Research on Economic Impacts on Cyberattacks on Small Businesses

SC&A, Inc.
2200 Wilson Blvd., Suite 300
Arlington, VA 22201
(703) 893-6600
www.scainc.com

1.0 Understanding of the Challenge

1.1 Initial Review of Data Sources and Information

A survey of reports on the cost of cyber incidents to business indicates that no single document captures even the limited data on costs that are available to the public. The best single document appears to be the February 2018 report by the White House Council of Economic Advisers.[1] That report draws on several industry reports, notably from the Ponemon Institute (with Accenture);[2] however, that study missed other reports that provide some cost data for small businesses.[3] The cyber security industry generates reports, most recently from Verizon,[4] McAfee (with CSIS),[5] and Kaspersky.[6] These reports characterize the malicious cyber activity and provide little information on costs. Finally, the FBI publishes annual statistics of reported crimes, although at much lower levels than reflected in industry surveys.[7]

1.2 Data Challenges

The availability of data on the cost of malicious cyber activity has improved somewhat over the past five years, particularly for identifying trends; however, data available in the public domain on the cost of cyber incidents is sparse and inconsistent.[8] Most of the data on costs track back to insurance companies, but sample sizes for small business in particular are at most a few hundred. The Bureau of Justice Statistics only publicly posts data from 2005.[9] In particular, academic studies in general do not appear to be a good source of information on costs because victim data is treated as sensitive, private, or proprietary by the insurance and cyber security companies or law enforcement organizations that communicate with the victims.

Data sets vary widely from year to year, even for a single organization conducting the studies, in a way that cannot be explained by general trends in cyber threats (for example, the average cost reported by the National Small Business Association went from about $8.7K in 2012 to $20.7K in 2014 and then down to $7.1K in 2015).[10] The averages are heavily skewed by the largest incidents. Thus reported "averages" per incident for small companies range from about $7,100[11] to $149,000.[12] Median data might be more meaningful but are not consistently provided. The best estimate, from NetDiligence involving 259 firms with revenue less than $50 million in 2015,

---

[1] https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
[2] https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50
[3] For example, NetDiligence, 2017 Cyber Claims Study.
[4] Verizon, 2018 Data Breach Investigations Report.
[5] https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd&utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-194093869
[6] https://usa.kaspersky.com/blog/security_risks_report_financial_impact/
[7] https://pdf.ic3.gov/2016_IC3Report.pdf
[8] See Deloitte on lack of data: https://www2.deloitte.com/insights/us/en/industry/financial-services/demystifying-cybersecurity-insurance.html
[9] https://www.bjs.gov/index.cfm?ty=tp&tid=41
[10] http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf
[11] http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf
[12] https://usa.kaspersky.com/blog/security_risks_report_financial_impact/

provides an average cost of about $125,000, whereas the median cost was only about $39,000.[13] Other challenges include:

- **Reporting Bias:** The best data comes from insurance companies,[14][15][16] which means the victims had to meet basic standards of due diligence to qualify for the insurance and thus likely suffered lower losses. Most incidents (attempts) and many breaches (confirmed loss) are not reported or the data on the incidents is vague.[17] Understanding of legal requirements to report to the U.S. Government (e.g., the Securities and Exchange Commission (SEC) or a sector specific agency such as the Department of Energy) appears to be inconsistent. Small businesses may not even be aware of a breach unless notified by a third party (e.g., the FBI) and may not have the experience, resources, or even motivation to delve into the situation if the business continues to function. Some companies do not survive the event and rarely get included in any statistics. In addition, privately-owned small businesses are not subject to SEC reporting requirements.

- **Unsubstantiated Data:** Many reports repeat earlier data without sourcing or substantiation.[18][19][20] A study of the most dire claims found that they were decades old, untraceable, or even wrong.[21] In particular, a widely reported statistic of "60 percent of breached companies failed" was refuted by the organization cited as the origin in most reports.[22]

- **Reporting Time Lags:** Discovery and containment of malicious activity may take weeks to months. The actual costs may not be known for months. For example, Merck Pharmaceutical reported third quarter losses from the 2017 NotPetya incident but expected similar losses to be reported in the following quarter, in part because of what was still an ongoing disruption of some of its production lines.[23] Analysis and reporting of aggregated results from the industry surveys cited elsewhere in this proposal generally lag incidents by one or two years. Few organizations persist with such surveys beyond two or three annual intervals.[24]

- **Focus on Big Firms:** The definition of "small" varies among reports cited elsewhere in this report. These surveys almost exclusively focus on larger companies with 1,000 employees or more. The data creates some opportunities for extrapolation but do not consider the disproportionate impact on a smaller organization. Small businesses in general may be less attractive targets for financial crime but may serve as less-protected

