ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION

Paper ID #44802

Unveiling Cyber Threats: A Comprehensive Analysis of Connecticut Data Breaches

Dr. Robin Chataut, Quinnipiac University

Robin Chataut is an assistant professor of Cybersecurity and Computer Science at the School of Computing and Engineering at Quinnipiac University. He earned his Ph.D. in Computer Science and Computer Engineering from the University of North Texas.

His research interests lie in the areas of network security, cybersecurity, AI, ML, and next-generation networks. His significant contributions to the field are evidenced by his design, implementation, and optimization of complex algorithms and systems architectures. He has authored several research articles and has secured multiple research grants, underlining his commitment to advancing cybersecurity and computer science.

Beyond his research and academic commitments, he remains an active participant in the academic community. As an IEEE Senior Member, he serves in multiple international scientific journals and conferences, contributing significantly to the advancement of his fields of expertise.

YUSUF USMAN, Quinnipiac University

Yusuf is a rising cybersecurity professional pursuing an MS in Cybersecurity at Quinnipiac University. His research centers on the innovative applications of machine learning (ML) and artificial intelligence (AI) for advanced threat detection and mitigation, focusing on phishing attacks, automated defense mechanisms, and malware identification. Yusuf's unique perspective on AI-driven security is further informed by his research on autonomous vehicles.

Prior to his graduate studies, Yusuf gained valuable experience as a Graduate Research Assistant at Quinnipiac University, an Information Security Analyst at the National Assembly of Nigeria, and an IT Support Specialist at LamidoTex NIG LTD. These diverse roles solidified his foundation in networking, cloud network design, and operating system security.

Yusuf's commitment to continuous learning, his passion for exploration through travel, and his interest in the intersection of technology and business strategy make him a well-rounded cybersecurity expert.

Dr. Frederick Scholl, Quinnipiac University

Unveiling Cyber Threats: A Comprehensive Analysis of Connecticut Data Breaches

Abstract

Data breaches continue to be a pervasive threat in the digital landscape, impacting both businesses and individuals. This study conducts a thorough empirical analysis of Connecticut's data breaches in 2022, analyzing the data provided by The Office of the Attorney General, Connecticut. Our methodology involves a detailed examination of the breach records, focusing on the types of companies affected, methodologies of the attacks, and specific information compromised. We applied statistical analysis techniques to uncover patterns and trends within the data. Our investigation reveals a significant vulnerability in smaller businesses, with the healthcare and financial sectors facing the most severe challenges. Ransomware and phishing emerge as the most frequent attack methods, often leading to the compromise of sensitive personal data. Additionally, we found that smaller businesses were more frequently targeted and took longer to detect and report breaches, exacerbating the impact. In response to these findings, the study underscores the urgent need for enhanced cybersecurity measures, particularly for small businesses. It provides a detailed understanding of the current cyber threat landscape and serves as an essential resource for businesses, particularly smaller ones, to comprehend and strengthen their defenses against these evolving threats. The recommendations offered are designed to assist businesses in bolstering their cybersecurity measures, thus safeguarding against the complexities brought about by an increasingly interconnected digital world. The findings are especially pertinent in growing interconnectivity and information sharing, highlighting the necessity for businesses and policymakers to adapt and reinforce their cybersecurity frameworks to effectively counter these sophisticated threats. The study's comprehensive analysis and actionable recommendations offer a roadmap for enhancing digital security in an increasingly interconnected world.

Introduction

In the era of rapid digital transformation, the escalation of cyber threats has become a parallel and perilous reality. The advent of widespread digitalization, while facilitating unprecedented connectivity and efficiency, has also opened the floodgates to numerous cybersecurity challenges. As businesses, government entities, and individuals increasingly rely on digital platforms for their operations, the stakes in protecting sensitive data have soared. This paradigm shift has ushered in a new age where data breaches are not just occasional disruptions but regular occurrences with potentially devastating consequences.

