Article

Not peer-reviewed version

A Qualitative Study on The Reduction of Dwell Time Exceeding 200 Days

Abdul Rahman *

Posted Date: 24 October 2024

doi: 10.20944/preprints202410.1609.v2

Keywords: cybersecurity dwell time; information security (infosec); qualitative inquiry; protection motivation theory (PMT)

Article

A Qualitative Study on The Reduction of Dwell Time Exceeding 200 Days

Abdul Rahman[1 2,*]

[1] School of Business, Technology and Health Care Administration
Capella University; arahman7@capellauniversity.edu
[2] Affiliation 2; arahman7@capellauniversity.edu
* Correspondence: arahman7@capellauniversity.edu

Abstract: This qualitative study investigates why dwell times, defined as the period between the emergence and detection of a cybersecurity threat, exceed 200 days. By uncovering these insights, U.S. InfoSec professionals can develop strategies to shorten dwell times and mitigate the costs associated with security breaches. The overarching issue is the escalating costs of U.S. cybersecurity breaches, which surged by 10% annually, surpassing $9.48 million per breach in 2023. The duration of dwell time, notably exceeding 200 days, is identified as a critical factor contributing to these costs yet remains poorly understood. This study employed a generic qualitative inquiry (GQI) methodology to explore perceptions surrounding dwell time and its impact on an organization's cybersecurity posture, making it pertinent to understanding and addressing cybersecurity breach dwell time. Through interviews with ten seasoned U.S. InfoSec professionals, this study sheds light on their perspectives regarding the duration between threat deployment and detection. The findings highlighted the importance of proactive measures and timely detection in mitigating cybersecurity risks and enhancing organizational resilience against malicious cyber-attacks.

Keywords: cybersecurity dwell time; information security (infosec); qualitative inquiry; protection motivation theory (PMT)

1. Introduction

This qualitative study delves into the prolonged dwell times in cybersecurity breaches, particularly those exceeding 200 days within U.S. organizations that staff at least 500 employees. It explores strategic measures and underlying reasons for these extended detection periods, emphasizing the significant operational and financial impacts these durations impose on organizations [1]. By investigating these lengthy dwell times, this research aims to provide actionable insights that could help reduce undetected breaches' duration and associated costs. These costs are substantial, with the average financial burden of breaches detected after 200 days being significantly higher than those identified sooner [1]. This discrepancy underscores the critical need for enhanced detection capabilities, as cybersecurity breaches have grown increasingly costly, with U.S. companies experiencing average losses of $9.48 million per incident [2].

The concept of dwell time, the period between the initial occurrence of a breach and its detection, serves as a critical metric in cybersecurity management [1]. Studies reveal that the average cost associated with breaches having dwell times under 200 days is considerably lower than those detected after prolonged periods [1]. This economic disparity highlights the financial benefits of improving detection capabilities and catalyzes organizations to refine their cybersecurity strategies. As technological advancements such as machine learning, cloud computing, and the Internet of Things expand the attack surface, they introduce complex security challenges [3,4]. The increase in internet usage, with approximately 3.9 billion global users by the end of 2018 [5], further exacerbates the potential for significant security breaches, necessitating robust security measures to safeguard increasingly complex IT infrastructures.

Early detection and timely response are pivotal in curtailing the impact of cybersecurity incidents [6]. This study emphasizes the necessity for U.S. organizations to adopt proactive strategies

 doi:10.20944/preprints202410.1609.v2

that detect threats earlier and address them swiftly to prevent extensive operational disruptions. The capacity to detect threats promptly extends beyond technical challenges; it encompasses a strategic imperative that involves organizational readiness and comprehensive threat intelligence [1]. Organizations face prolonged outages and disruptions without such proactive measures, underscoring the importance of timely and efficient threat detection and response strategies.

The theoretical framework of this study is anchored in the Protection Motivation Theory (PMT), which offers a psychological perspective on how individuals and organizations respond to threats [7]. PMT is particularly pertinent in analyzing the cybersecurity landscape, assessing threats, and deploying coping strategies [8]. This theoretical lens is instrumental in examining how different organizations perceive and react to cyber threats, potentially influencing the duration of dwell times. By understanding these perceptions and reactions, InfoSec professionals can better tailor their strategies to detect and mitigate threats more effectively, thereby shortening the costly periods of undetected breaches.

Contemporary research highlights the widespread use of the PMT framework in health, namely, with people diagnosed with non-communicable illnesses or infectious viruses [9]. However, the researcher views that PMT aligns with the study objectives because cyber threat assessment and remediation can be linked to both the risk of threats and coping evaluations vis-à-vis cybersecurity [8]. The perceptions of U.S. InfoSec professionals regarding what shapes the approach to reducing dwell time over 200 days may shed light on cyber threat assessment and mitigation that drive timely responses to business interruptions due to cyber-attacks.