[13] For example, NetDiligence, 2017 Cyber Claims Study.
[14] NetDiligence, 2017 Cyber Claims Study.
[15] Sasha Romanosky, "Examining the costs and causes of cyber incidents," Journal of Cybersecurity, 2(2), 2016, 121–135, doi: 10.1093/cybsec/tyw001, 8 August 2016
[16] Lloyds, Cyence, "Counting the Costs, Cyber Exposure Decoded," 2017.
[17] Verizon, 2018 Data Breach Investigations Report.
[18] For example: https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html
[19] This problem also appears in reports on disaster costs in general. See https://www.waytek.com/wp-content/uploads/2015/03/HP_Download_ImpactofDisaster.pdf.
[20] https://www.cyberdot.com/cyber-security/cyber-insurance/
[21] http://www.continuitycentral.com/feature0440.htm
[22] https://www.nextgov.com/cybersecurity/2017/05/how-fake-cyber-statistic-raced-through-washington/137542/
[23] https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/
[24] For example, the National Small Business Association published data from 2013 to 2015 and not more recently.

gateways to information from a larger partner enterprise (e.g., through a law firm). As noted in a recent Congressional report in support of a proposed "Small Business Advanced Cybersecurity Enhancements Act," small businesses make up an essential part of the supply chain to some large companies, many of which are in critical infrastructure sectors including the financial, transportation, power, water and healthcare sectors.[25] Many small businesses do not have dedicated IT departments and must outsource IT functions or assign these duties to an employee as a secondary function.

- **Distortion of Large Events:** The biggest events have a disproportionate influence on the perception of costs for an average business either because a large firm was the focus of a determined, sophisticated adversary (as opposed to a random victim) or because large events can spill over to many firms not intended as targets. The 2017 incidents WannaCry and NotPetya had global impact because of highly virulent malware and an intentionally destructive payload perpetrated, according to the U.S. Government, by nation state actors.[26]

- **Inconsistent Measures:** Surveys cited elsewhere in this proposal use inconsistent measures (by record, by incident, per employee). Costs get averaged across different time periods, sample sizes, and different types of activities. The counting of incidents can vary depending on the criteria for including attempts versus confirmed breaches.[27] The measures also are affected by inconsistent understanding of what happened. According to OMB, even federal agencies have trouble identifying what occurred in cyber incidents.[28] Finally, costs can be measured in dollars, percentages, or relative to local GDP.

[25] https://www.congress.gov/bill/115th-congress/house-bill/4668
[26] https://www.wired.com/story/white-house-russia-notpetya-attribution/
[27] Verizon, 2018 Data Breach Investigations Report.
[28] https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf

- **Uncontrolled Variables:** Reports cited elsewhere in this proposal include different types of losses, different regions of the world (see Figure 1), different periods of time, spans of different numbers of years (one to three typically), and different types of cyber events. Different companies count events depending on whether there was a "confirmed" data breach, as opposed to a denial of business capability.[29] Likelihood and costs also vary considerably by industry sector, according to these industry reports (see figures 2 and 3).

Region (World Bank)	Region GDP (USD, trillions)	Cybercrime Cost (USD, billions)	Cybercrime Loss (% GDP)
North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America and the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
MENA	3.1	2 to 5	0.06 to 0.16%
World	**$75.8**	**$445 to $608**	**0.59 to 0.80%**

Regional Distribution of Cybercrime 2017

FIGURE 1: Data from McAfee[30] demonstrating the regional variation of cyber crime.

[29] Verizon, 2018 Data Breach Investigations Report.
[30] https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd&utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-194093869