Connecticut, mirroring the global trend, has witnessed a significant uptick in cyber incidents, particularly data breaches. These incidents are not merely isolated events; they reflect a broader trend of escalating cyber threats that target the very core of personal and organizational privacy and integrity. The state's diverse economic landscape, encompassing healthcare, finance, insurance, and manufacturing sectors, presents a varied and rich target for cyber adversaries. This variety amplifies the potential impact of data breaches and underscores the necessity for a comprehensive understanding of these incidents. Analyzing data breaches in Connecticut is not

just about quantifying incidents; it is about dissecting the anatomy of these breaches to unveil patterns, identify vulnerabilities, and understand the evolving tactics of cyber adversaries.

This study aims to provide an in-depth analysis of data breaches in Connecticut for the year 2022, focusing on identifying the types of businesses most affected, the nature of the compromised data, and the methods employed by cyber attackers. By examining records of data breaches, this study endeavors to offer a granular view of the current state of cybersecurity in Connecticut. Furthermore, the study seeks to extrapolate these findings to understand future trends in cyber threats. This forward-looking perspective is crucial in equipping businesses, policymakers, and cybersecurity professionals with the insights needed to fortify defenses against the cyber threats of tomorrow.

Literature Review

The landscape of cybersecurity is rapidly evolving, as evidenced by the increasing prevalence of cyberattacks on businesses of all sizes, particularly small businesses. The IBM Security report highlights a worrying trend, with the global average data breach cost soaring to $4.45 million, a clear indicator of the financial strain these incidents place on organizations. This increase underscores the complexity of breach investigations and the paramount importance of AI and automation in curtailing breach lifecycle costs. Despite the apparent advantages of these technologies in enhancing detection and response speeds, the reluctance among organizations to bolster their security budgets, opting instead to offset costs to consumers, reveals a significant gap in cybersecurity readiness and consumer protection [1].

IdentityIQ's report underscores the sheer volume and variety of cyberattacks in 2023, noting a 14% increase in data breaches over the previous record, affecting over 66 million individuals [2]. The top ten data breaches over the last twelve months further illustrate the diverse nature of cyber threats, ranging from massive data leaks to targeted attacks on specific organizations, as shown in Table 1. These incidents have collectively affected billions of accounts and highlighted vulnerabilities across various sectors, necessitating the implementation of more robust security measures such as multifactor authentication [3].

Table 1: Top ten data breaches over the last 12 months [3]

Rank	Name of the Breach/Attack
1	**Russian Web Hosting Data Leak** (February 2024**)** Hundreds of senior executive accounts were compromised through phishing and cloud account takeovers.
2	**Microsoft Azure Data Breach (**February 2024**)** Hundreds of senior executives accounts were compromised through phishing and cloud account takeovers.
3	**Bank of America Data Breach** (February 2024) Cyberattack on Infosys McCamish Systems compromised names, SSNs, and account details.
4	**Cyber Attack on Russian Center for Space Hydrometeorology** (January 2024) 2 petabytes of data deleted, impacting entities like the Ministry of Defense

5	**Mother of All Breaches** (January 2024) Massive data leaks of over 26 billion records from various platforms emphasize global cybersecurity concerns.
6	**Trello Data Breach** (January 2024) Security breach affected over 15 million users, compromising email addresses and usernames.
7	**Indian Telecom Data Breach (**January 2024) Data of 750 million users compromised and sold on the dark web, highlighting security risks.
8	**Indian Council of Medical Research Data Breach (**October 2023) Identification and passport details of 81.5 million citizens exposed, raising data security concerns.
9	**23andMe Data Leak** (October 2023) Unauthorized access affected 6.9 million user accounts, highlighting the risks of sharing genetic information online.
10	**MOVEit Data Breach** (May 2023) Attack targeted over 62 million individuals and 2,000 organizations, costing an estimated $10 billion.

