2022

# CIVIIC: Cybercrime in Virginia: Impacts on Industry and Citizens Final Report

Randy Gainey
*Old Dominion University*, rgainey@odu.edu

Tancy Vandecar-Burdin
*Old Dominion University*, tvandeca@odu.edu

Jay Albanese
*Virginia Commonwealth University*

Thomas Dearden
*Virginia Polytechnic Institute and State University*

James Hawdon
*Virginia Polytechnic Institute and State University*

*See next page for additional authors*



## Original Publication Citation

Gainey, R., Vandecar-Burdin, T., Albanese, J., Dearden, T., Hawdon, J., & Parti, K. (2022). *CIVIIC: Cybercrime in Virginia: Impacts on industry and citizens final report*. Commonwealth Cyber Initiative Coastal Virginia. https://covacci.org/wp-content/uploads/2023/01/CV-004-Gainey-CIVIIC_COVA_FinalReport.pdf

Authors
Randy Gainey, Tancy Vandecar-Burdin, Jay Albanese, Thomas Dearden, James Hawdon, and Katalin Parti

# CIVIIC: Cybercrime in Virginia: Impacts on Industry and Citizens Final Report

Submitted to COVA CCI

December, 2022

Randy Gainey, PhD - Old Dominion University

Tancy Vandecar-Burdin, PhD – Old Dominion University

Jay Albanese, PhD – Virginia Commonwealth University

Thomas Dearden, PhD – Virginia Tech

James Hawdon, PhD – Virginia Tech

Katalin Parti, PhD – Virginia Tech

## Table of Contents

## Introduction

Victimization from cybercrime is a major concern in Virginia, the US, and the world. As individuals and businesses spend more time online, it becomes increasingly important to understand cybercrime and how to protect against it. Such an understanding is dependent on valid and reliable baseline data that identifies the specific nature, extent, and outcomes of cybercrime activity. A better understanding of cybercrime activity is needed to target and prevent it more effectively, minimize its consequences, and provide support for both individual and corporate victims. Before that can occur, however, better baseline data are required, and this project was designed to provide those data for the Commonwealth of Virginia. The purpose of this study was to describe the experiences of Virginia residents and businesses around cybercrime, identify the specific vulnerabilities that are exploited, and discover the consequences of victimization.

Virginia presents a disinctive intersection of cyber-physical systems with a large workforce in the maritime, defense, technology, and transportation sectors, combined with an educated and mobile workforce making it a uniquely targeted area. Production of transportation equipment (boats and ships, motor vehicle parts, trucks) is the third largest industry in the state, and Virginia is a leading crab and oyster producing state. The most valuable services industries in Virginia produce income through computer programming and engineering companies, repair shops, private health care, hotels, and motels. Virginia's growth sector is in technology with opportunities for computer programmers, consultants, engineers, and researchers. The world's largest Internet service provider is based in Virginia. The Pentagon, the headquarters of the CIA, and several military bases are all located in Virginia (Netstate, 2022). Of Virginia's largest companies, seven of the top 10 are in the maritime, defense, transportation, and technology sectors (Kolmar, 2021).

As one of the 50 states of the US, Virginia is the 12th most populous state and ranks high on a number of measures (World Population Review, 2022). In aggregate, Virginia ranked No. 7 overall across a group of eight categories: Crime & Corrections, Economy, Education, Environment, Fiscal Stability, Health Care, Infrastructure, and Opportunity. The rankings are based on more than 70 metrics (Callahan, 2021). Virginia has the fourth-best public schools overall in the United States, ranking fourth for quality and third for safety (World Population Review, 2022a).

On the other hand, Virginia closely matches the remainder of the US on other attributes. For example, Virginia is in the middle quintile in both per capita income growth and per capita personal consumption expenditures (U.S. Department of Commerce, 2021; 2022). Growth in GDP in Virginia closely matches the US as a whole (-1.7% versus -1.6%, comparing the last quarter of 2021 with first quarter of 2022) (U.S. Department of Commerce, 2022a).
The US population is highly urbanized, with 82.3% of the population residing in cities and suburbs. Virginia is similar with 88 % residing in urban areas (Virginia Rural Health Plan, 2022). Virginia also ranks in the middle of the pack on other attributes, such as 24th in the United States for its economic outlook, and 30th for its economic performance (American Legislative Exchange Council Center for State Fiscal Reform, 2022; Virginia Employment Commission, 2022). Two-thirds of Virginia residents have at least some college, similar to the percentage

nationwide (69%) (Ryan & Bauman, 2016). The median age in the US is 38.8 years. In Virginia, it is 38.4, and life expectancy is the same in the state as it is in the nation at 78 years (World Population Review, 2022c). Therefore, there exist a number of interesting similarities and differences between Virginia and the United States overall, so the results of this study will have unique implications when examining the nature, frequency, harm, and vulnerabilities of cybercrime.

## Business Survey

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 granting permission to use their data 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.

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: 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% |

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: 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% |

## Business 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 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). On average, the questionnaire took approximately 12 minutes to complete.

**Business Survey 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 potential 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: 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 |

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

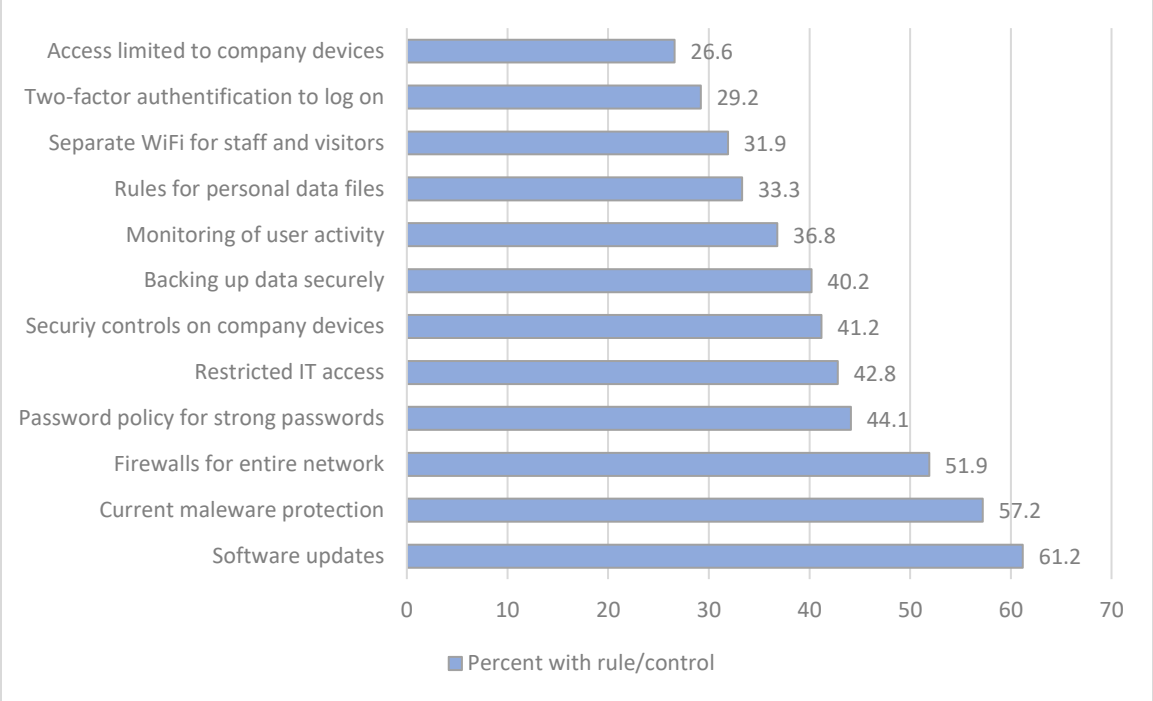
low, cybersecurity importance varies by sector. For example, over 90% of the companies in defense, transportation, IT, finance, communications, and real estate say cybersecurity is a high or very high priority for their company. Conversely, only 78.9% of the companies in consumer discretionary, 63.6% 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. To assess behaviors or practices that could potentially make a business vulnerable to a cyberattack, 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 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: Cybersecurity Practices/Controls Currently Used by Virginia Businesses (%)**

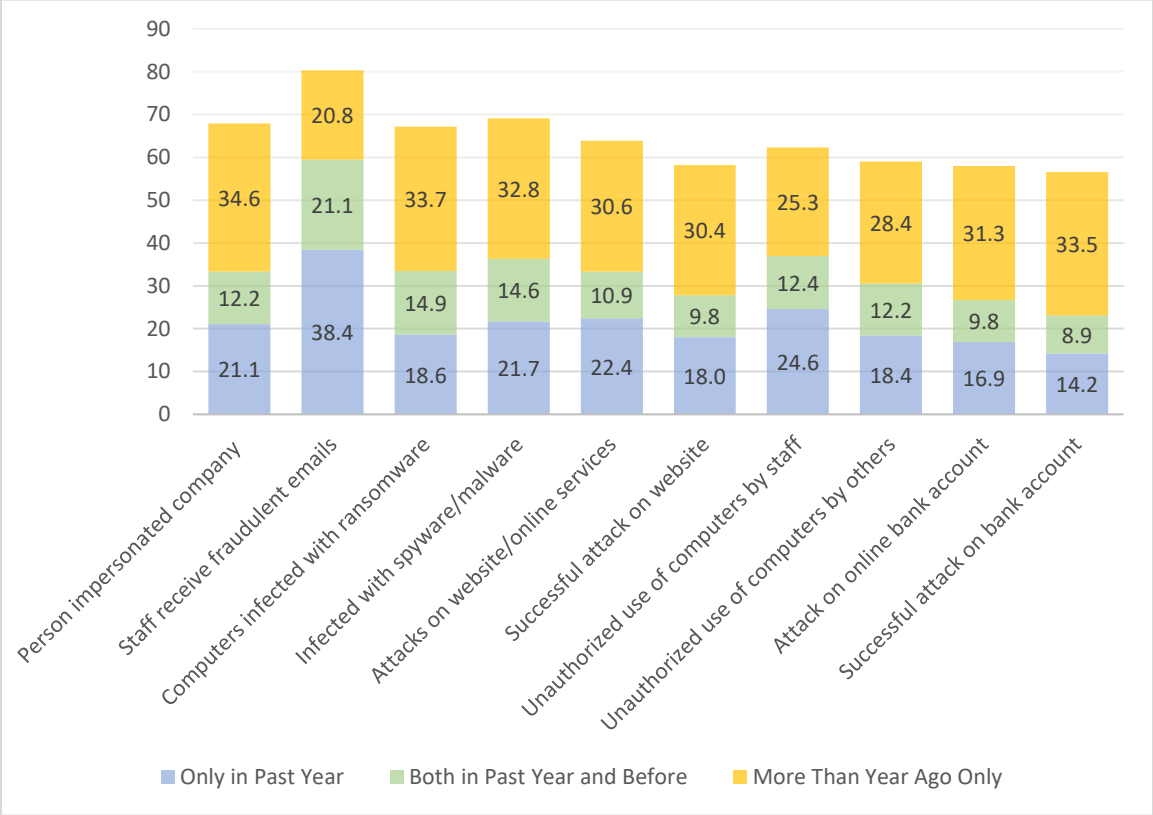



## Victimization

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: Types of Cybercrime Experienced by Virginia Businesses**