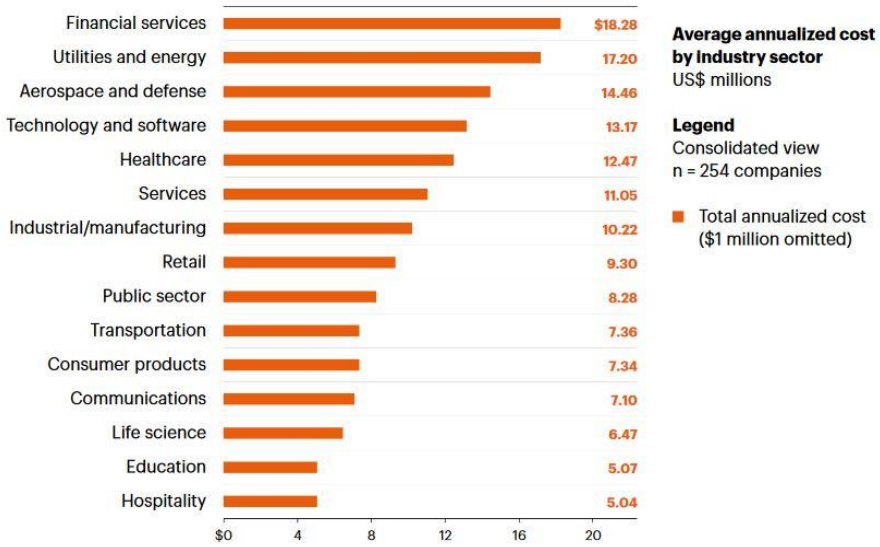


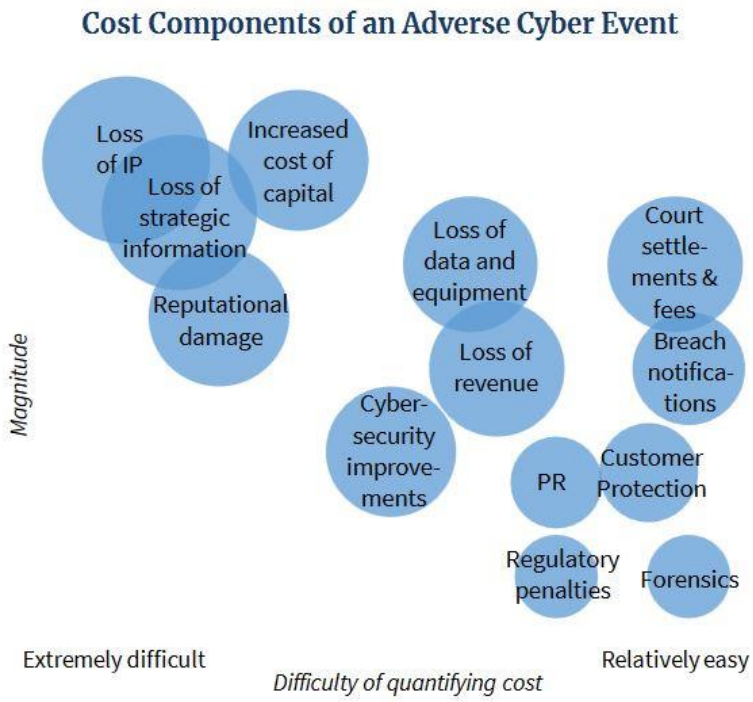
FIGURE 2: Data from Ponemon *showing the variation in costs by industry sector.*[1]

	Incidents				Breaches			
	Large	Small	Unknown	Total	Large	Small	Unknown	Total
Accommodation (72)	40	296	32	368	31	292	15	338
Administrative (56)	7	15	11	33	5	12	1	18
Agriculture (11)	1	0	4	5	0	0	0	0
Construction (23)	2	11	10	23	0	5	5	10
Education (61)	42	26	224	292	30	15	56	101
Entertainment (71)	6	19	7,163	7,188	5	17	11	33
Financial (52)	74	74	450	598	39	52	55	146
Healthcare (62)	165	152	433	750	99	112	325	536
Information (51)	54	76	910	1,040	29	50	30	109
Management (55)	1	0	1	2	0	0	0	0
Manufacturing (31–33)	375	21	140	536	28	15	28	71
Mining (21)	3	3	20	26	3	3	0	6
Other Services (81)	5	11	46	62	2	7	26	35
Professional (54)	158	59	323	540	24	39	69	132
Public (92)	22,429	51	308	22,788	111	31	162	304
Real Estate (53)	2	5	24	31	2	4	14	20
Retail (44–45)	56	111	150	317	38	86	45	169
Trade (42)	13	5	13	31	6	4	2	12
Transportation (48–49)	15	9	35	59	7	6	5	18
Utilities (22)	14	8	24	46	4	3	11	18
Unknown	1,043	9	17,521	18,573	82	3	55	140
Total	**24,505**	**961**	**27,842**	**53,308**	**545**	**756**	**915**	**2,216**

Table 1. Security incidents and breaches by victim industry and organization size

FIGURE 3: Verizon data showing variations in cost by industry sector.[31]

[31] Verizon, 2018 Data Breach Investigations Report.



1.3 Types of Losses

Cyber losses range from the immediate to long term to terminal (bankruptcy). Most surveys only include the immediate costs, and few seek to measure reputational costs (e.g., through stock prices). Most of the reports seem to include only the most immediate costs and do not look at the overall impact on the business, where the loss may be greatest, or even the cost of subsequent bank thefts enabled by earlier cyber thefts. When Equifax suffered a data breach in 2017, the stock prices of the other major credit monitoring firms declined along with the stock value of Equifax.[32] When the power went out in Ukraine in 2015 and again in 2016 because of cyber attacks, hundreds of thousands of people suffered indirect costs.[33] The data sets cited in this proposal in general do not include the impact of companies going out of business or the second and third order effects and liabilities related to partners, investors, employees, suppliers, and customers. In the other direction, reports also do not consider that not all "losses" are irretrievable given that many opportunities or sales can return once an event is over. Types of losses included in these reports range from immediate incident response expenditures to long-term loss of business viability and valuation (see Figure 4). *FIGURE 4:* Council of Economic Advisers breakdown of costs by size and difficulty to quantify.[34]

[32] https://money.usnews.com/investing/stock-market-news/articles/2017-09-19/credit-monitoring-companies-should-survive-equifax-efx-breach
[33] https://www.wired.com/story/crash-override-malware/
[34] https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

- **Investment in Cyber Security:** While the cost of cyber security is not a direct result of an incident, companies spend varying amounts of money on threat perception, size, and experience (see Figure 5).

