Cybercrime Victimization among Virginia Businesses:

Frequency, Vulnerabilities, and Consequences of Cybervictimization

James Hawdon [1]

Katalin Parti [1]

Thomas Dearden [1]

Tancy Vandecar-Burdin [2]

Jay Albanese [3]

Randy Gainey [2]

[1] Virginia Tech

[2] Old Dominion University

[3] Virginia Commonwealth University

Key words: Cybercrime; Victimization; Cybersecurity

Funding provided by COVA CCI (Coastal Virginia Center for Cyber Innovation Commonwealth Cyber Initiative) Number: C-Q122-ODU-05.

Cybercrime Victimization among Virginia Businesses: Frequency, Vulnerabilities, and Consequences of Cybervictimization

Abstract

The Commonwealth of Virginia, US, is one of the most vulnerable states to cyberattacks and breaches. Analyzing data from 428 online surveys collected from Virginia businesses from multiple vendors and several unique resources, this study provides an in-depth view of the nature and extent of cybercrime victimization in Virginia, highlighting specific vulnerabilities, how the victimization occurred, the consequences of victimization, and if and to whom these breaches were reported. In addition, we describe the extent to which businesses perceive their vulnerabilities, the extent in which companies engage in behaviors that can potentially make them vulnerable, the policies and practices they have in place to reduce vulnerability, and their experiences with victimization. The results provide a quality baseline for understanding cybercrimes against businesses in Virginia.

Acknowledgement: Funding provided by COVA CCI (Coastal Virginia Center for Cyber Innovation Commonwealth Cyber Initiative) Number: [C-Q122-ODU-05].

Cybercrime Victimization among Virginia Businesses

Introduction

The virtual world, with its billions of anonymous actors, provides an environment ripe for a variety of crimes. Personal data on our computers, cell phones, and other "smart" internet of things (IoT) devices have become targets for cybercriminals. Indeed, surveys find that approximately 23 percent of American households experience some sort of cybercrime annually (Reinhart, 2018), cybercrime cost the world $6 trillion in 2021, and experts predict cybercrime costs will reach $10.5 trillion annually by 2025 (Morgan, 2020). Thus, cyber-theft will far outstrip more traditional forms of thievery, such as larceny and robbery.

In an attempt to combat the growing threat of cybercrime, global spending on cybersecurity was expected to exceed $145 billion in 2020 (Smith & Lostri, 2020). While cybersecurity efforts undoubtedly help, better information is needed to know whether or not this spending is adequate and directed at the greatest risks. That is, a better understanding of cybercrime activity is needed to prevent it more effectively, minimize its consequences, and provide support for victims. Such an understanding is dependent on valid and reliable baseline data that identifies the specific nature, extent, and outcomes of cybercrime activity. Some important efforts have been made through various surveys conducted on specific types of cybercrime, with different samples of respondents, and often designed for specific audiences (Criminologists Without Borders, 2018; Drew, 2020; Harrell, 2019; Hawdon, Parti & Dearden, 2020; Langton, 2011; National Retail Federation, 2020; Ponemon Institute, 2018; Prislan et al., 2019; Rantala, 2008), but these are limited in many respects. Here we attempt to address some of the limitations of other efforts by creating surveys for businesses and administering them to business representatives in the Commonwealth of Virginia. Our results provide an in-depth view

of the nature and extent of cybercrime victimization in Virginia highlighting specific vulnerabilities, how the victimization occurred, the consequences of victimization, and if and to whom these breaches were reported.

The impact of cybercrime on businesses

There is a significant shortage of studies examining cybercrime in businesses. Among the few studies published, only a handful of them are written by academics (e.g., Anderson et al., 2013; Klahr et al., 2016; 2017) and all concern Western European countries. Moreover, except for a very few (Weijer van de et al., 2021; Paoli et al., 2018) that collected their own data, they overwhelmingly rely on secondary datasets. These analyses aimed to measure the scope of cybercrimes suffered by businesses, the harms and costs of cybercrimes and breaches, the vulnerabilities, and businesses' levels of preparedness. In the following, we provide an overview of the studies examining businesses' cybervictimization and the harm they suffered. Then we shift to describing the results of the first comprehensive research examining Virginia businesses' cybercrime victimization. We conclude by discussing what it means in terms of vulnerabilities and offer recommendations both for businesses and law enforcement.

The Bureau of Justice Statistics was among the first to conduct a comprehensive survey on cybercrimes affecting businesses. Among the 7,818 businesses that responded to the National Computer Security Survey (Rantala, 2008), 67% reported at least one cybercrime in 2005. Of the businesses responding to the survey, telecommunications businesses (82% of these businesses), computer system design businesses (79%), and manufacturers of durable goods (75%) had the highest prevalence of cybercrime. The most common offenses included getting a computer virus (58%), denial-of-service attack (16%), vandalism or sabotage (5%), fraud (5%), theft of intellectual property (3%), and theft of personal or financial data (3%). Most (86%) victimized

businesses detected more than one incident, and large businesses were more likely to experience cybercrimes than smaller businesses. Among the detected incidents, 80% were reported within the business (updating the senior management), 15% were reported to law enforcement and another 15% were reported to another outside organization.

To measure impact, harm, and costs, Paoli et al. (2018) administered a web-based survey to a national representative sample of businesses in Belgium in the summer of 2016. They elicited 310 valid responses (4.9% response rate). Participation was voluntary, resulting in large businesses being overrepresented and small businesses underrepresented in the final sample. Two-thirds of the businesses (66.5% or 181 businesses) had been victims of at least one cybercrime in the last 12 months. Specifically, 50% of impacted businesses reported illegal access and 44% data/system interference; however, 24.1% admitted cyber extortion (i.e., ransomware), fewer (12.9%) reported internet fraud (8 advance fee fraud, 22 internet banking fraud, one auction fraud), and 3.6% cyber-espionage. Out of the cybercrimes suffered, the most impactful was extortion, where 59 of the 66 victimized businesses reported having been requested to pay ransom money, some of them having to pay protection money as well. The majority of victimized businesses suffered multiple attacks, 83.2% of the victims reported repeated incidents of illegal access, 72.7% of data/system interference, 62.9% of internet fraud, 57.4% cyber extortion, and 40.0% of cyber espionage. Overall, victimization rates were higher for large businesses than for medium-size businesses and higher for medium-size businesses than small businesses. As for the harms suffered, most victimized businesses resolved the last incident of illegal access, data system interference, and cyber extortion in less than a business day.

In another study, by Statistics Canada (Wanamaker, 2019), 10,794 Canadian businesses with ten or more employees across all sectors except government and public administration were

sampled in 2017. Only 20.8% of businesses experienced cybercrimes with larger organizations experiencing more offenses than smaller ones. Private sector enterprises in Europe report similar victimization rates – between 2% and 16 % – for acts such as data breaches due to intrusion or phishing (UNODC, 2013).

The UK Cyber Security Breaches Survey (2020) consisted of a random probability telephone survey of 1,348 UK businesses in 2019. The data were weighted to statistically represent businesses in the UK. Regarding vulnerabilities, around half of businesses (53%) said that their organization allows the use of personal devices such as personal non-work laptops to carry out work-related activities, known as bring-your-own-device (BYOD). Almost half of businesses (46%) reported having at least one cybersecurity breach or attack in the last 12 months. The most frequently experienced cybercrime within the past 12 months was getting fraudulent emails or being directed to fraudulent websites with 86% of businesses that suffered a cybercrime experiencing it. Impersonation of the organization (26%), getting viruses, spyware and malware (16%), hacking or attempted hacking of online bank accounts (9%), ransomware (8%), unauthorized use of computers, networks or servers by outsiders (6%), unauthorized use of computers, networks or servers by staff (3%), and other breaches or attacks (5%) were also reported. Among the 46% of businesses that have experienced breaches or attacks in the past 12 months, phishing attacks were considered by far the most disruptive types of attack.

Veenstra et al. (2015) conducted an online survey study among a randomly selected sample of 8,000 small and medium enterprises (SMEs) in the Netherlands, consisting of 2-50 employees. Out of the selected, 1,203 participated in the survey. They found that only 28.5% of SME suffered cybercrime in the last 12 months. The most common forms of cybercrime among entrepreneurs were malware, e-fraud, phishing and hacking. However, just five years later,

Weijer van de et al. (2021) found that 57.8% of Dutch businesses were victimized by cybercrime in the past 12 months. The latter study used a sample of 529 Dutch SME owners and examined the characteristics of the offense, and victims' reporting activities. Respondents were most likely victimized by phishing (23.0%), malware (22.2%), and online consumer fraud (14.3%). In line with previous studies (Wanamaker, 2019), the results show that most SME-owners do not report cybercrime victimization to the police. Only 14.1% of the victims reported the crime to the police, but 32.3% reported to other organizations such as banks, credit card companies, online marketplaces, and helpdesks.