## Predictors of Victimization

We also investigated what factors, if any, could predict victimization. To predict which businesses were victimized in the past year, we conducted 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 engaging in the behavior and "0" if they did not report engaging in 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 approached 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: 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 |
| No separate Wi-Fi for visitors | .606 * | .296 | 4.18 | 1.83 |
| Constant | .058 | .727 | .006 | 1.060 |

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

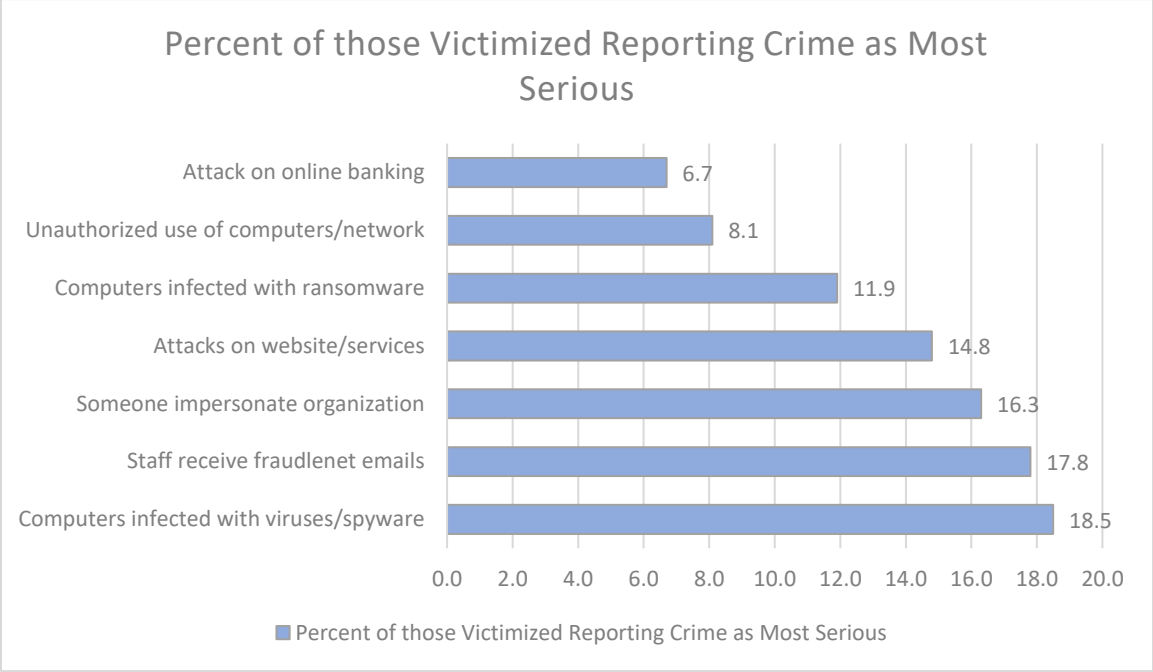
Company size significantly increased the likelihood of being victimized in the past year (odds ratio = 1.19; p = .031). Companies without separate Wi-Fi for visitors and employees were significantly more likely to experience a victimization in the past year than were those with such policies (odds ratio = 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.

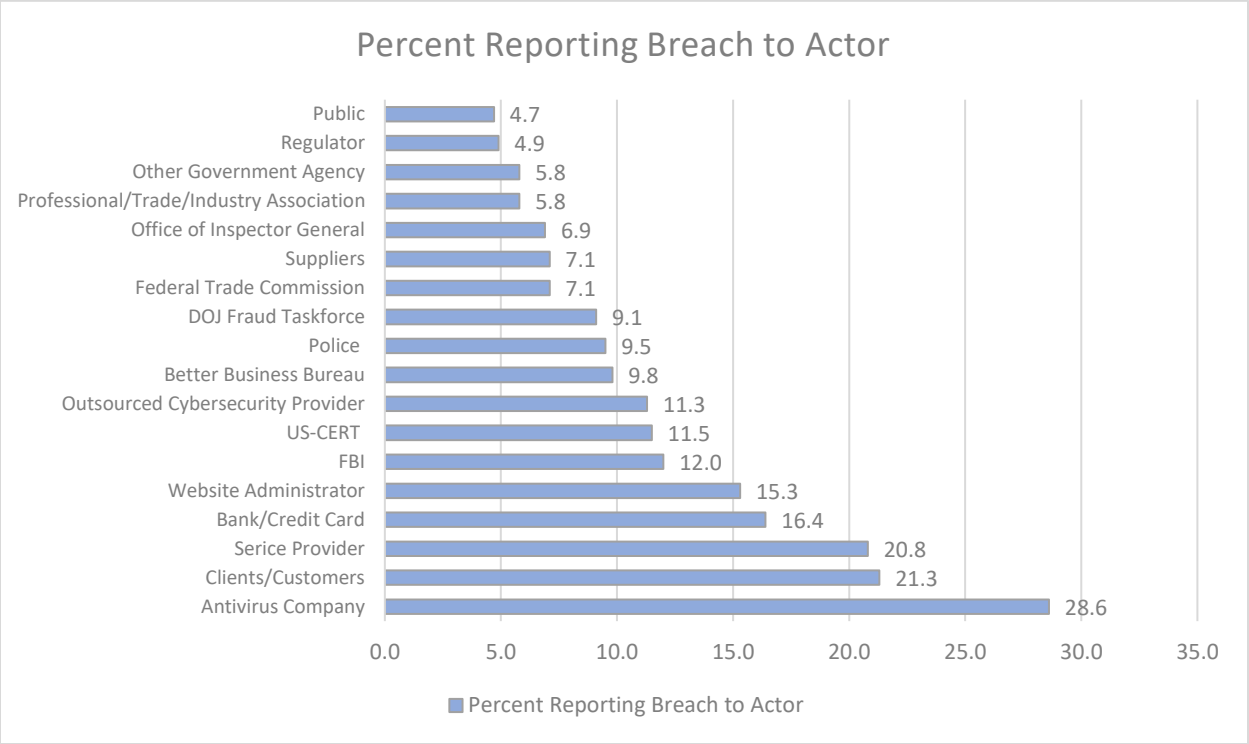
**Figure 3: Most Disruptive Cybercrime in Past Year Identified by 135 Victimized Companies (%)**




## 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: Percent of Victimized Companies Reporting Crime to Various Actors**




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 displays the number of agencies or actors to which the company reported their victimization.

**Table 5: Number of Agencies/Actors the Company Reported the 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% |

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 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: How Was the Breach or Attack Discovered?**

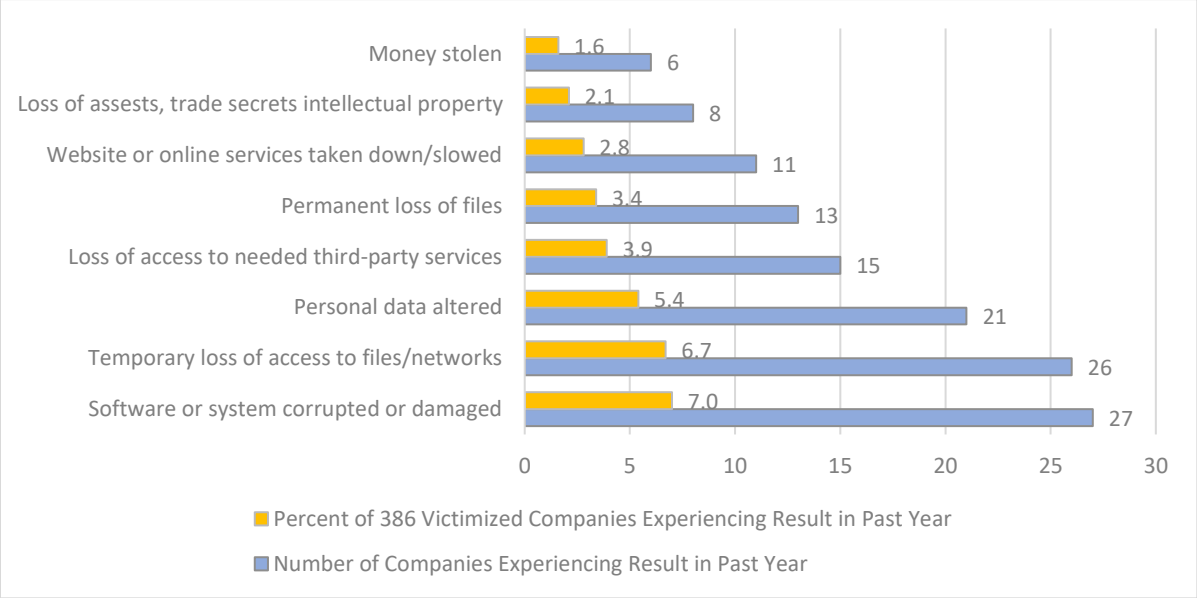
| | Frequency (N=62) | Percent |
|---|---|---|
| By accident | 4 | 6.5% |
| By antivirus/anti-malware software | 15 | 24.2% |
| Disruption to business/staff/users/service provision | 6 | 9.7% |
| From warning by government/law enforcement | 4 | 6.5% |
| Breach/attack reported by the media | 2 | 3.2% |
| 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% |

