SCHOOL OF PUBLIC POLICY
CENTER FOR INTERNATIONAL & SECURITY STUDIES AT MARYLAND

A Proposed Hierarchical Taxonomy for Assessing the Primary Effects of Cyber Events: A Sector Analysis 2014-2016

By Charles Harry, PhD

CISSM Working Paper

February 2018

Center for International and Security Studies at Maryland
4113 Van Munching Hall, School of Public Policy
University of Maryland
College Park, MD 20742
(301) 405-7601

Abstract

Publicity surrounding the threat of cyber-attacks continues to grow, yet immature classification methods for these events prevent technical staff, organizational leaders, and policy makers from engaging in meaningful and nuanced conversations about the risk to their organizations or critical infrastructure. This paper provides a taxonomy of cyber events that is used to analyze over 2,431 publicized cyber events from 2014-2016 by industrial sector. Industrial sectors vary in the scale of events they are subjected to, the distribution between exploitive and disruptive event types, and the method by which data is stolen or organizational operations are disrupted. The number, distribution, and mix of cyber event types highlight significant differences by sector, demonstrating that strategies may vary based on deeper understandings of the threat environment faced across industries.

Introduction

Network security is increasingly recognized as a strategic vulnerability as a growing number of corporate intrusions are reported. These breaches can affect customer privacy, confidence in a company's ability to protect core intellectual property, and essential operations. Large numbers of intrusions have also occurred into government networks, with recent high-profile breaches including a significant compromise at the Office of Personal Management (OPM) and at the credit monitoring service Equifax.

As the private and public sectors grapple with the problem of cyber events, disagreement remains regarding what can and should be done. Technical solutions, organizational resiliency, employee education, and improvements in system controls are among many options to reduce risk. Yet, they are rarely evaluated as part of a strategic approach for addressing diverse threats, which vary by industry.

Confusion about threats and response options originates in part from imprecision in how we categorize and measure the range of disruptive cyber events. By failing to recognize the distinctions between specific forms of attack, the effects they produce on the targeted networks, the financial strain they place on the targeted organizations, or their broader effects on society, this confusion leads to the misallocation of resources.

This paper provides a new taxonomy that expands on earlier work by the author and colleagues to classify cyber incidents by the range of disruptive and exploitative effects produced. It applies the taxonomy in a sector-based analysis of 2,431 publicized cyber events from 2014-2016. It finds some striking differences across industries in the scale, method of attack, and distribution of effect. Government and Professional Services face the largest number of attacks. Governments experience a mix of disruptive and exploitive events, whereas retail and hotel operators primarily face exploitive attacks. These findings highlight the need for deeper analysis by sector to assess the risk for specific organizations and critical infrastructure. They also suggest the importance of tailoring risk mitigation strategies to fit the different threat environments in various sectors.

Cyber Taxonomies

A confusing array of cyber threat classification systems have been proposed over the past two decades. Some are based on different phases of the hacking process, while others focus on specific targets. For example, de Bruijne et al (2017) has created a classification of actors and methods, whereas Gruschka (2010) develops a taxonomy of attacks against cloud systems. Other classification approaches focus on specific techniques, such as Distributed Denial of Service or DDoS attacks (Mirkovic 2004); specific targets, such as browsers (Gaur 2015); or particular IT capabilities, such as industrial control systems (Zhu 2017) and smart grids (Hu 2014).

Few taxonomies in the information security literature seek to classify events by impact on the target, the key question for risk assessment. Only two (Howard 1998) and (Kjaerland 2005) directly propose categories of the effect to the victim. Others including Hansman (2005) focus on the attack vector, vulnerabilities, and exploits, while incorporating Howard's work on effect categories as part of their broader classification system.

Howard's widely cited taxonomy includes classification methods for attackers, objectives, tools, access, and impact. He divides the impact of cyber activity, described as the "unauthorized results," into five categories: Corruption of Data, Disclosure of Information, Denial of Service, Increased Access, and Theft of Service.

Kjaerland (2005) classifies cyber effects differently and as belonging to one of four categories: Disrupt, Distort, Destruct, and Disclosure. He develops these categories in concert with other dimensions of analysis to evaluate the linkage between sector, actor, method, and target.

Both of these effect-based taxonomies fail to meet basic standards of a well-defined taxonomy (Ranganathan 1957), including:

Exclusiveness - No two categories should overlap or should have the same scope and boundaries.

Ascertainability - Each category should be definitively and immediately understandable from its name.

Consistency - The rules for making the selection should be consistently adhered to.

Affinity and Context - As you move from the top of the hierarchical classification to the bottom, the specification of the classification should increase.

Currency - Names of the categories in the classification should reflect the language in the domain for which it is created.

Differentiation -When differentiating a category, it should give rise to at least two subcategories

Exhaustiveness - The classification should provide comprehensive coverage to the domain of interest.