Recent studies have indicated the gradual application of the PMT framework in cybersecurity. For example, PMT has been used to guide a study focused on government employees' cybersecurity behaviors and their role in mitigating the risks associated with cyberattack mitigation [10]. De Kimpe et al. [11] used PMT as their publication's framework to determine the relationships between perceived knowledge, internet integrity, and risk aversion from a cybersecurity perspective. Lee and Kim [12] examined a South Korean survey sample's protection behaviors and cybersecurity awareness using the PMT as a guiding framework. The application of PMT in cybersecurity fields continues to increase within academic circles [10–12].

However, the way PMT is used in studies relevant to cybersecurity fields does not address the study gap, which focuses on potential reasons that underly cybersecurity dwell times. Studies focusing on cybersecurity dwell times apply other scientific frameworks, such as the Lyapunov stability [13]. Another study analyzed the multi-agent system fault-tolerant consensus tracking during cyberattacks in addition to dwell times, using a graph theory-based framework rooted in equations [14]. Applying quantitative or equation-based frameworks is common in studies examining dwell times during cyberattacks due to the system-based aspects of cybersecurity infrastructure [15].

The financial implications of not addressing long dwell times are stark. With a notable 23% cost increase associated with breaches exceeding 200 days, there is a compelling economic argument for reducing these periods [1]. In this research, the authors are interested in identifying why breaches go unnoticed for long periods to establish general knowledge-based methods to reduce such times, which can be cost-effective. Furthermore, the types of threats continue to grow more complex and diverse, and the strategies and approaches used by countries and organizations must also change to address the emerging threat landscape effectively [16,17].

The outcomes of this study hold particular relevance for information security (InfoSec) professionals who are on the front lines of defending organizational data. These professionals have a better chance of identifying the factors that cause long dwell times and what can be done to reduce them, thereby mitigating threats. Conclusively, this study seeks to fill an existing knowledge void regarding dwell times in cybersecurity to facilitate much stronger security postures and minimize monetary losses occasioned by data breaches. Hence, the findings target a broad cross-section of stakeholders, such as IT managers, organizational leaders, and policymakers, to enhance their understanding of the factors that affect dwell times in cybersecurity.

2. Materials and Methods

 doi:10.20944/preprints202410.1609.v2

Research Design

This research adopted a Generic Qualitative Inquiry (GQI), strategically selected to explore the complex factors contributing to prolonged cybersecurity attack dwell times exceeding 200 days. Qualitative research was chosen mainly because of its ability to provide an extensive and rich context within the personal accounts and beliefs of the professionals operating in the cybersecurity sphere. This is an exploratory study, and because of its inherent flexibility, the GQI was effective when probing for emergent themes. This allowed a clear focus on participants' views, which offered insight into the nuanced and complex factors that shape dwell times, which might not be possible if framed by a more structured theory. This flexibility of the approach facilitated the evolution of the study while collecting data so that all the potential reasons behind the prolonged dwell times, as explained by the InfoSec professionals, would be investigated.

Participant Selection and Sampling

The study focused on InfoSec professionals in the United States with adequate experience in the field using purposive sampling methods to capture participants with a deep understanding of how cybersecurity threats are developed and managed. In this study, the participants included ten professionals covering a wide range of experiences and job positions in the context of cybersecurity. This number was deemed adequate for reaching the point of data saturation when nothing new could be wanted to gain a sufficient understanding of the phenomena studied. Purposive sampling played its part in ensuring that some specific participants with elaborate understanding were picked, making the case study more useful in analyzing the factors that led to long dwell times.

Materials

Digital tools and platforms such as Zoom and various transcription services were the primary materials used in this study. These tools enabled recording the interviews conducted digitally and the word-by-word transcription of the conversations achieved, which was necessary for the subsequent and more particular analysis. The interview schedule for this research was purposely constructed to have an over-arching semi-structured interview format, which ensured that all the essential areas of discussion were covered systematically while at the same time creating room for these interviews to follow deeper discussions on emergent areas of interest. This methodological setup proved important for collecting detailed information that shed light on the extended duration of stays observed in cybersecurity cases.

Data Collection Procedures

The study employed face-to-face, semi-structured interviews lasting 45 to 60 minutes to obtain in-depth discussions regarding the factors leading to long dwell times. Participants were first informed about the study's purposes at the beginning of every session and were mainly assured about anonymity and their willingness to participate. The interviews were conducted with the participant's permission, and the recorded information was used for data analysis only. This systematic process of gathering data was very important in making the data-rich and profound for the study's results.

Data Analysis Techniques

Data analysis commenced with complete verbatim transcription of all the interviews without omissions. Transcripts were coded following Braun and Clarke's [18] six-phase thematic analysis method, and the initial themes that emerged were then reviewed and collapsed into bigger categories. NVivo 14 software was used to sort the collected data and to assist in the thematic construction that helped to discern the specific patterns concerning the long stays in the cybersecurity industry. This thorough analysis helped to provide a sequenced, complete, and empirical understanding of the presented study from the participants' perspective.