Harm and costs

There are two different kinds of harms that exist: quantifiable (material) and unquantifiable (non-material). While loss of revenue and monetary indicators (e.g., stock exchange price) are quantifiable, loss in reputation and privacy, as well as time spent on recovery are difficult to quantify or are unquantifiable; hence, it is difficult to measure harm according to these factors. The UK Cyber Security Breaches Report (2020) shows that, besides direct costs associated with breaches, recovery costs include additional staff time needed to deal with the breach or to inform customers or stakeholders, costs to repair equipment or infrastructure, and other associated repair costs. In contrast, the long-term costs of breaches include: the loss of share value, loss of investors or funding, long-term loss of customers, costs from handling customer complaints, compensation, fines, and legal costs.

Research shows that incidents related to security vulnerabilities in a company's server can result in long term indirect financial effects, such as losing customers due to privacy concerns. Acquisti et al. (2006) found that data breaches affecting the integrity of personal information resulted in significant loss of trust and in reputation which had measurable

ramification on the company's market share and stock prices (Johnson et al., 2018). The larger the firm, the more significantly their trust reputation is likely to be affected by negative reports (Acquisti et al., 2006). Social media exposure of data breach further exacerbates the stock price reaction to a data breach announcement (Rosati et al., 2019). Moreover, there is a high correlation between company size and the existence of repeat data breaches (Johnson et al., 2017), as large firms are more likely to experience subsequent data breaches than smaller ones.

Examining over 12,000 cyber events, including data breaches, security incidents, privacy violations, and phishing, Romanosky (2016) found that cybercrime had a relatively modest impact on US businesses between 2004 and 2015. Specifically, the cost of a typical cyber incident was less than $200,000, or about the same as the firm's annual IT security budget -- which represents only 0.4% of their estimated annual revenues.

Overall, the results do not show a dramatic financial impact of cybercrimes on businesses: just under half of the businesses admitted to having suffered at least one cybersecurity breach in the past 12 months (Paoli et al., 2018). Almost 60% of the victimized businesses indicated that the breach had no significant impact. The median cost for all breaches experienced in the last 12 months, even for the most disruptive breach, was zero dollars. However, a few businesses suffered a serious breach with losses increasing with business size (Klahr et al., 2017; Paoli et al., 2018). Serious harm includes monetary loss, recovery costs, time and money spent on recovery/neutralizing the attack/breach, and loss of services to customers, as well as loss to reputation and privacy. Even in cases of cyber extortion (ransomware), only a few businesses reported catastrophic harm that led to the business reporting bankruptcy. On the other hand, business data breaches resulted in more serious outcomes involving reputational, privacy, and perhaps subsequent harms when stolen identifying information is sold or distributed to third

parties. Major data breaches against Yahoo, Target, Adobe, Marriott, Facebook, Anthem health insurance, the U.S. Office of Personnel Management, among others, exposed both personal and financial information of many millions of victims (Todd, 2022; Vojinovic, 2022). The long-term impacts of these breaches are difficult to measure, but are significant at least in the short term (Setiawan et al., 2018; Smith et al., 2019).

Controls in place and vulnerabilities

Controls in place prevent cybersecurity breaches. According to the UK Cyber Security Breaches Survey (2020), 90% of organizations applied software updates, 88% applied updated malware protection, 83% had firewalls covering entire IT networks and individual services, 69% backed up data frequently, 69% allowed to access data only through company-owned devices, 57% of businesses had rules in place for storing and moving personal data securely, 38% monitored user activity, and 35% maintained separate Wi-Fi networks for visitors (UK Cyber Security Breaches Survey, 2020).

Amrin (2014) conducted a pilot study with 16 interviews with small and medium enterprises (SMEs) in the Netherlands, Austria, and the UK (organizations with fewer than 250 persons) in cyber victimization, prevention, and cyber security practices. Results showed that antivirus, anti-malware, anti-spam, and anti-phishing software were the most commonly used security technologies in SMEs. IT security policies were still not common practice among SMEs, as less than half of the participants had written IT security policies in place. In addition, almost 62% of respondents said they allowed their co-workers to work on their own devices. However, most participants did not take preventive measures such as remotely wiping stolen devices or using mobile device management software for BYOD threats.

Reporting incidents

Even though the breaches can put companies on hold with operations and push them to spend extra amounts on recovery, they are not necessarily reported, and evidence suggests that they are often not reported. According to the UK Cyber Security Breaches Report (2020), among the 46% of businesses that identified breaches or attacks, 91% informed their senior managers of the most disruptive breach, but only 38% of them reported them to an agency outside the organization. Even among external agencies, the police were informed only in 9% of the cases, after banks, credit card companies (22%), internet service providers (17%), and customers (13%). The main recurring reason that organizations gave for reporting a breach externally was that it resulted in a significant loss of internal data or money. Similarly in Canada (Wanamaker, 2019), only 10% of victims reported incidents to the police. Overall, the larger the size of the business, the more likely it reported cyber incidents to the police. Incidents were often resolved internally or through an IT consultant or were thought to be too minor to report.

Other studies (Weijer, van de et al., 2019; 2020; 2021) found that cybercrime victims more often report their victimization to organizations other than the police. Many victims who did previously report cybercrime victimization to the police were (very) unsatisfied with the way the police handled their reports, as the police were indifferent, and their problems were not solved (Weijer van de et al., 2021). Previous studies also reported dissatisfaction with how the police deal with victims of cybercrime, as they often feel like they are not taken seriously or even sent away from the police station (Cross et al., 2016; Leukfeldt et al., 2019). In contrast to previous studies (Veenstra et al., 2015; Wanamaker, 2019), according to which large businesses are more inclined to report, Weijer van de et al. (2021) found no relationship between business size and cybercrime reporting intentions and behavior.

In summary, the above studies found that most businesses do not experience significant cyberattacks and breaches, and if they do, they handle the effects in a short time neutralizing the situation. In addition, only larger businesses were significantly more affected than smaller ones; however, they did not report most of the incidents to external organizations (such as the police) fearing that the spread of the news would cause reputational damage. That means, most incidents stay unreported.

Below we summarize our empirical findings from Virginia with two goals in mind. First, these data can hopefully help guide a strategy to collect reliable cybercrime data. We believe an ongoing effort similar to the Bureau of Justice Statistics' *National Crime Victimization Survey* that is devoted to cybercrime among businesses is needed in the US. These data, while limited in scope to Virginia, provide guidance for how to collect such data. Our second goal is to demonstrate the value of such data. Specifically, these data can guide efforts to combat cybercrime by detailing which cybercrimes should be prioritized given their frequency, methods used, harms caused, and incident responses. The traditional approach toward cybersecurity of relying on target hardening is fundamentally insufficient because it excludes major parts of the criminal event, including an understanding of the offender, victim, and the interaction between the two. These data will improve our *understanding of the human element* of the criminal event, which is fundamental to reducing vulnerability to offenders (De Kimpe, Walrave, Verdegem & Ponnet, 2021).

We begin with the results of the survey conducted with Virginian businesses. We then offer a preliminary analysis of what factors predict victimization. Next, we turn to the implications of the results by discussing what these data mean for cybersecurity efforts,

including efforts to better educate residents, business owners, and law enforcement on ways to deter cybercriminals.

Methods and Sample

Our goal was to provide basic information about the cybercrime experiences of businesses in Virginia. To obtain sufficient numbers of participants, we relied on multiple vendors and several unique resources. These resources included 2,810 business contacts from a paid vendor, *Exact data* and 241 Virginia business contacts through the Virginia Tech alumni network. A random sample was selected from these lists of businesses, and employees identified as being involved with the business's IT were sent invitation emails. When we could not identify a specific individual involved with IT, we emailed the manager or owner. We also attempted to call a subset of these sampled businesses. In addition to these businesses, we also identified an additional 50 businesses from local library directories, and these businesses were contacted by email and follow-up phone calls. Finally, we collected 428 online surveys from Virginia businesses using respondents recruited by CINT USA, the largest consumer network for digital survey-based research. In total, we had 479 completed surveys. However, 13 respondents did not answer the initial IRB question and 15 businesses were not located in Virginia, so these 28 cases were removed from the sample. Removing these respondents resulted in a final sample of 451 Virginia businesses. Due to multiple sampling procedures, data collection took place from February 11 till May 10, 2022, the largest sample (CINT) being collected May 9-10, 2022.