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 Costs

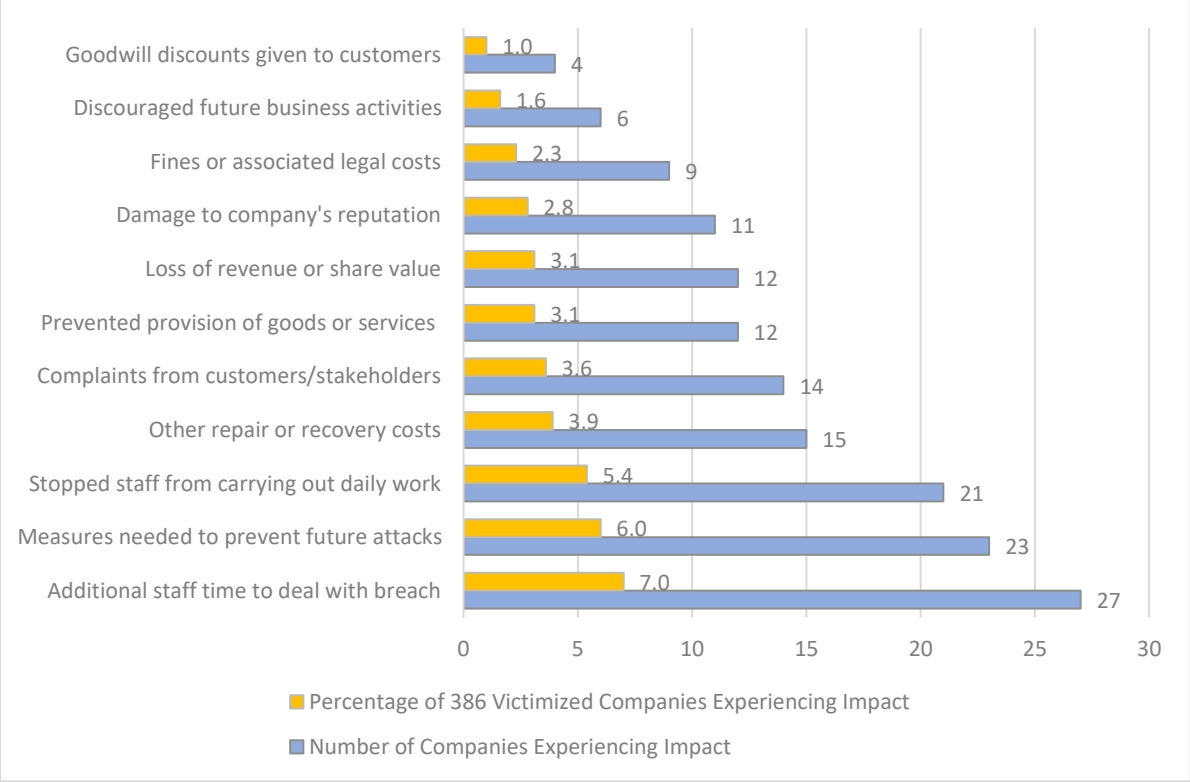
Finally, we also explored the consequences that companies suffered because of cybercrime victimization. First, respondents were asked to think of all the cybersecurity breaches or attacks experienced in the last 12 months and to identify all of the adverse results of the attacks. Figure 5 presents the 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: Reported Adverse Results of Cyberattacks**




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

**Figure 6: Impacts of Victimization**



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: 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% |

## Resident Survey

The resident survey was conducted using accepted techniques of survey research that involve telephone interviews (Daikeler, Bošnjak & Lozar, 2020; Evans & Mathur, 2018; Kalton, 2019) and web-based surveys. Telephone and web surveys were conducted with a sample of 1,206 adults, ages 18 or older, living in Virginia. Telephone interviews were conducted by landline (n=256) and cell phone (n=449) as well as via an on-line survey panel (n=501) provided by CINT USA. The telephone interviews and web surveys were conducted in English language during Spring, 2022.

A combination sample was used consisting of listed and random digit dial (RDD) numbers for both landline and cellular numbers to reach adults in Virginia who have access to either a listed or unlisted landline or cellular telephone number. As many as seven attempts were made to contact landline telephone numbers, and as many as five attempts were made to contact cell phone numbers. Calls were made at different times of the day and different days of the week to maximize the chance of contacting potential respondents.

For the telephone survey, the introductory language directed the interviewer to speak with the member of the household who was 18 years of age or older with the most recent birthday. Selecting respondents in this manner has been shown to result in data that closely mirror the population in terms of age.

**Sample Demographics**

Of the 1,206 respondents surveyed, 72.1% were white, 17.7% were Black or African American, and 8.3% considered themselves to be another race/ethnicity. This includes 2.6% identifying as Asian, 2.0% Multiracial, 1.8% American Indian or Alaskan Native, and 0.1% Native Hawaiian or Pacific Islander. In a separate question, 4.3% of respondents indicated that they were of Hispanic/Latino origin.

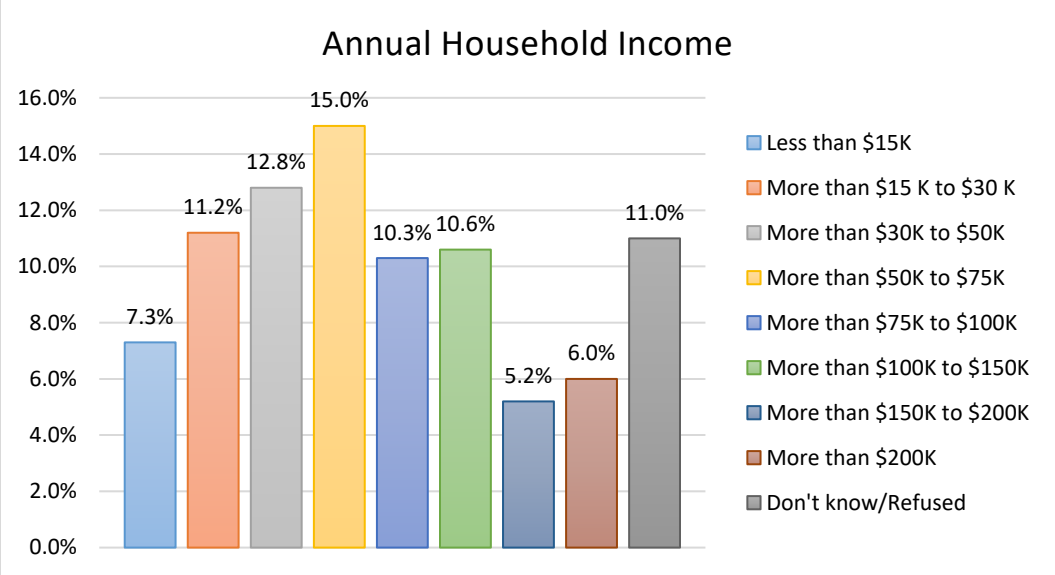
More than 60 percent of respondents were female (64.7%) and 34% were male. More than one in three (40.6%) of the respondents received a high school diploma or GED, completed trade or professional school, or attended some college. An additional 46.1% of respondents completed an undergraduate or graduate degree. Half of the respondents surveyed were married (50%) and 18% were divorced, separated, or widowed. Less than one-quarter of those surveyed were single and not living with a partner (21.0%) while a small portion of single people reported living with a partner (8.1%). Less than 5% were in the military or lived with a spouse or partner who was active-duty military. Almost 20% of participants reported their annual household income as $30,000 or less, 27.8% reported earning more than $30,000 to $75,000, while 32.1% earned more than $75,000.

**Table 8: Survey Respondent Demographics**

| **Race** | **Percentage** |
|---|---|
| White | 72.1% |
| Black/African-American | 17.7% |
| American Indian or Alaskan Native | 1.8% |
| Asian | 2.6% |
| Native Hawaiian or Pacific Islander | 0.1% |
| Multiracial | 2.0% |
| Other | 1.8% |
| Don't Know/Refused | 1.9% |
| **Hispanic/Latino Origin?** | **Percentage** |
| Yes | 4.3% |
| No | 92.8% |
| Don't know/Refused | 1.8% |
| **Gender** | **Percentage** |
| Male | 34.0% |
| Female | 64.7% |
| Prefer to self-identify | 0.8% |
| **Highest level of school completed** | **Percentage** |
| Some grade school | 0.5% |
| Some high school | 2.7% |
| High school diploma/GED | 16.5% |
| Completed trade/professional school | 2.4% |
| Some college | 21.7% |
| Associate's degree | 8.0% |
| Bachelor's degree | 25.0% |
| Graduate degree | 21.1% |

| | |
|---|---|
| Other | 0.5% |
| Don't Know/Refused | 0.9% |
| **Age** | **Age in years** |
| Average age (years) | 52.2 |
| **Marital Status** | **Percentage** |
| Single, not living with partner | 21.1% |
| Single, living with partner | 8.1% |
| Married | 50.0% |
| Divorced/separated | 10.8% |
| Widowed | 7.2% |
| Don't Know/Refused | 1.0% |

**Figure 7: Annual Household Income**




## Resident Survey Results

The results of this survey provide multiple insights into the nature, frequency, harm, and vulnerability of the residents included in our large sample. Six insights from this empirical study are highlighted in this article.

### Frequency, Vulnerability, and Usage

The results show that vulnerability is increased by usage. Some individual behaviors have become so common, they are no longer variables to be studied. Instead, they are accepted behaviors practiced by the vast majority of people. For example, *online connection to the Internet is extremely common*. Almost 98% of those interviewed use the internet or email, at least occasionally and 88% of residents reported being online one or more hours per day with 74% online three or more hours per day, with 75% having access to broadband internet. It is

notable that almost everyone surveyed has access to the internet at all times, as 94% reported having an internet-enabled smartphone. Additionally, 78% had a laptop in their household, 62% had a tablet or other similar computing device, and 52% had a desktop computer. Only 7% indicated they do not have any of these devices in their household. This high level of exposure to digital content from around the world clearly has impact on victimization. Studies in other locations have had the same finding (Chen, Chan & Chou, 2020; Milani, Caneppele & Burkhardt, 2022; Ngo et al., 2020).

