

# Categorizing Cyberspace Insider Threat Activity

By

Marcus L. Green, State University of New York, Brockport

Cyber-attacks continue to impede businesses from every industry (Aslan et al., 2023). Data shows these attacks continue to occur and are increasing at an incredible, unfortunate pace (AL-Hawamleh, 2023). One of the latest attacks involved the telecommunication giant ATT. The data breach is estimated to have affected over 7 million current and 65.4 million former customers (Grantham-Philips, 2024). Another recent data breach involving Dropbox, LinkedIn, and Twitter reportedly involved an estimated 26 billion records (Winder, 2024). Company employees, known as insider threats, are major contributors to some of these attacks (Cram et al., 2024). Currently, within the cybersecurity industry, cyber insider threat incidents are labeled

as either incidents or non-malicious incidents (Burns et al., 2023). What is explicitly lacking is a comprehensive classification of human factor drivers, which pairs employee intentions with cognizant level. This qualitative study aimed to better understand individual insider

threat drivers and classifications of these drivers. Data was collected by interfacing with actual cybersecurity subject matter experts with years of experience dealing with insider threat incidents. The grounded theory methodology approach (Strauss & Corbin, 1994) was used to build a sensible classification model. The model revealed relational constructs between

human factor drivers and solutions. More importantly, the data uncovered differentiations of employee insider threat activities. Previous models (Gretitzer et al., 2014; Gretitzer & Frincke, 2010) provided a linkage of employee unintentional insider threats in the context of social engineering attacks but lacked the actual relationship between employee intentions and cognizant levels. Our model takes a novel ap-

proach by categorizing activities based on motivation and cognization levels. Further, these activities were categorized to assist organizations in better understanding the why behind the insider threat attacks.

**This qualitative research provides insights to help executives, managers, and information security professionals better understand insider threat activities by providing a sensible classification system. Using interview data from cybersecurity subject matter experts, a novel construct was developed that demystifies employee infraction intentions by introducing categorizations of unwitting, witting, un-malicious, and malicious.**

**Keywords:** Information Security, Cybersecurity, Insider Threats, Cyberspace, Information Systems, Human Factors

## Methodology

Qualitative research was conducted for this study through structured interviews. This type of research was chosen because previous researchers identified this to be a successful method in collecting data within all industries (Horton et al., 2004), but more specifically within the cybersecurity industry (Khan et al., 2022). Previous research has also shown a severe lack of qualitative data collection methods existing within the same cybersecurity industry (Jeong et al., 2019). This researcher believed the best way to gather data was through interfacing with actual information security and information technology professionals. Creswell's frameworks were extensively reviewed and chosen to be the best construct for conducting quality interviews during this process (Creswell & Poth, 2016). Our qualitative method would enable data collection from subject matter expert experiences in dealing with insider threat attacks, activities, and motivations. Interviews were conducted from 2020 to 2021. The interview schedule had to be adjusted multiple times due to the global COVID-19 pandemic occurring during that time.

Participants were selected from three industries: government, healthcare, and information security. The government was chosen because of recent attacks towards them and because their sector normally drives policy. Healthcare was selected due to the continual increase in ransomware attacks. The information security industry was chosen because of their overall expertise on the subject. One major constraint that limited the number of participants revolved around non-disclosure agreements that information security professionals are required to sign prior to beginning employment at most companies.

Prior to subject selection, a set of criteria was established. These standards ensured subjects had a good blend of experience, knowledge, and formal education. Every participant was screened to ensure they possessed at least five years of industry experience, held an industry information security certification, and had been awarded at least a master's degree; no other participant biases were used during the screening process. A summary of the participants is presented in Table 1. Interview scripts were developed to keep the sessions under 45 minutes. The scripts were slightly refined after feedback from every three to four sessions. Interviews were conducted virtually via Microsoft Teams and recorded using a digital recorder.