The final sample provided good variability in terms of company size and sector. Nearly a quarter of all companies had fewer than 10 employees, but another fifth had more than 1,000. Table 1 reports information about the businesses' number of employees.

< Table 1 >

The modal sector was "other," representing the diversity of Virginia's economy; however, the information technology sector was well represented with nearly one-quarter of respondents coming from that sector. This reflects the fact that Virginia has the highest number of technology workers in the country (Migiro, 2020). The healthcare and financial sectors are also well represented in the sample. Table 2 present data on the businesses' sector.

< Table 2 >

Survey tool

In compiling the survey tool, we applied a shortened version of the UK Cyber Security Breaches Survey (2020). The questionnaire was distributed via QuestionPro, a web-based survey platform. The survey link was sent out to businesses' representatives, asking screening questions in the email about whether the addressee was the most knowledgeable about the organization's cybersecurity experiences. If the addressee was not the most knowledgeable, they were asked to forward the survey link to a representative meeting this criterium. After a brief introduction section that informed participants about the goal of the research, anonymity, voluntariness, and IRB details, the survey asked whether the participant wished to proceed, had they considered themselves being the most knowledgeable about the business' past cybersecurity experiences. The survey included a screening question about the businesses' location, in order to be able to filter out non-Virginian businesses. Next, the survey asked about business demographics (e.g., sector, number of employees), vulnerabilities (e.g., the company's online presence, option for customers to order online, customer data stored electronically, whether BYOD is allowed), actual preparedness or controls in place (e.g., how high a priority is cyber security to your company; do you provide regular cyber security training for employees), cybercrime attacks and

breaches (e.g., has your company experienced the listed cyberattacks or breaches; what was the most recent breach; did you report it externally or internally), 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), perceived preparedness to cyberattacks (e.g., how likely do you think in the next five years the US or your public infrastructure will experience a significant cyberattack; how well prepared do you think businesses, and your business are to prevent such attacks, all with a 1-4 Likert scale). The questionnaire took approximately 12 minutes to complete.

Results

We focus primarily on descriptive statistics as our goal is to describe the cybercrime experiences of Virginian businesses. Specifically, we aim to describe the extent to which these companies perceive their vulnerabilities, the extent to which these companies engage in behaviors that can potentially make them vulnerable, the policies and practices they have in place to reduce vulnerability, and their experiences with victimization. We then include a preliminary analysis that predicts if a company was victimized or not based on their vulnerabilities and practices and policies they use to reduce their vulnerabilities. Finally, a description of what type of attack or breach is most damaging, if they reported the incident to anyone, and the consequences of the attack is also provided.

Perceived Vulnerabilities

First, to assess perceptions of vulnerability of Virginia businesses, respondents were asked how likely they thought the United States would experience a significant cyberattack on our public infrastructure such as our air traffic control system or power grid. Respondents were

pessimistic about the nation's cyber-safety. Of the 446 respondents who provided answers, 316 (70.8%) said that such an attack would probably or definitely happen, with a full 28.5% saying it would definitely happen. Only 38 respondents (8.9%) said a major cyberattack definitely would not happen within the next five years. Respondents were also somewhat pessimistic about the preparedness of U.S. businesses to prevent cyberattacks. Only 69 of 422 respondents (16.4%) said they thought that U.S. businesses were "very prepared" for preventing an attack. However, respondents were more optimistic about their own company's preparedness as 128 of 422 respondents (30.3%) said their business was very prepared to prevent an attack on their system. As can be seen in Table 3 that reports the complete results for these two items, the contrast in perceptions of preparedness of the country's businesses as a whole compared to the respondent's business is striking. While over 81% of respondents believe their company is at least somewhat prepared for an attack, only 57% of respondents think that is true of the business community at large.

< Table 3 >

This relative confidence about their company's preparedness is also reflected in the responses about how businesses prioritize cybersecurity. Most businesses (380 or 86.6%) say that cybersecurity is of high or very high priority for their company. While this may seem somewhat low, cybersecurity importance varies by sector. For example, over 90% of the companies in defense, transportation, IT, finance, communications, and real estate say cybersecurity is a high or very high priority for their company. Conversely, only 78.9% of the companies in consumer discretionary, 63.6% of the companies in materials, and 79.1% of those in "other" sectors report that cybersecurity is of high importance. It therefore appears that the respondents from businesses in sectors that operate more in the virtual world and are therefore

the most vulnerable to cybercrime are most likely to believe their company considers cybersecurity to be a high priority.

Actual vulnerabilities

Yet, it is possible that respondents are under-estimating their businesses' vulnerabilities. A majority of businesses are connected to Internet in at least one way that increases their vulnerability. For example, 290 (64.3%) have accounts or pages on social media sites such as Facebook, Twitter, or LinkedIn. Another 256 (56.8%) provide their customers with the ability to order, book, or pay for products online, 250 (55.4%) store customer's personal information electronically, and 241 (53.4%) have online bank account for the company. Only 23 (5.1%) businesses we contacted reported that they are not linked to the virtual world in any of these ways. Moreover, 356 (78.9%) said employees in their company use personally owned devices to carry out regular work activities and, perhaps more concerning, another 14 (3.1%) did not know if this was the case. All of these behaviors or practices provide possible avenues for cybercriminals. Despite these relative risks of victimization, only 58.8% (265) of the surveyed businesses provide regular cybersecurity training to their employees, and approximately 20% of companies update their senior management about cybersecurity only once a year or less.

Moreover, it appears that not as many companies are following recommended safety precautions as probably should be. Respondents were presented with several rules or controls that are recommended to protect computers or systems from cyberattacks, and then, in a multiple answer question, they were then asked to indicate which of these rules or controls their business had in place. As can be seen in Figure 1, a majority of surveyed business failed to have most controls in place. The most frequently used controls were technological solutions for computer viruses and malware. Routine software updates were mentioned by 61.2% of respondents, and

57.2% and 51.9% of respondents noted their companies used current malware protection and used firewalls for the company's network. It is somewhat surprising that less than two-thirds of companies took these basic cybersecurity precautions, but even fewer took additional steps to avoid attacks. Less than half of respondents noted their companies did such routine security practices as having policies that required strong passwords, restricted IT access to a few employees, or backed up data. Approximately one-third of companies monitored user activities, had rules for personal data files, or had separate Wi-Fi for staff and visitors. Somewhat surprisingly, only 29.2% of respondents said their companies used two-factor authentication for logging on to the company's network, and only 26.6% of respondents said their company limited access to the company's devices. Looking at these figures, it appears that Virginia's businesses are seriously vulnerable to cyberattacks.

< Figure 1 >

Victimization

We then investigated the extent to which Virginia businesses experienced cybercrime attacks. Respondents were asked about a series of cybercrimes and to identify the ones their companies had suffered. They were asked to identify those that the company ever suffered, those experienced in the past 12 months, and those experienced both in the past 12 months and prior to the past 12 months. In total, 386 of the 451 companies (85.6%) have been victimized by a cybercrime at some time, and 323 (71.6%) of the companies had suffered some sort of cybercrime victimization in the past year. Well over half (59.8%) of Virginian companies experienced at least two types of victimizations in the past year, and over 40 companies (9.5% of the total) experienced 9 or 10 victimizations in the past year. Clearly, cybercrime is common, and Virginian businesses are frequent targets.

The most common type of attack is for staff to receive fraudulent emails or being directed to fraudulent websites. Over 80% of companies report that this has happened at some point, and 268 (59.4%) report that this has happened in the past 12 months.

< Figure 2 >

Predictors of Victimization

We also investigated what factors, if any, could predict victimization. To predict which businesses were victimized in the past year, we conduct a binary logistic regression analysis. Companies were coded as victimized in the past year (1) or not (0), and this variable was regressed on the size of the business, if the business places a high priority on cybersecurity, if they engage in behaviors/practices that increase their vulnerability and if there are measures they take to reduce vulnerabilities. The behaviors that can possibly increase vulnerability included having pages on social media sites, providing customers the ability to order/purchase online, storing customer's personal information electronically, having an online bank account for company, or allowing employees to use personally owned devices to carry out business. All of these variables were coded as 1 if they reported doing the behavior and 0 if they did not report doing the behavior. Similarly, the 12 cybersecurity policies and practices reported in Figure 1 were also entered as indicator variables. These include software updates, malware protection, firewalls for entire network, password policies for strong passwords, restricted IT access, security controls on company devices, backing up data securely, monitoring user activity, having rules for personal data files, having separate Wi-Fi for staff and visitors, the use of two-factor authentication to log on to company computers, and limiting access to company devices.

