found to experience heightened anxiety and workload from the major breaches that occur at other organizations that they are not even affiliated with (Arora and Hastings, 2024). In other words, the prospect of a massive attack on one organization may induce stress and anxiety among incident response workers of another organization that could experience a similar fate. The added element of stress as a result of data breaches occurring at different organizations from the worker's employer is important to understand as there are a plethora of factors leading to stress in this profession.

Another study that focuses on the immediate and long-term consequences of employee burnout in cybersecurity is Rangarajan et al (2025). Specifically, this study introduces other consequences that organizations face when burnout goes unaddressed. For instance, Rangarajan et al (2025) identifies that organizations face the consequences of employee turnover and decreased productivity when employees are faced with continuous stress and pressure. Nobles (2022) would suggest that organizations may also suffer from critical mistakes caused by burnout-induced decision-making. Additionally, these consequences are complimented with deteriorating defenses (Rangarajan et al, 2025). With this in mind, the consequences brought

upon incident response teams will negatively affect the organization as a whole if deteriorating production has an impact during an incident response scenario.

On the contrary, the effects of stress and pressure have different, yet similarly detrimental, consequences for individual associates. Budimir et al (2021) discusses the effects that cyber incident-induced stress has on individuals. This study employs a very interesting method as it involves analyzing individuals based on personality traits using the Big Five personality model as well as gender and age demographics. Using this method, Budimir et al (2021) concludes that predictions can be made regarding long-term mental health issues among individuals depending on personality traits. While this study does not exclusively pertain to participants employed in an information security profession, the results show that mental health implications are a predictable consequence of cyber breach stresses to the typical individual. Likewise, Chowdhury et al (2019) conclude their systematic literature review with the understanding that recurring time-sensitive phenomenon in cybersecurity have the potential to have lasting effects on individuals in both their professional and personal lives. These claims add to the imperativeness to shed light on this topic as career incident responders may be taking their work-life stress home with them on a daily basis. Additionally, they add to the present stresses related to job security if employees were to fail at a task that may lead to a catastrophic incident such as a data breach.

To take the individual effects issue further, Spring and Illari (2021) discuss specific attributes of the response procedures that are at risk when this impact is present. For instance, Spring and Illari (2021) have identified specific decisions such as what tools and methods to use in a situation and what information to report and communicate in the event of an incident. Moreover, key aspects of successful incident response are at risk of manipulation through poor

decision making that is influenced by the effects of stress and pressure that associates experience. These results are very significant as they provide a visual as to what exact decisions in the incident response scenario are at risk of being incorrect or absent.

In summary, the impact of stress and pressure on incident response associates is stated to be, at the very least, present in these scenarios. Moreover, consequences of incident response burnout exist in various forms for both organizations and individuals. Identifying and understanding the role of stress and pressure among incident response associates is key to mitigating consequences associated with decision making in these high-stress situations as well as maintaining the mental health of these associates.

Associated Risks of Incident Response Burnout

While understanding this impact and the underlying causes of it is paramount to this study, understanding what its presence in the incident response environment indicates is also critical. In other words, specific risks of employee burnout in the incident response profession as well as the underlying causes of it. This is another area where there is a severe lack of existing literature and research.

To put into perspective what is at risk when addressing stress among incident response associates, Nobles (2018) identifies that humans are the significantly prominent weakness in information security. In other words, human errors are responsible for the strong majority of cyber-related incidents as opposed to technology. The risk of human error is compounded by the impact of stressed-out associates who may show poor decision making in incident response scenarios. Specifically, Nobles (2018) identified time pressure and heavy workloads as leading factors of human error in the field. Additionally, Seppänen and Virrantaus (2015) identify that irrelevant and low-quality information pertaining to the incident at hand also may hinder

responders' efforts. This would make sense as employees who are in high-stress situations would reasonably become more stressed out when provided irrelevant or incorrect direction. While these remain significant impacts on the potential effectiveness of information security processes, other studies dive into incident response associates specifically.

One cohort study, in particular, is that of Nepal et al (2024) that explores and discusses the factors and impacts of burnout among incident response associates. This study ties together the previous points by describing incident response as a field that can be detrimental to associates and organizations alike for different reasons. Furthermore, Nepal et al (2024) stresses that the processes of incident response must be carried out effectively and this can be hindered by the continuing stress that incident response associates face on a daily basis. Specifically, these associates experience burnout from their profession. Nepal et al (2024) also introduces another impact of stress and burnout that I had not previously discussed or identified. This impact is that of turnover among associates. Moreover, organizations that fail to address burnout among their incident response associates are likely subject to dealing with experienced associates leaving and having to replace them with new, unexperienced employees.

Furthermore, Nepal et al (2024) describes the very attributes of the incident response career that led to burnout among associates. For instance, the findings of Nepal et al (2024) identify attributes such as burnout prevalence, personal resources, job content, personal wellbeing, social resources, on-job digital activity, and job demand are all factors that play a role in associate burnout. On the individual side of things, participants in the cohort study showed significant signs of poor wellness such as poor sleep, depression, and high amounts of stress (Nepal et al, 2024). These impacts are significant to the current study as these are attributes that must be addressed by organizational policymakers.