 doi:10.20944/preprints202410.1609.v2

Ethical Considerations

Ethical considerations incorporate the morality problems and questions researchers must address when selecting and conducting a research study with human participants [42]. The research abided by all ethical standards requiring human subjects' consent. Permission to collect data was obtained from Capella University's Institutional Review Board (IRB). Each participant received a signed informed consent form before data collection. The informed consent form included the study's rationale, the data collection method, and the risks and benefits of participation. Informed consent ensures that potential participants understand how their data was integrated and utilized before deciding to participate in the study. Participants were informed that their participation in the study was purely voluntary and would not be at risk if they opted out at any time. Other ethical issues, such as confidentiality and anonymity of the participants' responses, were maintained by assigning participant identifiers with cross-references between names and identifiers kept in a separate encrypted file. All data gathered during the interviews, consisting of audio recordings and transcription, remained confidential. To ensure the secure treatment of collected data, cloud recordings, and transcriptions were downloaded to an encrypted, removable drive at the end of an interview and then deleted from the cloud. Privacy and security measures include encryption and password protection or the drives containing data in a secure, locked physical space for seven years, after which the data was deleted and the drives reformatted. I was the only person with access rights to the participants' identities and contact information.

3. Results

This generic qualitative inquiry study aimed to explore potential reasons underlying cybersecurity attack dwell times of more than 200 days among U.S. InfoSec professionals. The following research questions (RQ) and sub-questions (SQ) guided this study:

RQ1: Why do dwell times for cybersecurity data breaches exceed 200 days?

SQ1-1: Why do U.S. InfoSec professionals believe cybersecurity data breaches exceed 200 days?

SQ1-2: Why do U.S. InfoSec professionals believe some cybersecurity data breaches are more accessible to detect?

RQ2: What measures do U.S. InfoSec professionals take to reduce dwell times over 200 days?

SQ2-1: What tools have U.S. InfoSec professionals used to identify cybersecurity data breaches over 200 days?

SQ2-2: What methods have U.S. InfoSec professionals used to decrease dwell times over 200 days?

The researcher engaged ten U.S. InfoSec professionals with at least five years of relevant experience to explore extended cybersecurity attack dwell times. Participants, who consented voluntarily, provided in-depth insights during semi-structured interviews conducted via Zoom, with each session lasting between 45 to 60 minutes. The university's institutional review board (IRB) approved the data collection and interviews, ensuring adherence to ethical standards. All interactions were recorded and transcribed, with confidentiality rigorously maintained through pseudonyms and secure data storage practices. The interviews were analyzed using NVivo 14 software utilizing Braun and Clarke's [18] thematic analysis method, including familiarizing the data, initial coding, and thematic induction. This process allowed for a detailed examination of the factors contributing to extended dwell times in cybersecurity, culminating in the identification of several key themes that were further analyzed and validated through the study's robust methodological framework. Each RQ was divided into multiple SQ and results are presented in Tables 1 to 4 below.

RQ1: Why do dwell times for cybersecurity data breaches exceed 200 days?

SQ1-1

Why do U.S. InfoSec professionals believe cybersecurity data breaches exceed 200 days? Themes 1 through 3 in Table 1 emerged from the data that helped address this question. The table summarizes the number of participants and references for SQ1-1 themes.

Table 1. SQ1-1 Themes.

 doi:10.20944/preprints202410.1609.v2

Theme	Frequency
Inadequate personnel, resources, and poor management	9
Poor system and slow response to attacks	8
Evolving cyber intrusion tactics by hackers	5

Note. Why do U.S. InfoSec professionals believe cybersecurity data breaches exceed 200 days?

Theme 1: Inadequate Personnel, Resources, and Poor Management.

Nine participants contributed to this theme nine times. The finding indicated that most companies do not have adequate InfoSec professionals to counter attacks by hackers. There is also a lack of adequate resource allocation, which makes it difficult for InfoSec Professionals to counter attacks by hackers. Cybersecurity data breaches exceed 200 days due to ineffective management by the leadership. Participant 1 elaborated that limited resources cause cybersecurity data breaches. The participant explained that companies do not invest in resources that can be used in monitoring attacks and said:

> *Many times, it has to do with limited resources within a company. My perception is that's probably due to largely financial reasons in terms of hiring and just not having enough staffing.*

Participant 3 mentioned that the process is critical in managing cybersecurity data breaches. The participant explained that processes guide how InfoSec professionals should handle various incidences even though they do not have a process implemented by the management, stating, "Process is something that gives us teeth. We do not have a process set in place, and it has been, you know, approved by management and whoever else needs to approve it in the C-suite." Participant 1 explained that many companies do not have adequate personnel as they purchase hardware and software for different company activities, such as logs. The participant explained that ignorance by companies to have adequate personnel results in continuous attacks on their systems, stating:

> *I do not want to say that many companies do not have enough people… but that is really what it comes down to… However, to actually have someone or a group of people who know what to do with that data and can do something with it. That takes many man hours and it is and it's not really making you any money, so. It's hard for some companies to justify spending the money to bring the people.*

Participant 1 mentioned that leadership's lack of authoritativeness results in many incidents not being handled correctly and at the right time. The participant explained that if leadership is keen on company policies and guidelines and identifies the right personnel to handle various incidents, it can significantly help decrease dwell time.

Theme 2: Poor System and Slow Response to Attacks.