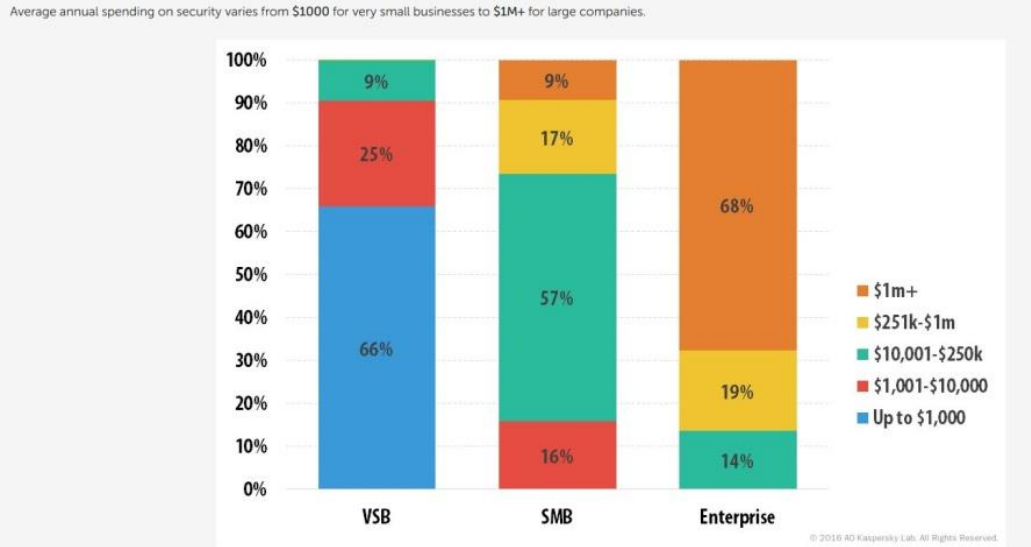


FIGURE 5: Data from Kaspersky *showing the range of spending on cyber security for different size businesses (very small, small-medium, enterprise).*[35]

- **Consumption of Resources:** Even without a company response, the company may be losing money as the adversary consumes IT resources and bandwidth.

[35] https://usa.kaspersky.com/blog/security_risks_report_financial_impact/

- **Incident Response:** The diversion of personnel and other resources to the immediate detection and containment of an incident is the most apparent loss (see Figure 6). Although some costs can be viewed as fixed costs, existing staff could be using this time more productively.

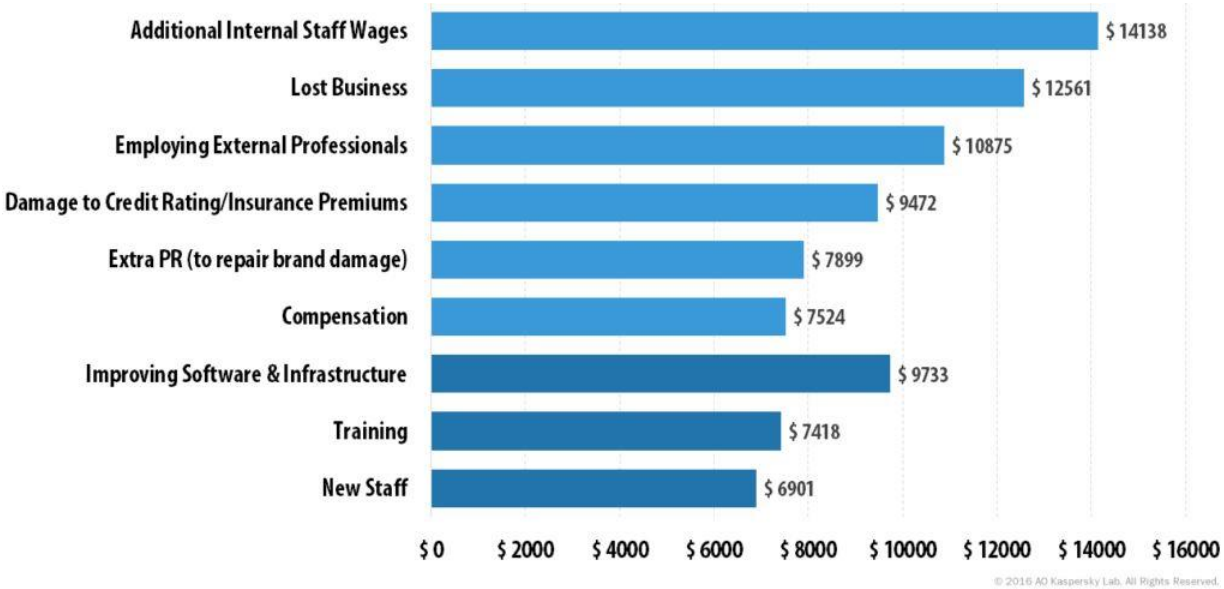


FIGURE 6: Data from Kaspersky *showing the breakdown of costs for cyber incident response.*[36]