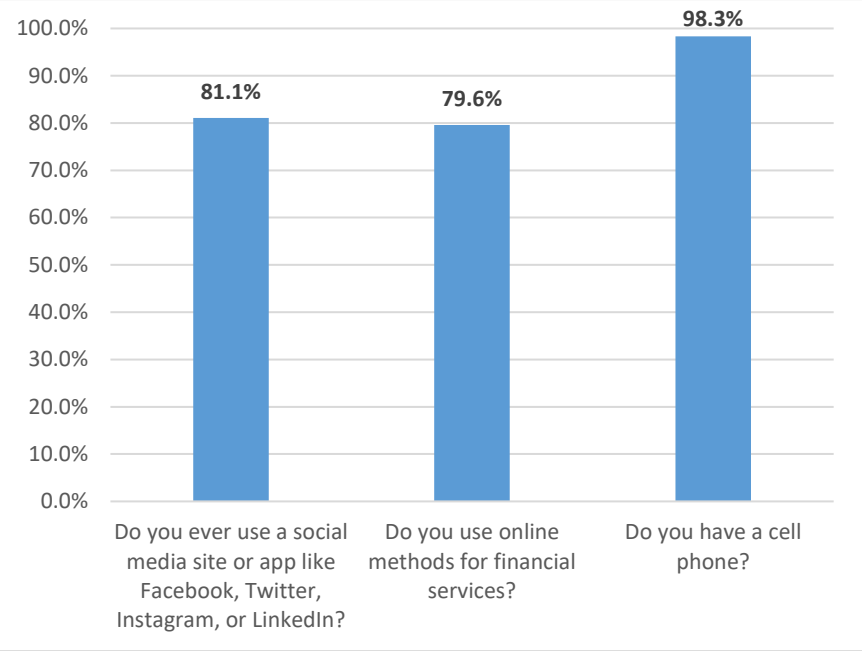
**Table 9: Do you or anyone else in your household have any of the following?**

| Tool | Percentage |
|---|---|
| Desktop Computer | 52.0% |
| Laptop | 78.2% |
| Tablet or other similar computing device | 61.9% |
| None of these | 7.0% |

Part of the explanation for this significant time of Internet connection is that *virtually everyone has a cell phone*. Our survey found that 98% of respondents have a cell phone. This makes the percentage of those without cell phones too small to be studied. A second part of the explanation *connects online exposure to the choice of sites visited*. The survey found that 81% of respondents use social media sites, which involve the sharing of personal information through the information required to subscribe, hold membership, and make postings viewable by others.

Other kinds of legitimate online behaviors further expose individuals to potential victimization. Almost 80 % of those surveyed do their banking or pay bills online. Online payments have replaced paper mailing of bills, and paper checks sent in the mail. It is much more convenient, but the convenience requires account numbers and related personal information to be held by banks, companies, businesses, and other individuals. This information can be hacked by third parties who gain unauthorized access to personal data, and there have been numerous instances demonstrating the insecurity of these data (Amir, Levi & Livne, 2018; Legg, 2021; Wang & Johnson, 2018).

**Figure 8: Social Media, Online and Cell Phone Use**




## Self-Protective Behaviors

Another finding is that *individuals overrate their self-protective behaviors*. In Virginia, 82% of respondents reported that they are always careful when clicking links or attachments sent to them via email, text, or social media. More than 71% believe they are somewhat or very prepared to prevent cyberattacks on their own personal computer. Another 55% reported having received training about how to safely use the internet.

But, at the same time, 34% had their credit card used to obtain money or buy goods without permission. In addition, internet-enabled devices in the household were infected or interfered with by a virus or malicious software, according to 35% of respondents. Online frauds and viruses such as these have been reported as the two most common forms of victimization in studies around the world (Van de Weijer, 2019; Woods, 2022).

Respondents were asked to indicate their level of expertise with the internet. The majority, 74%, either identified themselves as having an intermediate expertise (being able to download applications, manage internet settings, fix some computer problems, and have knowledge of hardware and software) or an expert (being a computer specialist, web developer, comfortable manipulating or writing computer programming). Additionally, 19% identified their internet expertise as "beginner," meaning they are able to go to specific web pages and use social media. Only 6% percent said they are uncomfortable using a computer.

The finding in Virginia raises questions about individuals' self-reported care when moving about online and raises concern about the high level of frequency of online fraud and malware. This suspicion is confirmed by the response to a later question in the interview asking if they have ever used social media account (e.g., Facebook, Twitter) information to log into another website.

Using social media to access other accounts results in sometimes unintended sharing of personal information to a third party, increasing risk. Forty-four percent of respondents have done this.

Respondents were asked how likely they thought it was that in the next five years the United States will experience a significant cyberattack on public infrastructure, such as air traffic control system or power grid. The majority of respondents stated they thought it would either probably happen (51.9%) or definitely happen (30.4%). Less than 2 in 10 thought it would either probably not happen (12.1%) or definitely not happen (1.9%). However, there is more hope that US businesses are prepared to prevent cyberattacks on their own systems. Half of respondents (49.5%) felt that US businesses were at least somewhat prepared and another 8 percent feel that US businesses are very prepared to prevent cyberattacks on their own systems.

Passwords are a crucial part of computer and internet safety. Respondents were asked how similar their passwords are that they use for various online accounts. The majority of respondents said their passwords were either very different (35.3%) or somewhat different (26.9%). Another quarter said their passwords were somewhat similar and only 8 percent said their passwords are very similar. Additionally, 37 percent stated they have shared a password to one of their online accounts with a friend or family member.

**Nature of Victimization**

C*yber frauds are most common*. Fraud is the most frequent cybercrime self-reported by victims and also reported to authorities (FBI Internet Crime Report, 2022; Reep-van den Bergh & Junger, 2018). More than 60% (62.9%) of respondents experienced some type of cyber fraud ever and 28% experienced some type of fraud in the past year.

**Figure 9: Experiences of cyber fraud**

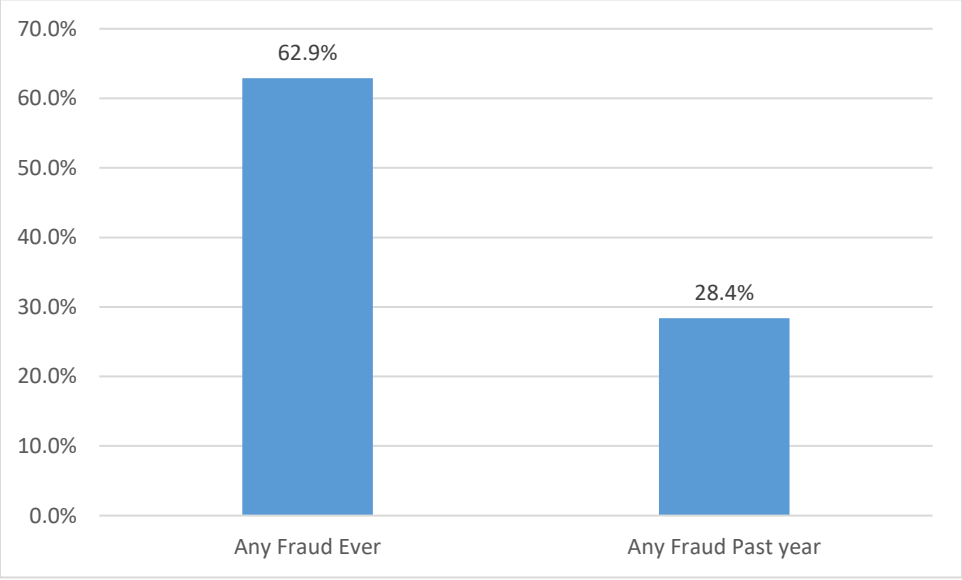



Table 10 depicts nine different types of cyber-related frauds reported by Virginia residents – those that they or someone in their household ever experienced and those that occurred during the past year. They range from a low of 4% reporting non-payment fraud (1.1% in the past year) to a high of 34% reporting unauthorized use of credit card (11% in the past year).

**Table 10: Cyber fraud types**

| Nature of Fraud | Percent victimized ever[1] | Percent victimized in past year[2] |
|---|---|---|
| Tricked or deceived out of money or goods by email, text, or online via the internet | 17.2% | 5.2% |
| Bought a product or service via the internet, but the product or service was never delivered | 22.2% | 9.0% |
| Sold a product or service via the internet, and delivered it, but never received any money | 3.7% | 1.1% |
| Without permission, use or attempt to use your, or a household member, personal information to open any NEW accounts | 16.8% | 4.1% |
| Someone claimed an income tax refund or unemployment benefits in your name, or a household member, without permission | 4.6% | 1.8% |
| Had your credit card, or that of a household member, used to obtain money or buy goods or services without permission | 33.7% | 10.9% |
| Had your bank account, or that of a household member, illegally or fraudulently debited | 21.9% | 8.0% |
| Had your social security number, or that of a household member, used for fraud or theft | 6.3% | 1.6% |
| Transferred money to someone who contacted you or someone in household via email or internet with a false story about earning money | 4.1% | 1.2% |

It can be seen that fraud online occur very frequently and are the is reported type of crime online in both surveys and to authorities (FBI Internet Crime Report, 2022; Fonseca, Moreira & Guedes, 2022; Lee, 2021). The high incidence of fraud illustrates that online shopping and commercial dealings are a primary online activity, placing the exchange of funds in large numbers of transactions globally at a higher risk of compromise or abuse (Button & Cross, 2017; Rungsrisawat, Sriyakul & Jermsittiparsert, 2019).

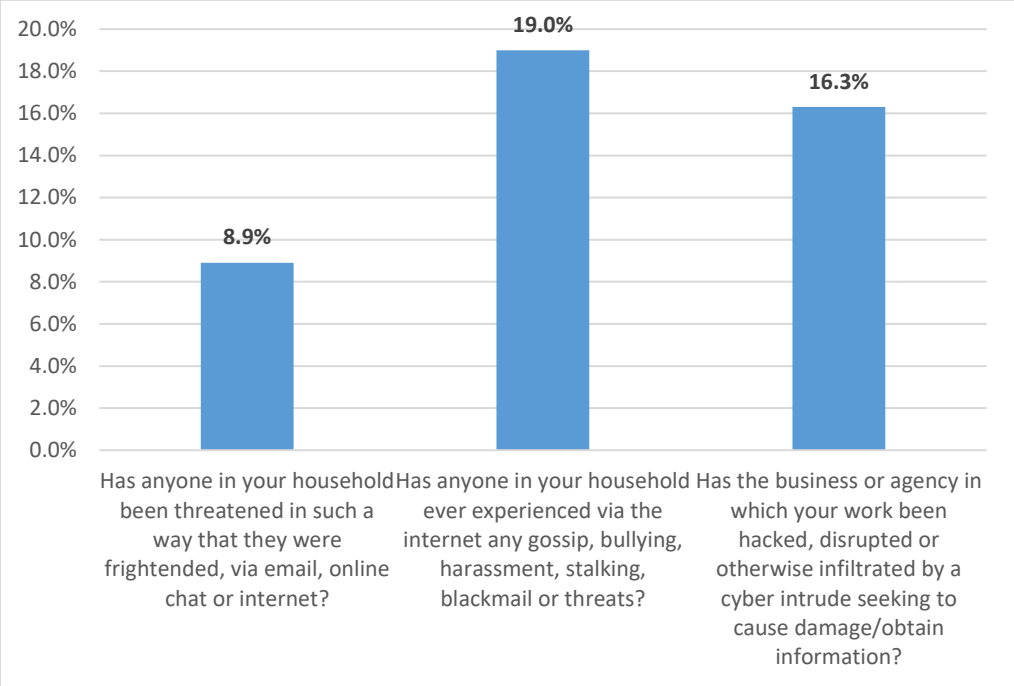
For non-fraud crimes, victimization rates were lower, but the threats were often serious. Nine percent of respondents reported affirmatively that someone in their household was threatened in such a way that they were, or a household member was, frightened, via email, online chat, or the internet. However, 19% experienced gossip, bullying, harassment, stalking, blackmail, or threats via the Internet. The nature of the victimization was serious in that more than half of those interviewed (62%) reported the threats were moderately or severely distressing. There have been multiple studies that have identified the link between online bullying, threats, and harassment with stress, depression, and other harms (Gini, Card & Pozzoli, 2018; Ryan & Curwen, 2013).