Data supporting this theme was drawn from seven individual interviews. The finding revealed that cybersecurity data breaches exceed 200 days because InfoSec professionals have poor working systems and take long before responding to attacks. Their systems can be log compromised, and there are inconsistencies in logs. Participant 5 talked about not responding to attacks on time due to doing many activities. This increases dwell time, stating: "And I sometimes waited until the last minute because I was doing so many other things." Participant 1 explained that their system does not have centralized log management configured or deployed. The lack of centralized log management makes correlating multi-system synchronized access information with their corresponding timestamps difficult. Lack of centralized log management results in a system having unreliable logs, stating:

> *You need really good, centralized log management so that you can get access to stuff that has… timestamps synchronized across multiple systems. The initial system could have been compromised because those logs are no longer reliable.*

Participant 9 explained that companies lack end-point detection and response (EDR) or antivirus (AV) in their systems. The EDR or AV may be full of expectations or expired. This results in having the firewalls not figured correctly, stating:

 doi:10.20944/preprints202410.1609.v2

You do not have your EDR or antivirus enabled everywhere, and if you do, it might be full of exceptions [and] it might be out of date…your firewall might not be configured correctly. Let alone you might not even have the people…who have enough time to monitor all those things.

Theme 3: Evolving Cyber Intrusion Tactics by Hackers.

Five participants referenced the first theme five times. The finding revealed that hackers use evolved cyber intrusion techniques to conduct cybercrimes. They use more advanced processes than the ones used by U.S. InfoSec professionals. They also use low-level techniques that U.S. InfoSec professionals ignore and cannot imagine hackers can use to compromise their systems. In addition, hackers use the same tools regular employees use, thus intruding on their systems. Participant 4 explained that hackers are using new professionals that InfoSec professionals are unaware of. The participant indicated that it gets difficult for InfoSec professionals and emphasized the need for cybersecurity professionals who can easily detect attacks. Hackers are getting creative day by day, stating:

I think it is some of the new processes that they have in place, many of which we are not even aware of. So, I think it is just that they are just becoming better and better at what they do. Moreover, it is making it very difficult for us and when I say us, I just mean cybersecurity professionals to detect these kind of things from happening earlier. And I think they're finding out way is that we're preventing their attacks and they're [i.e., hackers] looking for more creative solutions and it's working.

Participant 8 elaborated that hackers are using low-level techniques. The low-level techniques are not silenced in many instances with gradual progress until the main goal is arrived at, stating, "They're using low-level techniques that aren't being alerted in most times and then laterally mov[ing] and elevating a little bit at a time to reach their ultimate target goal." Participant 1 talked about hackers using the same tools that InfoSec professionals use. Using the same tools makes detecting attacks difficult for InfoSec professionals, stating, "When they're using the same tools as your regular employees, it is difficult to detect that."

SQ1-2

Why do U.S. InfoSec professionals believe some cybersecurity data breaches are easier to detect? One theme that answered this question emerged: knowledge of hacker processes, expertise, and tools. Table 2 summarizes the number of participants and references of SQ1-2 themes.

Table 2. SQ1-2 Themes.

Theme	Frequency
Knowledge of Hacker	23
Processes	9
Expertise	10
Tools	4

Note. Why do U.S. InfoSec professionals believe some cybersecurity data breaches are easier to detect?

Theme 4: Knowledge of Hacker (Processes, Expertise, and Tools).

This theme was referenced by nine participants 23 times. The finding showed that professionals working together results in easier detection of data breaches. InfoSec professionals being knowledgeable and having the right tools results in easier detection of data breaches. Participant 2 explained that they have a good process for detecting hacking activities and are professionals who get things done. Having technicians who sort issues at different levels and work together makes detecting cybersecurity data breaches easier. The participant elaborated that everyone knows their role, making it easier to solve an incident when it arises, stating:

We have a pretty good process for detecting these things and getting people at … the technician level to talk. We only have a couple of people who have the authority to say, this is an incident we need to get all

 doi:10.20944/preprints202410.1609.v2

hands-on deck and pull everybody in and start working this and sometimes there's a fear that you don't want to cry wolf so you sit on something longer than you should.

Participant 3 emphasized that an open and honest team with each other makes it easier to solve incidents that arise. InfoSec professionals focusing on their strengths makes it easier to solve incidents that arise and helping each other improve their weaknesses without shaming each other can significantly improve the unity among employees, hence, solving challenges when they arise. The participant also emphasized the need for effective communication within a team, stating:

As far as team compositions go: an open and honest team that can communicate with one another…capable of shoring up each other's weaknesses. Let's say I'm fairly particularly strong at reverse engineering and malware triage. Whereas maybe one of my other leads is better about going through network packet analysis and stepping through how that works in the networking portion. Build a team that's communicative, dedicated, and passionate for the work and shores up each other's weaknesses without shaming one another for them is one way to develop a team that will be effective at handling any potential issues.

RQ2: What measures do U.S. InfoSec professionals take to reduce dwell times over 200 days?

SQ2-1

The first sub-question for RQ2 was: What tools have U.S. InfoSec professionals used to identify cybersecurity data breaches over 200 days? Two themes emerged that addressed this question. These were: (a) InfoSec tools: EDR, XDR, SIEM, automated tools, MSSP, Splunk, user behavior analytics, and Arctic wolf tools, and (b) Third-party threat intelligence and internal applications. The number of participants and references of SQ2-1 themes are summarized in Table 3.