[36] https://usa.kaspersky.com/blog/security_risks_report_financial_impact/

- **Disruption of Process:** Company activities may be slowed down, opportunities may be lost during the interim, and employee productivity can decline drastically. In some cases, manufacturing processes come to a complete halt, either directly because of an attack or indirectly through loss of infrastructure services such as bandwidth or power. The Merck Pharmaceutical experience in 2017 suggests this could be the greatest source of near-term losses.[37]

- **Loss of Physical Assets:** While less common, equipment can be rendered irreparable or destroyed (see Figure 7). Maersk in 2017 had to replace about 4,000 servers and 45,000 work stations.[38] In some cases, irreplaceable information is lost because it was not backed up (e.g. Atlanta police in 2018).[39]

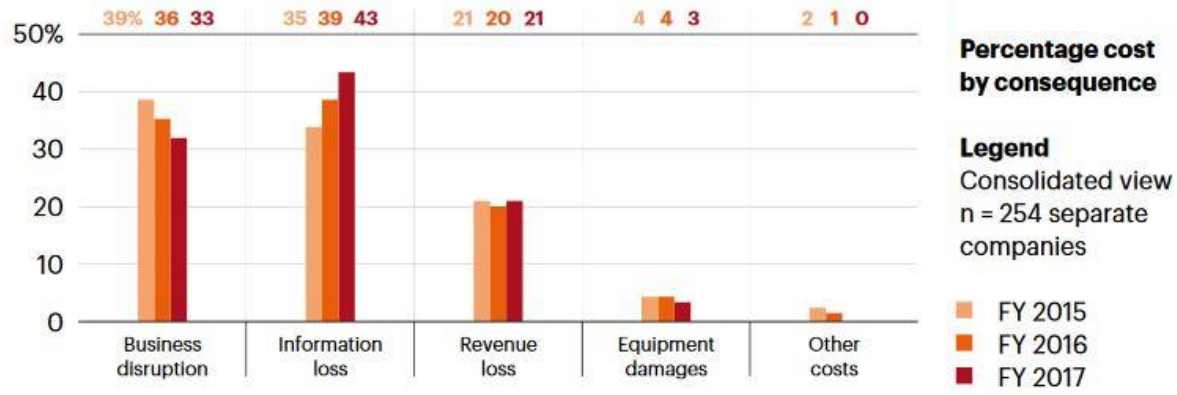


FIGURE 7: Data from Ponemon 2017[1] showing the distribution of sources for costs in a cyber incident beyond just incident response.

- **Loss of Intellectual Property:** This may be the most difficult loss to measure as it can lead to lost business opportunities to competitors, disadvantages in negotiations, or even loss of national security capabilities. The experience of companies that have lost intellectual property to China, as documented by USTR, suggests that this could be the greatest long-term cost or cause businesses to go bankrupt.[40]

- **Liability:** In the wake of a data breach, companies may have to compensate customers for fraud, credit monitoring, and delays or failures in production. Companies may also face significant legal costs to deal with law suits and regulators.

- **Direct Financial Loss:** Industry reports that make a distinction, show much greater losses when cyber events lead to infiltration of bank accounts,[41] in the worst cases potentially leading to bankruptcy. The greatest financial losses have involved direct

[37] https://www.reuters.com/article/us-merck-co-results/merck-says-cyber-attack-halted-production-will-hurt-profits-idUSKBN1AD1AO
[38] https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/
[39] https://www.hstoday.us/exclude-from-homepage/atlanta-police-lost-years-of-dashcam-footage-in-data-breach/
[40] https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF
[41] http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf

penetration of bank networks, providing access to all accounts, although such cases largely if not entirely have occurred outside the United States.[42]

- **Reputation:** As noted by the Council of Economic Advisers, company stock prices generally decline in the first seven days after a publicized cyber incident. In some cases, the price recovers; however, in others where reputation has suffered, the decline can represent a significant fraction of the company value (e.g., Equifax in 2017) and have impact on other related companies. Customers could lose faith in the ability of the company to execute, and companies may face increased borrowing costs or accelerated requirements to settle debts. Oddly, the data shows an increase in stock value for smaller firms, possibly an artifact of the number of smaller companies in the sample (see Figure 8).

