Differentiating Insider and Outsider Cyberattacks on Businesses

Dearden, T.

Parti, K.

Hawdon, J.

Gainey, R.

Vandecar-Burdin, T.

Albanese, J.

CITE: Dearden, T.E., Parti, K., Hawdon, J. *et al.* Differentiating Insider and Outsider Cyberattacks on Businesses. *American Journal of Criminal Justice* 48, 871–886 (2023). https://doi.org/10.1007/s12103-023-09727-7

Abstract

The use of information and communication technologies in business has opened several new ways for employees to commit cybercrimes against their employers. Utilizing opportunity theory, the current paper investigates the characteristics of businesses victimized by employee-committed cyberattacks and compares insider- and outsider-committed cybercrime in terms of the damage they cause to the business. We used online sampling to obtain information on 350 businesses in the Commonwealth of Virginia, revealing 29 outsider cases and 17 insider attacks that were clearly identified. We found that insider attacks were more costly, resulting in more damage than external attacks; the most frequent attack type was impersonating the organization online for insiders, and viruses, spyware, and malware for outsiders. Our data suggested restricting personal devices, making cybersecurity a priority, cybersecurity updates among management, and employee training do not significantly lessen the risk or mitigate the effects of insider attacks. We suggest that organizational security culture must be refined and strengthened to identify and prevent insider attacks successfully.

Keywords: insider cyberattack, businesses, opportunity theory, cost, harm

Acknowledgement: The research was funded by the Coastal Virginia Center for Cyber Innovation (COVA CCI), 2021/2022.

Differentiating Insider and Outsider Cyberattacks on Businesses

The importance of information and communications technology (ICT) for business is unquestioned, as ICT can increase productivity and facilitate innovation (see Atkinson, 2018). Worldwide retail e-commerce sales, which are dependent on ICT, are projected to reach $8.1 trillion by 2025 (eMarketer, 2022). Despite the apparent importance of ICT to various industries, the use of computers by businesses creates vulnerabilities by exposing them to potential cybercrimes. Indeed, cyberattacks against businesses have long been a problem. As early as 2005, over two-thirds of businesses responding to the National Computer Security Survey detected at least one computer security incident within the past year, with the majority of victimized businesses detecting multiple incidents (Rantala, 2008; also see Das & Nayak, 2013). In total, businesses reported losing approximately $1.8 billion to cybercrime in 2019 (Hiscox, 2020). Cyberattacks against businesses are relatively common in other nations as well, including those in Belgium (Paoli et al., 2018), the Netherlands (Weijer, van de et al., 2021; Veenstra et al., 2015), other European nations (UNODC, 2013), the United Kingdom (UK Cyber Security Breaches Survey, 2020; Information Security Breaches Survey (ISBS), 2015), and Canada (Wanamaker, 2019).

While a growing body of research is documenting cybercrimes committed against businesses (e.g., Anderson et al., 2013; Farahbod et al., 2020; Hawdon et al., forthcoming; Klahr et al., 2017), there is still a relative lack of scholarly attention to the issue. One specific gap in the literature on business cybervictimization concerns whether these crimes are committed by employees or company outsiders. Despite some notable exceptions (e.g., Collins et al., 2016; Williams et al., 2019), few studies have explored employee-committed cybercrimes, and those focused on these crimes have generally investigated the characteristics of businesses that made them vulnerable. While we consider the types of companies victimized by employee-committed

cybercrimes, we also compare insider- and outsider-committed cybercrimes in terms of the damage they cause to the business. Using a sample of businesses operating in the Commonwealth of Virginia, the current study explores whether insiders are more likely to commit different cybercrimes than outsiders, what factors predict if cybercrimes are committed by insiders or outsiders, and if opportunity theory can account for any observed differences.

Literature Review

Most businesses experience employee-committed crimes that cut into profits. In fact, according to Weisbrot (2021), 95% of all businesses suffer from theft in the workplace, and 75% of employees admitted to stealing from their employers at least once, while 37.5% of employees have stolen from their employers at least twice. Yet, employees steal more than property or inventory; they also can steal "time" by purposefully reducing their productivity (Hollinger et al., 1992; also see Brock et al., 2013; Sao et al., 2020), intellectual property (Cappelli et al., 2012; also see Code42, 2022; Greenberg, 1997; Hollinger & Clark, 1983; Rantala, 2008), and other employees' personal information and identities (Shreve, 2004; Daks, 2005; Sauser, 2007). Employees also steal from their employers by committing procurement or contractual fraud, payroll theft, misrepresenting financial statements, and asset misappropriation (Peters & Maniam, 2016; Milenkovic, 2021). While employee theft is a problem for most businesses, small businesses appear particularly susceptible to employee theft (Complete Controller, 2019; Milenkovic, 2021).

The consequences of employee theft are staggering. U.S. companies are estimated to lose nearly $110 million daily because of employee-related crimes (Milenkovic, 2021). While much of this theft is petty, a high percentage of cases involve substantial losses. For example, the *Marquet Report on Embezzlement* discovered over 2,000 cases of employee theft over a five-year

period where losses exceeded $100,000 (Powell, 2014). In fact, it is estimated that businesses lose approximately five percent of their annual revenue to employee-committed fraud and theft, with an average loss-per-case of over $1.5 million and a median loss-per-case of $125,000 (Bell, 2021). According to data from the *Service Management Group*, employee theft is the primary reason for more than 30% of business bankruptcies (Bell, 2021). There are also reputational costs that dissuade consumers from doing business with the company, negative effects on employee morale, adverse consequences for the overall work environment and intra-organizational relationships and resulting regulatory actions that entail businesses incurring additional costs related to compliance (see Peters & Maniam, 2016; The Investopedia Team, 2022).