Table 3. SQ2-1 Themes.

Theme	Frequency
Third-party threat intelligence subscriptions	16
InfoSec Tools: EDR, XDR, SIEM, automated tools, MSSP, Splunk, user behavior analytics, and Arctic Wolf tools	15

Note. What tools have U.S. InfoSec professionals used to identify cybersecurity data breaches over 200 days?

Theme 5: Third-Party Threat Intelligence and Internal Applications.

Ten participants contributed to this theme 16 times. The finding revealed that InfoSec professionals prefer using third-party threat intelligence to identify cybersecurity data breaches. InfoSec professionals design and develop internal applications with the specificities they use to identify cybersecurity data breaches. Participant 1 talked about how third-party threat intelligence is useful. Third-party threat intelligence provides InfoSec professionals with information when they are being targeted by hackers so that they can prepare themselves. Third-party threat intelligence also provides InfoSec professionals with the appropriate updates to make to ensure they are safe, stating:

Tactics, Techniques, Procedures (TTPs) that we could look for that they might have, or we could use it to find stuff in our environment faster. That I think would be very useful. The threat intelligence that we use…we also pay a company and they do curated threat intelligence based on our technology stack.

Participant 4 explained that they built an internal application to enhance confidence in the firm or company. Using third parties may not be adequate; hence, the need to have internal applications to boost confidence, stating:

We definitely have developed proprietary sort of homegrown, apps and the biggest motivation was just to have something built in-house even if you're using third parties it helps to have processes in-house. So, I think that's what's what the motivating factor was and then in terms of the effects it was great I mean I feel like we were able to see improvements and see benefits right away.

 doi:10.20944/preprints202410.1609.v2

Theme 6: InfoSec Tools.

All 10 participants contributed to this theme. The findings revealed that most InfoSec Professionals use the following InfoSec tools: EDR, XDR, SIEM, automated tools, MSSP, Splunk, user behavior analytics, and Arctic Wolf tools to identify cybersecurity data breaches over 200 days. Participant 3 mentioned they use EDR or SIEM tools. InfoSec professionals use EDR or SIEM tools to determine the activity being worked on and changes made. Participant 4 discussed how EDR, XDR, and SIEM tools have worked effectively. The tools are effective in understanding the impacts of the threats imposed. The tools are also effective in identifying the duration of the threats, stating:

> *One of the things that, has worked really well for us, is some of those response tools that I've mentioned, EDR, XDR, and SIEM tools. They do a great job of helping you understand impacts and what the exact well time was, and how long. The threat lasted how long before it kicked off, how long afterward there's a lot of monitoring. Capabilities are built into those as well. Participant 8 mentioned they use multiple InfoSec tools, including Defender EDR and Rapid 7 SIEM. The Rapid 7 SIEM tool acquires security and management alerts. Defender EDR and Rapid 7 pick up malware on servers or endpoints immediately isolate the endpoints and disable the primary users.*

Participant 8 stated, "We have multiple tools. It's got about 35 event sources that it's just conglomerating data from. And it's churning like churning through millions and millions of events a day."

SQ2-2

The second sub-question for RQ2 was: What methods have U.S. InfoSec professionals used to decrease dwell times over 200 days? Four themes emerged that answered this question. The themes were as follows: (a) teamwork and good management, (b) frequent audit logging and cybersecurity assessment, (c) integrated automation and documentation, and (d) cyber kill chain, MITRE adversarial tactics, techniques, and common knowledge (ATT&CK), and National Institute for Standards and Technology (NIST) cybersecurity frameworks. The number of participants and references for the SQ2-2 themes are summarized in Table 4.

Table 4. SQ2-2 Themes.

Theme	Frequency
Teamwork and good management	22
Integrated automation and documentation	18
Frequent audit logging and cybersecurity assessment	9
Cyber Kill Chain, MITRE ATT&CK, and NIST cybersecurity frameworks	7

Note. What methods have U.S. InfoSec professionals used to decrease dwell times over 200 days?

Theme 7: Teamwork and Good Management.

Data supporting this theme was drawn from 10 individual interviews. The finding indicated that collaboration among InfoSec professionals helps in detecting attacks. Input from management significantly determines the efforts made by InfoSec professionals to detect and counter-attacks by hackers. Participant 10 explained that working for a long time as a team helps solve incidents when they arise. Lack of hiring often means that there is no training for new employees on how to handle operations, stating:

> *When it comes to team composition, the most effective is a team that does not rotate out. If you could have a solid team that stays together for years…that'd be great because that way we don't have to keep training new people on how we do things and all it works.*

Participant 3 talked about the need for a strong team of InfoSec professionals familiar with handling InfoSec operations. It's easier to handle attacks when they arise because everyone is familiar with their role, stating: "Making sure I had a strong set of analysts capable and familiar with an

 doi:10.20944/preprints202410.1609.v2

environment would be my top priority first because with an analyst. Everything else falls under that." Participant 1 mentioned that identifying the strengths of each InfoSec professional greatly helps in being aware of whom to solve an incident when it arises. Documentation may not always be available; hence, there is a need to know where each member of the staff accurately fits. The participant emphasized the need for diversity among InfoSec professionals and being intelligent in various capacities, stating:

> *The best information you can have [is] to know the subject matter expert for the different business applications. Someone who knows the front end and also someone who can tell you what the logs mean. Because a lot of times, that's not documented very well. You have to have that to understand what happened and to put the pieces together. You definitely need analysts who are good at taking a lot of data and crunching it and pulling out the correlations [and] you need people who are good at communicating across business and technology.*

Theme 8: Integrated Automation and Documentation.