[1] Denominator = 1,206 (all respondents)

[2] Denominator = 1,206 (all respondents)

Regarding malware, 35% reported a computer or other internet-enabled device in the household was infected or interfered with by a virus or malicious software during the past year. In addition, 16% of respondents reported that the business or agency in which they work was hacked, disrupted, or otherwise infiltrated by a cyber-intruder in the past year seeking to cause damage or obtain information. Although victimization from malware was high, 72% of respondents reported they were "somewhat" or "well prepared" to prevent cyberattacks on their own personal computer systems.

**Figure 10: Cybercrime Threats/Bullying & Business Attacks**




## Harm and Costs

The survey results also show that cyber *victimization results in harms more serious than financial loss*. As indicated in Table 11, more than 60 percent of victims in this sample reported no (unreimbursed) financial loss or a loss less than $500. This finding reflects both the size of the transactions engaged in by most online users and that most of these transactions are conducted using credit cards, which indemnify victims for any losses suffered by fraudulent transactions.

**Table 11: Financial losses**

| Estimate of total loss from cyber victimizations | Percentage of respondents |
|---|---|
| None ($0) | 28% |
| $1 to $500 | 28% |
| $500 to $1000 | 9% |
| $1000 to $5000 | 11% |
| $5000 or higher | 4% |

On the other hand, Table 12 indicates the level of stress reported by survey respondents. Even though the financial losses are often not large, nearly 70% of victims reported it causing "moderate" or "severe" distress to them.

**Table 12: Stress of Victimization**

| How distressing or stressful were misuse or attempted misuse of your personal information to you? | Percentage of respondents |
|---|---|
| Not at all distressing | 7% |
| Mildly distressing | 23% |
| Moderately distressing | 34% |
| Severely distressing | 36% |

There is financial stress for many who cannot afford to miss a single rent or car payment, and lack financial reserves or support. In addition, there is uncertainty about whether compensation will ultimately occur, or whether their personal information or privacy will be exploited again, or by others (Buchanan & Whitty, 2014; Leukfeldt, Notté & Malsch, 2020).

**Response**

Many respondents took action in response to their victimization. These actions included checking their credit report (21%), changing passwords on financial accounts (31%), purchasing identity theft protection (8%), relying on credit monitoring or identity theft insurance (11%), or shredding or destroying documents containing personal information (17%). Despite these efforts, only 22 percent reported their most recent victimization to the police.[3] Although of those who did so, about two-thirds (64.6%) reported being satisfied or very satisfied with the response received. Of those who did not report their victimization to the police (n=345), more than half (54.2%) said that they did not contact law enforcement because their credit card company, bank, or other organization took care of the problem. More than one in five (22.9%) did not report

[3] Due to a branching error in the web-based survey, not all persons who reported victimization at any time ever were asked if they reported their most recent victimization to the police. These findings are based on the 441 respondents who were asked if they reported to the police.

because they did not think that the police would do anything and 20% did not report because they took care of the issues themselves.

## Conclusion & Next Steps

With most (85.6%) companies reporting instances of 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). Cybervictimization for the general public is also fairly common (62.9%) and distressing. The results show that Virginians are victimized even when they are somewhat careful or feel confident that they are adequately prepared. Both businesses and residents perhaps overestimate their preparedness and ability to remain cyber secure. The results show an obvious opportunity for additional and improved prevention efforts and education.

Reliable cyber victimization data is critically important as a foundation for designing more effective prevention strategies – including education of the cybersecurity workforce and the general public. Cybersecurity traditionally focuses on target hardening by attempting to make computers and networks more secure through increased technological interventions. In order to understand how to protect public and private systems and how to educate those who are vulnerable to cyber threats, we must first understand the experience of the general public and businesses as they live, work, and operate in the virtual world. While these surveys provide a useful baseline for understanding cybercrime in Virginia, they are cross-sectional data. Additional data – including longitudinal/panel data – are needed to more fully understand the nature, scope, distribution, and correlates of cybercrime in Virginia. Longitudinal data collected from the same individuals and businesses over time would increase our understanding of both risk and protective related to victimization and provide empirical evidence to develop strategies to reduce cybercrime.

The research team intends to seek funding to establish a longitudinal panel of respondents (both residents and businesses) that would complete the cybercrime victimization survey multiple times over the course of multiple years. Education, awareness, and training efforts could be identified, as well as implications for criminal justice policy. The research team has already submitted a proposal for Congressionally Directed Spending/Community Funding Projects to the Arts & Letters Dean at Old Dominion University to be considered by the Assistant Vice President for Federal Relations. Other potential funding sources include the National Science Foundation (e.g., Secure and Trustworthy Cyberspace - SaTC) and the National Institute of Justice (e.g., Research and Evaluation of Technology-Facilitated Abuse for Criminal Justice Purposes and Research and Evaluation on White Collar Crime: Health Care and Elder Fraud.) and foundations such as the Allstate Foundation, the Commonwealth Fund, the Ford Foundation, the Jerry Lee Foundation and others.

The research team has already disseminated initial findings of the CIVIIC study to local/state, national and international stakeholders. We also have two journal articles – one focused on the business results and the other on the residential results – under review by the *Criminal Justice Studies* journal. Please see the list of publications and presentations below.

**Peer-Reviewed Manuscripts Under Review**

2022 Gainey, R., Vandecar-Burdin, T., Albanese, J., Dearden, T. E., Parti, K., & Hawdon J., Routine Citizen Internet Practices and Cyber Victimization: A State-wide Study in Virginia. Manuscript under Review.

2022 Hawdon, J., Parti., K., Dearden, T. E., Vandecar-Burdin, T., Albanese, J., & Gainey, G. Cybercrime victimization among Virginia Businesses: Frequency, vulnerabilities, and consequences of cybervictimization. Manuscript under Review.

**Manuscripts in Progress**

2022 Albanese, J., Dearden, T.E., Gainey, R., Hawdon, J., Parti, K. & Vandecar-Burdin, T. Do Inside Hackers Do More Damage? Using Opportunity Theory to Empirically Examine Insider Damage. Manuscript in Progress.

**Conference Presentations**

2022 Vandecar-Burdin, T, Dearden, T., Gainey, R., Hawdon, J., Albanese, J., Parti, K. Social Cybervictimization Experiences across Virginia: Implications for Educating Industry and Citizens. CCI CyberCon Conference. Williamsburg, VA. September 19, 2022.

2022 Dearden, T. E., J. Albanese, T. Vandecar-Burdin, K. Parti, R. Gainey, J. Hawdon. (September) Measuring Cybercrime among Virginian Residents and Businesses: Prevalence and Correlates. Southern Criminal Justice Association. Asheville, N.C. September 14, 2022.

2022 Dearden, T. E., J. Albanese, T. Vandecar-Burdin, K. Parti, R. Gainey, J. Hawdon. (September) Cybervictimization Experiences Across Virginia: Implications for Educating Industry and Citizens. COVA CCI Cybersecurity Education and Research Conference, Williamsburg, VA. September, 2022.

2022 Albanese, J., Dearden, T., Gainey, R., Hawdon, J., Parti, K., Vandecar-Burdin, T. (September) Cybercrime against individuals and businesses in Virginia. Prevalence and Correlates. European Society of Criminology 2022, Malaga, Spain, Sept 21-24, 2022.

2022 Albanese, J., Dearden, T., Gainey, R., Hawdon, J., Parti., K., & Vandecar-Burdin, T. (April). Cybercrime in Virginia: Statewide Surveys of Residents and Businesses. Commonwealth Cyber Initiative Symposium. Richmond. April 4, 2022.

2022 Albanese, J., Dearden, T. E., Gainey, R., Hawdon, J., Parti, K., & Vandecar-Burdin, T. (March). Cybercrime in Virginia: Results from Statewide Surveys of Residents and Businesses. Las Vegas, NV: Academy of Criminal Justice Sciences.

## References


American Legislative Exchange Council Center for State Fiscal Reform. (2022). *Rich States, Poor States: ALEC-Laffer State Economic Competitiveness Index*. https://www.richstatespoorstates.org/states/VA/

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, 23(3), 1177-1206.

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.

Breen, C., Herley, C., & Redmiles, E. M. (2022, April). A Large-Scale Measurement of Cybercrime Against Individuals. In *CHI Conference on Human Factors in Computing Systems* (pp. 1-41).

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime & Law*, 20(3), 261-283.

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge.

Callahan, E. (2021). *Virginia ranked as No. 7 for 'Best State,' according to U.S. News & World Report*. https://www.whsv.com/2021/03/09/virginia-ranked-as-no-7-for-best-state-according-to-us-news-world-report/

Cheng, C., Chan, L., & Chau, C. L. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. *Computers in Human Behavior*, *108*, 106311.

Daikeler, J., Bošnjak, M., & Lozar Manfreda, K. (2020). Web versus other survey modes: an updated and extended meta-analysis comparing response rates. *Journal of Survey Statistics and Methodology*, 8(3), 513-539.