While employee theft is not a new phenomenon (see Tucker, 2018), its nature certainly has changed recently. The now-common use of ICT in business has opened several new ways for employees to commit crimes against their employers. For example, cyber-identity theft (Close et al., 2004), cyber-loafing (Sao et al., 2020), data breaches (Code42, 2022; Verizon, 2019; ISBS, 2015), fraudulent email scams, virus infections, and hacking into company bank accounts (Hawdon et al., forthcoming; ISBS, 2015) are all a result of, or significantly facilitated by ICT. More generally, Collins and colleagues (Collins et al., 2016: 6) identify broad types of "malicious threats" faced by companies that involve an employee intentionally exceeding or using their access to their company's ICT to negatively affect the congeniality, integrity, or availability of the organization's ICT. Using data from 734 known cases of insider-committed cybercrimes against businesses, Collins and associates (2016) identified four broad threats: fraud, ICT sabotage, theft of intellectual property, and "miscellaneous" (Collins et al., 2016). These types of insider-committed crimes appear to be relatively common. For example, in 2005,

75% of cyber-thefts were committed by employees, and company insiders were especially likely to be the criminals behind embezzlement and theft of intellectual property (Rantala, 2008; also see Collins et al., 2016). Similarly, nearly 60% of data breaches involved employees (Verizon, 2019).

Not only are there new forms of employee-committed crimes and opportunities for crimes, but these types of crimes may also be increasing. According to data from the United Kingdom (ISBS, 2015), "insider-victimization" increased by 58 percent for large-sized companies and 22 percent for small companies compared to the previous year. Recent trends created by the COVID-19 pandemic, including the "Great Resignation" (Demirkaya et al., 2022), employee turnover, and dramatic increases in remote work, have created unprecedented opportunities for employees to steal valuable data from their company. In a survey of 700 companies with 500 employees or more, 73% of respondents reported that protecting corporate data from insiders is a "big problem within their company," especially when employees leave the company (Code42, 2022).

Therefore, it appears that employee-committed cybercrime against their employers is a costly problem, and this type of crime is increasing. While the Information Security Breaches Survey (ISBS, 2015) has routinely recorded high levels of insider-committed cybercrimes against businesses, the threat of insider-committed cybercrimes has increased recently due to the expanded use of remote access computing, cloud computing, and social media (ISBS, 2015; Williams et al., 2019).

Other business characteristics and practices also correlate with employee-committed cybercrimes. The increased allowance or even encouragement of "bring-your-own devices" significantly increases the risk of insider-committed cyber-fraud, and organizations that provide

staff with devices such as mobile phones and tablets are more likely to experience insider security breaches (Ponemon, 2013; Williams et al., 2019). Compared to businesses that do not store confidential data, those that do store such data are nearly three times more likely to suffer an insider-committed cybercrime. Company size also appears to increase the likelihood of being victimized by an employee, as companies with over 250 employees are almost 12 times as likely to be victimized than those with ten or fewer employees (Williams et al., 2019; also see ISBS, 2015).

Cybercrimes committed against businesses by insiders likely differ from those committed against businesses by outsiders, and the insider-committed crimes may be more costly to the company. But why would this be the case? Opportunity theory provides a conceptual model of victimization to derive hypotheses regarding these issues.

Opportunity Theory and Employee-Committed Cybercrimes

Criminal opportunity theory considers opportunities for crimes to play a fundamental role in all criminal activity (see Felson & Clarke, 1998). These opportunities, concentrated in time and space, shape the interaction between criminals and their potential victims (see Felson & Clarke, 1998; Lee, 2000). At the heart of opportunity theory is the assumption that criminal offending is rational, purposive behavior (see Cornish & Clarke, 2014). Potential offenders make rational decisions using the information they have. In any given circumstance, potential offenders evaluate the likely gains and risks associated with committing the crime, and they will commit a crime when they perceive the gains as outweighing the risks. While the evaluation of the rewards associated with the crime is essentially a function of the victim's characteristics (see Cohen & Felson, 1979; Finkelhor & Asdigian, 1996), the risks associated with the crime are essentially a function of the environment in which the crime is to occur.

Various perspectives that adopt a basic opportunity theory approach have been developed, and these primarily apply at differing levels of social life. For example, routine activity theory (Cohen & Felson, 1979), which argues crime occurs when a motivated offender and suitable target come together in an environment that lacks capable guardians who can prevent the crime, explains variations in the opportunities for crime at the social level. Crime pattern theory (Brantingham & Brantingham, 1984) focuses on the local environment by considering how the built and social environment, combined with the routine movements of the population, generate opportunities for crime that are attractive to potential offenders. Rational choice theory (see Cornish & Clarke, 2014) explains the individual actor's decision within the social and local environments (see Clarke & Felson, 1993; Felson & Clarke, 1998). Thus, broad social trends and the local environment either create or limit the commission of crimes by determining the opportunity structure potential criminals must consider when deciding if, and when they might commit a given crime. While these opportunities are concentrated in both time and space, depending on the routine movements of people, they tend to be highly specific (Felson & Clarke, 1998).