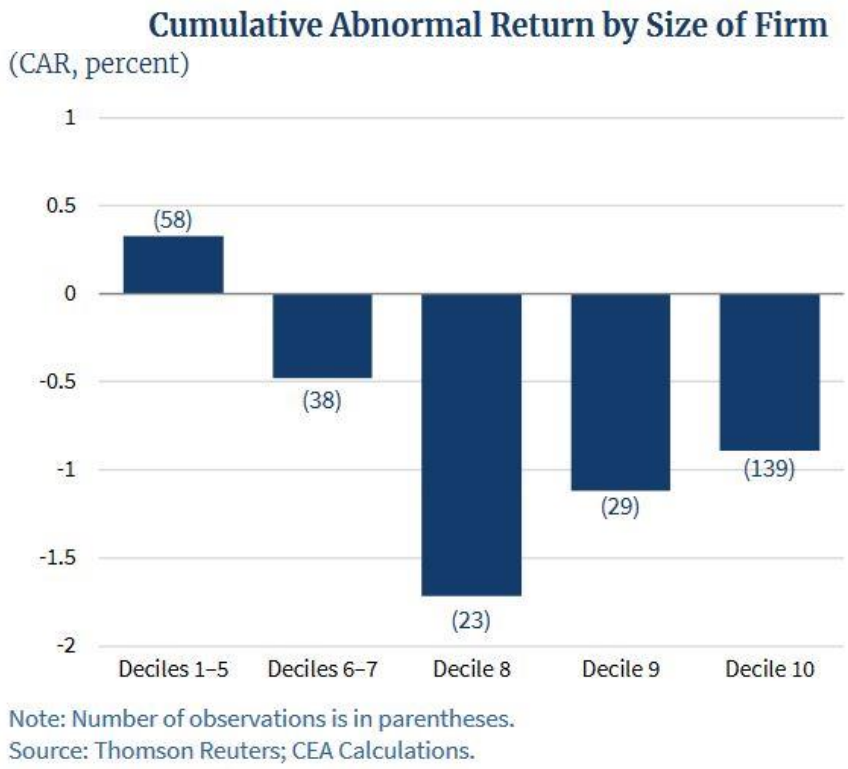


FIGURE 8: Council of Economic Advisers analysis of stock prices for companies experiencing a cyber incident.[43]

[42] https://web.archive.org/web/20150217133401/https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/
[43] https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

1.4 Overall Estimates

No single published number provides an overall answer. The Council of Economic Advisers assesses total national costs for 2016 in the range of 0.3 – 0.7 percent of GDP (also see Figure 10).[44] McAfee estimates 0.7 – 0.9 percent of GDP in the United States and Europe, but sees lesser percentages elsewhere. FBI notes that *reported*[45] losses from crime for the same year add up to only about 1 - 2 percent of the value noted by the Council of Economic Advisers,[46] but FBI also notes a trend of increasing cost per incident (see Figure 10). Kaspersky provides better data for smaller companies, but these are from around the world. Kaspersky estimates a cost of $149,000 per breach for smaller companies and $2 million for larger companies.[47] Ponemon estimates a cost of about $1,700 per employee ("seat") for the smallest quartile of the 257 companies it surveyed in 2017.[48]

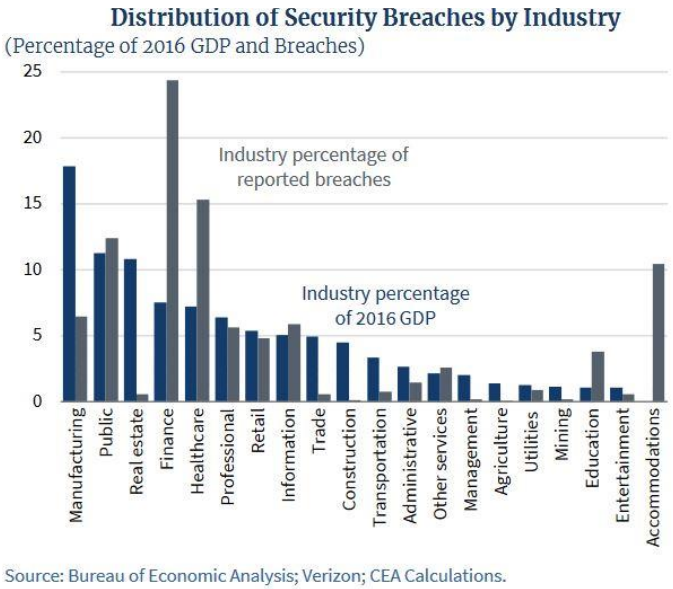


FIGURE 9: Council of Economic Advisers analysis showing relative contribution to GDP of industry sectors experiencing cyber incidents.[49]