To take things to another perspective, Nepal et al (2024) also identifies the source of the issues at hand. Instead of burnout being related to an associate's personal life or personality, Nepal et al (2024) suggests that a systematic problem with the organization's control and high workloads are higher predictors of stress and burnout among associates. In other words, unreasonable expectations and demand for 24/7 availability are examples of factors that quickly lead to burnout among associates. For this reason, organizations must take into consideration that they have the influence and ability to alleviate these factors of stress through policy and procedure. By doing so, research suggests that they may be reducing the risk of not only a cyber incident caused by a burned-out associate, but also the risk of significant employee turnover. On the other hand, effort can be made by the organizations to better the lives of their associates as well. When referenced to the results of Nobles (2022), organizations can ultimately have control over their employees' productivity and efficiency in decision-making in stressful scenarios. To take this further, Arora and Hastings (2024) discuss that unrealistic expectations, unsupportive organizations, and the overall demanding nature of the industry lead to high volumes of cybersecurity professionals reporting severe stress and burnout from their work. Specifically, 44% of the surveyed cybersecurity professionals reported themselves as experiencing severe stress and burnout from their work (Arora and Hastings, 2024).

The findings of Paul and Dykstra (2017) back these statements as their study focuses on the outcome of individual operations. Moreover, Paul and Dykstra (2017) express that impacts such as fatigue, cognitive workload, and frustration steadily increase over the course of a given situation. This is significant as this study applies to the cognitive stressors that incident response associates experience in incident response or similar scenarios. The study's findings include that fatigue and frustration increase significantly throughout the duration of the operation (Paul and

Dykstra, 2017). Groombridge et al (2019) and Nobles (2022) both contribute similar findings. It is important to note that Paul and Dykstra (2017) found a significantly positive relationship between the two factors as well. Meaning, when one of frustration or fatigue increases within an associate, the other will also increase significantly. Moreover, a subsequent study by Dykstra and Paul (2018) is conducted by the same researchers that involves a survey of stress in cyber operations that they developed to be employed across multiple studies by various researchers. The survey in their study provided significant feedback as it validates the survey's credibility. This survey may provide myself with a useful guideline or resource for gathering information in the research portion of this study.

Furthermore, the more severe cases in incident response can introduce the worst types of risk for associates. For instance, incidents that reach the levels of disaster for the organization are those that may be deemed as more severe situations. When incident response workers are met with disasters at their workplace, they may be at risk of heavy mental health and well-being impacts as evidenced by Sandifer and Walker (2018). Moreover, Sandifer and Walker (2018) describe such risks as decreased mental health, substance abuse, post-traumatic stress disorder, domestic violence, and others. Of course, these are primarily risks of worst-case situations, but they are still prevalent in the cybersecurity industry. Also, this work by Sandifer and Walker (2018) further illustrates how work life for cybersecurity and incident response workers may affect their overall well-being and life outside of their profession. Sandifer and Walker (2018) conduct their research in the context of natural disasters, but the research is applicable to disasters in the workplace as well.

The studies of Paul and Dykstra (2017) and Nepal et al (2024) are perfect resources for this study. Specifically, Nepal et al (2024) discusses the role of stress and burnout and how it

impacts organizations and individuals over the course of time while Paul and Dykstra (2017) discuss the more immediate roles of stress and cognitive workload in an operation-by-operation focus. Moreover, both include critical information relevant to the study at hand by providing key information about the specific roles that stress plays in different aspects of the incident response environment. Additionally, both studies suggest that their results are hopes to be applied towards reducing workforce turnover in incident response and cybersecurity as well as reducing associate burnout. What's more is that Paul and Dykstra (2017) also express their concerns over the severe lack of literature and research on burnout in incident response.

Recommended Improvements

Fortunately, many studies offer recommended improvements for alleviating the impacts presented by stress and pressure in incident response. For example, Groombridge et al (2019) demonstrates that the presence of cognitive aids for critical situations can significantly improve an associate's decision-making ability. Specifically, non-technical skills are the focus of improvement with the referenced cognitive aids (Groombridge et al, 2019). Despite researching improvements for clinical and medical environments, the findings of Groombridge et al (2019) remain applicable to the information security environment as well. Moreover, universal non-technical skills such as teamwork and communication are at risk of deterioration in high-stress scenarios, as indicated by Spring and Illari (2021). Moreover, programs that focus on the mitigation of fatigue should be a primary focus based on the findings of Groombridge et al (2019), Nobles (2022), and Paul and Dykstra (2017).

Additionally, improving elements for cybersecurity and incident response can be as simple as motivation and thorough explanations. In a study that exposed cyber operators to high levels of cognitive and physical stress, Helkala et al (2016) discovered that simple aspects of

explaining the task at hand can show significant improvement in performance and efficiency compared to a control group. In addition, the experiment group in this study was also shown to exhibit improvement over the control group when motivated by the overall significance of the tasks at hand (Helkala et al, 2016). In other words, improvement in efficiency in high-stress situations can be accomplished by relaying the importance of the tasks to associates. While it may seem trivial in comparison with other controls, emotional controls can be as effective as maintaining motivation within incident response teams.

Conversely, improvements for individuals are evident in the existing literature as well. For instance, Nobles (2022) stresses the importance of human-centered programs where the focus is to prevent fatigue among cybersecurity professionals. Likewise, specific anti-fatigue programs within organizations are paramount to maintaining efficient performance among cybersecurity teams (Nobles, 2022). In terms of incident response, initiating programs to focus on mitigating fatigue must be an achievable goal for organizations and their employees. Sandifer and Walker (2018) offer a similar solution by stating that improving or implementing behavioral health programs to offer stress reduction resources in the event of a disaster.

Similarly, employees will benefit from the ease of overall burnout from their professions. Nepal et al (2024) identifies the approach of fostering supportive work environments as one potential solution to burnout. Nepal et al (2024) describes this approach as encouraging a collaborating culture and mentorship to instill confidence and reassurance for incident responders. Also, Nepal et al (2024) introduces the potential solution in the form of proactive workload monitoring where associates check in with each other and workloads are balanced to reduce burnout among employees. These would all provide great solutions for employees as methods towards mitigating employee burnout. For instance, having procedures to prevent

straining workloads and regular check-ins would have positive effects on employees. As the results of Nobles (2022) suggest, employee burnout is an element of information security that must be addressed to uphold adequate decision-making in times of incident response.