This perspective can easily be applied to employee-committed cybercrimes against businesses. First, several studies of workplace crime note that the most important facilitating factor leading to employee theft is the opportunity to commit the crime (Hollinger & Clark, 1983; Kantor, 1983; Mustaine & Tewksbury, 2002; Tucker, 2018). As Hollinger and Clark (1983: 70) state, findings "tend to confirm that an employee's involvement in theft may be related to the physical opportunities furnished by his or her occupation." Given their insider position, employees have ready opportunities and access to their employer's desirable property. In addition, employees have inside knowledge of and access to ICT systems, security processes,

and trade secrets. Thus, compared to outsiders, employees have greater knowledge of both the risks and rewards presented by various opportunities to commit a crime. Given this, insiders would be more likely to engage in successful crimes than outsiders as they would be better able to correctly assess the risks and rewards, all else being equal. The greater knowledge of how the business operates and tries to protect its assets that insiders have relative to outsiders can help explain why their crimes tend to go undetected for long periods and typically result in more damage to the company. For example, employee theft cases often take more than a year to detect (Chilingerian & Schafer, 2019), and the average time it takes to detect a typical employee theft scheme is 14 months (Milenkovic, 2021).

Next, as noted by Felson and Clarke (1998), social and technological changes create new crime opportunities, and businesses' widespread adoption of ICT has clearly done that. Creating new ways to access property, data, and company information has allowed employees to victimize their employers. Since these new ICT-enabled means of accessing property can be done remotely, the likelihood of being observed stealing from the company is greatly reduced. Moreover, when businesses place their primary focus on protecting against outsider-committed crimes, they become vulnerable to insider attacks. Consequently, adopting ICT by businesses likely reduces the guardianship of the workplace. That is, now that much of employees' work occurs behind computer screens, it is more difficult for co-workers and supervisors to know what the employee is up to and if the employee is committing a crime. Knowing there is a lack of capable guardians protecting the environment, this may increase the likelihood that the rewards of the crime would outweigh the punishments associated with the crime or even the risk of being detected.

In the meantime, the more capable guardians (tools, policies, requirements) are provided to both co-workers and managers to identify vulnerabilities and weaknesses, the more likely insider attacks can be prevented and detected early. For instance, developing strong cybersecurity policies, frequently updating managers about security policies, and requiring cybersecurity training and compliance from co-workers at all levels can increase cybersecurity awareness (Khando et al., 2021) and reduce insider cyberattacks within companies. For example, Akter et al. (2022), in a systematic literature review, found that besides technical preparedness and infrastructure capabilities, companies' personnel capabilities (such as knowledge, positive attitude, and behavior towards cybersecurity), both on the employee and the managerial level are essential to developing an enhanced security culture in an organization. It is especially true for insider attacks due to human behavior (Maalem Lahcen et al., 2020). Moreover, insiders know the system vulnerabilities and often have access rights enabling data breaches. Thus, elements of the enhanced security culture are employee and management tendencies to respect policies, training and education on cybersecurity, institutional policy compliance and training programs, and introducing strict policies and cutting-edge technologies for security (Akter et al., 2022). In a security culture where both employees and management understand, and respect shared security values, insider attacks can be better prevented, more easily isolated, and early intervention can better mitigate harm.

Applying opportunity theory to employee-committed cybercrimes would therefore lead us to several hypotheses when comparing cyberattacks committed by insiders against their employers versus cyberattacks committed by outsiders.

H1: Insider attacks will be more costly than outsider attacks.

H2: Insider attacks will result in more damage, both financially and time required to mitigate and resolve them, than will outsider attacks.

H3: Companies that provide their employees with personal devices will suffer more insider attacks than those that do not.

H4: Insider attacks will be more likely in larger companies than outsider attacks.

H5: The more frequently managers are debriefed concerning ICT issues, the less likely insiders will victimize the company.

H6: The more frequently employees are trained in cybersecurity, the less likely insider attacks will occur.

Methods and Sample

We utilized online sampling to obtain information from businesses in Virginia. We collected 642 online surveys from Virginia businesses using respondents recruited by CINT USA, the largest consumer network for digital survey-based research. Data collection took place May 9-10, 2022. First, we excluded individuals who did not accept the IRB consent (n=30). Second, we excluded individuals who completed the survey in under three minutes (n=243). Finally, we excluded 19 participants as they indicated that their business was not located in Virginia. This left us with a total sample of 350 participants. We utilized pairwise deletion, allowing for slight variations in the models below but maximizing statistical power in the relatively small sample.

Survey questions were taken from the UK Cyber Security Breaches Survey (2020). The survey asked about characteristics of the business (e.g., industry sector, number of employees), ICT information and vulnerabilities (e.g., online presence, online ordering option, electronic storage of customer data, bring your own device (BYOD) policy), cyber security readiness or

controls (e.g., how important cyber security is to your organization; do you provide employees with regular cyber security training), cybercrime attacks and breaches (e.g., has your company been affected by the listed cyberattacks or breaches; which breach was most significant; was it reported internally or externally), harms and costs (e.g., please list the consequences, in loss, reparation costs, and downtime, of the most disruptive cybersecurity breach in the last 12 months), actual preparedness (e.g., which of the listed rules or controls your company has in place), the perception of cyberattack preparedness (i.e., how likely are you to expect a significant cyberattack against your company or the US in the next five years; on a Likert scale of 1-4, what do you think businesses and your company are doing to prevent attacks of this type). The questionnaire took an average of 7.5 minutes to complete.