Table 4 reports the results of this analysis. Given the exploratory nature of the analysis, we only include the variables that approached statistical significance. Overall, the trimmed model including only those variables that approach statistical significance was an improvement over the baseline model ($\chi^2_{4\ df} = 30.61$; $p < .001$; -2 log likelihood 444.03; Nagelkerke $R^2 = .105$).

< Table 4 >

Company size significantly increased the likelihood of being victimized in the past year (odds ratio = 1.19; p = .031). Companies without separate Wi-Fi for visitors and employees were significantly more likely to experience a victimization in the past year than were those with such policies (odds ratio = 1.83; p = .041). Not having such a policy increased victimization chances by approximately 83%. Companies without strict data storage policies were more likely to be victimized, but the effect only trended toward statistical significance (odds ratio = 1.54; p = .128). The extent to which a company places priority on cybersecurity was positively related to victimization (odds ratio = 1.41; p = .031). This result is either ironic or, more likely, it is the result of companies that have been victimized are more likely to make cybersecurity of priority. Unfortunately, we are unable to determine if this is indeed the case since we lack longitudinal data.

Most Disruptive Attacks

Respondents were also asked to identify one cybersecurity breach, or related series of breaches or attacks, that caused the most disruption to their company in the last 12 months. Only 135 of the 323 companies that were attacked in the past year provided answers to the question, but their responses are nevertheless informative. The most disruptive type of attack among the

companies that provided a response was their computers becoming infected with viruses or spyware, as 25 companies (18.5%) mentioned this crime as the most disruptive. Almost as many companies reported fraudulent emails to staff and someone impersonating their company as being the most disruptive (24 and 22 companies, respectively). Figure 3 reports the type of attack that each of the 135 reporting companies considered to be the most disruptive over the past year. It should be recognized here that these numbers do not necessarily reflect that computer viruses should be considered more disruptive than ransomware or attacks on a company's online banking. Instead, these numbers simply reflect the attack each company considered to be the most disruptive. If the only attack a company suffered was a computer virus, that would obviously be the most disruptive for them. Given the missing data on this question and the fact that companies had different victimization experiences over the past year, we cannot identify what crime is ultimately the most disruptive.

< Figure 3 >

Who Reported

It is widely acknowledged that most cybercrimes go unreported. The Department of Justice estimates that only about one in seven cybercrime incidents are reported to authorities, and under-reporting is especially pronounced among businesses (U.S. Department of Justice 2018). Our data reflects this widespread under-reporting. Of the 386 companies that were victimized, 76 (19.7%) did not report the crime to anyone, and only a few respondents said they reported the incident to law enforcement. Only 12.0% of victimized businesses reported the incident to the FBI, 9.5% reported to the police, and 9.1% reported to the Department of Justice Taskforce. Another 7.1% reported the incident to the Federal Trade Commission, and another 6.9% reported to the Office of the Inspector General. Thus, reporting to government authorities

was not a common practice for our respondents. Figure 4 reports the percentage of victimized reporting the attack to various actors.

< Figure 4 >

However, of those that reported, several victimized companies reported the incident to multiple agencies or actors. For example, 69 (17.9%) reported to two agencies and 72 (18.7%) reported to three agencies or actors. Table 5 reports the number of agencies or actors to which the company reported their victimization.

< Table 5 >

While there are a variety of reasons cybercrimes go underreported, one factor that drives this is that respondents must know they have been victimized and must realize they have been victimized in a timely manner. To determine how businesses became aware of cyberattacks, respondents were asked to think about an incident that caused the most disruption to the company in the last 12 months and how was this breach or attack identified. Of the 62 companies that provided information, most (15 or 24.2% of those reporting) reported they discovered the breach or attack through antivirus or anti-malware software. An additional 10 (16.1%) reported that their staff noticed the breach. Table 6 reports the various ways victimized companies discovered the breach or attack.

< Table 6 >

When asked if they knew the identity of the person, persons, or entity (e.g. a hacking group) who committed the most significant cybersecurity breach, 25 of the 61 companies who reported said they knew the identity of the culprit, and of these, 15 of 24 (62.5%) said that the

person who committed the breach was an employee and 9 (37.5%) said it was an outsider (one did not answer the question). Among the 30 who did not know the identity of their attacker, 7 (23.3%) suspected an employee while 23 (76.7%) suspected an outsider.

Harm and cost

Finally, we also explored the consequences that companies suffered because of cybercrime victimization. First, respondents were asked to think of all the cybersecurity breaches or attacks experienced in the last 12 months and to identify all of the adverse results of the attack. Figure 5 presents the responses for the 386 companies that experienced a victimization. The figure includes both the number of companies experiencing each adverse result as well as the percentage of the victimized companies that experienced the specific result in the past year. Companies could list more than one adverse result.

< Figure 5 >

We also asked respondents if any of the breaches or attacks on their companies impacted the organization in various ways. Again, companies were able to report numerous impacts. Figure 6 reports the number of companies experiences each impact as well as the percentage of the 386 victimized that experienced each impact.

< Figure 6 >

Finally, we asked how much of an effect the cybersecurity breach had on their company. Only 62 companies provided answers to the question, but of those 39 (62.9%) said the breach had a “moderate” or “major” effect. About one third of those who responded said it had a “minor” effect, and only one respondent said the breach had no effect. Finally, we asked respondents to estimate the financial cost of the breach. Once again, only a handful of

respondents could provide answers, but the numbers from those who did are telling. Table 7 presents these results.

< Table 7 >

Discussion

This study provides the first of its kind in measuring the victimization, vulnerabilities (controls in place), and preparedness of businesses to cyberattacks and breaches in the Commonwealth of Virginia, US. On a large sample of businesses operating in the Commonwealth (n=451), we find a slightly different picture than communicated by previous studies on businesses' cybervictimization and prevention practices.

With most (85.6%) companies experiencing cybercrime, business victimization in our sample is much higher than in previous studies (Rantala, 2008; Paoli et al., 2018; Anderson et al., 2013; Klahr et al., 2017). In addition, well over half (59.8%) of businesses experienced at least two types of cybervictimization in the past 12 months, and 9.5% of all companies were frequent targets of cyberattacks, with staff receiving fraudulent emails being the most common and one of the most disruptive cybercrimes experienced. Besides fraudulent phishing emails, computer viruses, malware and spyware caused the most disruption. This is unsurprising since these types of attacks are subtle and can affect computer systems for a long time without the owner's knowledge (Jang-Jaccard & Nepal, 2014).

Businesses anticipate a significant cyberattack on the US public infrastructure in the near future. Media attention to ransomware attacks on critical infrastructure such as the Colonial Pipeline ransomware attack in the spring of 2021 that resulted in the shutdown of operations on the East Coast for six days (Turton & Mehrotra, 2021) likely influenced this anticipation.

Similarly, participants did not think businesses are generally prepared to fend off cyberattacks. However, they drew a much rosier picture about their own (perceived) preparedness. Given that participants do not have information about businesses' preparedness, this is likely a cognitive bias. According to the just-world theory (Lerner, 1980), people need to – or rather want to – believe that they live in a just world where they will receive what they earn and consequently earn what they receive. Therefore, it is feasible to think that participants consider their own businesses relatively more prepared for cyberattacks than they think businesses in general are because they have a false belief of being protected. Next, although an overwhelming majority of businesses considered cyber security a high priority in our study, only sectors operating mostly in the virtual world (having more online presence) considered it a *very* high priority. These businesses might be well aware of their vulnerabilities but nonetheless assume that other businesses can do better when it comes to prevention measures.

Yet our data show that businesses might falsely assume that they are protected from cybercrime. The majority of businesses are connected to the internet by having social media accounts, offering customers online ordering, storing customer information electronically, and having online bank accounts for the company, all of which increases vulnerabilities. Moreover, the BYOD practice (Amrin, 2014) that became mainstream because of pandemic-induced lockdowns and home-based working conditions (LexisNexis, 2021) further increase vulnerabilities. Despite most businesses admittedly making cybersecurity a high priority, just over half of Virginia businesses provides regular cybersecurity training to employees and only a fifth of businesses debrief senior management about cybersecurity on a regular level. This is slightly different from the UK Cyber Security Breaches Survey (2020) which reported that 66% of businesses updated senior management at least once a year about cybersecurity issues.