Overall, the various solutions provided by Nepal et al (2024) and other previously mentioned literature offer practical advice for organizational policymakers. Moreover, they all contribute to the notion that organizations can and should make further efforts to address stress and burnout among cybersecurity employees.

Final Thoughts

After a thorough review of existing literature regarding the impact that high levels of stress has on an individual's decision-making, a conclusion can be made that there is relevant evidence to suggest that a negative impact may variably be present. While many additional psychological resources exist to back this statement, only handful of literature is included pertaining to this aspect as to maintain an information security-focused perspective as opposed to one of psychology.

While literature on the general subject matter exists, there is very little on the exact issue as evidenced by the literature included in this review. For instance, Paul and Dykstra (2017) and Dykstra and Paul (2018) both acknowledge that there is very little research on the human factors of incident response for cybersecurity operations. While this absence of literature is not explained by any literature, it may be a result of the industry still being in the early stages of fully understanding incident response procedures and the effects that prolonged stress that they can have on employees. Also, it may be as a result of the information security industry being secondary in the interest of researchers to the medical or business industries. Whatever the reason, there exists a significant absence in literature pertaining to stress and pressure in incident

response environments. One of the primary goals of this study is to add further understanding of the impacts presented by stress and pressure in incident response to the existing literature.

Regardless, the existing literature provides significant findings pertaining to the potential consequences of unaddressed burnout among incident responders as well as the underlying risks. Additionally, studies such as Nepal et al (2024) and Paul and Dykstra (2017) provide a fundamental picture of what the underlying causes of burnout may be for incident responders. This study strives to identify other risks and causes of burnout.

Lastly, there is an adequate amount of literature suggesting improvements that can be made for addressing and preventing burnout among incident responders. While the existing literature provides generally good recommendations, another goal of the following research is to understand current trends and procedures for addressing stress in incident response environments.

Methods

Design

As this study maintains the qualitative approach, there was no experiment or test to be conducted in order to collect data. This decision was made as the goal of this study is to gain an understanding of the phenomenon behind stress and pressure inside an incident response environment. Moreover, the lack of literature and current research on the subject make it a very complex phenomenon. With the topic of stress in the incident response profession being as understudied as it is, the qualitative approach greatly assists with developing theories as to how stress and pressure impact incident responders as well as opening a new perspective on an otherwise neglected issue.

Additionally, the combination of information security and psychology fields adds complexity to this matter. While combining or complementing fields of study for research is not uncommon, focusing on the fields of information security and psychology together is not a common theme in modern research. This could be due to a number of reasons such as the information security field still being relatively new to academic research. Furthermore, the ability to address subjective experiences among participants in a flexible manner is practically a requirement for this study. Lastly, conducting qualitative research provides the opportunity for a comprehensive discussion that may open paths for future research opportunities. This fulfills the goal of providing a path for more researchers to study this problem.

Data Collection and Analysis

The primary method of data collection that was used for this study was through interviews with the participants. While the aforementioned discrepancy in available resources by itself helps prove that the issue is understudied, the direct effects and potential solutions needed to be uncovered through other means. These elements were uncovered through the answers provided by the interview participants. Overall, two interviews were conducted with volunteers from different organizations and industries. Specifically, one participant is an incident response engineer within the financial services industry located in Chicago, IL and the other an incident response engineer within the education industry located in Northeast Illinois.

Furthermore, the selected participants all stem from the information security profession. They have been selected based on their profession and their exposure to incident response procedures or associates. Individuals who are working in incident response situations or those who oversee them are key as only they can provide reliable, first-hand knowledge of how stress and pressure have affected their associates and the potential they may have in the future. The

best efforts were made to provide the study with a variety of participants based on company and industry when possible. The initial goal was to obtain at least one participant from each of the banking, healthcare, and business industries to be available to conduct an interview. This goal was set to obtain an insight into how incident response may differ based on industry, as they may have differing viewpoints to offer on the subject. Moreover, selecting the participants from different organizations also provides insight into how incident response can differ from one organization to another. While the goal to interview participants from the three aforementioned industries was not achieved, the goal to interview participants from different industries in general was achieved.

Moving on, validity of these personal communications was not a concern as the participants were verified to have been employed within the cybersecurity industry prior to conducting the interviews. Also, they were verified to have had experience in incident response procedures as well. This is important as the answers they provided were based on their experiences as experts in their field, leaving the accuracy of these answers to not be a limitation of the research.

As previously mentioned, this study is highly limited in terms of research methods to employ due to the complexity of the subject as well as being a qualitative study. The best method of collecting data in this study was to conduct interviews with the subjects. These interviews were to be conducted over telephone calls, in-person, or by other virtual means such as Zoom or Google Meets meetings based on the availability of the participants. Furthermore, these interviews were structured with pre-designed open-ended questions for the subjects to fully express their insights into how stress has affected their organization’s incident response associates. Also, this provided the interviewees with an opportunity to express their opinions on

how their organization may or may not address their concerns regarding stress in these scenarios. The only tools that were required for this method were one sound recorder and one notepad to take notes on for the duration of the interview. Therefore, the primary method used to collect data was through the audio recorder.

