How a Cyber Attack Can Ripple a Company's Operation?

Khalil Hassan

Abstract

- This paper researches how cyberattacks affects business operations. Companies lost $1.8 billion to cybercrime in 2019, according to business insurer Hiscox. Few businesses are safe, and big companies with a big online presence are heavily targeted. Companies in the energy, financial services, manufacturing, technology, and pharmaceutical sectors endured the heaviest losses. There are six major ways that impact a business. A company can face major increase in cost, lost in revenue, reputational damage, stolen intellectual property, altered business practice, and operation business practice. As cybercrime becomes more sophisticated, businesses will have to stay one step ahead.

Intro

- There are 6 major ways a cyber attack can affect a company's operation.

1. Increase in Cost
2. Lost Revenue
3. Reputational Damage
4. Stolen Intellectual Property
5. Altered Business Practice
6. Operational Disruption

Method

- The research method is observational. Where I research cyber attacks impact on a company in the various six ways. I will provide examples of several cyber attacks. There has been a plethora of recent cyber attacks to big name companies that illustrate the 6 major ways of rippling a company's operation. The cyber security dataset analyzed in this study is an open dataset published by the Bureau of Justice Statistics and the National Cyber Security Division of the U.S. Department of Homeland Security. The dataset contains a survey sample of 35 596 businesses including those with more than 5000 employees and fortune 500 companies. The businesses in the dataset represent several industries such as agriculture, chemical and drug manufacturing, finance, healthcare, telecommunications, transportation, insurance, retail, advertising and others.
- The "Liquid Web Cybersecurity Actions and Attitudes Study" was launched to understand specific consequences of these attacks, how they responded after an attack, and gauge preparedness against future attacks.

Increase in Cost

- Cyber attacks cost money before they even happen.
- Cyber Security technology and information is a costly resource to prevent cyber attacks.
- Insurance Premiums
- Public Relations report

Increase in Cost

- Cyber Security services costs around 10 % of a company's IT budget.
- This means if Microsoft has an IT budget 10 million, around 1 million is spent on cybersecurity.
- Gartner, a tech research and advisory firm, estimated that spending on information security will total $172 billion in 2022.

Increase in Cost- Insurance Premiums

- Cyber insurance generally covers your business' liability for a data breach involving sensitive customer information, such as Social Security numbers, credit card numbers, account numbers, driver's license numbers and health records.
- In 2021, the average cost of cyber insurance was $1,589 per year, compared with $1,485 in 2020. Since that time, we found that with the increase in ransomware attacks and data breaches, the average cost of premiums has risen approximately 25%, with some policyholders paying over an 80% higher rate in 2022.

Increase in Cost

- When Cyber attacks happen, companies have to pay law firms significant amount of money to combat attacks.
- These lawyers specialize in staying in compliance with cyber security regulations

Increase in Cost

- According to Hiscox, 6% of companies paid a ransom in 2019, creating $381 million in losses.
- Equifax endured 2017 data breach that compromised the personal data of 147 million customers. As a result of subsequent litigation, the company agreed to pay up to $425 million to assist affected individuals.

Lost Revenue

- Cyber attacks can cause sudden decrease in revenue in many ways.
- Customers tend to move their business elsewhere in order to protect themselves
- Companies can also lose money to hackers who try to extort their victims.

Lost Revenue

- A massive cyberattack May 1 cost Scripps Health $112.7 million through the end of June, with lost revenue bearing most of the cost.
- “As of June 30th, we estimate total lost revenues to be $91.6 million and incremental costs incurred to address the cyber security incident and recovery were estimated at $21.1 million,” the earnings report said.

Lost Revenue

- Sony Pictures came under attack in 2014 as it prepared to release “The Interview,” a comedy which depicted an assassination attempt on North Korean leader Kim Jong Un.
- Hackers pilfered sensitive information, including embarrassing e-mails and performance evaluations from its staff. North Korea is widely believed to be behind the attack, although it denied the allegations.
- Sony Pictures pulled the film from most theaters in favor of an online release, a move that cost it $30 million, according to the National Association of Theater Owners.

Lost Revenue

- Ransomware is a cyber-extortion tactic that uses malicious software to hold a user's computer system hostage until a ransom is paid.
- Ransomware can prevent workers from accessing IT systems unless the company pays off a hacker, can also create a major financial burden.
- Ransomware attackers often demand ransom in cryptocurrency such as Bitcoin due to its perceived anonymity and ease of online payment.