Furthermore, in the Virginian sample, many businesses failed to have recommended controls in place, which is similar to previous studies (Amrin, 2014; Cross & Gillett, 2020; Rantala, 2008; UK Cyber Security Breaches Survey, 2020). In these cases, like in Virginia, most businesses applied technology-based solutions such as antivirus and anti-malware protections, but less than half of respondents arranged routine security practices such as having policy that require strong passwords, IT access being restricted, or frequent data backups. Although two-factor authentication is increasingly popular as the number of businesses applying it grows every year (Cyberthreat Defense Report, 2022), our data show that only a quarter of companies limit employee activities to devices owned by the company.

According to research (National Cyber Security Centre UK, 2018; Barracuda, 2022), small and medium sized businesses might be more likely targeted by cyberattacks but, larger companies have increased capacity to recognize and fend off cybercrime, and it is possible that they apply more appropriate prevention and risk mitigation measures than smaller firms. Nevertheless, our data, in line with previous studies (Paoli et al., 2018; Anderson et al., 2013; Klahr et al., 2017; Rantala, 2008), suggest that larger businesses experience more cyberattacks and breaches than smaller companies.

In addition, among the controls in place, not having separate Wi-Fi for visitors and employees increased cyber victimization by a staggering 83%. (Although it was not possible to identify whether companies not offering separate guest Wi-Fi opened their Wi-Fi to the public at all.) Not having strict data storage policies were correlated with increased chances of victimization, although the effect was not statistically significant. Finally, prioritizing cyber security was positively associated with victimization, although we cannot tell if placing high priority on cyber security was a consequence of past victimization or they were victimized

despite taking cyber security seriously. A longitudinal analysis would be necessary to answer this question.

Despite cyberattacks and breaches being widely experienced, most cybercrimes go unreported (Weijer, van de et al., 2021; Kemp et al., 2021a; Kemp et al., 2021b; Wanamaker, 2019). Even if businesses report their loss, it is most likely to their own management or outside organizations rather than to law enforcement (Rantala, 2008; Kemp et al., 2021a; Wanamaker, 2019). Our findings are in line with past research, emphasizing that only a fraction of businesses that experienced cybercrimes reported the incident to government agencies such as the local law enforcement (9.5%), the FBI (12.0%), and the Department of Justice Taskforce (9.1%). Our study did not ask the reasons for such low reporting activities; however, other than fears of the negative publicity (Rantala, 2008), researchers have found that people do not believe government organizations can make a difference or they refrain from reporting because they already had unsatisfying experiences with them (Cross, 2020; Cross & Gillett, 2020; Kemp et al., 2021a). Cross (2020) found that individual victims of online fraud often report that their communications with government agencies were frustrating, and they often caused additional harm to the victim. While case handling might be different when businesses are victimized, as cybercrime against businesses more often lead to international arrests (Cross & Gillett, 2020), the risk of reputational damage of an organization likely drives the silence and failure to disclose this type of victimization to the police or the general public. Nevertheless, our data show that those who report (59.1% of the victimized businesses) usually report it to two or more outside agencies. Therefore, it is evident that businesses do want to report to someone, but maybe not to government agencies. It is therefore recommended that law enforcement make businesses and the public aware of the steps for reporting a cybercrime, why reporting is important, the possible

outcomes/benefits of reporting, and to be generally more transparent about the process after filing a report. In addition, the identity of the offender might explain the lack of reporting as 62.5% (n=15) of the companies who reported knew that the offender was an employee. In contrast, only 37.5% (n=9) said it was an outsider, although this must be interpreted with caution because of the low number of responses for this question.

Yet, we can say that businesses are adversely affected by these incidents so a lack of being harmed is not why they avoid reporting the crime to authorities. Contrary to previous studies stating that the median loss was $0 and the total recovery time was 24 hours even for the most disruptive attacks (Paoli et al., 2018; Anderson et al., 2013; Klahr et al., 2017), we find that cybercrime causes more loss and has a more serious impact on businesses in general. Most of the businesses that suffered loss and answered the question of impact size (n=62), said the breach had a moderate or a major effect. Only one third of impacted businesses said it had minor effect and just one organization admitted having no effect whatsoever. When it comes to monetizing harm, most businesses only lost less than $500, but half of the businesses lost somewhere between $10,000 and $500,000.

Government agencies spend a significant amount of money and human resources on investigating cybercrimes and educating citizens on prevention techniques (Dodge & Burruss, 2020). Keeping the above results in mind, it might be time for government agencies to reform investigation and awareness raising techniques. Instead of solely emphasizing target hardening, government agencies might consider building collaborations with private companies to improve response and with researchers to conduct program evaluations (Dodge & Burruss, 2020). A good example of such cooperative effort is the Electronic Crime Task Forces (ECTFs) established by the US Patriot Act in 2001. The ECTFs bring together local, state, and federal law enforcement

agencies along with prosecutors, private sector companies, and academics to investigate cyberattacks on financial and critical infrastructures (Dodge & Burruss, 2020). Yet, it seems that small and medium businesses may not be represented in this multidisciplinary, multi-agency approach and do not get support and encouragement to report cybercrime.

Limitations

The survey results are not directly comparable to other surveys for various reasons. First, we did not use a probability sample but instead, we strategically attempted to obtain a diverse and reasonably representative sample across the state. Similar to previous studies of cybercrimes among businesses (Amrin, 2014), it was hard to find participants. Second, although we have not anticipated that the length of the questionnaire (10-15 minutes in average) would hinder responses, it still might be one reason that we had used multiple sampling frames. A shorter questionnaire may have resulted in more participation but would clearly have reduced the value of the information we obtained. In fact, from our perspective, it would have reduced the importance of the study tremendously.

Further, we cannot tell exactly who might have been responding to the survey and variation in levels of knowledge among the respondents. If the person who filled out the questionnaire was not the most knowledgeable of the cybersecurity preparedness and victimization of the company, we asked them to forward the questionnaire to the person who was. This element potentially added to the self-selection bias already incorporated by making survey participation voluntary. In smaller organizations it is most likely to be someone in the management team who can fill out the survey with confidence. In larger organizations it might be the person responsible for IT security. However, we cannot control whether the survey was completed by the most knowledgeable person.

An additional concern to data validity derives from the fact that private and business internet use is strongly intertwined, and the majority of small and medium business owners use their computer for both private and business purposes (van de Weijer et al., 2021). As a result, it may be difficult to make distinction between private and work-related victimization. In addition, the data was collected after major ransomware incidents, such as the Colonial Pipeline attack, already have taken place. Indeed, such major incidents could alter companies' cybersecurity preparatory measures and how they react to cyberattacks. The current dataset, being cross-sectional in nature, could not specifically measure the effects of recent cyberattacks. However, this did not affect the sample's internal validity.

An additional concern involving the history effect is that while collecting the data, Strengthening American Cybersecurity Act of 2022, a significant legislative piece requiring businesses to report ransomware payment was passed by the Senate on March 1, 2022. Since most of the data was collected afterwards, it is likely that this legislation influenced the reporting of ransomware payments. However, being in the midst of the data collection, we could not possibly alter the survey; hence, the history effect of the legislation cannot be measured.

Taking into consideration all the above limitations, our assessment cannot draw a full picture of cyberattacks and their impacts on businesses. However, these limitations are common to most survey-based studies on cybercrime, and respondents' unawareness and unwillingness to report affect all studies relying on self-report victimization (Paoli et al., 2018). Thus, we are generally confident of the quality of the data as well as the diversity and representativeness of the sample. The data provide a quality baseline for understanding cybercrimes against businesses in Virginia.

Conclusion

This report is expected to help inform stakeholders: businesses, insurance companies, and policymakers. Given the major data breaches and cyberattacks that have occurred in the US and around the world, these data suggest that there may be wide variations in risk among states and other jurisdictions. In addition, given the fact that nearly two-thirds of our sample indicated moderate or major impacts from their cybervictimization, there are multiple kinds of costs and harms to be examined in the future beyond financial loss, including reputation, market-share, customer privacy, cybersecurity, and related harms that can be difficult to quantify.