The coding process (Saldaña, 2021) used logical steps from data to themes and, finally, factors. Two coding cycles were utilized. The first coding iteration consisted of memoing and exploratory, in vivo, procedural, and holistic coding. This was followed by a second cycle of pattern, focused, axial, and theoretical coding. Every interview was painstakingly coded multiple times to ensure accuracy. Data was then refined and scrutinized to make better sense of relationships and groupings. Categorizations of these groupings were then developed, finally followed by themes. This researcher's information security expertise and experience drove the data coding, categorizations, and thematic development.

## Findings

Multiple themes were identified when analyzing the data, three of which were dominant. These themes pointed to the individual employees committing insider threat infractions. The first theme was related to employees who committed infractions without knowledge. The second theme concerns employees committing actions with knowledge but without malicious intent. The third and final theme focused on the employee who knowingly committed the action and had nefarious intentions. Overall, 125 codes were identified, with the interviewees referencing these codes a total of 889 times throughout the interviews. Figure 1 details data code distributions from the research.

- **Theme 1 Category: Unwitting-Unmalicious (UW-UM) Infractions:** The first major theme the codes pointed to was employees unwittingly committing infractions without knowing they were committing the infraction. The incidents

associated were all unmalicious. Employees committing these infractions had received proper training or were novices with their assigned technologies. The specific thematic title assigned was: "*Employees lacking foundational technological knowledge unwittingly commit cyber contraventions.*" This thematic area contained 33 codes and was identified throughout the interviews 138 times. The dominant human factor was awareness. All codes within this theme were categorized as being Unwitting-Unmalicious (UW-UM).

- **Theme 2 Category: Unwitting-Malicious (UW-M) Infractions:** A second theme emerged during the process. Only one code fell into this category. However, a code was identified when an interviewee posited that employees who did not know they were committing an infraction could not have malicious intent. This had to be coded because the interviewee voiced their belief on the subject.

**Table 1. Participant Summary by Industry, Occupation, Education Level, Experience, and Certifications**

Number of Participants	Industries	Occupations	Formal Education Level	Experience (years)	Certifications
15	Cybersecurity - 6 Government - 5 Healthcare - 4	Cybersecurity Consultant - 5 Cybersecurity Exercise Designer - 2 Chief Information Security Officer - 2 Cybersecurity Auditor - 2 Cybersecurity Branch Manager - 1 Senior Director of Security - 1 Cybersecurity CEO - 1 Chief Technology Officer - 1	Doctorate – 3 Doctoral Student - 1 Master’s - 7 Bachelor’s - 3	12–30 years	CISSP - 12 CISA - 1 CHCIO - 1 Security Plus - 1

- Theme 3 Category: Witting-Unmalicious (W-UM) Infractions:** A third theme began to emerge during the coding process. This theme related to employees who wittingly commit infractions but with unmalicious intent. Employees within this category knew right from wrong but committed the infraction because they wanted to complete their assigned tasks. The theme *Cyber infractions are sometimes committed with a belief that harm will not come to others*, had two dominant human factors: caring and devotion. There were 50 codes in this group; they appeared 389 times throughout the interviews. The third theme was identified as employees committing Witting-Unmalicious (W-UM) infractions.
- Theme 4 Category: Witting-Malicious (W-M) Infractions:** The final theme involved infractions related to employees who knowingly violated company policy and meant to harm the company. The name assigned for this theme was *Selfishness becomes the dominant behavioral factor when employees commit malicious cybercrimes*. Employees in this area were cognizant of the fact that they were committing the infraction and had intent to do harm. Coding grouped 42 codes into the category. Codes in this group were referenced 362 times by the interviewees. Infractions within this code group were classified as Witting-Malicious (W-M).