Reputational Damage

- Although tough to fully quantify, companies that fall victim to larger cyberattacks may find their brand equity significantly tarnished.
- Customers, and even suppliers, may feel less secure leaving their sensitive information in the hands of a company whose IT infrastructure was broken at least once before.

Reputational Damage

- Target saw its reputation take a hit after a 2013 data breach involving the credit card information of more than 40 million customers, a security failure that cost it $18.5 million to settle.
- The company said net earnings were $520 million in the quarter, down 46 percent from the same period a year earlier, when earnings were $961 million. Earnings per share were 81 cents, down from $1.47 the year before. Target executives repeatedly called 2013 a “challenging” year on Wednesday.

Reputational Damage

- In 2014, JP Morgan Chase & Co. data of its banking customers was compromised. Hackers gained access to the names, addresses, phone numbers, and email addresses of 76 million household accounts and seven million small business accounts.
- Security researchers Comparitech studied 40 data breaches at 34 companies listed on the New York Stock Exchange. It found that the share prices of compromised companies fell an average of 3.5% following an attack, and underperformed the Nasdaq by 3.5%.

Stolen Intellectual Property

- A company’s product designs, technologies, and go-to-market strategies are often among its most valuable assets.
- Intangible assets accounted for 87% of the value of S&P 500 companies in 2015, according to intellectual property advisory Ocean Tomo.
- Much of this intellectual property is stored in the cloud, where it's vulnerable to cyberattacks. Nearly 30% of U.S. companies report having their intellectual property stolen by a Chinese counterpart within the past 10 years.

Stolen Intellectual Property

- A cyber operation spearheaded by the notorious Chinese state actor, APT 41, has siphoned off an estimated trillions in intellectual property theft from approximately 30 multinational companies within the manufacturing, energy and pharmaceutical sectors.
- The hackers obtained hundreds of gigabytes of intellectual property and sensitive data, including blueprints, diagrams, formulas, and manufacturing-related proprietary data from multiple intrusions, spanning technology and manufacturing companies in North America, Europe, and Asia.

Altered Business Practice

- Cybercrime can impact businesses in more than just financial ways. Companies have to rethink how they collect and store information to ensure that sensitive information isn't vulnerable.
- Many companies have stopped storing customers' financial and personal information, such as credit card numbers, Social Security numbers, and birth dates.
- Some companies have shut down their online stores out of concern they cannot adequately protect against cyberattacks.

Operational Disruption

- Companies often face indirect costs from cyberattacks, such as the possibility of a major interruption to operations that can result in lost revenue.
- Cybercriminals can use any number of ways to handcuff a company's normal activities, whether by infecting computer systems with malware that erases high-value information, or installing malicious code on a server that blocks access to your website.

Operational Disruption

- In 2010, for example, hackers sympathetic to WikiLeaks retaliated against credit card giants Mastercard and Visa by conducting attacks that temporarily crashed their websites.
- The whistle blower website WikiLeaks to begin publishing part of the 250,000 US Embassy Diplomatic cables. These confidential cables provide an insight on U.S. international affairs from 274 different embassies, covering topics such as analysis of host countries and leaders and even requests for spying out United Nations leaders.

Operational Disruption

- A massive cyberattack May 1 cost Scripps Health $112.7 million through the end of June, with lost revenue bearing most of the cost.
- The attack led to a major disruption in patient care and forced providers to use paper records. Scripps said at the time that its facilities remained open for care but hasn’t until now divulged the financial impact of the attack.
- Scripps restored all its systems May 26 after hiring computer consulting and forensic firms to help investigate the attack and restore its systems.

Operational Disruption

- Elekta, the Swedish supplier of the software, said that their cloud-based data storage system experienced a "data security incident" in early- and mid-April. The company will not say whether or not the attack involved ransomware or was limited to attempted data theft.
- Elekta cut off access to the data storage, which led to disruptions of radiation therapy sessions at 42 healthcare sites in the U.S., according to a report in the Atlanta Journal Constitution.
- "We do not have the ability to operate the [radiation therapy] machines because the information that is programmed into those machines is up in the cloud," explained Marna Borgstrom, MPH, chief executive officer, Yale New Haven Health, New Haven, Connecticut