Evans, J. R., & Mathur, A. (2018). The value of online surveys: A look back and a look ahead. *Internet Research*, 28, 854-887. DOI 10.1108/IntR-03-2018-0089

*FBI Internet Crime Report 2021*. (2022). https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Fonseca, C., Moreira, S., & Guedes, I. (2022). Online Consumer Fraud Victimization and Reporting: A Quantitative Study of the Predictors and Motives. *Victims & Offenders*, *17*(5), 756-780.

Gainsbury, S. M., Browne, M., & Rockloff, M. (2019). Identifying risky Internet use: Associating negative online experience with specific online behaviours. *New Media & Society*, 21(6), 1232-1252.

Gini, G., Card, N. A., & Pozzoli, T. (2018). A meta-analysis of the differential relations of traditional and cyber-victimization with internalizing problems. *Aggressive Behavior*, 44(2), 185-198.

Kalton, G. (2019). Developments in survey research over the past 60 years: A personal perspective. *International Statistical Review*, 87, S10-S30.

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

Kolmar, C. (2021). *The 100 Largest Companies in Virginia for 2022*. https://www.zippia.com/advice/largest-companies-in-virginia/

Lee, C. S. (2021). Online fraud victimization in China: A case study of Baidu Tieba. *Victims & Offenders*, *16*(3), 343-362.

Legg, J. (2021). Pushing Back Against the Rising Tide of Cybercrime. *Forbes*, July 19.

Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2020). Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. *Victims & Offenders*, 15(1), 60-77.

Milani, R., Caneppele, S., & Burkhardt, C. (2022). Exposure to cyber victimization: Results from a Swiss survey. *Deviant Behavior*, *43*(2), 228-240.

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

Netstate.com (2022). *Virginia Economy*. https://www.netstate.com/economy/va_economy.htm#:~:text=Falls%20Church%20and%20Richmond%20are,%2C%20mail%20order)%20services%20group.

Ngo, F. T., Piquero, A. R., LaPrade, J., & Duong, B. (2020). Victimization in cyberspace: Is it how long we spend online, what we do online, or what we post online? *Criminal Justice Review*, 45(4), 430-451.

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*, 397420. https://doi.org/10.1007/s10611-018-9774-y

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

Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime science*, *7*(1), 1-15.

Rungsrisawat, S., Sriyakul, T., & Jermsittiparsert, K. (2019). The era of e-commerce & online marketing: risks associated with online shopping. *International Journal of Innovation, Creativity and Change*, 8(8), 201-221.

Ryan, C.L. & Bauman, K. (2016). *Educational Attainment in the United States*. U.S. Census Bureau.

https://www.census.gov/content/dam/Census/library/publications/2016/demo/p20-578.pdf

Ryan, K. N., & Curwen, T. (2013). Cyber-victimized students: Incidence, impact, and intervention. *SAGE Open*, 3(4), 2158244013516772.

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

U.S. Department of Commerce. Bureau of Economic Analysis. (2021). *Personal Consumption Expenditures by State, 2020*. https://www.bea.gov/sites/default/files/2021-10/pce1021.pdf

U.S. Department of Commerce. Bureau of Economic Analysis. (2022). *Personal Income by State*. https://www.bea.gov/data/income-saving/personal-income-by-state

U.S. Department of Commerce. Bureau of Economic Analysis. (2022a). *Gross Domestic Product by State, 1st Quarter 2022*. https://www.bea.gov/news/2022/gross-domestic-product-state-1st-quarter-2022

van de Weijer, S. (2019). Predictors of cybercrime victimization: Causal effects or biased associations? In *The human factor of cybercrime* (pp. 83-110). Routledge.

Virginia Employment Commission. (2022). *Statewide Economic Analysis Report*. https://virginiaworks.com/_docs/Publications/LMI-Publications/Statewide-Economic-Analysis/PDF/SEA-2021.pdf

Virginia Rural Health Plan. (2022). *Defining Rurality in Virginia*. https://www.vdh.virginia.gov/content/uploads/sites/76/2022/01/Virginia-Rural-Health-Plan_2-Defining-Rurality.pdf

Wang, P. & Johnson, C. (2018). Cybersecurity incident handling: a case study of the Equifax data breach. *Issues in Information Systems*, 19(3).

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, 26, 277-292

Woods, D. W., & Walter, L. (2022, June). Reviewing Estimates of Cybercrime Victimisation and Cyber Risk Likelihood. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 150-162). IEEE.

World Population Review. (2022). *US States - Ranked by Population 2022*. https://worldpopulationreview.com/states

World Population Review. (2022a). *Public School Rankings by State 2022*. https://worldpopulationreview.com/state-rankings/public-school-rankings-by-state

World Population Review. (2022c). *Virginia Population 2022*. https://worldpopulationreview.com/states/virginia-population

# APPENDIX

## Business Survey

You are invited to participate in a research study involving a short survey focusing on cybercrime in Virginia. This survey is sponsored by VT, ODU, and VCU. The survey is designed to help understand both the nature and significance of the cybersecurity threats businesses and companies in the Commonwealth face and ways the try to stay secure. Results from this survey will be used to inform future policy and research in this area. The survey should take approximately 10 minutes to complete. Participation is voluntary, so you may withdraw at any time or skip any questions you do not want to answer. Your responses are anonymous and we will not identify your business or company so no one will be able to associate your answers to you or your business. Please do not include your name or other identifying information in your responses that can identify you. If you have any questions or concerns about the research, please feel free to contact Dr. James Hawdon (Tel.: 540-231-7476; Email address: hawdonj@vt.edu).

Please note that participation in the survey is completely voluntary. Do you want to continue on to the survey?

1. Yes
2. No

We ask that the survey respondent be the person most knowledgeable about your business' past cybersecurity experiences. Are you the person most knowledgeable about your business' past cybersecurity experiences?

1. Yes
2. No

Is your business or business you work for headquartered or located in Virginia?

1. Yes
2. No

On a scale of 1 to 10 where 1 is "not at all knowledgeable" and 10 is "extremely knowledgeable," how knowledgeable are you about your businesses IT operations?

1. 1 (Not knowledgeable at all)
2. 2
3. 3
4. 4
5. 5
6. 6
7. 7
8. 8
9. 9
10. 10 (Extremely knowledgeable)

How many years have you worked for this business?

What is the primary sector of your business?

1. Defense
2. Transportation
3. Maritime
4. Information Technology
5. Healthcare
6. Financials
7. Consumer Discretionary
8. Communication Services
9. Industrial
10. Consumer Staples
11. Energy Utilities
12. Real Estate
13. Materials
14. Other

Approximately how many employees work in your company, including yourself?

1. Fewer than 10
2. 10-49
3. 50-249
4. 250-999
5. 1,000 or more
6. I don't know

Which of the following, if any, does your company currently have or use? Select all applicable answers

1. Accounts or pages on social media sites (e.g. Facebook, Twitter, LinkedIn, etc.)
2. The ability for customers to order, book, or pay for products or services online
3. An online bank account for your company
4. Customer's personal information stored electronically
5. I don't know
6. None of these

As far as you know, does anyone in your company use personally-owned devices, such as smartphones, tablets, home laptops or desktop computers to carry out regular work-related activities?

1. Yes
2. No
3. I don't know

The remainder of the survey will be focused on cybersecurity. For the purposes of this survey, cybersecurity is defined as any strategy, processes, practices or technologies that companies have in place to secure their networks, computers, programs or the data they hold from damage, attack or unauthorized access.

How high or low a priority is cyber security to your company?

1. Very high
2. High
3. Low
4. Very low
5. I don't know

Approximately how often is your company's senior management updated about cybersecurity?

1. Never
2. Less than once a year
3. Annually
4. Quarterly
5. Monthly
6. Weekly
7. Daily
8. Each time there is a breach or attack
9. I don't Know

Does your company's insurance policy protect against cyberattacks?

1. Yes
2. No
3. I don't know

Which of the following aspects, if any, are covered within your cybersecurity-related policy, or policies? Select all applicable answers.

1. What can be stored on removable devices (e.g. USB devices, external hard drives, etc.)
2. Remote or mobile working (e.g. working from home)
3. Staff activities on your organization's IT devices
4. Use of personally owned devices for business activities
5. Use of cloud related services
6. Data classification (e.g. public, internal use, confidential, etc.)
7. Document Management System - software that can store, manage, and track files or documents on a company's network. It can help manage things like version control and who has access to specific files or documents.)

8. Other
9. I don't know
10. None

Do you provide regular cybersecurity training to your employees?

1. No
2. Yes
3. I don't know

Has your company experienced the following cyberattacks or breaches? If the attack happened to your company, please indicate if this was in the past 12 months or at some time before then. If it has not happened to your company, please leave blank.

| | More than 12 months ago | In the past 12 months | It happened multiple times, both in the past 12 months and before then |
|---|---|---|---|
| People impersonated your company in emails or online | ❑ | ❑ | ❑ |
| Staff received fraudulent emails or being directed to fraudulent websites | ❑ | ❑ | ❑ |
| Computers became infected with ransomware | ❑ | ❑ | ❑ |
| Computers became infected with other viruses, spyware or malware | ❑ | ❑ | ❑ |
| Attacks that tried to take down your website or online services | ❑ | ❑ | ❑ |
| Unauthorized use of computers, networks, or servers by staff, even if accidental | ❑ | ❑ | ❑ |
| Unauthorized use of computers, networks, or servers by someone other than staff | ❑ | ❑ | ❑ |
| Attacks that have succeeded in taking down your website | ❑ | ❑ | ❑ |
| An attempt to attack your company's online bank account | ❑ | ❑ | ❑ |
| A successful attack on your company's online bank account | ❑ | ❑ | ❑ |

Has your business or agency been hacked, breached, or otherwise disrupted by a cyber-intruder seeking:

| | Yes | Yes, in the past 12 months | No | I don't know |
|---|---|---|---|---|
| To cause damage to your physical or intellectual property | ❑ | ❑ | ❑ | ❑ |
| To steal physical or intellectual property | ❑ | ❑ | ❑ | ❑ |

Who was the most recent breach or attack reported to? Select all applicable answers:

1. Antivirus company
2. Bank, building society or credit card company
3. Better Business Bureau
4. Federal Bureau of Investigation (FBI)
5. Federal Trade Commission
6. Department of Justice Fraud Taskforce
7. Office of Inspector General
8. US-CERT Cybersecurity and Infrastructure Security Agency (CISA)
9. Clients / customers
10. Internet / Network Service Provider
11. Outsourced cyber security provider
12. Police
13. Professional / Trade / Industry association
14. Regulator
15. Suppliers
16. Was publicly declared
17. Website administrator
18. Other government agency
19. Other
20. None
21. I don't know

For the following questions, please indicate which of the following rules or controls your company has in place:

1. Applying software updates when they are available
2. Up-to-date malware protection
3. Firewalls that cover your entire IT network, including individual devices
4. Restricting IT admin and access rights to specific users
5. Any monitoring of user activity
6. Specific rules for storing and moving personal data files securely
7. Security controls on company-owned devices (e.g. laptops)
8. Only allowing access via company-owned devices
9. Separate WiFi networks for staff and for visitors
10. Backing up data securely via other means
11. A password policy that ensures users set strong passwords
12. Two-factor authentication to log onto the company's system
13. Other
14. None

Which of these measures were put into place because of a security breach or attack? Please select all that apply.