### Limitations

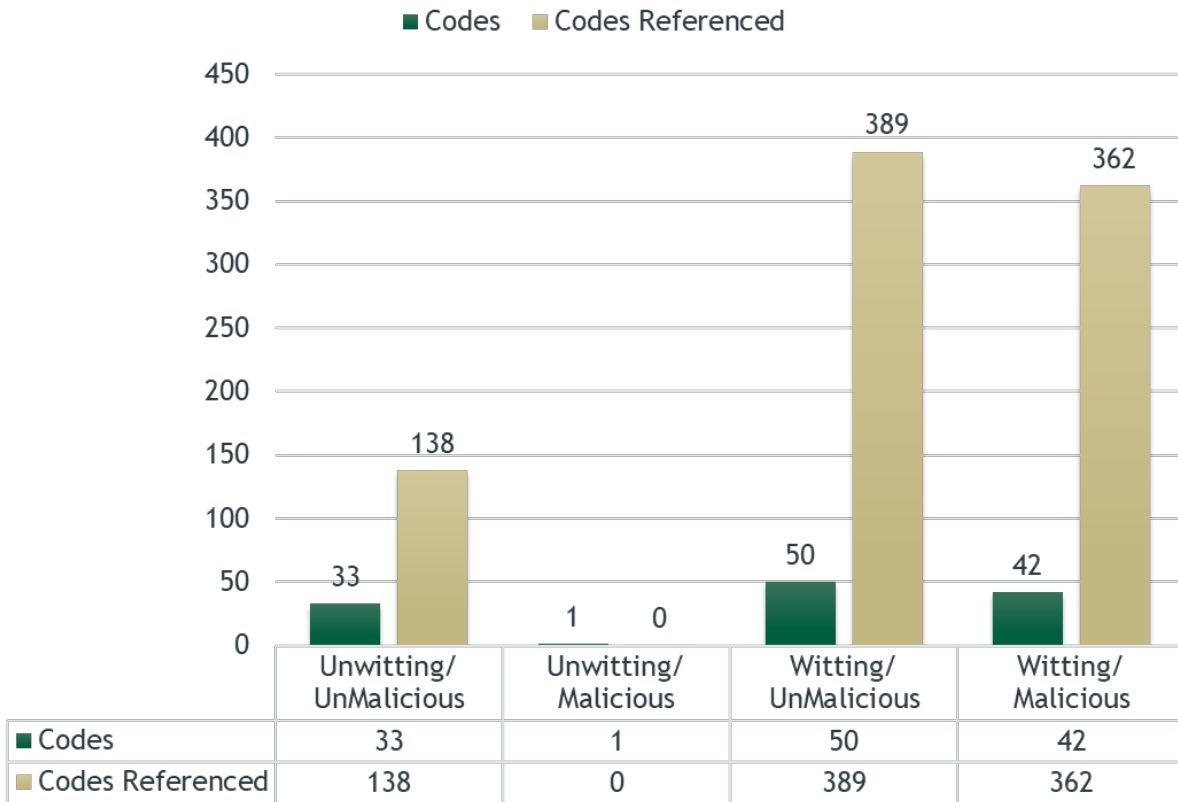
Some limitations were apparent during this study. One limitation was the lack of access to insider threat actors, mainly due to the study's timeline. The timeline also contributed to another limitation: the inability to interview professionals from multiple cybersecurity companies that fell into the large

business category. Another critical limitation surrounded the type of information security professional. Most of the interviewees were experienced professionals with multiple years of cybersecurity expertise as well as necessary information security certifications. However, more junior-level cybersecurity professionals could have been interviewed to provide their first-hand account experiences. Another limitation was the lack of insider threats interviewed; future research should focus on gaining access to these individuals to prove the concepts proffered in these studies. Finally, another limitation involved the lack of interviewing insider threat experts. The shortened timeline contributed to interviewing these experts. It is recommended that follow-up research consider these limitations and institute steps to mitigate these shortfalls.