Moving on, the subjects that have been selected for the research and agreed to participate are being interviewed as experts in their industry. Therefore, IRB approval was not needed as a prerequisite to conduct the research. However, the opportunity to provide informed consent has been offered to all participants. In the case that the participants wished for informed consent to be provided, the consent process included informed consent as well as explaining the purpose of the study as well as the potential risks and benefits to the participants. Complete understanding of the study from the participants was declared before moving into the interview questions. Lastly, all participants were notified that all data collected during the interviews were to be destroyed no later than the project's completion on November 10, 2025.

As far as risks are concerned, the only realistic risk that needed to be addressed was the matter of confidentiality. This element has been maintained and explained as access to the information being limited only to myself. Moreover, the notes and sound recorder have only been accessed through a digitally locked safe accessible only to me. Also, the participants' names and contact information were discarded upon conclusion of the data processing stage of the study. Furthermore, all data acquired from the interviews have been deleted and erased from all devices used throughout the study. This includes the wiping of audio recorders and hard drives in addition to shredding all notes taken during interviews. Lastly, the participants were all informed that their participation is voluntary prior to the beginning of their respective interviews, and that they may withdraw from the interview or choose for their information to be discarded at

any moment. For reasons pertaining to confidentiality, the two participants were interviewed anonymously and therefore will be represented by their title and industry for the remainder of this paper.

As mentioned previously, the research subjects were selected as experts in the fields of information protection and cybersecurity. This served the purpose of seeking knowledgeable individuals in the field so that a greater perspective could be gained. Since these individuals were sought out, there was no primary method of sampling to be utilized prior to beginning the interviews.

All interviews have been analyzed independently in order to fully understand each participant's perspective on the subject. Afterwards, the data collected from the interviews was analyzed together to understand common themes and issues brought during the different interviews. Moreover, thematic analysis has been employed for analyzing the data collected at this point in the study. Since this method has been established for data analysis, there was no need for the assistance of technology or software to analyze the relatively small number of interviews.

Other Considerations

As far as permissions are concerned, the only entity that may have required permission to be obtained from aside from the institution is the organizations by which the participants are employed. Some organizations may require permission to interview their employees as corporate policy suggests or if the participant wishes for that permission to be granted first. This concern could have been negated by reaching out to the organization's human resources team before the interview in order to inquire about necessary permissions. Fortunately, this action was not necessary for the participants. There could have been a small element of risk associated with this,

however, as failure to obtain required permission by an organization has the potential to cause the subject to break a confidentiality agreement that they had previously agreed to with the organization.

Similarly, had the conversation during the interview moved into discussing specific incident response scenarios and procedures, the participant may have disclosed critical information of the organization. In order to avoid this situation, great care was taken regarding moving the conversation along in a manner so that sensitive information does not get disclosed. Depending on the individual being interviewed, it may be difficult for them to avoid disclosing sensitive information accidentally.

As mentioned earlier, validity of the answers provided by the participants is not a concern for the results. However, reliability serves as a potential limitation for using personal communication interviews as the method of data collection. For instance, different answers among participants may provide inconsistency across the results of the study.

In terms of ethical considerations, one that had been taken prior to conducting the research for the study pertains to the subject matter being discussed during the interviews with the subjects. Since the information security and incident response fields elicit relatively high amounts of stress in high stakes and time constricting situations, care was taken so that sensitive matters would not elicit strong emotional responses from the interview participants. Had the subject matter of the interviews become too sensitive for the interview participants, they were given the opportunity to stop the interview at any moment or to not discuss the subject. However, the subject of incident response and cyber security in itself is not considered a sensitive topic. There remained the possibility that participants could have elicited stronger emotional responses as a result of their personal experiences in the industry.

Ultimately, the methods presented for conducting the research and handling the data were low risk as all the necessary steps were followed throughout the process. Additionally, the interview subjects are not considered to be pulled from an at-risk population. As a result, the study was performed with little concern for ethical constraints, legal issues, or conflict of interest.

Results

The interviews that were conducted with the two participants provided a plethora of data pertaining to the presence and overall impact that stress and pressure hold on the incident response profession in addition to the entire cybersecurity industry. Moreover, both interview participants offer similar insights which reflect the purpose of the study as well as the research questions. On the other hand, they also provided contrasting insights into some of the questions presented to them.

Presence of an Impact

Upon being asked about the overall presence of stress in the cybersecurity industry, the financial services incident response engineer proclaimed that it remains an element that is prevalent across everyone within the industry. Moreover, the impact that it presents is more significant in incident response. This individual compares incident response environments to those of emergency rooms where emergencies are constant. Additionally, incident response teams suffer from burnout regularly as they are constantly assigned high volumes of low-priority tasks in addition to these emergency situations. Not only does this individual identify that an impact is present, but they also state that it is the biggest risk to incident response teams and individual associates.

The education information security engineer backs this statement by claiming that pressure comes from various factors in incident response including pressure from the attack, the investigation, recovery procedures, and from leadership. This participant also noted that the presence of stress and pressure persists across the entire cybersecurity industry in addition to the smaller incident response profession. This participant alludes to the idea that a significant number of incident response and cybersecurity workers must cope with the possibility of losing their job with so much as one single incident.

Furthermore, both participants provide insights that align with the hypothesis that there is an impact on the cybersecurity and incident response professions that stress and pressure hold. The results do vary, however, as to what this impact results from and how it affects these associates directly.

Decision Making

There were mixed results pertaining to the element of decision making under stress in incident response. For instance, the financial services incident response engineer stresses that delayed decisions remain a massive issue and cause added stress among associates. Specifically, decisions may take hours before being made due to the nature of the investigation at hand as well as additional incidents stacking on each other. Scenarios such as this remain a primary concern regarding stressors according to this individual. Also, the financial services incident response engineer offers insight on how decisions may be incorrect in stressful situations. For instance, incorrect or overall poor decisions have been made in this individual's profession in which smaller incidents were prioritized over more serious emergencies. The financial services incident response engineer claims that this decision was a result of the stressful scenario in which the associate was in.