1. Applying software updates when they are available
2. Up-to-date malware protection
3. Firewalls that cover your entire IT network, including individual devices
4. Restricting IT admin and access rights to specific users
5. Any monitoring of user activity
6. Specific rules for storing and moving personal data files securely
7. Security controls on company-owned devices (e.g. laptops)
8. Only allowing access via company-owned devices
9. Separate WiFi networks for staff and for visitors
10. Backing up data securely via other means
11. A password policy that ensures users set strong passwords
12. Two-factor authentication to log onto the company's system
13. Other
14. None

For the remainder of the survey, please concentrate on the most disruptive breach your company has experienced to date.

Identify one cybersecurity breach, or related series of breaches or attacks, that caused the most disruption to your company in the last 12 months. Which of the following occurred? Select all applicable answers.

1. Computers becoming infected with ransomware
2. Computers becoming infected with other viruses, spyware or malware
3. Attacks that try to take down your website or online services
4. Hacking or attempted hacking of online bank accounts
5. People impersonating your organization in emails or online
6. Staff receiving fraudulent emails or being directed to fraudulent websites
7. Unauthorized use or hacking of computers, networks or servers by people outside your company
8. Any other types of cybersecurity breaches or attacks

Thinking again about one cybersecurity breach, or related series of breaches or attacks, that caused the most disruption to your company in the last 12 months, how was this breach or attack identified? If this has happened more than once, think about the one that caused the most disruption to your organization.

1. By accident
2. By antivirus/anti-malware software
3. Disruption to business/staff/users/service provision
4. From warning by government/law enforcement
5. Breach/attack reported by the media
6. Similar incidents reported in the media
7. Reported or noticed by either: customer(s), beneficiaries, service users, donors, students, and/or customer complaints
8. Reported or noticed by staff (including contractors and/or volunteers)
9. Routine internal security monitoring
10. Other internal control activities not done routinely (e.g., reconciliations, audits, etc.)
11. Other
12. None of these
13. I don't know

How long, if any time at all, did it take to restore business operations back to normal after the breach or attack was identified?

1. No time at all
2. Less than one day
3. Between one day and under a week
4. Between one week and under a month
5. One month or more
6. I don't know

Are business operations back to normal, currently?

1. Yes
2. No
3. I don't know

Thinking again about the most significant cybersecurity breach, do you know the identity of the person, persons , or entity (e.g. a hacking group) who committed this breach?

1. Yes
2. No

Was this person/persons an employee or an outsider?

1. Employee
2. Outsider

Thinking of all the cybersecurity breaches/attacks experienced in the last 12 months, which, if any, of the following happened as a result? Select all applicable answers.

1. Software or system were corrupted or damaged
2. Personal data (e.g., on customers, staff, etc.) was altered, destroyed or taken
3. Permanent loss of files (other than personal data)
4. Temporary loss of access to files or networks
5. Loss of stolen assets, trade secrets or intellectual property
6. Money was stolen
7. Your website or online services were taken down or made slower
8. Loss of access to any third-party services you rely on
9. Other
10. None
11. I don't know

Have any of these breaches or attacks impacted your organization in any of the following ways? Select all applicable answers.

1. Stopped staff from carrying out their day-to-day work
2. Loss of revenue or share value/income
3. Additional staff time to deal with the breach or attack, or to inform customers / beneficiaries / stakeholders
4. Any other repair or recovery costs
5. New measures needed to prevent or protect against future breaches or attacks
6. Fines from regulators or authorities, or associated legal costs
7. Damage to the company's reputation
8. Prevented provision of goods or services to customers/beneficiaries or service users
9. Discouraged you from carrying out a future business activity you were intending to do
10. Complaints from customers/beneficiaries/stakeholders
11. Goodwill compensation or discounts given to customers
12. Other
13. None
14. I don't know

How much did the cybersecurity breach affect your company?

1. It had a minor effect
2. A moderate effect
3. A major effect
4. None
5. I don't know

What was the financial cost of the breach? Was it approximately…

1. Less than $500
2. $500 to less than $1,000
3. $1,000 to less than $5,000
4. $5,000 to less than $10,000
5. $10,000 to less than $20,000
6. $20,000 to less than $50,000
7. $50,000 to less than $100,000
8. $100,000 to less than $500,000
9. $500,000 to less than $1,000,000
10. $1 million to less than $5 million
11. $5 million or more
12. I don't know

How likely do you think it is that in the next five years, the United States will experience a significant cyberattack on our public infrastructure, such as our air traffic control system or power grid?

1. Definitely not happen
2. Probably not happen
3. Probably happen
4. Definitely happen

How well-prepared do you think U.S. businesses are to prevent cyberattacks on their own systems?

1. Not at all prepared
2. Not too prepared
3. Somewhat prepared
4. Very prepared

How well-prepared do you think your business is to prevent cyberattacks on your own systems?

1. Not at all prepared
2. Not too prepared
3. Somewhat prepared
4. Very prepared

## Resident Survey

Start of Block: Default Question Block

INTRO We need your help to understand how to protect people from cybercriminals. A hacker attacks someone online every 32 seconds. Yet we do not know how this affects the people of Virginia. We are asking you to complete a brief survey about your use of the internet and computers.

Your participation is voluntary and your responses will remain confidential. You must be 18 years of age or older. By clicking "next", you agree to participate. If you have any questions about the survey, please contact Randy Gainey at rgainey@odu.edu.

Page Break

VIRGINIA Do you live in Virginia?

- ○ Yes
- ○ No

*Display This Question:*

*If Do you live in Virginia? = No*

END_DNQ Thank you for your willingness to participate in this survey, however, we are only surveying Virginia residents. Please click next to exit out of the survey.

End of Block: Default Question Block

Start of Block: Block 1

Q1 Do you use the internet or email, at least occasionally?

- Yes
- No
- Don't know/Don't wish to answer

*Skip To: Q32 If Do you use the internet or email, at least occasionally? = No*
*Skip To: Q4 If Do you use the internet or email, at least occasionally? = Don't know/Don't wish to answer*

Page Break

Q2 Is your internet access broadband internet?

- Yes
- No
- Don't know

Q3 How often do you use the internet?

- Less than one hour per day
- One or two hours per day
- Three to five hours per day
- Six to seven hours per day
- Eight to nine hours per day
- Ten or more hours per day

Page Break

Q4 Do you have a cell phone?

- Yes
- No
- Do not wish to answer

*Skip To: Q5 If Do you have a cell phone? = No*

Page Break

Q4A Is your cell phone a smartphone? (For example: can you access the internet from your phone)

- Yes
- No
- Don't know

Page Break

Q5 Do you ever use a social media site or app like Facebook, Twitter, Instagram, or LinkedIn?

- Yes
- No

Q6 Do you use online methods for financial services? (For example:  paying bills, banking, transferring funds, etc.)

- ○ Yes
- ○ No

Page Break

Q7 Do you or anyone else in your household have any of the following? (select all that apply)

- ☐ Desktop Computer
- ☐ Laptop
- ☐ Tablet or other similar computing device
- ☐ ⊗ None of these

Page Break

Q8 Now we have some questions about your use of the internet and related expertise.

Please indicate your level of expertise with the internet.

- ○ I am uncomfortable using a computer
- ○ I am able to go to specific web pages and use social media (Beginner)
- ○ I am able to download applications, manage internet settings, fix some computer problems, and have knowledge of hardware and software (Intermediate)
- ○ I am a computer specialist, web developer, comfortable manipulating or writing computer programming (Expert)

Q9 Have you received training about how to safely use the internet or how to stay safe on the internet?

- ○ Yes
- ○ No

Page Break

Q10A Please respond to the following statements about your computer/internet habits with either always, sometimes or never.

| | Always | Sometimes | Never |
|---|---|---|---|
| I am careful when clicking links or attachments sent to me via email, text, or social media. | ○ | ○ | ○ |
| I use security alerts for my email and social media accounts. | ○ | ○ | ○ |
| I am able to tell if a website is legitimate. | ○ | ○ | ○ |
| I use personal information to create my passwords. | ○ | ○ | ○ |
| I update my passwords frequently. | ○ | ○ | ○ |
| I save my passwords in a digital/online password keeper. | ○ | ○ | ○ |

Page Break

Q11 This next set of questions has to do with experiences of fraud and data theft.

Has anyone in your household...?

- ☐ Been tricked or deceived out of money or goods by email, text, or online via the internet
- ☐ Bought a product or service via the internet, after which the product or service was never delivered because the seller was deceptive.
- ☐ Ever sold a product or service via the internet, and delivered it, but never received any money from the buyer because the buyer was deceptive
- ☐ Had someone without permission, use or attempt to use their personal information to open any NEW accounts such as cellphone accounts, credit card accounts, loans, bank accounts, online payment accounts, or something else
- ☐ Had someone claim an income tax refund or unemployment benefits in your name without your knowledge or permission
- ☐ Had their credit card be used to obtain money or buy goods or services without their permission or knowledge
- ☐ Had their bank account illegally or fraudulently debited
- ☐ Experienced fraud or theft because someone used their social security number
- ☐ Transferred money to someone who contacted them via email or the internet with a false story about earning money through an inheritance, investment, lottery, or something similar
- ☐ ⊗ None of the above
- ☐ ⊗ Don't know/Don't wish to answer

*Skip To: Q21 If This next set of questions has to do with experiences of fraud and data theft. Has anyone in your... = None of the above or Don't know/Don't wish to answer*

*Carry Forward Selected Choices from "This next set of questions has to do with experiences of fraud and data theft.Has anyone in your household...?"*

Q12 Have any of these things happened to you or someone else in your household in the PAST YEAR?