Results and Discussion

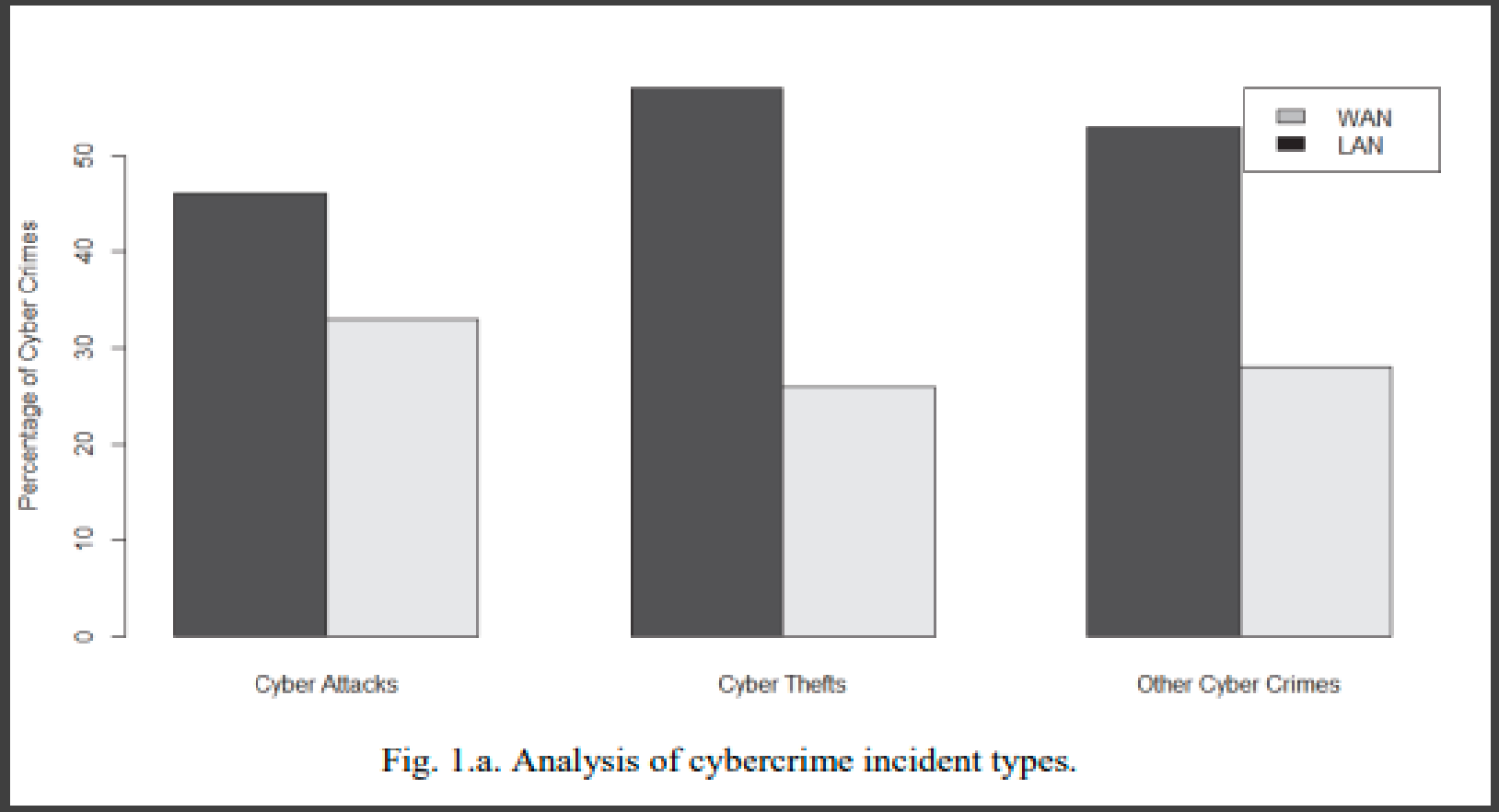