Additionally, the financial services incident response engineer offers a new insight that hadn't been previously considered where important steps may be overlooked or skipped in critical situations. This individual highlights this scenario in an example they provide in which an associate overlooked key steps in resolving an incident as a result of the stress they were experiencing.

On the other hand, the education information security engineer claimed that decision making rarely is delayed as a result of stress since the speed at which decisions are made is a direct result of the rapid response environment. This individual, however, did state that the overall decision-making processes are altered as a result of stress in this line of work. Specifically, the combination of situational intensity and leadership demands can result in associates making unconventional decisions.

Overall, both individuals who were interviewed perceive notable effects that stress and pressure hold on the decision-making element of incident response. However, the participants identify effects that differ from one another.

Attention from Management and Research

One primary concern brought up by the financial services incident response engineer is the lack of support by management in cybersecurity and incident response departments. According to this individual, poor leadership is a leading cause of failures in departments as well as poor work life conditions for associates within the departments. Furthermore, neither management nor research gives adequate attention towards this impact that stress and pressure hold in incident response. The financial services incident response engineer was adamant that this lack of attention is the biggest risk towards incident response teams.

Furthermore, the financial services incident response engineer had stated that their own management implements methods and procedures to help alleviate the stress that their incident response teams experience. The method that this organization uses is to remove incident response associates from incident response work for a period of time so that they can learn new topics or tasks. This method reportedly saw significant results in lowering burnout throughout the department without negatively impacting productivity among associates and teams.

Similarly, the education information security engineer also emphasizes that both research and management exhibit a major lack of attention towards this issue. Specifically, this individual stresses that associates throughout the industry have minimal to zero training in mitigating stress and pressure as a result of this lack of attention. Moreover, this participant stated that he has never experienced or heard of organizational measures or programs to assist with mitigating stress among incident response or cybersecurity associates.

Ultimately, both participants provide insights that insist that there exists a major lack of attention from leadership and researchers towards stress in incident response. Moreover, both individuals agreed that the entire industry would benefit from assistance from their leadership or from developments in research.

Perceived Effects on Associates

Moving on, the financial services incident response engineer offered great insight on the negative effects that stress may have on incident response associates. First, this individual stressed that the major impact is how associates can suffer from poor amounts of sleep as well as irregular sleeping patterns since many incident response employees work on an on-call basis during time outside of regular work hours. For instance, they highlight that there are instances in which incident response associates are woken up in the middle of any given night by alerts of

intrusion on up to five distinct occasions. This individual highlighted this effect as a primary factor in the daily lives of his associates and all other employees in this profession.

Also, this individual stated that the presence of high levels of stress in his profession is a direct reason for high turnover rates across the industry. Moreover, he claims that the burnout experienced by associates in the field and the inability for them to relieve it remains a primary factor in high turnover rates.

Lastly, another effect that the financial services incident response engineer identified is the overall burnout from constant exposure to high levels of stress. Specifically, this individual identified the high numbers of false-positive alerts that must be addressed by team members. This is an issue that is often accompanied by lack of sleep, as stated by the individual.

Alternatively, the education information security engineer offers additional insights on how this impact of stress affects employees within the industry. Specifically, this individual mentioned that incident response workers are prone to suffer from this impact in their home and family life when major incidents are present in their work life. Lastly, this participant claimed that long-term exposure to high-stress events in incident response will directly lead to mental health concerns for associates in this industry. One such event, as described by the education information security engineer, is when associates experience events at their work that make them question whether or not their employment is at risk.

The difference between the education information security engineer and the financial services incident response engineer in terms of perceived effects of stress and pressure is that the education information security engineer did not claim to see how this impact directly affects turnover rates throughout the industry. Aside from this difference, the two participants see multiple ways in which incident response employees are negatively impacted by stress and

pressure in their work. One perceived effect that both participants pointed out is how repeated exposure to stressors at work can have negative impacts on home life and with family.

Perceived Effects on Organizations

Both participants had insights to offer on how organizations have suffered from burned out associates or incorrect or delayed decisions being made. First, the financial services incident response engineer stated that organizations suffer from inadequately handled incidents in a way that management and leadership lose the trust of the workers. Moreover, this individual explained that the mishandling of an incident situation is mostly the result of the organization's leadership failing to mitigate stress among incident response teams. Due to this, the organization's leadership loses trust from the executives and the workers.

Alternatively, the education incident response engineer describes other setbacks that organizations can suffer from as a result of stress-induced poor decision making. For instance, this participant describes the massive financial penalties that organizations can suffer from in addition to the negative views from the public. More significantly, this participant explains that the organization will also suffer from a massive loss in trust and goodwill among the industry that they reside in.

In summary, both interviewees recognized and explained that organizations will suffer from setbacks as a result of incidents not being handled correctly due to stressed and burned-out associates. Moreover, they both helped identify yet another negative effect that stress holds on the incident response profession.

Discussion

Impact of Stress in Incident Response

The interviews and the individuals who participated in them provided significantly valuable information pertaining to the role of stress in incident response. One of the key takeaways from the two interviews is that both participants notably agree that stress provides an immediate impact on the entire incident response profession regardless of what industry it resides in. The participants even go as far as to state that the impact presented by stress and burnout is the most significant risk in the incident response field. Perhaps the most significant comparison to the identified literature is the concerning lack of attention given by leadership and research as stated by works such as Paul and Dykstra (2017), Arora and Hastings (2024), and Singh et al (2023). Moreover, the participants from the interviews confirm both that there exists an impact from stress and burnout in incident response and that leadership and research fail to account for this impact. These are significant findings as they confirm the legitimacy of the problem statement and open up new opportunities for research and improvement regarding this impact. Additionally, the findings from the two interviews adequately address the study's research questions.