Given the data presented here, businesses will better understand the risks they face; insurance companies can better estimate the risks of their insureds in order to foster a healthy cyber insurance market. Policymakers will better understand the context and impact of cyber events across industry in Virginia. Finally, it can inform businesses operating outside of Virginia as well, in the vulnerabilities businesses face today.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *Twenty Seventh International Conference on Information Systems, Milwaukee 2006 and Workshop on the Economics of Information Security 2006.* Retrieved December 6, 2022 from https://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf

Amrin, N. (2014). *The impact of cyber security on SMEs.* University of Twente. Retrieved August 14, 2022 from http://essay.utwente.nl/65851/

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.

Barracuda (2022). *Spear Phishing: Top Threats and Trends.* Vol. 7. Retrieved December 6, 2022 from ttps://assets.barracuda.com/assets/docs/dms/Spear-phishing-vol7.pdf

Criminologists without Borders. (2018). *Criminal Justice Responses to Prevent and Counter Cybercrime*. *criminologistswithoutborders.org.*

Cross, C. (2020). Responding to individual fraud: Perspectives of the fraud justice network. In R. Leukfeldt & T.J. Holt (eds.), *The human factor of cybercrime* (pp. 359-388), Routledge.

Cross, C., & Gillett, R. (2020). Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. *Journal of Financial Crime, 27*(3), pp. 871-884.

Cross C.A., Richards K.M., Smith R., (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice, 518,* 1-14.

Cyberthreat Defense Report (2022). *Cyberthreat defense report.* Cyber Edge Group. ISC2.org. Retrieved August 14, 2022 from https://www.isc2.org/-/media/ISC2/Research/Cyberthreat-

Defense-Report/2021/CyberEdge-2021-CDR-Report-v10--ISC2-Edition.ashx?la=en&hash=60BC7C7969857E2FF07B714896F079EF5C9C1C39

De Kimpe, L., Walrave, M., Verdegem, P. & Ponnet, K. (2021). What We Think We Know about Cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, DOI: 10.1080/0144929X.2021.1905066

Dodge, C. & Burruss, G. (2020). Policing cybercrime: Responding to the growing problem and considering future solutions. In R. Leukfeldt & T.J. Holt (eds.), *The human factor of cybercrime* (pp. 339-358), Routledge.

Drew, J.M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, vol. 6, 17-33.

Harrell, E. (2019). *Victims of Identity Theft, 2016*. Washington, DC: Bureau of Justice Statistics.

Hawdon, J., Parti, K. & Dearden, T.E. (2020). Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. *American Journal of Criminal Justice, 45,* 546–562. https://doi.org/10.1007/s12103-020-09534-4

Jang-Jaccard, J. & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005.

Johnson, M.S., Kang, M.J., & Lawson, T. (2017). Stock price reaction to data breaches. *Journal of Finance Issues, 16*(2), 1-13.

Johnson, M.S., Kang, M.J., Lawson, T., & Singh, A.J. (2018). The Impact of Data Breaches on Hotel and Restaurant Firm Stock Returns. *Journal of Hospitality Financial Management, 26*(2), 75-86. https://doi.org/10.7275/v8kg-hy29

Kemp, S., Buil-Gil, D., Miro-Llinares, F., & Lord, N. (2021a). When do businesses report cybercrime? Findings from a UK study. *Criminology and Criminal Justice,* https://doi.org/10.1177/17488958211062359

Kemp, S., Buil-Gil, D., Moneva, A., Miro-Llinares, F., Diaz-Castano, N. (2021b). Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice, 37*(4) 480–501. https://doi.org/10.1177/10439862211027986

Klahr, R., Amili, S., Shah, J. N., Button, M., & Wang, V. (2016). *Cyber security breaches survey 2016.* Retrieved August 3, 2022 from www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf.

Klahr, R., Shah, J. N., Sheriffs, P., Rossington, T., Pestell, G., Button, M., & Wang, V. (2017). *Cyber security breaches survey 2017.* Retrieved August 3, 2022 from www.gov.uk/government/statistics/cyber-security-breaches-survey-2017

Langton, L. (2011). *Identity Theft Reported by Households, 2005-2010*. Washington, DC: Bureau of Justice Statistics.

Lerner, M. J. (1980). The belief in a just world, In M.J. Lerner (ed.) *The belief in a just world: A fundamental delusion,* (pp. 9-30), Springer. https://doi.org/10.1007/978-1-4899-0448-5_2

LexisNexis (2021). *The new cybercrime landscape. Global risks, regional trends, industry opportunities.* LexisNexis Risk Solutions Cybercrime Report July to December 2020. Retrieved July 25, 2022 from https://risk.lexisnexis.com/insights-resources/research/cybercrime-report

Leukfeldt, E.R., R.J. Notté & M. Malsch (2019) Exploring the needs of victims of cyberdependent and cyber-enabled crimes. *Victims and Offenders,* https://doi.org/ 10.1080/15564886.2019.1672229.

Migiro, G. (2020). *What are the biggest industries in Virginia?,* World Atlas. *https://www.worldatlas.com/articles/what-are-the-biggest-industries-in-virginia.html*

Morgan, S. (2020). *Cybercrime to Cost the World $10.5 Trillion Annually by 2025.* Cybercrime Magazine. Retrieved July 28, 2022 from https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

National Cyber Security Centre, UK (2018). *The Cyber Threat to UK Business. 2017-2018 Report.* National Cyber Security Centre & National Crime Agency. Retrieved December 6, 2022 from https://www.nationalcrimeagency.gov.uk/who-we-are/publications/178-the-cyber-threat-to-uk-business-2017-18/file

National Retail Federation. (2020). *2020 National Retail Security Survey*. https://nrf.com/research/national-retail-security-survey-2020

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

Ponemon Institute. (2018). *Measuring & Managing the Cyber Risks to Business Operations*. https://www.tenable.com/ponemon-report/cyber-risk

Prislan, K. et al. (2019). Cybercrime victimization and seeking help: A survey of students in Slovenia. *Proceedings of the Third Central European Cybersecurity Conference*, vol. 24, https://doi.org/10.1145/3360664.3360731

Rantala, R.R. (2008). *Cybercrime against businesses, 2005.* Bureau of Justice Statistics Special Report. Retrieved July 28, 2022 from https://bjs.ojp.gov/library/publications/cybercrime-against-businesses-2005

Reinhart, R.J. (2018). '*One in four Americans have experienced cybercrime',* Gallup Politics. https://news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 2016, 121–135. https://doi.org/10.1093/cybsec/tyw001

Rosati, P., Deeney, P., Cummins, M., van der Werff, L., & Lynn, T.G. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in International Business and Finance, 47,* 458-469. https://doi.org/10.1016/j.ribaf.2018.09.007

Setiawan, N., Tarigan, V. C. E., Sari, P. B., Rossanty, Y., Nasution, M. D. T. P., & Siregar, I. (2018). Impact of cybercrime in e-business and trust. *International Journal of Civil Engineering and Technology, 9*(7), 652-656.

Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society*, *17*(1), 42-60.

Smith, Z.M., Lostri, E., & Lewis, J.A. (2020). *The hidden costs of cybercrime*. McAfee. Retrieved August 17, 2022 from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

Todd, D. (2022). *Top 10 data breaches of all time*. March 24, 2022. Secure World. Retrieved August 17, 2022 from https://www.secureworld.io/industry-news/top-10-data-breaches-of-all-time

Turton, W. & Mehrotra, K. (2021). hackers breached colonial pipeline using compromised password. *Bloomberg*. Retrieved July 22, 2022 from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password#xj4y7vzkg

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

United States Department of Justice. (2018). *Report of the attorney general's cyber digital task force*. Office of the Deputy Attorney General: Washington, D.C.

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

Vojinovic, I. (2022). 10 of the biggest data breaches in history. July 22, 2022. Retrieved August 17, 2022 from https://dataprot.net/articles/biggest-data-breaches/

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

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

Weijer, van de, S.G.A., Leukfeldt R., Zee, van der, S. (2021). Cybercrime Reporting Behaviors Among Small- and Medium-Sized Enterprises in the Netherlands. In M. Weulen Kranenbarg & R.

Leukfeldt (eds), *Cybercrime in Context. Crime and Justice in Digital Society,* vol 1. Springer, https://doi.org/10.1007/978-3-030-60527-8_17.

Weijer, van de, S.G.A., Leukfeldt, E.R., & Bernasco, W. (2019). Reporting crime to the police: a comparison between traditional crime and cybercrime. *European Journal of Criminology, 16*(4), 486-508.