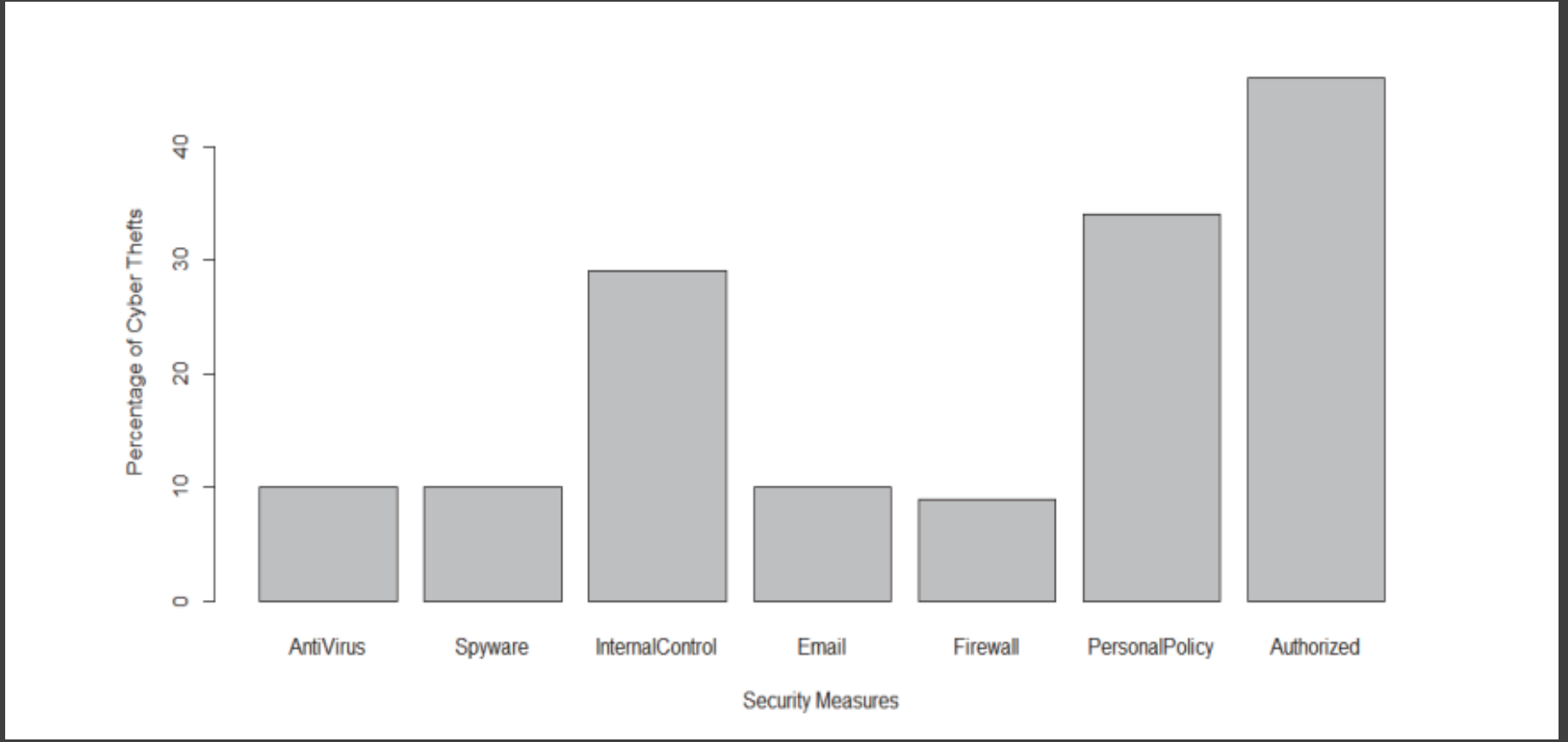