Howard's taxomony fails the *exhaustiveness* requirement because some important and increasingly common types of cyber events do not fit any of its categories. Examples of these omissions include attacks on Supervisory Control and Data Acquisition (SCADA) systems, data deletion resulting from the use of wiper viruses, or social media account hijacking and website defacement.

The Howard taxonomy also fails the test of exclusivity by including two overlapping effects categories: Increased Access and Theft of Resources. Most hackers seek greater access and misuse system resources as a means to an end, not as the final result. Their ultimate goal is not just access, but the illicit acquisition of information or the disruption of organizational services. For example, if a hacker wanted to illicitly gain and disseminate information about a company, they would first obtain unauthorized use of a specific computer or network. Using Howard's categorization of that activity we would have to define a hack of a company database as both a *Theft of Resources* as well as a *Disclosure of Information* event type.

Kjaerland's classification system also fails important tests for a well-designed taxonomy. By allowing the same event to be assigned to multiple categories, it violates the criteria of exclusivity and consistency. For example, Kjaerland's definition of *Destruct* notes that "Destruct is seen as the most invasive and malicious and may include Distort or Disrupt."

Kjaerland also fails the test of context by mixing impact classification (e.g. destruction of information) with specific tactics or tools. For example, in his definition of *Disrupt* he classifies use of a Trojan as a Disrupt event. However, a Trojan is a technique of hiding a malicious program in another. That technique can cause many different types of effects depending on whether it is used to steal or destroy information.

A New Taxonomy

This paper extends previous work (Harry 2015) (Harry & Gallagher 2017) to offer a new taxonomy for classifying the primary effects on a target of any given cyber event.

I define a cyber event as the result of any single unauthorized effort, or the culmination of many such technical actions, that *engineers, through use of computer technology and networks, a desired primary effect on a target*. For example, if a hacker used a spearphish email to gain access and then laterally moved through the network to delete data on five machines, that would count as a single event type whose primary effect resulted in the destruction of data. This encapsulation of hacker tactics and tradecraft into specification of the primary effect of those actions is what I define as a cyber event.

In the risk assessment framework developed at the Center for International and Security Studies at Maryland (CISSM), primary effects are the direct impacts to the target organization's data or IT-enabled operations. Cyber events can also cause secondary effects to the organization, such as the financial costs of replacing equipment damaged in an attack, a drop in the organization's stock price, due to bad publicity from the attack, or a loss of confidence in the organization's ability to safeguard confidential data. And, they can cause second order effects on individuals or organizations who rely on the targeted organization for some type of goods or services. These could include effects on the physical environment, the supply chain, or even distortions an attack might have on an individual's attitudes, preferences, or opinion deriving from the release of salacious information. While these are important areas to consider, they are outside of the scope of this paper.

Any given cyber event can have one of two types of primary objectives: the disruption to the functions of the target organization, or the illicit acquisition of information. An attacker might disrupt an organization's ability to make products, deliver services, carry out internal functions, or communicate with the outside world in a number of ways. Alternatively, hackers may seek to steal credit card user accounts, intellectual property, or sensitive internal communications to get financial or other benefits without disrupting the organization's operations.

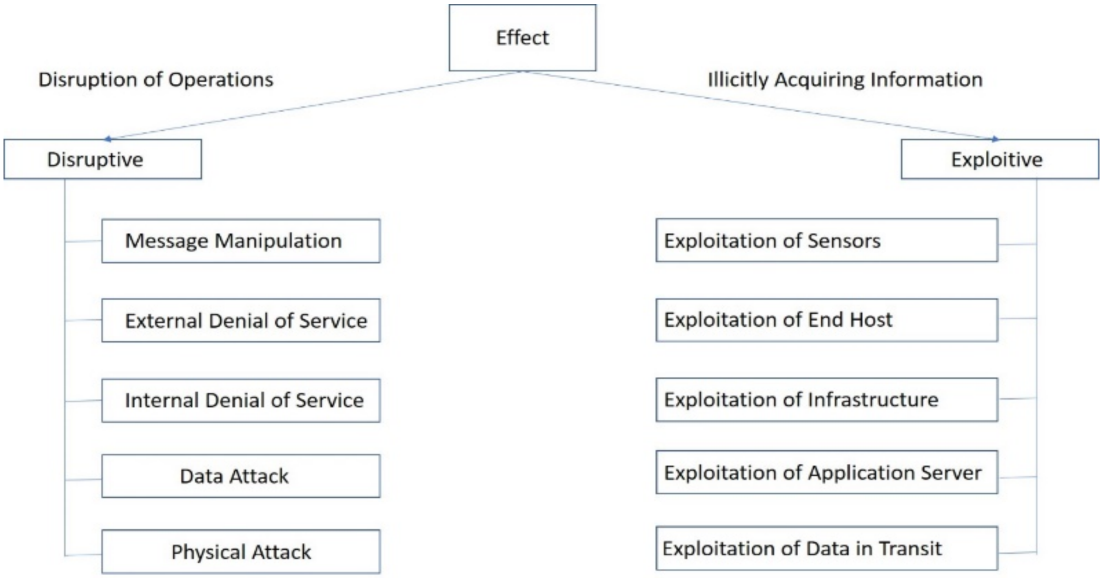

Effect
Disruption of Operations
Illicitly Acquiring Information
Disruptive
Exploitive
Message Manipulation
External Denial of Service
Internal Denial of Service
Data Attack
Physical Attack
Exploitation of Sensors
Exploitation of End Host
Exploitation of Infrastructure
Exploitation of Application Server
Exploitation of Data in Transit