### Conclusions

A major identified area uncovered during this study related to the thoughts and intentions of employees when committing cyber infractions. This study shows that employees commit infractions with differing cognizant levels of either witting or unwitting. These same infractions were shown to have been committed with differing employee intentions of either unmalicious or malicious intent. The research also shows that pairing of cognizant level and intention focus is present for all cyber infractions. The data codes clearly point to four distinct classifications of employee thinking and intentions combinations. The unique category/classifications that employee infractions fall into are either *UnWitting-UnMalicious (UW-UM)*, *UnWitting-Malicious (UW-M)*, *Witting-UnMalicious (W-UM)*, or *Witting-Malicious (W-M)*. Figure 2 reflects the flow chart developed during the research to properly classify infractions into the four distinct groupings.

## Individual Subcategory Code Distribution



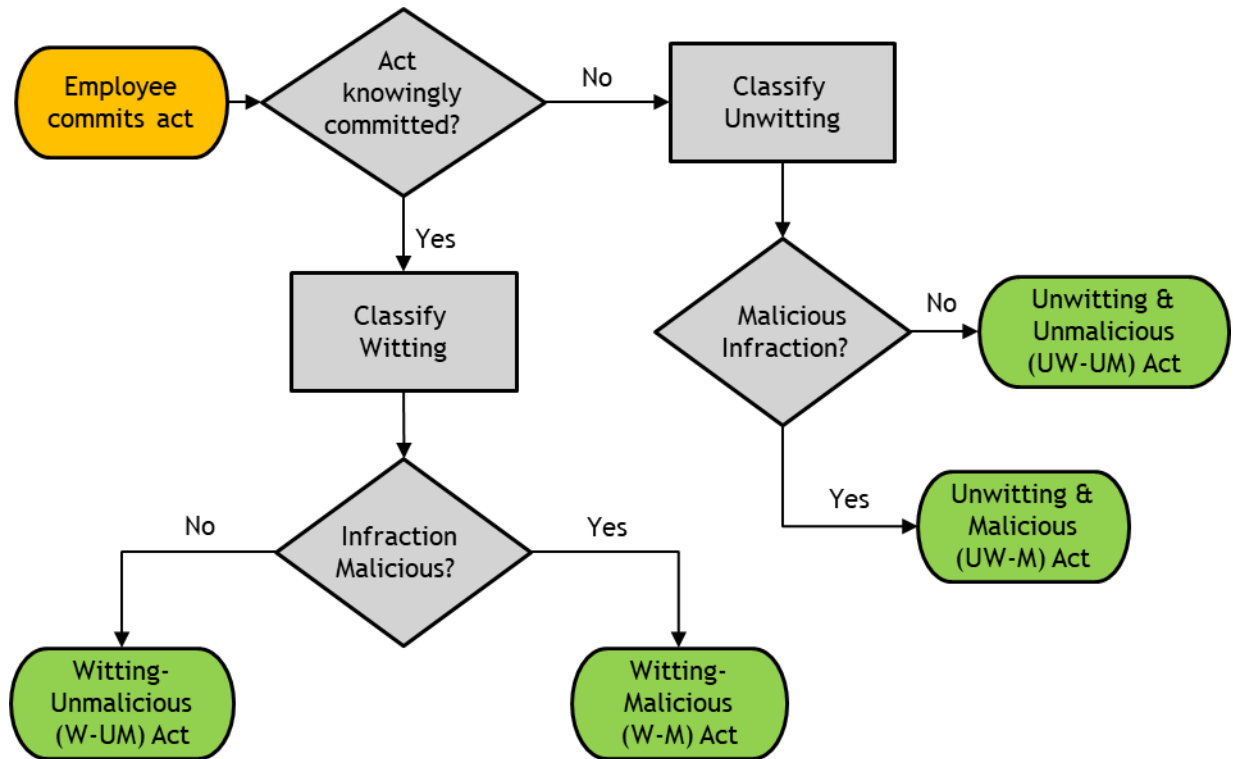
**Figure 1. Code Distribution**

- UnWitting-UnMalicious (UW-UM): This infraction classification contained 33 codes, which amounted to 26% of the total codes. Incident codes of this type were committed by employees who did not understand organizational security policies or who did not know of the policies. Interviewee examples included experiences with employees new to the organization or who were not provided with the proper cybersecurity training.
- UnWitting-Malicious (UW-M): An interviewee provided his thoughts on the impossibility of employees not knowing they were committing malicious acts. Other than this one reference, no other codes or threat activities are mentioned in this category. In actuality, it is impossible for an insider threat to commit a malicious infraction without being cognizant of the event.
- Witting-UnMalicious (W-UM): 50 types of these codes were identified during the process, accounting for 40% of the code population. This code category involved employees who consciously committed infractions but were more concerned with completing assigned tasks. Interviewee examples included nurses

who would focus on administering life-saving techniques to patients without regard to company security policies involving sign-in procedures while using nursing stations.

- Witting-Malicious (W-M): 34% of the codes, 42 in all, fell into this classification. This area contained cybersecurity incidents where the employee had knowledge of the attack and had malicious intent. Typical attacks associated with the witting-malicious classifications included embezzlement of company data and funds. The employees, in this case, knowingly had intentions to bring harm to the company. During the process, an interviewee shared one account where the employee of a company intentionally elevated network administrative rights to gain access to a company's sensitive data.

Most studies relating to this topic are quantitative in nature as opposed to qualitative. The coding aspect allowed this researcher to interface with the subject matter experts to ascertain their thoughts and views on why the insider threat problem continues to grow at an alarming rate (Schulze, 2024). This study shows that employees commit infractions with differing cognizant levels of either witting or unwitting. The study also shows that the same infractions are com-