- [ ] ⊗ None of these occurred in the past year
- [ ] Been tricked or deceived out of money or goods by email, text, or online via the internet
- [ ] Bought a product or service via the internet, after which the product or service was never delivered because the seller was deceptive.
- [ ] Ever sold a product or service via the internet, and delivered it, but never received any money from the buyer because the buyer was deceptive
- [ ] Had someone without permission, use or attempt to use their personal information to open any NEW accounts such as cellphone accounts, credit card accounts, loans, bank accounts, online payment accounts, or something else
- [ ] Had someone claim an income tax refund or unemployment benefits in your name without your knowledge or permission
- [ ] Had their credit card be used to obtain money or buy goods or services without their permission or knowledge
- [ ] Had their bank account illegally or fraudulently debited
- [ ] Experienced fraud or theft because someone used their social security number
- [ ] Transferred money to someone who contacted them via email or the internet with a false story about earning money through an inheritance, investment, lottery, or something similar
- [ ] ⊗ None of the above
- [ ] ⊗ Don't know/Don't wish to answer

*Display This Question:*

*If Have any of these things happened to you or someone else in your household in the PAST YEAR? != None of these occurred in the past year*

Q13 Can you provide an estimate of loss from all these events where someone used or attempted to use your personal information in the PAST YEAR?

- ○ $0
- ○ $1 to $250
- ○ More than $250-$500
- ○ More than $500 to $1000
- ○ More than $1000 to $2000
- ○ More than $2000 to $3000
- ○ More than $3000 to $4000
- ○ More than $4000 to $5000
- ○ More than $5000 (please estimate how much)

_____

Page Break

Q20 Based on the previous questions, how distressing was the misuse or attempted misuse of your personal information to you? That is, how stressful was this?

- ○ Not at all distressing
- ○ Mildly distressing
- ○ Moderately distressing
- ○ Severely distressing

Page Break

*Display This Question:*

*If Have any of these things happened to you or someone else in your household in the PAST YEAR? != None of these occurred in the past year*

*Or This next set of questions has to do with experiences of fraud and data theft. Has anyone in your... != None of the above*

*Or This next set of questions has to do with experiences of fraud and data theft. Has anyone in your... != Don't know/Don't wish to answer*

Q20A Which of the following actions did you take in response to any previous misuse of your personal information? You may select all that apply.

- ☐ Checked your credit report
- ☐ Changed passwords on any of your financial accounts
- ☐ Purchased identity theft protection
- ☐ Had credit monitoring or identity theft insurance
- ☐ Shredded or destroyed documents containing your personal information
- ☐ Checked your banking or credit card statements for unfamiliar charged
- ☐ Used security software program on your computer to protect it against loss or credit cards or card theft
- ☐ Other (please specify) _____
- ☐ ⊗ None of these/took no action

*Skip To: Q20B If Which of the following actions did you take in response to any previous misuse of your personal i... = None of these/took no action*

*Display This Question:*

*If Have any of these things happened to you or someone else in your household in the PAST YEAR? != None of these occurred in the past year*

Q20B Did you contact any law enforcement agencies or authority, such as the local police, a sheriff, or a federal law enforcement agency to report the most recent misuse or attempted misuse of your personal information?

- Yes
- No
- Don't know/Don't wish to answer

*Skip To: Q20D If Did you contact any law enforcement agencies or authority, such as the local police, a sheriff, o... = No*

*Skip To: Q21 If Did you contact any law enforcement agencies or authority, such as the local police, a sheriff, o... = Don't know/Don't wish to answer*

Page Break

Q20C How satisfied were you with the law enforcement agency's response when you reported the misuse of your personal information?

- Very satisfied
- Somewhat satisfied
- Somewhat dissatisfied
- Very dissatisfied

Page Break

*Display This Question:*

*If Did you contact any law enforcement agencies or authority, such as the local police, a sheriff, o... = No*

Q20D We would like to learn more about why people who experience these types of crimes do not report it to law enforcement.
Why did you decide not to contact a law enforcement agency? Select all that apply.

- ☐ Didn't know that I could report it
- ☐ Didn't think about reporting it
- ☐ Didn't know what agency was responsible for identity theft crimes
- ☐ I didn't lose any money/It was an attempt
- ☐ Not important enough to report/Small loss
- ☐ Took care of it myself
- ☐ Credit card company, bank, or other organization took care of problem
- ☐ Didn't think the police would do anything
- ☐ Didn't want to bother the police
- ☐ Didn't find out about the crime until long after it happened/too late for police to help
- ☐ Couldn't identify the offender or provide much information that would be helpful to police
- ☐ Occurred in another state or outside of the U.S.
- ☐ The person responsible was a friend or family member and I didn't want to get them in trouble
- ☐ Too inconvenient/Didn't want to take the time

☐ Other (please specify)

_____

☐ ⊗ Don't know/Don't wish to answer

Page Break

Q21 Has anyone in your household been threatened in such a way that they were frightened, via email, online chat, or internet?

○ Yes

○ No

○ Don't know/Don't wish to answer

*Skip To: Q22 If Has anyone in your household been threatened in such a way that they were frightened, via email,... = No*

*Skip To: Q22 If Has anyone in your household been threatened in such a way that they were frightened, via email,... = Don't know/Don't wish to answer*

Q21A Has this happened to you or someone else in your household **in the past year**?

○ Yes, myself

○ Yes, someone else in my household

○ Yes, myself AND someone else in my household

○ No, neither myself or anyone else in my household

Page Break

Q22 Has anyone in your household ever experienced via the internet any gossip, bullying, harassment, stalking, blackmail, or threats?

- ○ Yes
- ○ No
- ○ Don't know/Don't wish to answer

*Skip To: Q23 If Has anyone in your household ever experienced via the internet any gossip, bullying, harassment,... = No*

*Skip To: Q23 If Has anyone in your household ever experienced via the internet any gossip, bullying, harassment,... = Don't know/Don't wish to answer*

Q22A Has this happened to you or someone else in your household **in the past year**?

- ○ Yes, myself
- ○ Yes, someone else in my household
- ○ Yes, myself AND someone else in my household
- ○ No, neither myself or anyone else in my household

Page Break

*Display This Question:*

*If Has anyone in your household ever experienced via the internet any gossip, bullying, harassment,... = Yes*

*Or Has anyone in your household been threatened in such a way that they were frightened, via email,... = Yes*

Q23 Based on the previous questions, how distressing was the cyberbullying and/or threats? That is, how stressful was this?

- Not at all distressing
- Mildly distressing
- Moderately distressing
- Severely distressing

Page Break

Q24 Has a computer or other internet-enabled device in your household been infected or interfered with by a virus or malicious software?

- Yes
- No
- Don't know/Don't wish to answer

*Skip To: Q25 If Has a computer or other internet-enabled device in your household been infected or interfered wit... = No*

*Skip To: Q25 If Has a computer or other internet-enabled device in your household been infected or interfered wit... = Don't know/Don't wish to answer*

Q24A Has this happened to you or someone else in your household **in the past year**?

- ○ Yes, myself
- ○ Yes, someone else in my household
- ○ Yes, myself AND someone else in my household
- ○ No, neither myself or anyone else in my household

*Display This Question:*

*If Has this happened to you or someone else in your household in the past year? != No, neither myself or anyone else in my household*

Q24B Can you provide an estimate of loss from these events?

- ○ $0
- ○ $1 to $250
- ○ More than $250 to $500
- ○ More than $500 to $1000
- ○ More than $1000 to $2000
- ○ More than $2000 to $3000
- ○ More than $3000 to $4000
- ○ More than $4000 to $5000
- ○ More than $5000 (please estimate how much) _____

Page Break

Q25 Has the business or agency in which you work been hacked, disrupted, or otherwise infiltrated by a cyber-intruder seeking to cause damage or obtain information?

- Yes
- No
- I am unemployed/retired

Q26 How likely do you think it is that in the next five years the United States will experience a significant cyberattack on our public infrastructure, such as our air traffic control system or power grid? Do you think this will definitely happen, probably happen, probably NOT happen, or definitely NOT happen in the next five years?

- Definitely happen
- Probably happen
- Probably NOT happen
- Definitely NOT happen

Q27 How well prepared do you think U.S. businesses are to prevent cyberattacks on their own systems?

- Very prepared
- Somewhat prepared
- Not too prepared
- Not at all prepared

Page Break

Q28 How well prepared are you to prevent cyberattacks on your own personal computer and computer systems?

- Very prepared
- Somewhat prepared
- Not too prepared
- Not at all prepared

Q29 Thinking about all of the passwords you use to access your various online accounts, would you say that your passwords are....?

- Very similar
- Somewhat similar
- Somewhat different
- Very different

Q30 Have you ever shared a password to one of your online accounts with a friend or family member?

- Yes
- No

Page Break

Q31 Have you ever used your social media account (e.g. Facebook or Twitter) information to log into another website?

- Yes
- No

Page Break

Q32 We have a few questions about you and your household. Would you say your household is....?

- Cell phone only
- Cell phone mostly
- Landline mostly
- Landline only

Q33 What is your gender?

- Male
- Female
- Prefer to Self-identify (please specify) _____

Q34 What is your age?

_____

Page Break

Q35 How would you describe your race or ethnicity?

- White
- Black/African American
- American Indian/Alaskan Native
- Asian
- Native Hawaiian/Pacific Islander
- Multiracial
- Other (please specify) _____

Q36 Are you of Hispanic/Latino origin?

- Yes
- No

Page Break

Q37 What is your marital status?

- Single, not living with a partner
- Single, living with a partner
- Married
- Divorced/Separated
- Widowed

Q38 What is the highest level of school you have completed?

- Some grade school
- Some high school
- High school diploma or GED
- Completed trade/professional school
- Some college
- Associate's degree
- Bachelor's degree
- Graduate degree (Master's, PhD, Doctorate, MD, JD)
- Other (please specify) _____

Page Break

Q39 Are you or anyone in your household active duty military?

- ○ Yes, myself
- ○ Yes, my spouse/partner
- ○ Yes, BOTH myself and my spouse/partner
- ○ Yes, other (please specify) _____
- ○ No

Q40 What is your annual household income?

- ○ Less than $15,000
- ○ More than $15,000 to $30,000
- ○ More than $30,000 to $50,000
- ○ More than $50,000 to $75,000
- ○ More than $75,000 to $100,000
- ○ More than $100,000 to $150,000
- ○ More than $150,000 to $200,000
- ○ More than $200,000

Q41 What is your zip code?

_____