Data supporting the ninth theme was drawn from all 10 participants 18 times. The finding revealed that automation and all the systems running effectively significantly decrease dwell times over 200 days. Documentation of who and what measures to take when incidences occur helps decrease dwell times over 200 days. Participant 1 elaborated on the great documentation they have in the workplace, which shows that they are aware of the roles played by each InfoSec professional when incidences occur. The participant emphasized the need for having processes that detail incidents better, stating:

> *Once an incident starts. We've got great documentation on that. But as far as deciding when to call an incident or what constitutes an incident that's still basically left up to the couple of people who have that authority and they rely on people to bring them things … we also need to process what constitutes an incident better.*

Participant 9 mentioned using automation, such as written automation and third-party tools, that resulted in a playbook and hooking in various aspects. This increased the security budget and onboarding of many tools and personnel, stating:

> *The biggest need that arose from that is within the last three years we've had a massive increase in the security budget. So, we've onboarded a lot of tools and a lot of people. We went from a team of maybe 8 to 30.*

Participant 4 talked about effective processes that were put into place to measure shrinkage. The well-planned processes help in detecting attacks and the time of occurrence, stating:

> *It's really just being able to measure it throughout that process and understanding from the start of an attack to when it's detected to when it's completely taken care of …over the course of that time.*

Theme 9: Frequent Audit Logging and Cybersecurity Assessment.

Seven participants contributed to this theme nine times. The finding showed InfoSec professionals frequently conduct audit logging, activity changes and requests, and quality checks to ensure the systems possess good health status and detect attacks. InfoSec professionals often conduct cybersecurity assessments to search for and counter-attacks by hackers. Participant 6 elaborated on conducting audit logging, security audit logging, and event logging in their workplace. Adequate logging helps a company helps a company determine or find its core business, stating, "The biggest part is having enough logging in place." Participant 2 mentioned that one of their preventive measures is conducting weekly audits. Conducting regular audits helps ensure that suspicious attacks are not identified, stating: "We do like weekly audits, as sort of like a preventative measure… to make sure we don't see anything suspicious."

Participant 5 explained conducting weekly change requests to remove software vulnerabilities that could cause harm. Making regular change requests ensured that dwell time was reduced, stating:

 doi:10.20944/preprints202410.1609.v2

Making change requests was a weekly activity, and the change request in this case would be to remove the software to remove the vulnerability. I did not want to do it because it took too long…you had to wait until after hours. My philosophy there was to do the simplest thing…on a regular basis to make sure that everything was immediate.

Theme 10: Effective Frameworks.

Six participants contributed to this theme seven times. The finding indicated that InfoSec professionals use cyber kill chain, MITRE ATT&CK, and NIST Cyber Security frameworks to decrease dwell times over 200 days. Participant 3 mentioned that InfoSec professionals use the cyber kill chain framework to decrease dwell time. The cyber kill chain framework helps InfoSec professionals identify the start of an attack. It also helps in identifying the target of the attacks by hackers, stating:

Cyber kill chain to MITRE ATT&CK framework to the diamond model …have all played a part in influencing my opinion and my approach to dwell time. Some of them will dictate exactly the start to finish of this life cycle of an attack whereas others will enumerate the target of a specific adversary and what other sections they might be accessing.

Participant 6 explained that they use the NIST Cyber Security Framework to decrease dwell time, stating:

I'm using the NIST Cyber Security Framework (CSF), a lightweight framework for building a security program. And hypothetically, if you were to do those, all those objects are the 108 or so control objectives. You would hypothetically reduce dwell time.

Participant 10 talked about being great fans of the MITRE ATT&CK framework. MITRE ATT&CK framework has high-level attack and defense techniques. The high-level attack and defense techniques help in countering attack incidences when they occur, stating: "We follow many industry standards…like the MITRE ATT&CK framework…their attack and their defense framework …we follow closely."

4. Discussion

The findings of this study highlighted significant gaps in cybersecurity practices within U.S. organizations, particularly in managing dwell times that exceeded 200 days. The protection motivation theory provided a sound theoretical perspective for explaining these gaps as both the threat appraisal and coping appraisal mechanisms were either underemployed or not optimally congruent with cybersecurity threats in organizations. This misalignment was apparent in the long time it took to identify and contain cyber threats, putting more weight on reacting to threats instead of preventing them. Safi and Browne [19] observed that leaders and managers act based on the recency effect, addressing the latest incidences without a systematic plan, which results in disparities and poor cybersecurity.