[44] https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
[45] https://pdf.ic3.gov/2016_IC3Report.pdf
[46] https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
[47] https://usa.kaspersky.com/blog/security_risks_report_financial_impact/
[48] https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50
[49] https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

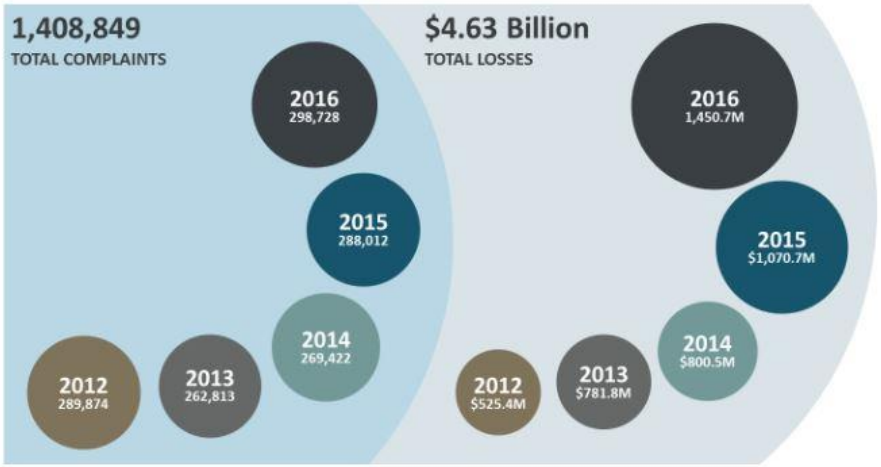


FIGURE 10: Data from FBI *showing the increasing costs from reported cyber crimes from 2012 to2016.*[50]

2.0 Strategy for Empirical Analysis

The key to any meaningful empirical analysis will be a comprehensive model of how cyber events can impact a small business (see Figure 11 below). This would begin with a broad representation of business activities and how they interact with IT systems and data. Activities would include sales, services, manufacturing, software and hardware development, data processing, automated process control, communications, administrative and logistic functions, and financial or banking transactions. The model would need to consider the internal enablers for the business (including the employees), facilities, and equipment. It would also need to consider external factors, such as utilities, suppliers, and third-party entities. In addition to direct costs (such as providing credit monitoring for victims of a data breach), the model would need to consider consumer and investor confidence, productivity, and overall company reputation. Finally, the model would need to consider the impact of government through regulation, taxes, and the judicial system. The general model could then be tailored to specific industry types.

Next, the analysis would need to consider the full range of direct and indirect impacts of malicious cyber activity on a small business (see Tables 1-3 below). Direct impacts on data include the theft of information, the loss of access to data, and the manipulation of data that could lead to fraud, reputation loss, or disruption. Business processes and transactions could be disrupted or damaged, resulting not only in direct impact on the business, but potentially in harm to third parties.

The analysis would then need to consider follow-on costs such as incident response and harm or delays in the actual business. These events, as businesses already experience with natural disasters, could require large capital outlaws to restore business capability, increased insurance premiums and credit costs, or even bankruptcy or sale of the company. Company employees

[50] https://pdf.ic3.gov/2016_IC3Report.pdf

may suffer layoffs or just move on while waiting for the company to recover. As attacks become more sophisticated against an increasingly cyber-dependent infrastructure, the stakes could rise to include environmental damage, injuries, and death.