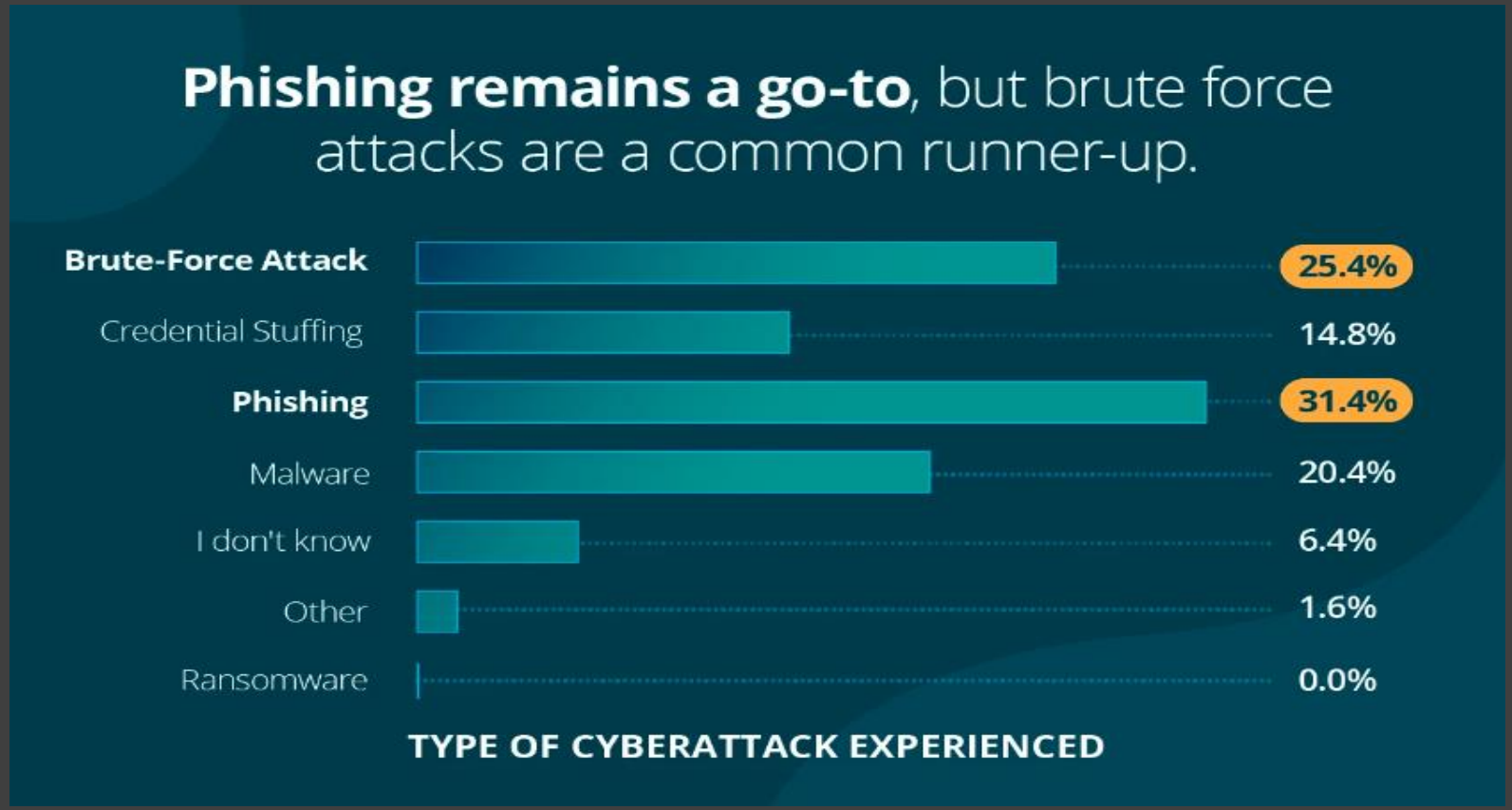