For this project, we were specifically interested in the most significant breach, and whether the attacks were orchestrated by those within the company versus those outside of the company. We asked a series of questions related to the most serious breach the company has experienced to date. The results section includes a brief discussion of general crimes experienced by businesses followed by a focus on whether their most significant cyberattack was conducted by an insider or outsider.

Results

Focusing on the entire sample (n=350), we find that businesses were frequently the victims of cyberattacks. Across all measures, more than 50% of participants reported that their companies had experienced a cyberattack. In fact, only 46 companies (13%) reported they had not been the victim of some type of completed or attempted cyberattack. The most common cyberattack against companies was staff receiving fraudulent emails (81%), and the least common was a successful attack against the company's bank accounts (59%).

Insert Table 1 about here

For the remainder of our analysis, we were interested in the most significant breach against a company in cases where the offender was identified. Far fewer participants reported this information. We suspect that participants were less likely to know this information as it would have required a rigorous and complete investigation of the cyberattack, including an understanding of who orchestrated the attack. This is likely only the case when the cyberattack causes enough damage to warrant further investigation. Overall, there were 29 clearly known outsider attacks and 17 clearly identified insider attacks. When considering the types of crimes conducted by insiders and outsiders, a few apparent differences are to be noted. For all reports, see Table 2.[1] The most common form of attack by an insider was impersonating the organization in emails or online (53%), whereas outsiders were most commonly causing damage through viruses, spyware, or malware (59%).

Insiders caused significantly more financial harm to companies than outsiders ($t(39)=-2.4$, $p=.02$). The median cost of damages by insiders was $20,000 to $100,000, whereas the median outsider caused $5,000 to $10,000 in financial costs. Beyond financial costs, participants reported that insider attacks had a greater overall effect on the company ($t(41)=-2.02$, $p=.05$). Finally, insider-caused damage lasted longer, the median being between one day to under a week, versus an outsider median of less than one day ($t(43)=02.2$, $p=.03$) to resolve.

Insert Table 2 about here

[1] Adds to more than 46 as attack categories were not mutually exclusive and could belong to more than one category.

There were no other differences as to which companies' insiders or outsiders would target. For example, there was no difference in insider/outsider targeting based on the company size ($t(42)=.62$, $p=.54$), whether the companies allowed personal devices ($\chi^2(44)=.02$, $p=.87$), the self-disclosed importance of cybersecurity ($t(42)=-1.1$, $p=.27$), how frequently management was updated on cyber security ($t(42)=1.2$, $p=.25$), or whether cybersecurity training was provided to employees ($\chi^2(43)=.19$, $p=.67$).

To understand the differences between inside and outside offenders further, we ran two logistic regressions presented in Table 3. Our first model included a series of independent variables addressed above. These were the cost of the victimization, how affected the organization was, the length of the attack, whether employees are allowed their own devices, the size of the organization, the perceived importance of cyber security, how often management is updated, and whether the organization carries cyberattack insurance. Despite a relatively small number of cases ($n=32$) and only a few independent variables, the explained variance was relatively high (pseudo $R^2=.42$). However, the cost of the crime was the only significant predictor found at the $p<.05$ level. Similar to the chi-square test, the cost of insider attacks was substantially higher than outsider attacks (OR=3.83). Employee count was significant at the $p<.10$ level tentatively suggesting that the larger the organization, the less likely they were to have experienced an insider attack (OR=.28).

Insert Table 3 about here

The second model included a series of variables related specifically to the damages from insider versus outsider attacks. In addition, we included the cost variable from the model above. We were interested in seeing if there were differences in how offenses were detected for insider versus outsider attacks. We used a series of binary indicator variables. See Table 4 for the logistic regression and all indicators. Two variables were dropped from the analysis as they were only reported in insider attacks. Specifically, there were two instances of a breach being reported by the media and two instances of other non-routine processes of detection. For the remainder of the model, no differences were found between the type of detection used in insider versus outsider attacks. Bivariate statistics (chi-square) generally confirmed this model, as only one significant difference was found. Outsiders were more likely to be detected by software than insiders ($\chi^2(46)=4.8$, p=.028).

Given the small sample size (n=37) and larger number of variables (8 or 10) we violate the customary rule of having ~10 cases per variable within the model. While our ratio of insiders to outsiders is helpful (37%), there are still some statistical concerns. In order to consider the validity of our findings we utilized bivariate statistics to ensure that the logistic regression yielded similar findings. However, a large number of bivariate statistics should also carry a penalty, and thus does not solve our problem. We attempted to utilize an exact logistic regression. This model helps when there are smaller sample sizes (Mehta & Patel, 1995). However, due to the complexity of estimating an exact regression we had to reduce the number of independent variables in the first model. For our first model we only included the variables with higher levels of significance in the original logistic regression (cost, employe count, cyber importance, and management updates). We found similar findings to the original logistic regression, except the cost odds-ratio was reduced from 3.8 to 1.8. Our second exact logistic

regression was run using all variables in the second logistic regression. We found no major differences between the original regression other than a slight reduction in the odds-ratio in cost (1.34 to 1.24). While no model is perfect given our small sample size, utilizing different models, including exact logistic regression, yielded similar results.