The organizational and operational factors revealed the poor distribution of resources and the lack of sufficient human resources, which are essential in responding to and preventing cyber threats. This research provided evidence to underpin Cooke's [20] claim that having an effective, offense-based cybersecurity strategy is crucial but not commonly implemented among American companies. The insufficient recruitment of cybersecurity personnel and the nonproactive approach to resource management are major factors that lead to protracted breach time, which, in turn, increases threats and expenses, as discussed by Petrosyan [2]. The necessity for complex cybersecurity approaches and compliance with regulations like the GDPR, as well as comparing the slower rates of implementing them in the United States to the European Union, were also established by adopting the findings of Neto et al. [21].

The data provided by InfoSec professionals offered a qualitative understanding of the type of problems faced by employees in the field, which pointed to a chronically inadequate security culture present in organizations. In line with the argument presented by Grody [22], reducing the average dwell time is possible by establishing and enforcing effective cybersecurity protection structures. This

 doi:10.20944/preprints202410.1609.v2

research shows that most organizations in the United States are still slow in implementing these measures, leading to poor protection and untimely response to cyber threats. The discussion underlined the need to implement AI and machine learning as advanced analytical tools and technologies to improve threat detection. This aligns with Tsiodra et al. [23] through the introduced CENSOR framework.

The findings highlighted organizational culture as a key factor in defining cybersecurity policies and measures. A security-oriented culture integrated with state-of-the-art technologies and clear procedures should be in place to mitigate dwell times and improve overall security. The above-stated changes call for improvement in technology and culture, disrupting the current cybersecurity architecture and its awareness at the organizational level. This corresponds with the guidelines for creating a positive environment for security initiatives and early threat identification to lower the consequences of attacks as much as possible.

The implications of this study revealed the need for organizations to persevere with enhancing cybersecurity awareness and implementing explicit measures for cybersecurity enhancement to raise awareness and enforce consistent cybersecurity best practices across different sectors. The PMT framework used in this study showcases how evaluating risk and coping measures can impact how organizations handle cyber threats. By developing these aspects, firms established in the United States will be in a unique position to combat the challenges posed by the modern world of cyber threats and, as a consequence, decrease the number and impact of the breaches.

5. Conclusions

This study aimed to address the existing gap in the literature concerning the qualitative analysis of cybersecurity attacks in the U. S. that go unnoticed for more than 200 days [1,2]. It is important to understand this problem to design measures to prevent cyber risks. Based on the PMT, the researcher interviewed InfoSec professionals online and identified ten themes from their experiences. The study showed inadequate staff, capital, and leadership to combat cyber threats, resulting in extended data breaches among the firms. Poor working systems and delayed responses prolonged these breaches. Furthermore, hackers' activities changed approaches that, sometimes exceeded the skills of InfoSec professionals or were considered minor threats. Nevertheless, knowledge of hackers' techniques and tools and the ability to utilize third-party threat intelligence were essential to identifying breaches more efficiently.

The study revealed that InfoSec professionals use tools like EDR, XDR, SIEM, and others like MSSP, Splunk, user behavior analytics, and Arctic Wolf to detect cybersecurity breaches for over 200 days. The ability to work in teams, collaborate, manage, integrate automation, and document was essential in identifying and preventing cyber-attacks, thus lowering dwell times. The daily audit logging and cybersecurity assessments based on the cyber kill chain, MITRE ATT&CK, and NIST also helped to increase the response time. The results support the PMT theoretical framework by stressing the need for InfoSec professionals, managers, and organizations to use multifaceted approaches to avoid long cyber-attack dwell times. To enhance the security of event logs, organizations should hire professional staff, review the event logs of daily activities, implement centralized log management systems, and adhere to strict security measures. Also, the proper coordination of InfoSec employees and contractors and the exclusion of low-level techniques is vital.

Author Contributions: Abdul Rahman (Conceptualization [lead], Formal analysis [Lead], Methodology [lead], Supervision [lead], Writing – original draft [Lead], Writing – review & editing [lead])