Fig. 1.a. Analysis of cybercrime incident types.

Results and Discussion



Results and Discussion



Results and Discussion

TABLE I

STATISTICS OF BUSINESSES IMPACTED BY CYBER CRIMES
(SOURCE: BUREAU OF JUSTICE STATISTICS, 2017)

Critical infrastructure	Percentage of businesses with monetary loss – $100 thou. or more	Percentage of businesses with system downtime of 25 hours or longer
All businesses	13	40
Agriculture	4	46
Chemical and drug manufacturing	18	33
Computer system design	13	41
Finance	29	38
Health care	14	39
Petroleum mining and manufacturing	12	30
Real estate	6	39
Telecommunications	12	47
Transportation/pipelines	11	40
Retail	18	42
Scientific research and development	12	43
Accounting	13	29
Advertising	12	26
Architecture and engineering	11	40
Business and technical schools	5	45
Insurance	20	41
Construction	8	41
Food services	11	33
Forestry, fishing, and hunting	8	50

Results and Discussion

TABLE II

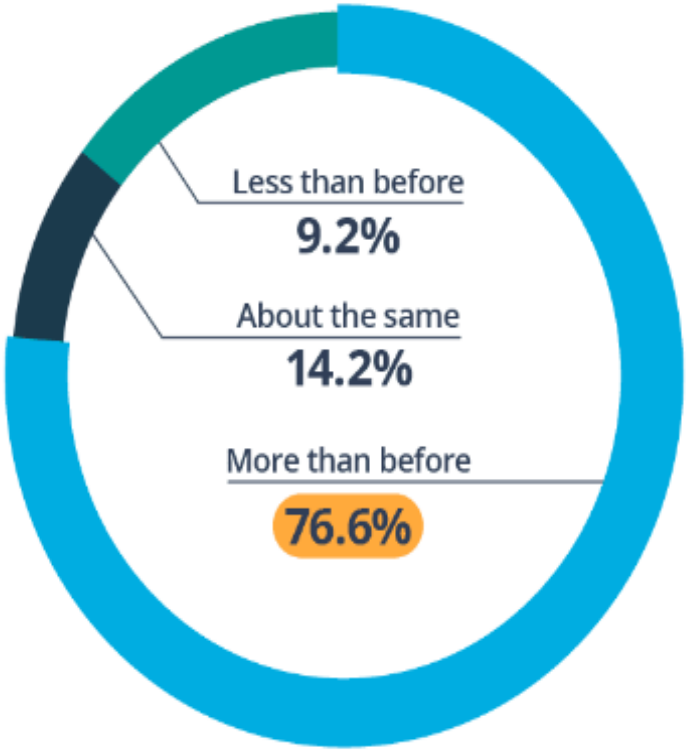
STATISTICS OF BUSINESSES IMPACTED BY CYBER CRIMES WITH SOME MONETARY LOSS

Critical infrastructure	Percentage of businesses with some monetary loss
All businesses	91
Agriculture	90
Chemical and drug manufacturing	91
Computer system design	98
Finance	93
Health care	91
Petroleum mining and manufacturing	89
Real estate	94
Telecommunications	91
Transportation/pipelines	90
Retail	94
Scientific research and development	93
Accounting	90
Advertising	88
Architecture and engineering	91
Business and technical schools	88
Insurance	96
Construction	92
Food services	87
Forestry, fishing, and hunting	87