Insert Table 4 about here

Discussion

There is a growing body of research on cybercrime against businesses. However, businesses' cybervictimization by insiders versus outsiders has not been studied extensively. The current paper aims to fill this gap. Besides investigating the characteristics of businesses that suffered employee-committed cyberattacks, the current paper compares insider and outsider-committed cyberattacks against businesses. Specifically, we compare the harm caused by insider and outsider cyberattacks, and the factors that predict such attacks using a large sample of businesses located in the Commonwealth of Virginia. Using this sample, we find distinct characteristics of employer-committed cyberattacks. In addition, the factors that predict business victimization by insiders can be explained by opportunity theory (Felson & Clarke, 1998), according to which criminal offending is rational and purposeful and people commit crimes if they perceive that potential gains outweigh the potential risks. This is precisely the situation with employees who know more about the company's operations, weaknesses and vulnerabilities than outsiders would. Insiders might already have access to business secrets and valuable data, and it usually takes more time to detect their obscure operations than outsider attacks (Chilingerian & Schafer, 2019). Further, ICT practices such as the digitization of customer data, applying cloud

services, having social media profiles, and allowing employees to use their own electronic devices while at work further widen opportunities and reduce the application of capable guardians. In light of the above, we hypothesized that insider cyberattacks would be less likely to be detected than outsider attacks; insider cyberattacks will be more costly and result in more damage than outsider attacks; companies that allow employees to use their personal devices will suffer more insider attacks than outsider attacks; and, the more frequently managers are updated and employees are trained in cybersecurity the less likely the company will experience insider cyberattacks.

The data partially support the above assumptions. Although only 36 businesses answered that they successfully identified their attackers, insider cyberattacks were indeed less likely (n=17) than outsider attacks (n=29). This corresponds with previous research findings (Kim et al., 2019). However, it is not possible to determine from the data whether there were, in fact, fewer insider attacks or whether insiders are simply harder to detect. The most common types of cyberattacks committed by insiders (impersonating the organization in emails or online; attempting to take down websites or online services) also match our opportunity theory-based anticipation. We suggested that, knowing more about their businesses' operations, employees will not need viruses, spyware, malware, or to hack into the system to breach company data. Instead of these tools, which outsiders most frequently utilize, insiders will use the knowledge they already have to harm their employers.

By using these techniques, insiders, in fact, caused more financial harm (*H1*), and had an overall greater effect on the business than outsider attacks did. Insider-caused damage also lasted longer than outsider-caused damage (*H2*). Even ranking the independent variables, the cost of insider attacks was substantially higher than that of outsider attacks. Although the survey

questions did not allow for detailed explanations, this finding parallels previous research findings according to which by having access privileges, insider attacks last longer and take longer to detect than outsider attacks (Milenkovic, 2021).

Surprisingly, our data did not support previous findings that larger companies experience more insider cyberattacks than outsider cyberattacks (*H4*) (ISBS, 2015; Williams et al., 2019). In fact, the more employees the company had, the less likely they were to experience an insider attack, although the relationship did not achieve statistical significance ($p=.095$). However, since the data did not allow us to unravel the details, it is possible that larger companies still have more disgruntled insiders or more offending opportunities than smaller ones do, they just cannot identify the attacker. Indeed, cyber offenders are hard to track down due to the ever-greater use of remote access computing, cloud computing, and social media (Williams et al., 2019; Akter et al., 2022). In addition, we only focused on the most significant cyberbreach. What could be occurring is that larger organizations experience several cyberattacks but are less likely to have the most significant attack being committed by an insider. Unfortunately, the data was no conducive to addressing this possibility.

Although the logistic regression analysis did not reveal any significant differences regarding different detection modes, bivariate statistics suggested that outsiders were more likely to be detected by software than insiders were. This indicates that software products are better at detecting malicious outsider operations. Research suggests that insiders use known information, personal connections, and access privileges (Khando et al., 2021) to retrieve data without authorization or to extend authorized access. Hence, it would be difficult to detect with software if someone accessed the system with access privileges or used other employees' access privileges. Thus, strengthening the company's security culture is recommended in addition to the

use of software products or automated processes. This includes introducing least-privilege access models where employees are given only those privileges needed for them to complete their tasks (Padayachee, 2015). Khando et al. (2021) recommend providing frequent computer and internet security training to employees involving mutual understanding and respect for company security culture. Their findings suggest that the attitudes and value system of employees and management together are responsible for a thriving security culture that can possibly eliminate insider threats. This aligns with our findings, suggesting that regular cybersecurity measures are not successful in preventing insider attacks. Indeed, allowing personal devices, cybersecurity importance, frequency of debriefing management about cybersecurity issues, and providing cybersecurity training to employees made no difference whether the company experienced more insider or outsider attacks (*H3, H5, H6*).