To take this further, one interview participant discussed that they have never seen or heard of controls being implemented to alleviate stress among incident response associates. This is a significant finding as it further proves the lack of attention and action from research and organizational leadership. This individual, the education incident response engineer, also discussed how neither they nor their associates had ever received any training towards mitigating stress. Another significant finding in this subject is that the other interview participant, the financial services incident response engineer, discussed one method that their organization

currently employs which both works to decrease stress and improve productivity within the incident response department. The method that this individual discussed during the interview is based entirely on temporarily removing associates from tasks that serve as stressors so that fatigue and stress may be reduced for a time. This method directly ties with the ideas presented by works such as Groombridge et al (2019), Nobles (2022), and Paul and Dykstra (2017) where the organizational programs must be focused on the reduction of fatigue to mitigate stress. However, the statement provided by the former participant proves that not all who work in the incident response field are benefiting from these organizational programs. This is concerning as a significant number of incident response employees may have no assistance from their organization's leadership with mitigating a stressful work life.

Another correlation with the work of Nobles (2022) is that an effect of stress that presents risk in incident response is the potential for noncompliance or voluntarily overlooking critical procedures. This is one of the risks identified by the financial services incident response engineer. Furthermore, this added risk adds emphasis to the issues that stress already presents in this profession.

Furthermore, the interview participants also provide great insight into what this existing impact presents for incident response employees. For instance, the financial services incident response engineer explains that the element of consistent stress for an incident responder has the potential for immense consequences on their quality of life to include lack of sleep, family life, and overall wellbeing. Moreover, this individual's statements directly coincide with the findings of Paul and Dykstra (2017) that explain how fatigue, frustration, and cognitive workload serve as major stressors in this profession that carry over into an individual's personal life. This can be perceived easily as the individual's statements pertaining to lack of sleep due to persistent

intrusion alerts can lead to all three of these stressors even outside of regular work hours. On the other hand, the education incident response engineer provides insight into how these stressors can negatively impact an associate's family life. This is a perspective that is not directly discussed in existing literature and remains significant as this effect may prove detrimental towards an incident response employee's personal life.

Additionally, both interviews provided details in terms of how organizations suffer from poorly executed incident response procedures as a result of burnout and stress. The financial services incident response engineer states that the organization suffers from internal conflicts in the event of poorly executed incident response procedures. Specifically, organizational management and leadership will experience a loss in trust among its employees. This is a significant finding as this effect is not found in any current literature. The education incident response engineer provided details about how organizations can suffer from negative impacts such as financial penalties in addition to public scrutiny and loss in trust from the rest of the industry. These details align well with the findings of O'Dowd (2017) and Schlackl et al (2022) which discuss real examples of how organizations can suffer from industry scrutiny and financial penalties, respectively.

While the interviewees provided mostly corresponding answers to the interview questions, one area that the two participants provided differing insights towards was how stress and pressure impact the decision-making aspect of responding to incidents. For instance, the financial services incident response engineer spoke of how decisions in stressful environments are regularly delayed, especially in situations where numerous incidents build upon each other. While this statement is not directly backed by existing literature, Paton (2003) does describe that decisions are found to be delayed if information cannot be interpreted correctly or in a timely

manner. On the other hand, the education incident response engineer claimed that there is no direct effect on the decisions that are made during incident situations, but rather the decision-making process itself. Moreover, this individual states that the stress stems from leadership demands more than from the severity or time sensitivity of the incident itself. This participant's statement regarding the decision-making process being altered as a result of leadership support correlates, to a degree, with the work of Groombridge et al (2019) where it is identified that negativity surrounding events can lead to altered decision making in the event of an emergency. In other words, inadequate support provided by leadership can result in negativity among an incident response team and, therefore, may lead to poor decisions being made. Additionally, the education incident response engineer's statement pertaining to the role of stress in the decision-making process is also supported by the work of Wemm and Wulfert (2017) which finds that this process is directly affected by heightened levels of stress.

Another area of contrast among the interview results pertains to how the cybersecurity industry as a whole suffers from employee turnover. The financial services incident response engineer insists that the impact that stress presents for this line of work and the daily lives of associates who work in it remains the top reason for its employee turnover. Similarly, Rangarajan et al (2025) discusses this exact issue that the cybersecurity industry persistently faces. Alternatively, the education incident response engineer states that there are no resources to confirm that the impact of stress and pressure is to blame for high turnover rates throughout the field. Also, this individual states that they cannot confirm it based on their own experience within the industry either.

Limitations

Overall, this study accomplished its goal of identifying the presence of an impact presented by stress and burnout in the incident response profession. However, a number of limitations were present throughout the study. For instance, the availability of interviews and participants presented a major limitation for gathering data to support the goal of the study. Of the 23 individuals who were contacted to inquire about participating in an interview, only five responded to the inquiry with only two agreeing to participate in the study. The addition of one or two more interviews could have benefited the study with further insight into the topics being discussed.

Furthermore, the number of participants willing to participate in the interview produced another limitation. This study may have been limited by the sample size. While two interviews were adequate for gathering data and the completion of the study, the gathered data may have been limited by the number of participants. The ultimate goal of the research was to conduct three interviews so that perspectives could be gained from incident response procedures in three distinct industries. This study was conducted with the perspective of those from two industries instead.