Methodology

The dataset central to this study comprises data breaches that occurred within Connecticut in the year 2022. This dataset was meticulously collected and compiled by the Connecticut state government, underscoring the state's commitment to understanding and mitigating cyber threats. Each record in the dataset represents a unique data breach incident, detailing the nature and extent of the breach, the type of business affected, the method of attack, and the kind of data compromised. To ensure the integrity and relevance of our analysis, stringent criteria were applied to include records in this dataset. The key criteria included:

- Geographical Relevance: Only incidents that directly impacted businesses, organizations, or individuals within the state of Connecticut were included.
- Time Frame: The dataset exclusively encompasses breaches that occurred within the calendar year of 2022, providing a focused snapshot of the cyber threat landscape within that period.
- Verification and Completeness: Each record had to be verified for accuracy and completeness, with sufficient details on the nature and impact of the breach.

To analyze this extensive dataset, we employed a combination of statistical tools and software, aiming to uncover patterns, trends, and insights from the data. The methodology was designed to address the multifaceted nature of data breaches and to provide a nuanced understanding of the cyber threat landscape in Connecticut. We Analyzed the metrics shown in Figure 1.

Dataset Analysis and Discussion

The analysis of the data breach records from Connecticut in 2022 yielded several critical insights into the nature, targets, and implications of cyber-attacks in the state. These findings are

significant in understanding the past year's cyber threat landscape and shaping future cybersecurity strategies and policies.

Figure 1: Metrics Analyzed

a. Size of Businesses Attacked

One of the most striking findings was the disproportionate impact of data breaches on small businesses. Based on the definition provided by the Connecticut Business & Industry Association (CBIA), a small business in Connecticut is defined as a firm with fewer than 500 employees. Given this definition, Figure 1 indicates that small businesses, particularly those with 1-99 and 100-999 employees, are attacked more often than larger businesses with 1,000 employees or more. This data suggests that smaller businesses are more frequently targeted. This finding aligns with the general vulnerability of smaller businesses, which may need more resources to invest in protective measures against various types of attacks, be they physical, cyber, or otherwise. It is essential for small businesses to be aware of these risks and to seek out resources and support, such as those offered by the various programs and initiatives mentioned in the text, which can help to mitigate them.

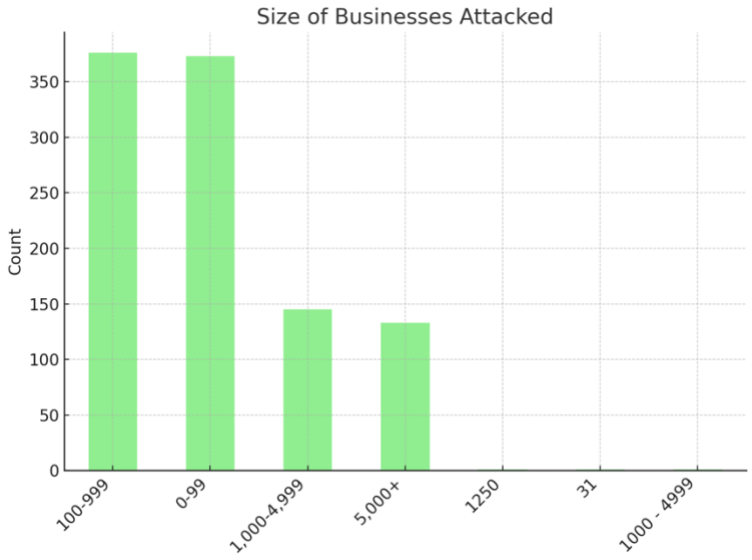

Figure 2: Distribution of attacks based on the size of the businesses, highlighting which business size categories were targeted most frequently.

b. Most Common Type of Cyberattack

We counted the occurrences of each type of breach in the dataset. These results indicate that Ransomware and Phishing/Email Compromise are the most common types of breaches, followed by External Systems and Other Breaches. The least common are Loss or Theft of a Device and Inadvertent Disclosure. The analysis of the frequency of different types of breaches:

- TRansomware (Systems Breach – Ransomware): 571 occurrences
- TBPhishingEmail (Systems Breach – Phishing/Email Compromise): 339 occurrences
- TBExtSysBreach (External Systems Breach – Other): 251 occurrences
- TBOther (Other types of Breach): 142 occurrences
- TBCredComp (Systems Breach – Credential Compromise): 75 occurrences
- TBInsiderMisuse (Employee Misuse or Insider Wrongdoing): 72 occurrences
- TBInadverDisclosure (Inadvertent Disclosure, e.g., misdirected email): 68 occurrences
- TBLossTheftDev (Loss or Theft of Device, Documentation, or Media): 15 occurrences

The high occurrence of ransomware attacks reflects a global trend where cybercriminals exploit organizational vulnerabilities for financial gain. Phishing/email compromises highlight the ongoing challenge of human factors in cybersecurity. The relatively lower frequency of incidents like loss or theft of devices and inadvertent disclosures suggests some success in physical and operational security measures. However, the diverse nature of breaches, including external system breaches and credential compromise, indicates a complex threat landscape. This necessitates a multifaceted cybersecurity approach, incorporating robust technical defenses and enhanced human factor training. The results call for targeted strategies to address the most prevalent threats while not neglecting the less common but potentially impactful types of breaches.

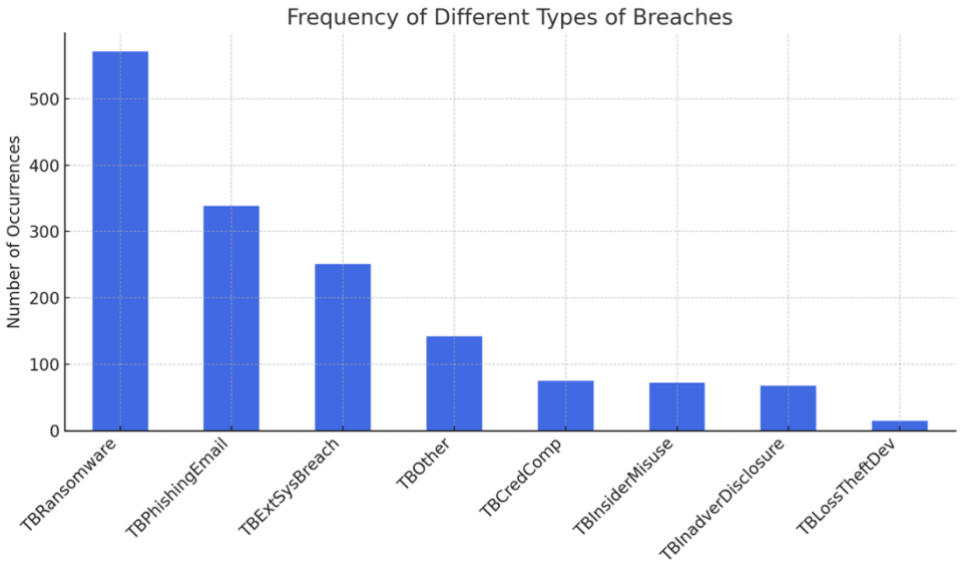

Figure 3: Most Common Type of Cyberattack

c. Type of Information Compromised

The types of information compromised in these breaches were predominantly personal data, including Social Security Numbers, medical information, and driver's license numbers. The high frequency of these data types, found in over 70% of the breaches, points to a focused strategy by attackers to target high-value personal information. This trend raises significant concerns about identity theft and financial fraud, illustrating the far-reaching consequences of these breaches. These results indicate that Social Security Numbers are the most frequently compromised type of information in data breaches, followed by medical information and driver's license numbers. This reflects the high value of such information for identity theft and fraud. A detailed analysis of the specific types of information involved in breaches.