Tables and figures

Table 1: Number of Employees in Sampled Businesses

	N	Percent
Fewer than 10	106	23.5%
10-49	74	16.4%
50-249	72	16.0%
250-999	75	16.6%
1,000 or more	97	21.5%
Missing or don't know	27	6.0%
Total	451	100%

Table 2: Sector of the Economy

	N	Percent
Defense	21	4.6%
Transportation	18	4.0%
Information Technology	101	22.4%
Healthcare	49	10.9%
Financials	29	6.4%
Consumer	19	4.2%
Communications	22	4.9%
Industry	19	4.2%
Real Estate	20	4.4%
Materials	12	2.7%
Other	141	31.3%
Total	451	100%

Table 3: Perceptions of Preparedness of US Businesses and Respondent's Business

	How Prepared are U.S. Businesses?		How Prepared is Respondent's Businesses?	
	Frequency	Percent	Frequency	Percent
Not at all prepared	40	9.5	16	3.8
Not too prepared	141	33.4	63	14.9
Somewhat prepared	172	40.8	215	50.9
Very prepared	69	16.4	128	30.3
Total	422	100.0	422	100.0

Figure 1: Cybersecurity Practices/Controls Currently Used by Virginia Businesses (%)

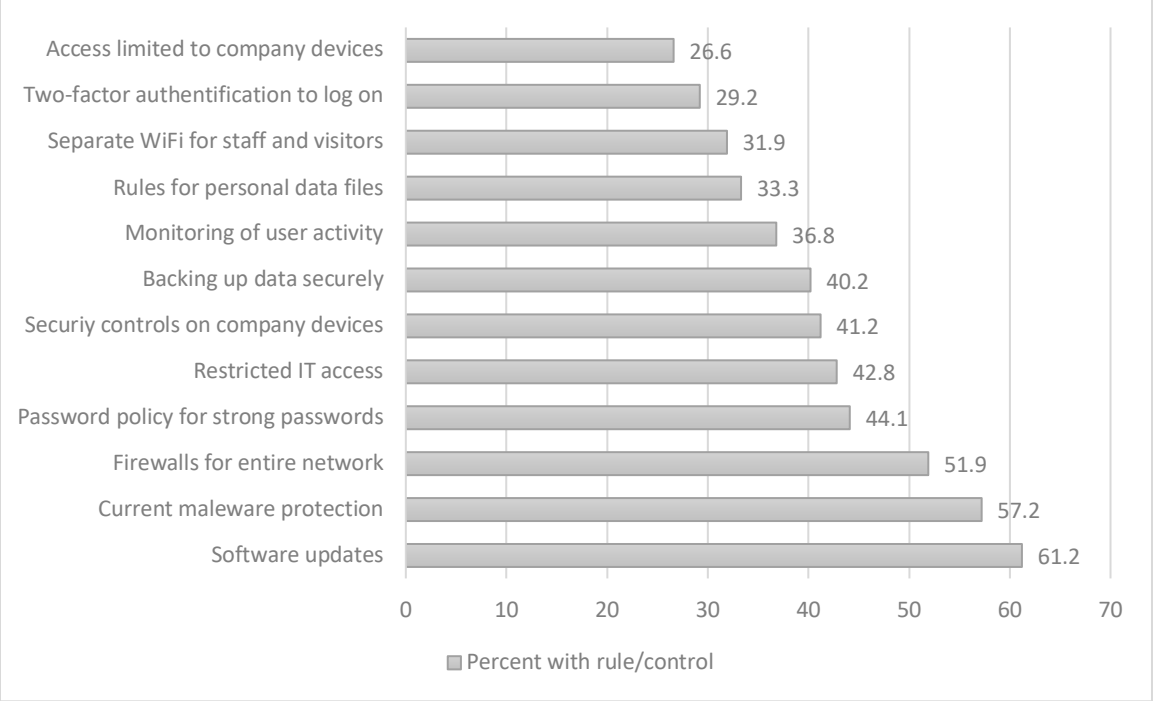

Figure 2: Types of Cybercrime Experienced by Virginia Businesses

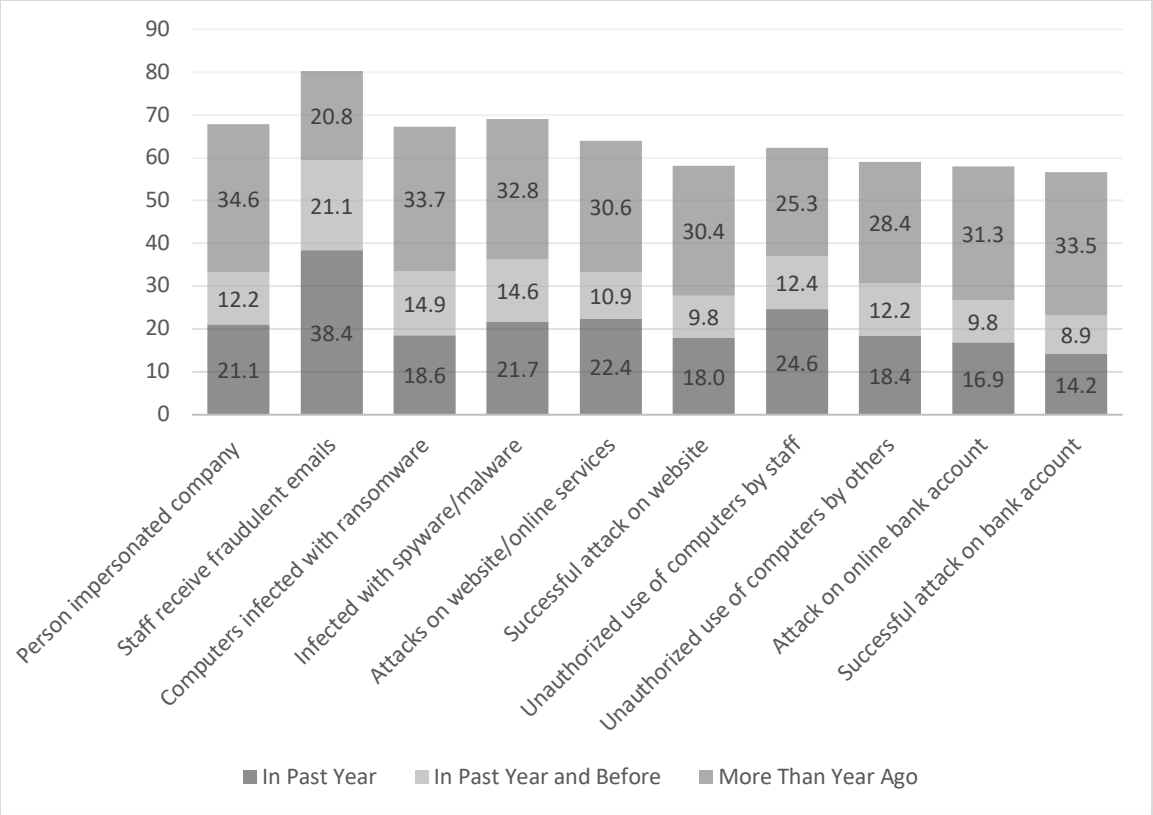

Table 4: Predictors of Past Year Victimization

	B	S.E.	Wald	Odds Ratio
Company size	.177 *	.082	4.67	1.19
Cybersecurity high priority	.344 *	.160	4.64	1.41
Company lacks strict data storage policies	.429 +	.282	2.32	1.54
Company has separate Wi-Fi for visitors	.606 *	.296	4.18	1.83
Constant	.058	.727	.006	1.060

+ $p<.10$; * $p< .05$

Figure 3: Most Disruptive Cybercrime in Past Year Identified by 135 Victimized Companies (%)