Limitations and Recommendations

The dataset contained a relatively small number of cases where the attacker's identity was clearly known as an insider or outsider. Hence, the study should be replicated on a larger sample where more extensive data on the attacker was collected to learn more about insider versus outsider threat characteristics. Furthermore, complementing the survey with a mixed methodology including qualitative data could reveal more about the opportunities, the rationale, and the protective and preventive factors of insider and outsider threats to businesses. We also suggest that future research investigate how remote access computing, cloud computing, company social media use, and different ICT operations individually affect risks of insider and outsider cyberattacks.

Variables included in this study allowed for measuring essential characteristics of the businesses as well as indicators of insider and outsider threats against businesses. However, due

to constraints in the length of the survey, we could not include many important variables to more fully test opportunity theory (Felson & Clarke, 1998). Future research should test other theories of crime and deviance explain insider versus outsider threats. For example, situational crime prevention theory (Willison, 2000; Warkentin & Willison, 2009), crime pattern theory (Brantingham & Brantingham, 1984), rational choice theory (Cornish & Clarke, 2014), routine activities theory (Cohen & Felson, 1979), the fraud triangle model (Cressey, 1953) or the revised fraud triangle model (Schuchter & Levi, 2016) could be tested on insider cybercrime in businesses.

Conclusion

Opportunity theories suggest that the situation and environment shape the potential for crime. Due to their position and access, insiders in a company have more opportunity to commit cybercrime. We empirically analyze insider and outsider cybercrimes. We find that insiders cause more damage and cost more than outsider attacks. The nature of the thefts suggests that strengthening the company's security culture is recommended as are software security products or automated processes. Our findings reveal that the attitudes and values of employees and management are mutually responsible for a strong security culture to deter insider threats. This is especially true given the increased impact of insider attacks against companies.

References

Akter, S., Uddin, M.R., Sajib, S., Lee, W.J.T., Michael, K., & Hossain, M.A. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Annals of Operations Research,* Published Ahead of Print. https://doi.org/10.1007/s10479-022-04844-8

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten,M. J. G., Levi,M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 265–300). Springer.

Atkinson, R. D. (2018). How ICT can restore lagging European productivity growth. *Information Technology & Innovation Foundation*.

Bell, R. (2021). Employee time theft: How to uncover and prevent it. *Workforce.* https://workforce.com/news/time-theft

Brantingham, P. J., and Brantingham, P. L. (1984). *Patterns in Crime.* New York: Macmillan.

Brock, M. E., Martin, L. E., & Buckley, M. R. (2013). Time Theft in Organizations: The development of the Time Banditry Questionnaire. *International Journal of Selection and Assessment*, *21*(3), 309-321.

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud)*. Addison-Wesley.

Chilingerian, N., & Schafer, T. (2019). *Hiscox Study Confirms Prominence of U.S. Employee Theft.* https://www.cutimes.com/2019/03/29/hiscox-study-confirms-prominence-of-u-s-employee-theft/?slreturn=20220931112146

Clarke, R. V., & Felson, M. (Eds.). (1993). Routine Activity and Rational Choice: Advances in Criminological Theory, 5. New Brunswick, NJ: Transaction Books.

Close, A. G., Zinkhan, G. M., Finney, R. Z., & Center, N. O. (2004). Cyber-identity theft: A conceptual model and implications for public policy. In *Proceedings of the American Marketing Association Summer Educator's Conference*.

Code42. (2022). Annual Data Exposure Report, 2022. https://www.code42.com/resources/reports/2022-data-exposure?utm_source=google&utm_medium=cpc&utm_campaign=ENT_Data%20Security%20-%20Search%20%7C%20cpg-evergreen&utm_term=employee%20stealing%20data&_bt=582231881890&_bk=%2Bemplo yee%20%2Bstealing%20%2Bdata&_bm=b&_bn=g&_bg=111371611886&gclid=CjwKCAj w5P2aBhAlEiwAAdY7dOP69NivG4BNYgkOkHIa_1lMpfKhXf_u0rkvGpvtUZJUxL17an8 utRoC7vYQAvD_BwE

Cohen, L. E. & Felson, M. (1979) Social change and crime rate trends: A routine activity approach. *American Sociological Review 44,* 588 – 608.

Collins, M., Theis, M., Trzeciak, R., Strozer, J., Clark, J., Costa, D., Cassidy, T., Albrethsen, M., & Moore, M. (2016). *Common Sense Guide to Mitigating Insider Threats*. 5th ed. Software Engineering Institute. Pittsburgh, PA.

Complete Controller (2019). Employee theft: Why most small businesses don't report it. https://www.completecontroller.com/employee-theft-why-most-small-businesses-dont-report-it/

Cornish, D. B. & Clarke, R.V. (Eds.) (2014). *Reasoning criminal: Rational choice perspectives on offending.* New Brunswick: Transaction Publishers.

Cressey, D. R. (1953). *Other People's Money: A Study in the Social Psychology of Embezzlement.* Glencoe: The Free Press.

Daks, M. C. (2005). Banks need to bolt the door twice. *NJBIZ, 18*(24), 3-4.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International journal of engineering sciences & Emerging Technologies*, *6*(2), 142-153.