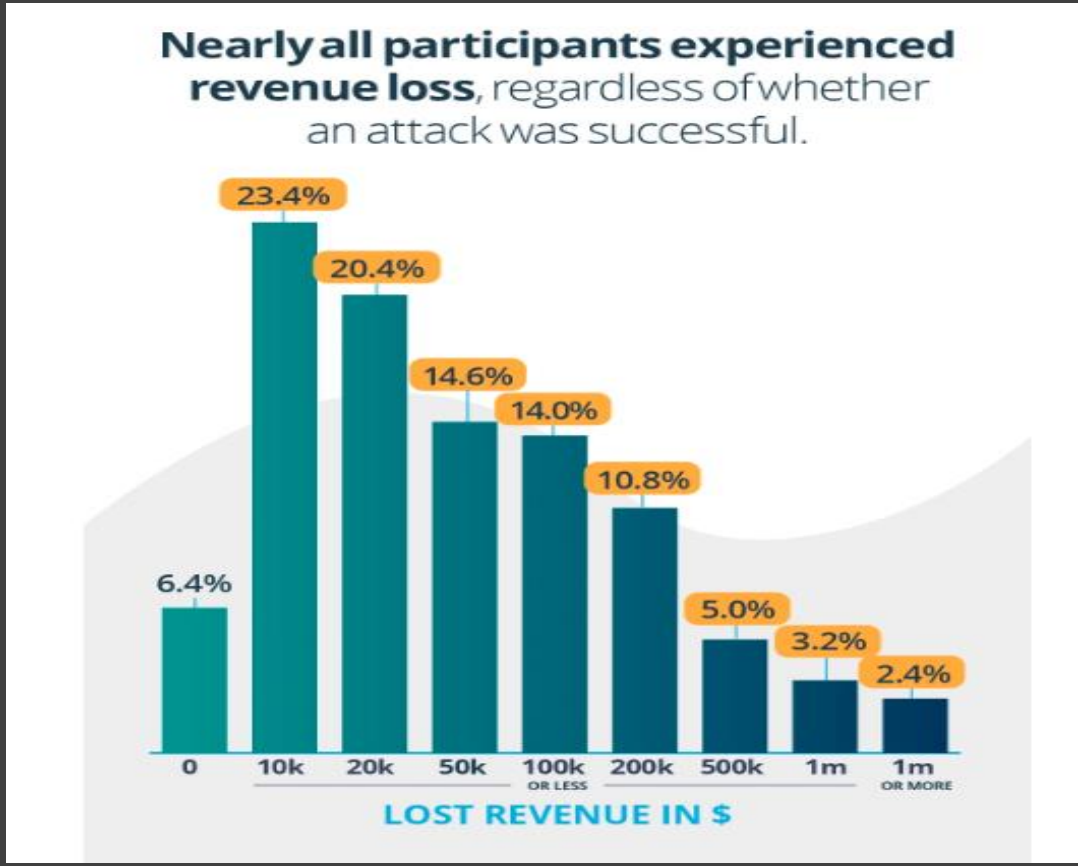
Results and Discussion

Results and Discussion

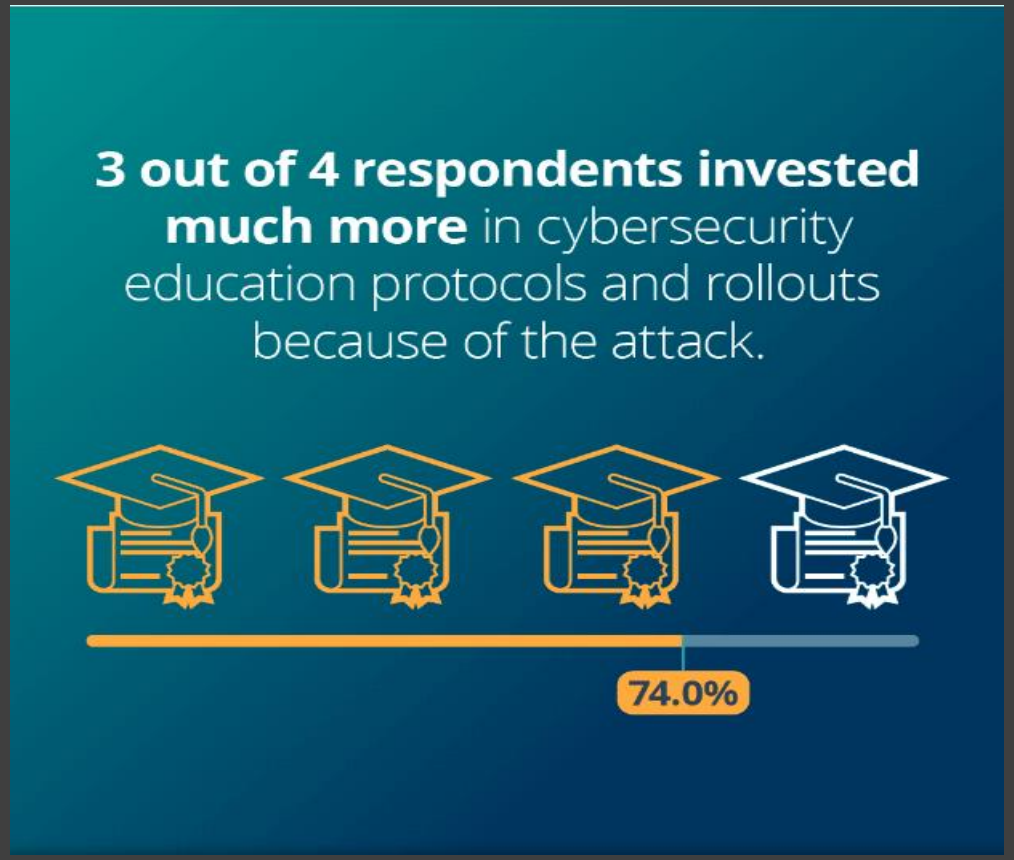
Over 76.6% increased spending on protective software and programs since their cyberattack.



Results and Discussion



Results and Discussion



Conclusion

- Protecting a business against cyberattacks is costly and can impact the relationship between the company and its customers.
- Businesses that come under cyberattack also incur higher costs from operational disruption and altered business practices.
- The biggest losses come from reputational damage. Companies that have lost control of their customers' data have paid millions to settle claims.

Reference Page

- Systematically Understanding the Cyber Attack Business: A Survey: ACM Computing Surveys: Vol 51, No 4
- https://www.emerald.com/insight/content/doi/10.1108/JHTT-05-2019-0080/full/html
- Hackers Are After More than Just Data: Will Your Company's Property Policies Respond When Cyber Attacks Cause Physical Damage and Shut Down Operations?: Environmental Claims Journal: Vol 28, No 4 (tandfonline.com)
- Data Analysis of Cybercrimes in Businesses | Balan | Information Technology and Management Science (rtu.lv)