**Figure 2. Employee Cyberspace Infraction Classification Process**

mitted with either unmalicious or malicious intent. Our research shows that pairing of cognizant level and intention focus is present for all cyber infractions. Identifying these groupings is key to understanding where glaring infractions are committed with intentions. What is specifically lacking in the cybersecurity industry is a comprehensive classification that focuses on intent and cognization that is meshed with the human factor element. This was attempted in previous studies using different models (Greitzer et al., 2014; Greitzer & Frincke, 2010), showing the linkage of psychosocial intent and unintentional insider threats to employees in the context of social engineering attacks. Our novel construct uses qualitative data from practitioner subject matter experts to establish linkage and classify employee insider threat activities based on cognition level and intent.

Categorizing infractions will allow companies to better understand why employees commit infractions, as opposed to just knowing that an infraction occurred. Executive and organizational leaders often struggle with properly identifying insider threat activities. Improper identification ultimately leads to struggles in creating secure company constructs, which leads to improper training directives for employees who violate security policies. This novel classification construct will allow organizations to better understand why insider threats occur. This will enable the organizations to look introspectively at the

infractions occurring within to better understand the how and why of their specific incidents. Better classification will further allow for the creation of better training programs that could increase organizational cyber hygienics. Fifteen cybersecurity subject matter experts provided data that points to the lack of adequate employee incident classifications. Continued research should center on further proofing these classifications. Future research should be quantitative and qualitative. The qualitative research will allow further data to be conducted in the form of real-world vignettes by industry cybersecurity experts who can provide synthesized experiences.

## Where to Find Out More

The source publications can be found below.

- Green, M. L. (2021). *Employees Breaking Bad with Technology: An Exploratory Analysis of Human Factors that Drive Cyberspace Insider Threats* (Publication Number 28771566) [D.B.A., University of South Florida]. Dissertations & Theses @ University of South Florida - FCLA; ProQuest Dissertations & Theses A&I; ProQuest Dissertations & Theses Global. United States -- Florida. <https://www.proquest.com/dissertations-theses/employees-breaking-bad-with-technology/docview/2595155354/se-2?accountid=14745>
- Green, M. L., & Dozier, P. (2023, July 31–August 2). *Understanding human factors of cyber-*

security: *Drivers of insider threats* (pp. 111-116). Paper presented at the 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy.