Lastly, waiting for responses from potential participants created a time constraint for gathering data. The research gathering was ultimately delayed by the lack of individuals willing to participate in the early and middle time periods that were dedicated to gathering data for the study. Since the final interview of the two was conducted on the final day of the research period, a time constraint was present at the time of the interview. Additionally, this limitation also pertains to the interviews themselves. Each interview was scheduled to last for a maximum of half an hour to respect the time of the interviewees. In the case of the financial services incident

response engineer, this amount of time for the interview was nearly inadequate as the participant was willing to provide more details than expected regarding the questions being asked. Moreover, the study would have certainly benefited from being able to discuss the subject for a longer period of time with this individual.

Opportunities for Future Research

One of the main goals of this study is to present new research opportunities due to the documented lack of existing literature on this subject. This goal was achieved as multiple areas of improvement were identified from both existing literature and the interviews. Furthermore, areas of improvement or further research were identified where the interview participants presented contrasting opinions.

First, the topic of how decision making is affected by stress in incident response, specifically, has already seen a concerning lack of research. This is evidenced by the lack of literature on this niche subject. While there are countless studies on how stress impacts decision making in general or in other specific professions or situations, there is no research that uncovers how this impact affects decision making in cybersecurity incident response in particular. Not only is the current lack of literature enough to build a case for further research on this subject, but also the fact that both interview participants offered different insights into how the impact of stress affects this profession. Ultimately, further research into how exactly stress affects decision making in the incident response discipline of cybersecurity would shine new light into this topic entirely in addition to assisting employees within the profession with their work.

Furthermore, a continuation of this current study would certainly benefit the topic by bringing in new insight from more individuals. For instance, a follow-up study to conduct more interviews may be a priority so that more data can be achieved. Specifically, individuals should

be targeted from different industries as the results of this study show how perspectives surrounding the problem may differ between incident response workers of different industries. An additional study containing interviews with incident response workers from industries including healthcare, retail, government, and security would provide a more adequate amount of data before continuing with other studies.

Next, the cybersecurity industry would benefit from further research into the causes of the high turnover rates that it experiences on a yearly basis. The interview participants offered contrasting statements regarding whether or not the impact of stress may be a root cause of high turnover rates across the incident response profession. Conducting a study to determine if the impact of stress is a reason for the high rates or not may prove beneficial to the cybersecurity field and its job market.

Lastly, a follow-up study may be conducted to identify elements for programs that benefit incident response employees by helping them mitigate stress. Incident response will remain a stressful profession without a doubt. However, organizations should implement programs to assist with the mitigation of stress for their associates. The financial services incident response engineer provided a great potential solution for such a program that their organization already has in place. Moreover, this program seems to work as the participant stated that it both alleviates stress and boosts productivity throughout the department. Diving deeper into this program to determine its overall effectiveness may provide the industry with much needed research on stress mitigation methods. On the contrary, another study may prove beneficial to seek answers to roughly how many organizations have solutions in place. Since the education incident response engineer stated that they have neither seen or heard of any such programs

being implemented in the industry, the true number of organizations with these methods may be concerningly low.

Conclusion

The sub-category of incident response in the cybersecurity industry has been known to consist of a stressful and time-sensitive nature of work. However, the presence of a significant impact of stress and pressure has not been declared or identified in current research. Furthermore, this dilemma has received a significantly inadequate amount of attention from both researchers and industry leadership alike.

Despite the lack of research on the subject, many sources point out that there exists a severe lack of literature about how stress affects both cybersecurity and its niche incident response discipline. Moreover, there is also a plethora of research regarding how stress and pressure can directly affect decision-making processes of individuals in their professions or in specific circumstances. However, none of these pertain directly to incident response within the cybersecurity industry. Despite this, all of these studies conclude that stress and pressure hold a significant impact over decision-making processes. Additional studies prove how an incorrect decision made in this profession can impact the organizations that the individual is employed by. Additionally, more studies exist that discuss how stress can have both short-term and long-term negative effects on individuals.

Two interviews were performed to all but confirm that the impact of stress and pressure on this profession does, in fact, exist. Also, both interview participants confirm that both research and industry leadership fail to properly address or even acknowledge the issue that it presents. These participants also provide valuable insights into how the impact negatively affects all of the individual workers, their organizations, and the entire cybersecurity industry alike. Thankfully,

one of the individuals identifies a possible solution or supporting program that may greatly assist individual workers mitigate stress in both their work and personal lives.

The impact of stress and pressure in the incident response profession exists and comes with significant consequences. For instance, individual workers in this field regularly suffer from burnouts and possible career setbacks in the event of poor performance at work as a result of stress. Also, organizations suffer from major incidents as a result of burned-out incident response employees. Lastly, the high turnover rates within the incident response profession may be a direct impact of consistent and unaddressed stress in the field, making for a negative effect across the entire cybersecurity industry. Furthermore, the impact presented by stress is present across all parties involved in incident response. All parties involved will continue to experience these setbacks until the problem is adequately addressed by industry and organizational leadership. Until then, the identified consequences will surely remain constant or may become more troubling.

Opportunities exist for future research to continue this study. The next stages of research on this topic should focus on how this impact affects decision-making processes in incident response specifically. Moreover, future research must also focus on improvements or solutions for mitigating stress and the risks associated with it within incident response departments. Conducting these studies would hopefully be followed by major improvements to the incident response profession.

In conclusion, the impact of stress and pressure within the incident response profession is real and it has major effects on the workers within the profession, their organizations, and the entire cybersecurity industry. Additionally, these negative effects are currently remaining unresolved by both research and industry leadership alike. As this problem persists, more issues

related to stress in this discipline may arise as the cybersecurity and incident response landscape changes over time much like technology and methodology. Furthermore, more research must be conducted to further understand and solve this issue, and cybersecurity industry leadership must take action to help their incident response teams perform their jobs at ease while preserving a sufficient personal life.