- Social Security Number (PIBSSNData): 1,139 occurrences
- Medical Information (PIBMedicInfo): 511 occurrences
- Driver's License Number/Non-Driver ID (PIBDrvrLic): 480 occurrences
- Financial Account Number & Security Code/Password (PIBFinNoSecCodPas): 435 occurrences
- Health Insurance Information (PIBHealthIns): 390 occurrences
- Other Information (PIBOther): 327 occurrences
- Credit/Debit Card Number (PIBPaymentCardInfo): 212 occurrences
- Passport Number (PassportNo): 149 occurrences
- Username/E-mail Address & Password (PIBUserNamePass): 139 occurrences
- Individual Taxpayer Identification Number (ITIN) (PIBITIN): 81 occurrences
- Biometric Information (PIBBioInfo): 11 occurrences
- Identity Protection Personal Identification Number (IP PIN) (PIBIPpin): 7 occurrences

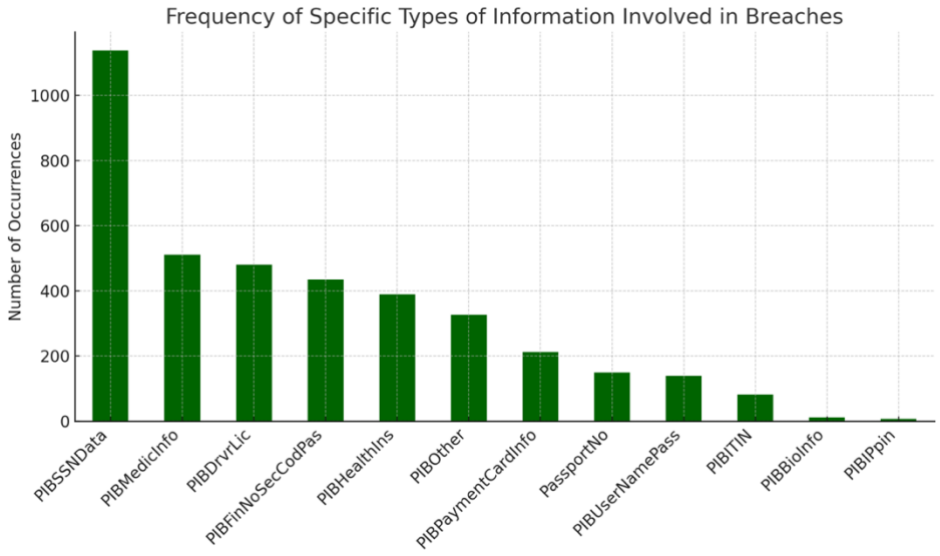

Figure 4: Type of Information Compromised during the Cyberattack

d. Types of Businesses Attacked

The analysis of the types of businesses attacked reveals a significant trend, particularly in the healthcare and finance sectors. The bar chart in the dataset highlights that categories like "Other," "Healthcare - Other," and "Healthcare - Hospital" are prominently represented. This indicates a focused targeting by cyber attackers in these sectors. With its wealth of sensitive personal and medical information, the healthcare sector presents a high-value target. Similarly, with its vast amounts of financial data, the finance sector is also highly attractive to cybercriminals. These trends emphasize the critical need for enhanced cybersecurity measures in these industries, especially considering their vital role in personal and economic well-being.