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. IBM. Cost of a Data Breach Report 2023; IBM: Armonk, NY, USA, 2023. Available online: https://www.ibm.com/reports/data-breach (accessed on 13 September 2024).
2. Petrosyan, A. Cost of a Data Breach in the U.S. 2022. Statista, 2023. Available online: https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach (accessed on 13 September 2024).
3. Alam, S. Cybersecurity: Past, Present and Future. ArXiv Preprint ArXiv, 2022. Available online: https://doi.org/10.48550/arxiv.2207.01227 (accessed on 13 September 2024).
4. Eling, M.; McShane, M.; Nguyen, T. Cyber Risk Management: History and Future Research Directions. Risk Manag. Insur. Rev. 2021, 24, 93–125. https://doi.org/10.1111/rmir.12169.
5. International Telecommunications Union. Global Cybersecurity Index (GCI) 2018; ITU: Geneva, Switzerland, 2019. Available online: https://www.itu.int/dms_pub/itu-d/opb/str/D-STRGCI.01-2018-PDF-E.pdf (accessed on 13 September 2024).
6. Cho, H.; Lee, S.; Kim, N.; Kim, B.; Park, J. Method of Quantification of Cyber Threat Based on Indicator of Compromise. In Proceedings of the International Conference on Platform Technology and Service (PlatCon), Busan, Korea, 29–31 January 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 182–188. https://doi.org/10.1109/platcon.2018.8472733.
7. Rogers, R.W. A Protection Motivation Theory of Fear Appeals and Attitude Change. J. Psychol. 1975, 91, 93–114. https://doi.org/10.1080/00223980.1975.9915803.
8. Howell, C.J.; Maimon, D.; Perkins, R.C.; Burruss, G.W.; Ouellet, M.; Wu, Y. Risk Avoidance Behavior on Darknet Marketplaces. Crime Delinq. 2022, 70, 519–538. https://doi.org/10.1177/00111287221092713.
9. Kim, J.K.; Crimmins, E.M. Age Differences in the Relationship Between Threatening and Coping Mechanisms and Preventive Behaviors in the Time of COVID-19 in the United States: Protection Motivation Theory. Res. Psychother. Psychopathol. Process Outcome 2020, 23, 485. https://doi.org/10.4081/ripppo.2020.485.
10. Sulaiman, N.S.; Fauzi, M.A.; Hussain, S.; Wider, W. Cybersecurity Behavior Among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. Information 2022, 13, 413. https://doi.org/10.3390/info13090413.
11. De Kimpe, L.; Walrave, M.; Verdegem, P.; Ponnet, K. What We Think We Know About Cybersecurity: An Investigation of the Relationship Between Perceived Knowledge, Internet Trust, and Protection Motivation in a Cybercrime Context. Behav. Inf. Technol. 2022, 41, 1796–1808. https://doi.org/10.1080/0144929X.2021.1905066.
12. Lee, C.S.; Kim, D. Pathways to Cybersecurity Awareness and Protection Behaviors in South Korea. J. Comput. Inf. Syst. 2023, 63, 94–106. https://doi.org/10.1080/08874417.2022.2031347.
13. Patel, A.; Roy, S.; Baldi, S. Wide-Area Damping Control Resilience Towards Cyber-Attacks: A Dynamic Loop Approach. IEEE Trans. Smart Grid 2021, 12, 3438–3447. https://doi.org/10.1109/tsg.2021.3055222.
14. Liu, C.; Jiang, B.; Wang, X.; Yang, H.; Xie, S. Distributed Fault-Tolerant Consensus Tracking of Multi-Agent Systems Under Cyber-Attacks. IEEE/CAA J. Autom. Sin. 2022, 9, 1037–1048. https://doi.org/10.1109/JAS.2022.105419.
15. Qi, W.; Lv, C.; Zong, G.; Ahn, C.K. Sliding Mode Control for Fuzzy Networked Semi-Markov Switching Models Under Cyber Attacks. IEEE Trans. Circuits Syst. II Express Briefs 2021, 69, 5034–5038. https://doi.org/10.1109/TCSII.2021.3137196.
16. Izycki, E.; Colli, R. Protection of Critical Infrastructure in National Cybersecurity Strategies. In Proceedings of the European Conference on Cyber Warfare and Security, Coimbra, Portugal, 2019. Available online: https://www.researchgate.net/publication/335760609 (accessed on 13 September 2024).
17. Gatzert, N.; Schubert, M. Cyber Risk Management in the U.S. Banking and Insurance Industry: A Textual and Empirical Analysis of Determinants and Value. J. Risk Insur. 2022, 89, 725–763. https://doi.org/10.1111/jori.12381.
18. Braun, V.; Clarke, V. Reflecting on Reflexive Thematic Analysis. Qual. Res. Sport Exerc. Health 2019, 11, 589–597. https://doi.org/10.1080/2159676x.2019.1628806.
19. Safi, R.; Browne, G.J. Detecting Cybersecurity Threats: The Role of the Recency and Risk Compensating Effects. Inf. Syst. Front. 2023, 25, 1277–1292. https://doi.org/10.1007/s10796-022-10274-5.
20. Cooke, D.M. Cybersecurity: Building a Better Defense with a Great Offense; Cybersecurity Journal: New York, NY, USA, 2021. https://doi.org/10.25776/g5cq-2423.
21. Neto, N.N.; Madnick, S.; Paula, A.M.G.D.; Borges, N.M. Developing a Global Data Breach Database and the Challenges Encountered. J. Data Inf. Qual. 2021, 13, 1–33. https://doi.org/10.1145/3439873.
22. Grody, A.D. Addressing Cyber Risk in Financial Institutions and in the Financial System. J. Risk Manag. Financ. Inst. 2020, 13, 155–162. Available online: https://www.ingentaconnect.com/content/hsp/jrmfi/2020/00000013/00000002/art00007 (accessed on 13 September 2024).

 doi:10.20944/preprints202410.1609.v2

23. Tsiodra, M.; Panda, S.; Chronopoulos, M.; Panaousis, E. Cyber Risk Assessment and Optimization: A Small Business Case Study. IEEE Access 2023, 11, 44467–44481. https://doi.org/10.1109/access.2023.3272670.