References

Arora, S., & Hastings, J. (2024). A survey-based quantitative analysis of stress factors and their impacts among cybersecurity professionals. *Proceedings of the Annual Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2025.736

Budimir, S., Fontaine, J. R., Huijts, N. M., Haans, A., Loukas, G., & Roesch, E. B. (2021). Emotional reactions to cybersecurity breach situations: Scenario-based survey study. *Journal of Medical Internet Research*, *23*(5). https://doi.org/10.2196/24879

Chowdhury, N. H., Adam, M. T., & Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: A systematic literature review. *Behaviour & Information Technology*, *38*(12), 1290–1308. https://doi.org/10.1080/0144929x.2019.1583769

Dykstra, J., & Paul, C. L. (2018). Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations. *11th USENIX Workshop on Cyber Security Experimentation and Test (CSET 18)*.

Groombridge, C. J., Kim, Y., Maini, A., Smit, D. V., & Fitzgerald, M. C. (2019). Stress and decision-making in resuscitation: A systematic review. *Resuscitation*, *144*, 115–122. https://doi.org/10.1016/j.resuscitation.2019.09.023

Helkala, K., Knox, B., Jøsok, Ø., Knox, S., & Lund, M. (2016). Factors to affect improvement in Cyber Officer Performance. *Information & Computer Security*, *24*(2), 152–163. https://doi.org/10.1108/ics-01-2016-0001

Nepal, S., Hernandez, J., Lewis, R., Chaudhry, A., Houck, B., Knudsen, E., Rojas, R., Tankus, B., Prafullchandra, H., & Czerwinski, M. (2024). Burnout in Cybersecurity Incident Responders: Exploring the factors that light the fire. *Proceedings of the ACM on Human-Computer Interaction*, *8*(CSCW1), 1–35. https://doi.org/10.1145/3637304

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

Nobles, C. (2022). Stress, Burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA – Journal of Business and Public Administration*, *13*(1), 49–72. https://doi.org/10.2478/hjbpa-2022-0003

O'Dowd, A. (2017a). Major global cyber-attack hits NHS and delays treatment. *BMJ*. https://doi.org/10.1136/bmj.j2357

Paton, D. (2003). Stress in disaster response: A risk management approach. *Disaster Prevention and Management: An International Journal*, *12*(3), 203–209. https://doi.org/10.1108/09653560310480677

Paul, C. L., & Dykstra, J. (2017). Understanding Operator Fatigue, Frustration, and Cognitive Workload in Tactical Cybersecurity Operations. *Journal of Information Warfare, 16*(2), 1-11,III-IV. https://proxy.davenport.edu/login?url=https://www.proquest.com/scholarly-journals/understanding-operator-fatigue-frustration/docview/1972150000/se-2

Rangarajan, A., Nobles, C., Dykstra, J., Cunningham, M., Robinson, N., Hollis, T., Paul, C. L., & Gulotta, C. (2025). *A Roadmap to Address Burnout in the Cybersecurity Profession: Outcomes from a Multifaceted Workshop* , 1–19. https://doi.org/10.48550/arxiv.2502.10293

Sandifer, P. A., & Walker, A. H. (2018). Enhancing disaster resilience by reducing stress-associated health impacts. *Frontiers in Public Health*, *6*. https://doi.org/10.3389/fpubh.2018.00373

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A

systematic review. *Information & Management*, *59*(4), 103638. https://doi.org/10.1016/j.im.2022.103638

Seppänen, H., & Virrantaus, K. (2015). Shared situational awareness and information quality in disaster management. *Safety Science*, *77*, 112–122. https://doi.org/10.1016/j.ssci.2015.03.018

Singh, T., Johnston, A. C., D'Arcy, J., & Harms, P. D. (2023). Stress in the cybersecurity profession: A systematic review of related literature and opportunities for future research. *Organizational Cybersecurity Journal: Practice, Process and People*, *3*(2), 100–126. https://doi.org/10.1108/ocj-06-2022-0012

Spring, J. M., & Illari, P. (2021). Review of human decision-making during computer security incident analysis. *Digital Threats: Research and Practice*, *2*(2), 1–47. https://doi.org/10.1145/3427787

Starcke, K., & Brand, M. (2012). Decision making under stress: A selective review. *Neuroscience & Biobehavioral Reviews*, *36*(4), 1228–1248. https://doi.org/10.1016/j.neubiorev.2012.02.003

Trope, R. L. (2019). When Incident Response Goes Awry: Cybersecurity Developments. *The Business Lawyer, 74*(1), 229-241. https://proxy.davenport.edu/login?url=https://www.proquest.com/trade-journals/when-incident-response-goes-awry-cybersecurity/docview/2199859398/se-2

Van der Kleij, R., Kleinhuis, G., & Young, H. (2017). Computer Security Incident Response Team Effectiveness: A needs assessment. *Frontiers in Psychology*, *8*. https://doi.org/10.3389/fpsyg.2017.02179

Wemm, S. E., & Wulfert, E. (2017). Effects of acute stress on decision making. *Applied*

Psychophysiology and Biofeedback, *42*(1), 1–12. https://doi.org/10.1007/s10484-016-9347-8

Young, D. L., Goodie, A. S., Hall, D. B., & Wu, E. (2012). Decision making under time pressure, modeled in a prospect theory framework. *Organizational Behavior and Human Decision Processes*, *118*(2), 179–188. https://doi.org/10.1016/j.obhdp.2012.03.005