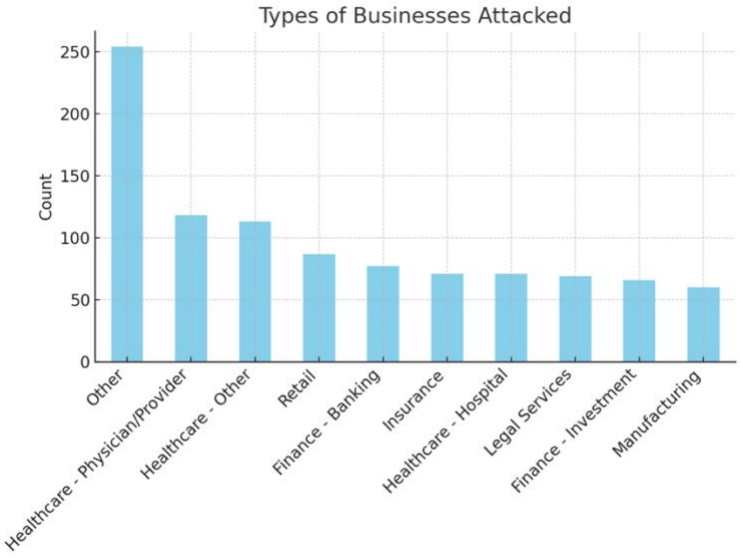

Figure 5: Types of Businesses Attacked

e. Average Number of Residents Affected

On average, approximately 416.41 residents were affected per incident. This statistic provides valuable insight into the scale of impact these breaches have on individuals. It highlights the extensive reach of each breach, not just as an abstract cybersecurity issue but as a real-world problem with tangible effects on a substantial number of people. While seemingly modest, this average figure underscores the cumulative effect of data breaches on the larger population and emphasizes the necessity for robust data protection measures to safeguard residents' sensitive information.

f. Average Time Taken to Report the Breach

The average time of 104 days to report a data breach, as found in the Connecticut dataset, is critical in understanding the response dynamics to cyber incidents. This duration, spanning over three months, signals a significant delay in breach detection or reporting. Such a lag not only exacerbates the damage caused by the breach but also raises concerns about compliance with legal and regulatory frameworks that often mandate timely breach notifications. This delay in

reporting could stem from various factors, including the time taken to detect the breach, confirm its scope, and undertake the necessary internal and legal reviews before public disclosure. It underscores the need for improved detection capabilities and faster response protocols in cybersecurity practices.

g. Seasonal Trends in Attacks:

The bar chart shows the number of attacks per month. This visualization can help identify if certain months have a higher frequency of attacks, indicating potential seasonal trends.

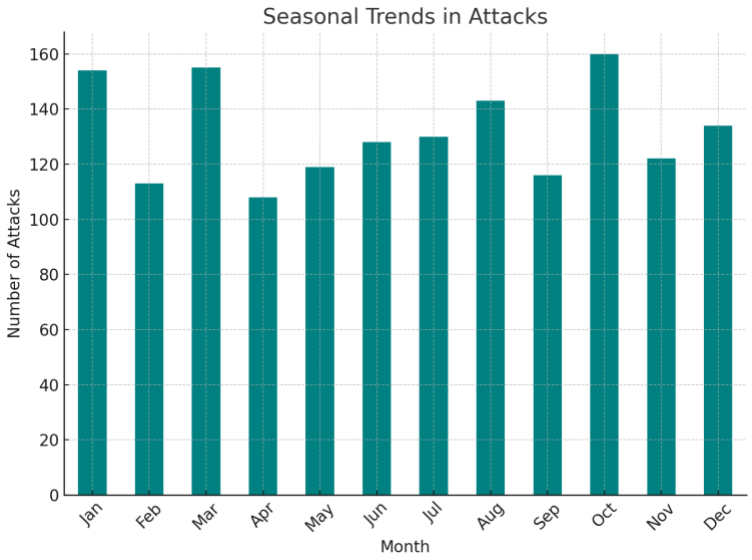

Figure 6: Seasonal Trends in Cyberattacks

g. Impact Analysis

Assess if the number of residents affected varies significantly across different businesses or industries. This involves comparing the average number of residents affected in each industry. There is a notable variation in the average number of residents affected by data breaches across different industries. The finance sector, specifically in the realms of real estate and accounting, shows a substantially higher average impact, with a significant number of residents affected. Healthcare providers also rank high on the list, likely due to the sensitivity and volume of personal data they handle. In contrast, industries like banking, education, and investment show a markedly lower average number of residents affected. This variation suggests that specific industries, due to the nature of the data they process and store, are more likely targets for breaches that affect larger populations.