Demirkaya, H., Aslan, M., Güngör, H., Durmaz, V., & Rodoplu Şahin, D. (2022). COVID-19 and Quitting Jobs. *Frontiers in Psychology*, *13*, 916222. https://doi.org/10.3389/fpsyg.2022.916222

eMarketer (2022). *Worldwide E-commerce Forecast*. Updated 2022. https://www.insiderintelligence.com/content/worldwide-ecommerce-forecast-update-2022

Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. Journal of Business and Behavioral Sciences, 32(1), 63-71.

Felson, M. & Clarke, R. (1998) Opportunity makes the thief: Practical theory from crime prevention. *Police Research Series, 98.* London: Home Office, Research, Development and Statistics Directorate. https://popcenter.asu.edu/sites/default/files/opportunity_makes_the_thief.pdf

Finkelhor, D., & Asdigian, N. L. (1996). Risk factors for youth victimization: Beyond lifestyle / routine activities theory approach. *Violence and victims 11*(1), 3-19.

Greenberg, J. (1997). The STEAL motive: Managing the social determinants of employee theft. In R.A. Giacalone and J. Greenberg (Eds.), *Antisocial behavior in organizations* (pp. 85-108). Thousand Oaks, CA: SAGE Publications.

Hawdon, J., Parti, K., Dearden, T., Vandecar-Burdin, T., Albanese, J., & Gainey, R.

(Forthcoming). Cybercrime victimization among Virginia businesses: Frequency, vulnerabilities, and consequences of cybervictimization. *Criminal Justice Studies*.

Hiscox (2020). *Hiscox cyber readiness report 2020.* Https://www.hiscox.co.uk/sites/uk/files/documents/202006/Hiscox_Cyber_Readiness_Report_2020_UK.PDF

Hollinger, R.C, & Clark, J.R (1983). *Theft by employees.* Lexington, MA: Lexington Books.

Hollinger, R., Slora, K. B., & Terris, W. (1992). Deviance in the fast-food restaurant: correlates of employee theft, altruism, and counterproductivity. *Deviant Behavior, 13*, 155-184.

ISBS (2015). *Information Breaches Survey: Technical Report*. London: Department for Business, Energy and Industrial Strategy.

Kantor, S. (1983). How to foil employee crime. *Nation's Business*, July, 38-39

Khando, K., Gao, S., Islam, S.M., & Salman, A. (2021). Enhancing employees' information security awareness in private and public organisations: A systematic literature review. *Computers & Security, 106,* https://doi.org/10.1016/j.cose.2021.102267

Kim, J., Park, M., Kim, H., Cho, S., & Kang, P. (2019). Insider threat detection based on user behavior modeling and anomaly detection algorithms. *Applied Sciences, 9,* 4018. https://doi.org/10.3390/app9194018.

Klahr, R., Shah, J. N., Sheriffs, P., Rossington, T., Pestell, G., Button, M., & Wang, V. (2017). *Cyber security breaches survey 2017.* www.gov.uk/government/statistics/cyber-security-breaches-survey-2017

Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity, (3)*10. https://doi.org/10.1186/s42400-020-00050-w

Lee, M. R. (2000). Community cohesion and violent predatory victimization: A theoretical extension and cross-national test of opportunity theory. *Social Forces*, *79*(2), 683-706.

Mehta, C. R., & Patel, N. R. (1995). Exact logistic regression: theory and examples. Statistics in medicine, 14(19), 2143-2160.

Milenkovic, M. (2021). Ripping Off the Boss: 33 Surprising Employee Theft Statistics. *SmallBizGenius*. https://www.smallbizgenius.net/by-the-numbers/employee-theft-statistics/#gref

Mustaine, E. E., & Tewksbury, R. (2002). Workplace theft: An analysis of student-employee offenders and job attributes. *American Journal of Criminal Justice*, *27*(1), 111-127.

Padayachee, K. (2015). A framework of opportunity-reducing techniques to mitigate the insider threat. *Proceedings of the Information Security for South Africa*, 1-8, 10.1109/ISSA.2015.7335064

Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium. *Crime, Law and Social Change, 70,* 397–420. https://doi.org/10.1007/s10611-018-9774-y

Peters, S., & Maniam, B. (2016). Corporate fraud and employee theft: Impacts and costs on business. *Journal of Business and Behavioral Sciences, 28*(2), 104-117.

Ponemon (2013). The Risk of Insider Fraud Second Annual Study. Traverse City, MI: Ponemon Institute.

Powell, T. (2014). The changing face of fraud. *CPA Practice Management Forum,* 20–25.

Rantala, R. (2008). Cybercrime against Businesses. *Bureau of Justice Statistics Special Report.* U.S. Department of Justice.

Sao, R., Chandak, S., Patel, B., & Bhadade, P. (2020). Cyberloafing: Effects on employee job

performance and behaviour. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(5), 1509-1515.

Schuchter, A. & Levi, M. (2016). The fraud triangle revisited. *Security Journal, 29*, 107-121. https://doi.org/10.1057/sj.2013.1

Shreve, M. (2004). Employers slow to recognize identity theft. *Business Insurance, 38*(36), 4-5.

Sauser Jr, W. I. (2007). Employee theft: Who, how, why, and what can be done. *SAM Advanced Management Journal*, *72*(3), 13-25.

The Investopedia Team (2022). *6 ways cybercrime impacts business*. Investopedia. https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx#citation-4

Tucker, J. (2018). Employee theft as social control. In G. Mars (Ed.), *Occupational Crime*, (pp. 65-80). Routledge.