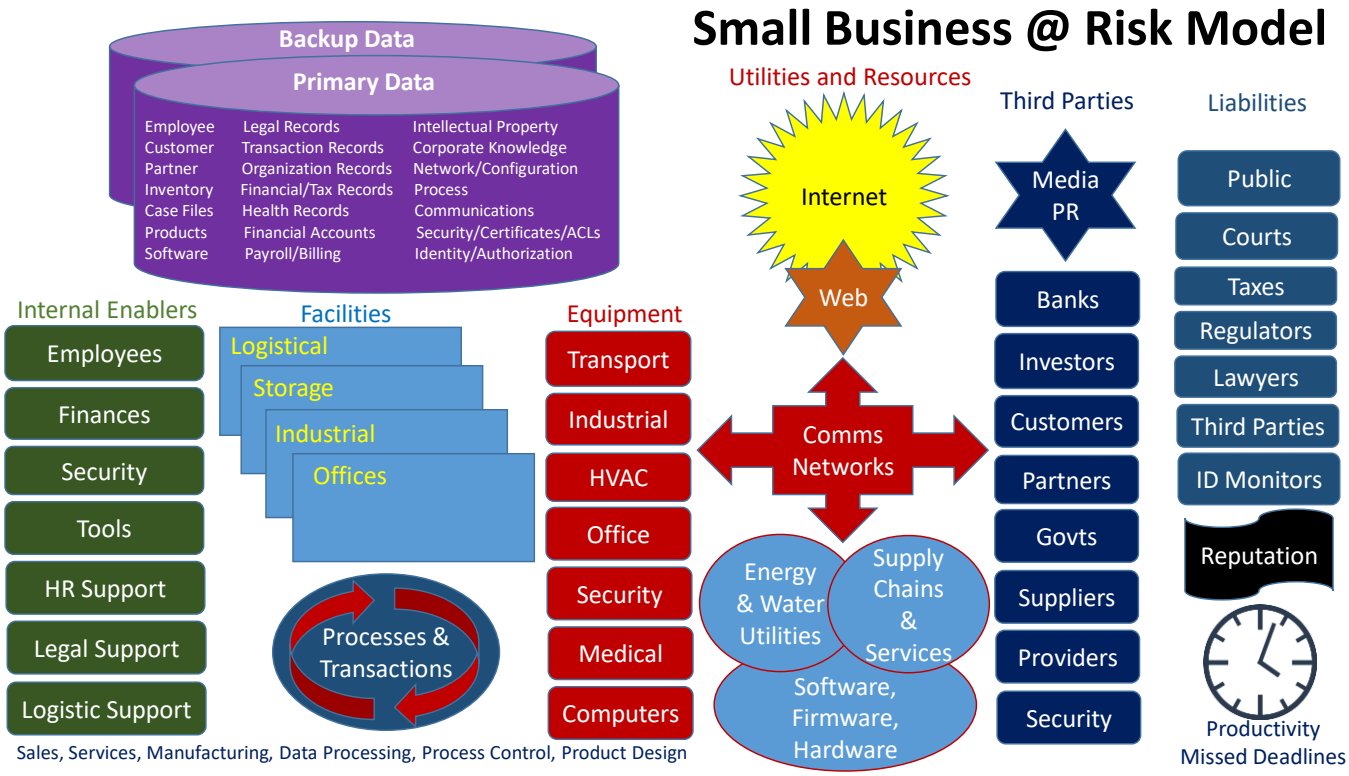


FIGURE 11: Potential business elements that could contribute to overall costs in a cyber incident.

Table 1: Categories and Types of Business Loss From Malicious Cyber Activities

Adversary Activity	Losses or Disruptions
Adversary Steals Copy of Data	Data that can be used for authentication of access to other records, processes, money (passwords, PII) Data that compromises privacy, reputation (e.g., health, e-mail) Content that can be used for business decision advantage (bargaining positions) Content that can be used for innovation/manufacturing advantage (know how)
Adversary Disrupts Access to Networks and Data	Inability to operate networks Inability to conduct financial transactions (payroll, billing, receipts, acquisition, investing) Inability to conduct administrative, sales, services, acquisition, or inventory activities Inability to communicate with employees, partners, suppliers, etc Inability to control physical logistical, medical, environmental, and industrial processes Inability to secure networks or physical systems
Adversary Manipulates Data, Systems, and Networks	Unauthorized identities/access (spoofing) Changes to data (hide or create false records of past activities, transactions, or history) Enabling of fraudulent activities (identities, permissions, transactions, configurations, set points) Creation of false documents or communications Disabling of normal transactions or controls (e.g., safety or security) Injection of malicious code into deployed software or supply chain Rerouting of network connections

Table 2: Impact of Malicious Cyber Activities on Business Processes

Impact on Business Networks, Facilities, Environment, and Personnel
Process data loss or access denied
Process or safety control denied, disrupted, or manipulated
Process software or firmware deleted, disrupted, or manipulated
Network hardware or process equipment physically damaged or destroyed or rendered unusable
Loss of utility services (power, water, telecommunications, HVAC)
Facilities or transportation systems physically damaged or destroyed or rendered unusable
Third-party services or processes delayed, blocked, or halted
Loss of control of hazardous substances (chemicals, petroleum related)
Environmental damage
People injured or killed

Table 3: Business Expenses in Wake of Malicious Cyber Activities

Category of Expense	Expenses
Incident Response	Company response resources (IT, PR, legal, leadership)
	Hiring of third-party security services and forensics
	Notification of harmed parties (call centers, mailings, etc)
	Monitoring of credit/financial status of harmed parties
	Data backup and service/process restoration
	Physical cleanup and repair
	Public relations cost
	Medical costs
	Legal and other advisory/consultant costs
Business Process	Reputational cost (loss of future customers and investors)
	Company value (stocks)
	Damage liabilities (law suits, settlements, reparations)
	Replacement costs (networks, equipment, software)
	Opportunity costs (loss of current time, productivity, and transactions)
	Missed deadlines (product delivery, legal and regulatory obligations)
	Loss of personnel (current forced to move on, future recruitment)
	Increase in future insurance premiums
	Increased cost of future credit
	Delays in health care
	Bankruptcy, collapse, or sale of company