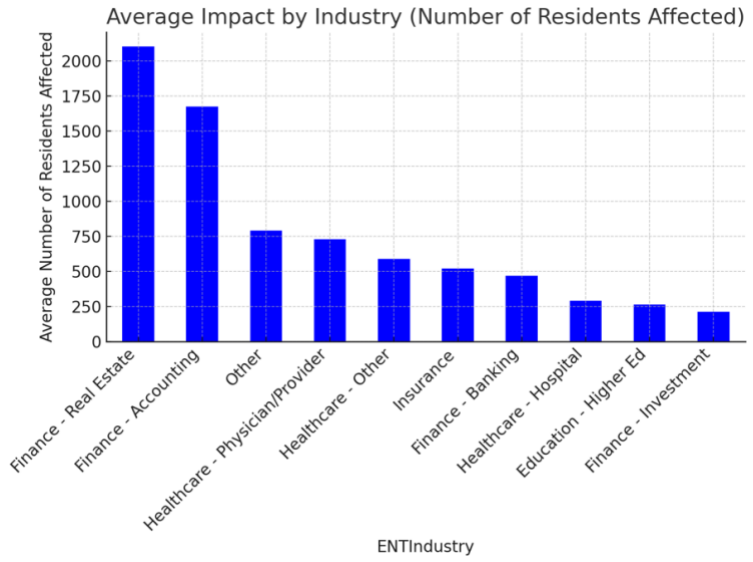

Figure 7: Average Impact by Industry (Number of Resident Affected)

h. Duration of Breaches

Analyze the duration of breaches by calculating the difference between 'BreachStartDate' and 'BreachEndDate.' We will then see if certain types of breaches, or breaches in certain industries, last longer than others. The analysis indicates that the average duration of breaches varies significantly across different industries. The agriculture sector has the longest breach duration, which suggests a lower capability or priority for breach resolution in this field. In contrast, industries such as education K-12, professional organizations, and long-term residential care have shorter breach durations, indicating better response mechanisms or smaller breach scopes. The data could imply that industries with longer breach durations may lack the necessary resources or protocols to quickly address and resolve cybersecurity incidents. This highlights the need for industry-specific cybersecurity measures and response plans.

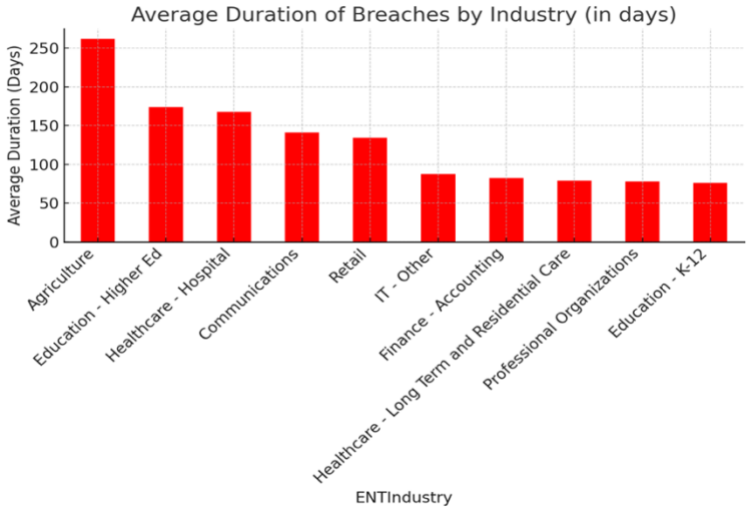

Figure 8: Average duration of breaches by industry

Impact on Small Business and Future Projection

Cyberattacks can have a profound impact on small businesses. Financially, they often face significant costs from data recovery, system repairs, and potential legal liabilities. There is also the loss of business and productivity during the downtime. Reputationally, a breach can damage a business's credibility with customers, leading to a loss of trust and future sales. Smaller businesses, with limited resources and less robust security infrastructures, are particularly vulnerable to these attacks, which can sometimes lead to business closure. The cumulative effect of these impacts underscores the critical need for effective cybersecurity measures in small businesses.