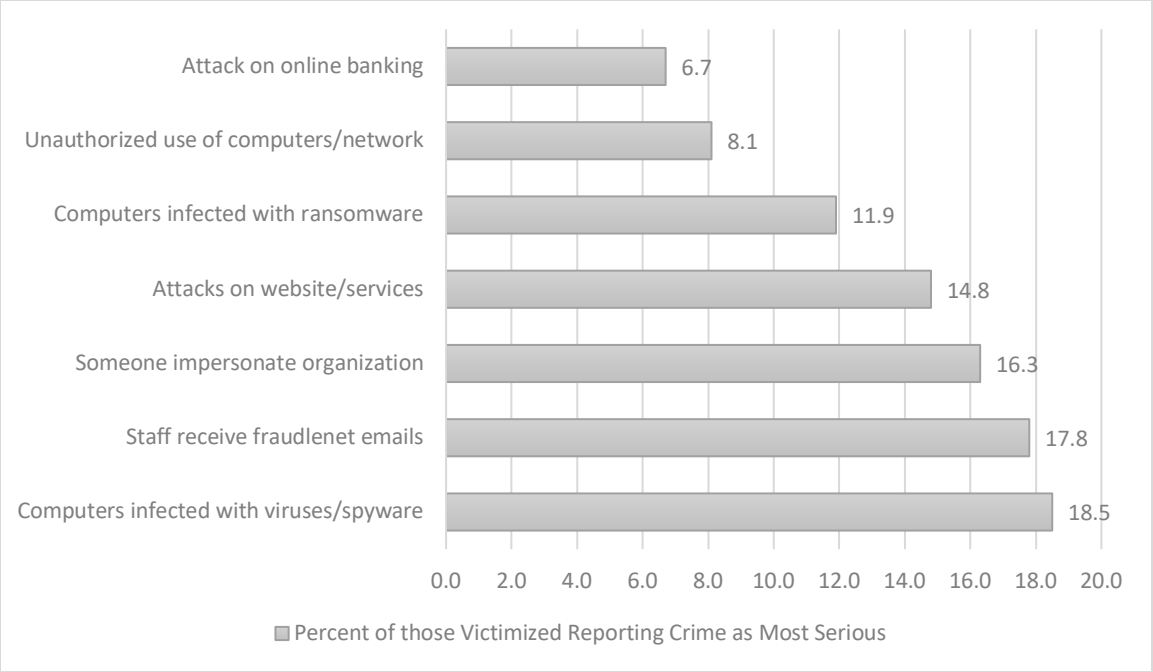

Figure 4: Percent of Victimized Companies Reporting Crime to Various Actors

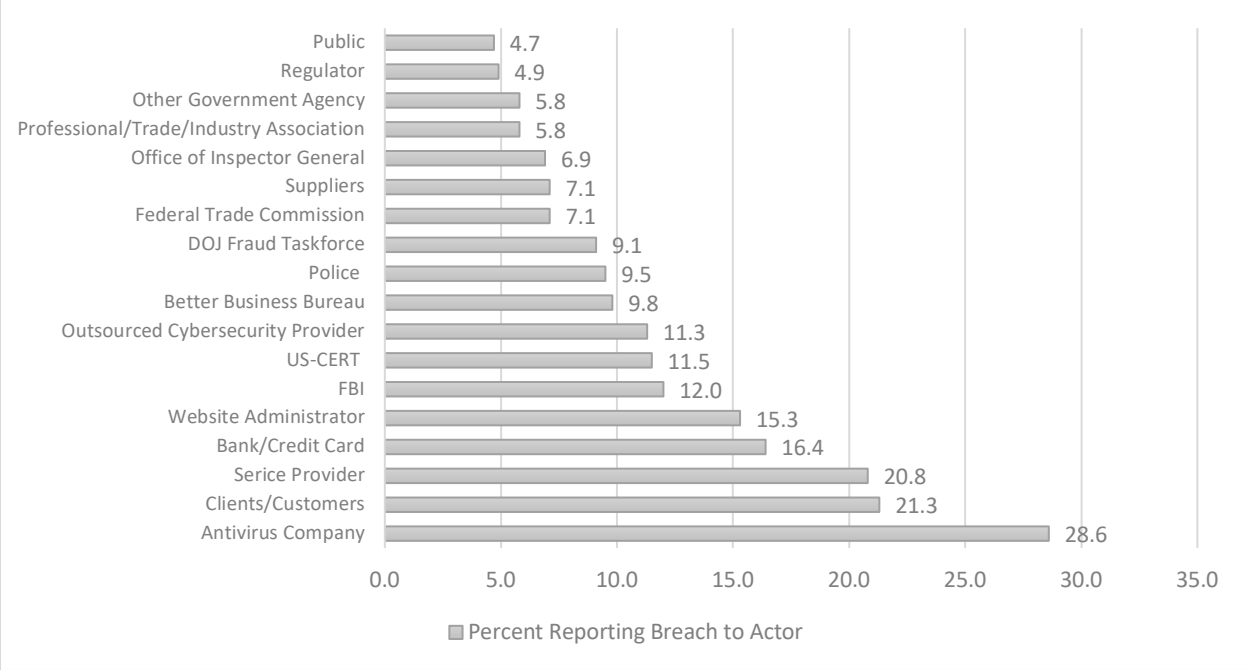

Table 5: Number of Agencies/Actors Company Reported Crime

	Frequency	Percent
Did not report victimization	76	19.7%
Reported to one agency	82	21.2%
Reported to two agencies	69	17.9%

Reported to three agencies	72	18.7%
Reported to four agencies	27	7.0%
Reported to five or more agencies	60	15.5%

Table 6: How was Breach or Attack Discovered

	Frequency (N=62)	Percent
By accident	4	6.5%
By antivirus/anti-malware software	15	24.2%
Disruption to business/staff/users/service provision	6	9.7%
From warning by government/law enforcement	4	6.5%
Breach/attack reported by the media	2	3.2%
Similar incidents reported in the media	9	14.5%
Reported or noticed by customer(s)/beneficiaries	7	11.3%
Reported or noticed by staff	10	16.1%
Routine internal security monitoring	2	3.2%
Some other means	3	4.8%

Figure 5: Reported Adverse Results of Cyberattacks

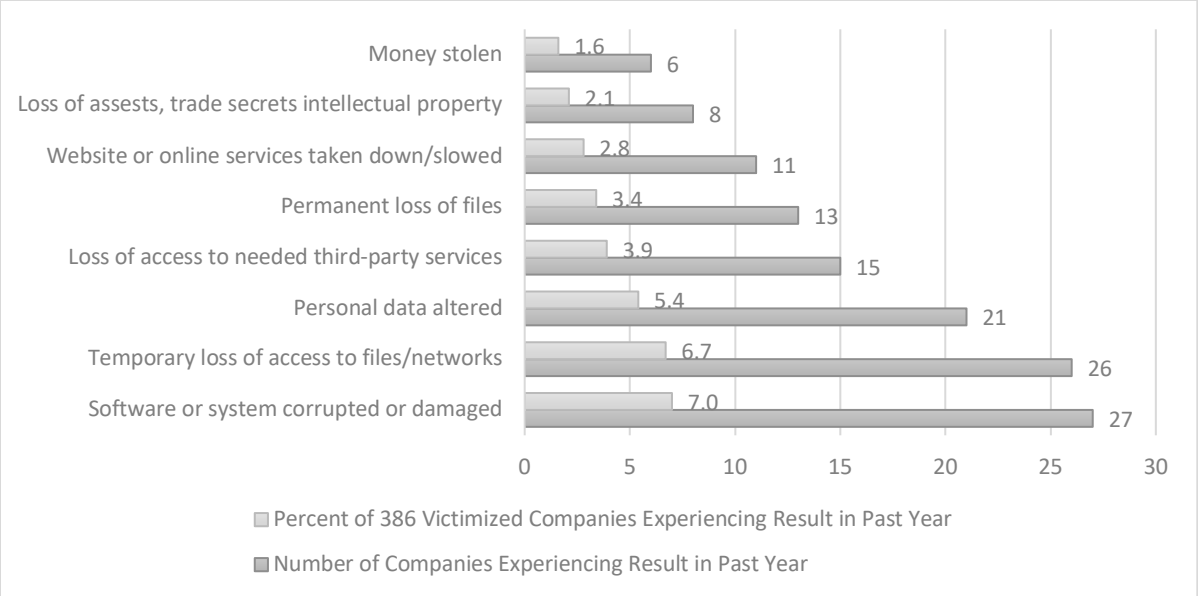

Figure 6: Impacts of Victimization

Table 7: Reported Financial Losses Due to Cybercrime Victimization

	Frequency	Percent
Less than $500	10	19.2%
$500 to less than $1,000	5	9.6%
$1,000 to less than $5,000	5	9.6%
$5,000 to less than $10,000	4	7.7%
$10,000 to less than $20,000	8	15.4%
$20,000 to less than $50,000	6	11.5%
$50,000 to less than $100,000	8	15.4%
$100,000 to less than $500,000	4	7.7%
$500,000 to less than $1,000,000	1	1.9%
$1,000,000 to less than $5,000,000	0	0.0%
$5,000,000 or more	1	1.9%
Total	52	100.0%