UK Cyber Security Breaches Report (2020). *UK cyber security breaches survey.* Department for Digital, Culture, Media, and Sports & Ipsos MORI. Retrieved Aug 5, 2022 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf

UNODC (2013). *Comprehensive study on cybercrime.* United Nations Office on Drugs and Crime. Retrieved Aug 10, 2022 from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Veenstra, S., Zuurveen, R., & Stol, W. (2015). *Cybercrime onder bedrijven. Een onderzoek naar slachtofferschap van cybercrime onder het Midden- en Kleinbedrijf en Zelfstandigen Zonder Personeel in Nederland.* Lectoraat Cybersafety, NHL Hogeschool & Politie

Academie Faculteit Cultuuren Rechtswetenschappen, Open Universiteit. Cybersafety Research and Education Network. Retrieved Aug 14, 2022 from https://cybersciencecenter.nl/media/1054/2015-05-13-cybercrime-onder-bedrijven-def.pdf

Verizon (2019). *Insider Threat Report*. Verizon. https://www.verizon.com/business/resources/reports/insider-threat-report/

Wanamaker, K.A. (2019). *Profile of Canadian businesses who report cybercrime to police.* Public Safety Canada.

Warkentin, M. & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*(2), 101-105, https://doi.org/10.1057/ejis.2009.12

Weijer, van de, S.G.A., Leukfeldt, E.R., & Zee, van der, S. (2020). Reporting cybercrime victimization: Determinants, motives, and previous experiences. *Policing: An International Journal.* https://doi.org/10.1108/PIJPSM-07-2019-0122

Weisbrot, E. (2021). 35+ Shocking Employee Theft Statistics to Know in 2022. *JW Surety Bonds.* https://www.jwsuretybonds.com/blog/employee-theft-statistics

Williams, M., Levi, M., Burnap, P. & Gunder, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior, 40*(9), 1119-113.

Willison, R. (2000). Understanding and addressing criminal opportunity: The application of situational crime prevention to IS security. *Journal of Financial Crime, 7*(3), 201-221.

Table 1: Cyber Attacks against Companies in Virginia

Type of Attack	More than 12 months ago	Past 12 months	Multiple times (both)	None	% attack ever
People impersonated company in emails	126	79	41	104	70%
Staff received fraudulent emails	77	137	70	66	81%
Computers became infected with ransomware	120	71	53	106	70%
Computers became infected with other viruses, spyware, or malware	122	75	51	102	70%
Attack attempted to take down website or online services	109	80	40	121	65%
Unauthorized use of computers, networks, or servers by staff	92	94	47	117	67%
Unauthorized use of computers, networks, or servers by outsider	108	63	47	132	63%
Attack succeeded in taking down website	114	60	36	140	60%
Attempted attack on company's online bank account	117	62	37	134	62%
Successful attack on company's online bank account	127	44	36	143	59%

Table 2: Insider Versus Outsider Attacks

Type of Attack	**Most Significant Breach**			
	Known Insider		Known Outsider	
	Count	Percent	Count	Percent
Ransomware	3	18%	10	34%
Viruses, Spyware or Malware	6	35%	17	59%
Attacks attempting to takedown website or online services	8	47%	9	31%
Hacking or attempted hacking of online bank accounts	2	12%	4	14%
People impersonating your organization in emails or online	9	53%	7	24%
Staff receiving fraudulent emails or being directed to fraudulent websites	5	29%	12	41%
Unauthorized use or hacking of computers	1	6%	10	34%
Other	0	0%	1	3%

Note: Percentages are based on 17 insider attacks and 29 outsider attacks; multiple categories could have been selected, so percentages will add to more than 100%

Table 3: Logistic Regression, Organizational Characteristics Predicting Insider Attacks

	Logistic Regression Model			
Variable	***B***	***SE(B)***	***p***	**OR**
Cost	1.34	0.53	.011	3.83
Affect	0.98	0.87	.258	2.68
Length	-0.43	0.82	.597	0.65
Personal Devices	2.17	1.87	.245	8.77
Employee Count	-1.27	0.76	.095	0.28
Cybersecurity Importance	1.56	1.19	.190	4.77
Management Updates	-0.81	0.54	.130	0.44
Cyber Insurance	1.03	1.70	.655	2.80
Constant	-5.80	3.88	.159	0.00
Pseudo R^2			.42	
LR Chi^2	17 (n=32)			

Table 4: Logistic Regression, Detection Predicting Insider Attacks

	Logistic Regression Model			
Variable	***B***	***SE(B)***	***p***	**OR**
Cost	.29	.19	.114	1.34
Accidentally detected	-1.77	1.85	.339	0.17
Software detected	-2.75	1.74	.113	0.06
Detected by disruption	-.41	1.71	.813	0.67
Law enforcement notification	-.08	1.87	.967	0.93
Media reported breach	*			
Media reported similar attacks	-1.20	1.57	.447	0.30
Customer reported/detected	-1.21	1.87	.519	0.30
Staff reported/detected	-0.76	1.88	.687	0.47
Other internal non-routine control	*			
Constant	-.84	1.65	.609	0.43
Pseudo R^2			.20	
LR Chi^2	10 (n=39)			

*Omitted due to perfect prediction