Small businesses must adopt a comprehensive approach to cybersecurity. This begins with thorough employee training on the importance of cybersecurity, how to identify suspicious emails and links, and the protocol for reporting potential threats. Strong passwords are crucial; businesses should mandate complex passwords that are changed regularly and consider using a password manager to maintain password integrity. It is also essential to keep all software and systems updated with the latest security patches to defend against known vulnerabilities. Frequent data backups are necessary to ensure that information can be recovered in the event of a cyber-attack. These backups should be stored securely, preferably offsite or on a secure cloud service. Wi-Fi networks must be encrypted, hidden, and password-protected to prevent unauthorized access.

Effective antivirus, anti-malware software, and a robust firewall must be installed and updated regularly to fend off threats. Businesses should only grant access to sensitive data to employees who need it and constantly monitor who has what level of access.
Implementing multifactor authentication (MFA) provides an additional security layer, making it harder for unauthorized users to gain access even if they have a password. Payment processing systems must be secure and PCI-compliant to protect financial data. Additionally, having a clear incident response plan in place is crucial. This plan should outline the steps to take in the event of a data breach, including how to contain the breach, assess the damage, notify affected parties, and prevent future incidents. This proactive planning can significantly reduce the damage a cyber incident may cause and ensure business continuity.

Looking ahead, the way we use technology is going to change, and this will affect how safe we are online. More devices connecting to the internet and faster internet speeds will mean more chances for hackers to try and steal information. The proliferation of Internet of Things (IoT) devices, the expansion of 5G networks, and advancements in artificial intelligence (AI) will likely create a broader attack surface for cybercriminals. The integration of these technologies into the fabric of daily operations will require a reimagining of cybersecurity strategies. We anticipate that cybersecurity will evolve from a defensive posture to an anticipatory, AI-driven approach that detects threats and predicts and neutralizes them preemptively. The cybersecurity expertise in any organization will need to become as fundamental as operational expertise, a non-negotiable pillar in the architecture of any digital enterprise. As technology continues to advance, the arms race between cyber defenses and cyber threats is expected to intensify, with the sophistication of security measures increasing to match the complexity of the emerging threats.

Conclusion

Our study of Connecticut's data breaches has shown us that there are many ways that online safety can be at risk. The analysis revealed a high frequency of ransomware and phishing incidents that prey on the personal information of individuals, highlighting the need for more formidable cybersecurity defenses. Particularly alarming is the focused targeting of healthcare and financial institutions, industries that deal with the most sensitive data, necessitating an urgent call for industry-specific cybersecurity measures. Moreover, the impact and duration of breaches are not uniform across sectors, calling for a nuanced approach to cybersecurity that is tailored to the unique needs of each industry. The study also brings to light the less frequent but equally concerning incidents of insider wrongdoing, emphasizing the importance of robust internal controls and vigilant employee training. The reality that organizations of all sizes are susceptible to attacks is a stark reminder of the universal need for improved cybersecurity protocols. In response to these findings, it is imperative for businesses and policymakers to take decisive action. Enhanced cybersecurity practices are no longer optional but necessary to safeguard against sophisticated cyber threats. Special attention to data protection is paramount, especially for personal and sensitive information. Security strategies must be adaptable and proactive, accounting for the dynamic nature of cyber threats that fluctuate with seasons and differ across regions. For industries at the epicenter of these attacks, there is a critical need to forge industry-specific cybersecurity protocols and emergency response plans. Internal security measures must be reinforced to mitigate threats from within organizations. This comprehensive analysis serves as a clarion call for an elevated, proactive stance on cybersecurity, emphasizing that vigilance and preparedness are the cornerstones of digital resilience in the modern era.

References

[1] "IBM Report: Cost of Data Breaches Soars to All-Time High During Pandemic," in *IEEE Innovation at Work*.

[2] Identity Theft Resource Center, "2023 Data Breach Report," [Online]. Available: https://www.idtheftcenter.org/publication/2023-data-breach-report/. [Accessed: 29-Feb-2024].

[3] "Biggest Data Breaches and Cyber Hacks of 2023 And 2024," *Techopedia*. [Online]. Available: https://www.techopedia.com/biggest-data-breaches-and-cyber-hacks. [Accessed: 29-Feb-2024].