## References

- AL-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. *International Journal of Advanced Computer Science and Applications*, 14(2), 801-809. <https://doi.org/10.14569/IJAC-SA.2023.0140292>
- Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1-42. <https://doi.org/10.3390/electronics12061333>
- Burns, A., Roberts, T. L., Posey, C., Lowry, P. B., & Fuller, B. (2023). Going beyond deterrence: a middle-range theory of motives and controls for insider computer abuse. *Information Systems Research*, 34(1), 342-362. <https://doi.org/10.1287/isre.2022.1133>
- Cram, W. A., D'Arcy, J., & Benlian, A. (2024). Time will tell: The case for an idiographic approach to behavioral cybersecurity research. *MIS Quarterly*, 48(1), 95-136. <https://doi.org/10.25300/MISQ/2023/17707>
- Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. SAGE Publications, Inc.
- Grantham-Philips, W. (2024). AT&T says a data breach leaked millions of customers' information online. Were you affected? *AP News*. <https://ap-news.com/article/att-data-breach-was-i-affected-f0dda2b1d266a6068ffc607afd94b779>
- Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. In C. W. Probst et al., *Insider threats in cyber security* (pp. 85-113). Boston, MA: Springer US.
- Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014, May). Analysis of unintentional insider threats deriving from social engineering exploits. In *2014 IEEE Security and Privacy Workshops* (pp. 236-250). IEEE. <https://doi.org/10.1109/SPW.2014.39>
- Horton, J., Macve, R., & Struyven, G. (2004). Qualitative research: Experiences in using semi-structured interviews. In C. Humphrey & B. Lee, *The real life guide to accounting research* (pp. 339-357). Elsevier.
- Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019, December). Towards an improved understanding of human factors in cybersecurity. In *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)* (pp. 338-345). IEEE. <https://doi.org/10.1109/CIC48465.2019.00047>
- Khan, N. F., Yaqoob, A., Khan, M. S., & Ikram, N. (2022). The cybersecurity behavioral research: A tertiary study. *Computers & Security*, 120, 102826. <https://doi.org/10.1016/j.cose.2022.102826>
- Saldaña, J. (2021). *The coding manual for qualitative researchers* (4th ed.). London: SAGE Publications Ltd.
- Schulze, H. (2024). New report reveals insider threat trends, challenges, and solutions. *Cybersecurity Insiders*. <https://www.cybersecurity-insiders.com/2024-insider-threat-report-trends-challenges-and-solutions/>
- Strauss, A., & Corbin, J. (1994). Grounded theory methodology: An overview. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 273-285). SAGE Publications, Inc.
- Winder, D. (2024). Warning as 26 billion records leak: Dropbox, LinkedIn, Twitter named. *Forbes*. <https://www.forbes.com/sites/daveywinder/2024/01/23/massive-26-billion-record-leak-dropbox-linkedin-twitter-all-named/>

## Review

This article was accepted under the **constructive peer review** option. For further details, see the descriptions at:

<http://mumabusinesreview.org/peer-review-options/>

## Author



**Dr. Marcus L. Green** is an Assistant Professor in the Department of Computing Sciences at the State University of New York (SUNY) Brockport. Marcus was recently selected as the inaugural Cybersecurity Program Director. His teaching assignment consists mainly of cybersecurity courses, including ethical hacking, information assurance and incident response, and database and web security. He graduated with a Doctorate of Business Administration from the University of South Florida (USF). His primary research interest focuses on human factors related to cyberspace insider threat activities. He holds a Master's in Information Technology Management from Webster University's Walker School of Business and Technology. Green has held many cybersecurity positions, including visiting assistant professor (USF), Incident Responder at the United States Special Operations Command (USSOCOM), Lead Security Engineer (Dept. of Navy), and Information Systems Security Officer (Oregon State University). He is a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and CompTIA Advanced Security Practitioner (CASP).