Figure 1: Cyber Event Taxonomy

Disruptive Events

A malicious actor may utilize multiple tactics that have wildly different disruptive effects depending on how an organization uses information technology to carry out its core functions. For example, an actor could delete data from one or more corporate networks, deploy ransomware, destroy physical equipment used to produce goods by manipulating Supervisory Control and Data Acquisition (SCADA) systems, prevent customers from reaching an organization's website, or deny access to a social media account.

Disruptive effects can be classified into five sub-categories depending on the part of an organization's IT infrastructure that is most seriously impacted, regardless of what tactic or techniques were used to accomplish that result. They are: Message Manipulation, External Denial of Service, Internal Denial of Service, Data Attack, and Physical Attack.

Message Manipulation. Any cyber event that interferes with a victim's ability to accurately present or communicate its "message" to its user or customer base is a Message Manipulation attack. These include the hijacking of social media accounts, such as Facebook or Twitter, or defacing a company website by replacing the legitimate site with pages supporting a political cause. For example, in 2015, ISIS affiliated hackers gained access to the YouTube and Twitter accounts for US CENTCOM. The hackers changed the password, posted threatening messages to U.S. Service members, and replaced graphics with ISIS imagery (Lamothe 2015). Similarly, in 2016, the website for the International Weightlifting Federation (IWF) was defaced after a controversial decision to disqualify an Iranian competitor (Cimpanu 2016). Both events used different tactics, but the primary effect on the targeted organization's ability to interact with its audience was the same.

External Denial of Service. If an attacker executes a cyber-attack from devices outside the target organization's network that degrades or denies the victim's ability to communicate with other systems, it is classified as an External Denial of Service event. For example, the 2016 Mirai botnet attack leveraged a compromised set of devices worldwide to overwhelm the DYN corporation with domain name look-up requests, causing a number of major internet platforms and services that rely on DYN's services to stop functioning for many hours (Woolf 2016). While there are many types of Distributed Denial of Service (DDoS) attacks (ICMP flood, SYN flood, ping of death, etc.), any of those techniques would produce outcomes that fit the External Denial of Service cyber event category.

Internal Denial of Service. When a cyber event executed from inside a victim's network degrades or denies access to other internal systems, it is an Internal Denial of Service attack. For instance, an attacker who had gained remote access to a router inside an organization's network could reset a core router to factory settings so that devices inside the network could no longer communicate with one another. The anti DDOS vendor Staminus apparently experienced such an internal denial of service attack in 2016. It issued a public statement that "*a rare event cascaded across multiple routers in a system-wide event, making our backbone unavailable." (Reza 2016).* An attacker using malware installed on a file server to disrupt data sent and received between itself and a user workstation would achieve a similar effect.

Data Attack. Any cyber event that manipulates, destroys, or encrypts data in a victim's network is categorized as a Data Attack. Common techniques include the use of wiper viruses and ransomware. Using stolen administrative credentials to manipulate data and violate its integrity, such as changing grades in a university registrar's database would also fit this category. For example, in 2017 the mass deployment of the NotPeyta ransomware resulted in thousands of data attack cyber events against individuals as well as to small, medium, and large businesses, with one case costing the shipping firm Maersk over $200 million (Matthews 2017).

Physical Attack. A cyber event that manipulates, degrades, or destroys physical systems is classified as a Physical Attack. Current techniques used to achieve this type of effect include the manipulation of Programable Logic Controllers (PLC) to open or close electrical breakers or utilize user passwords to access and change settings in a human machine interface to overheat a blast furnace, causing damage to physical equipment. For example, in the December 2015 cyber-attack on a Ukrainian utility, a malicious actor accessed and manipulated the control interface to trip several breakers in power substations. This deenergized a portion of the electrical grid and tens of thousands of customers lost power for an extended period of time (Lee et al 2016).

Exploitive Events

Some cyber events are designed to steal information rather than to disrupt operations. Hackers may be seeking customer data, intellectual property, classified national security information, or sensitive details about the organization itself. While the tactics or techniques used by malicious actors may change regularly, the location from which they get that information does not. I define five categories of an exploitive event below: Exploitation of Sensors, Exploitation of End Hosts, Exploitation of Infrastructure, Exploitation of Application Servers, and Exploitation of Data in Transit.

Exploitation of Sensors. A cyber event that results in the loss of data from a peripheral device like a credit card reader, automobile, smart lightbulb, or a network-connected thermostat is categorized as an Exploitation of Sensor event. The attack on Eddie Bauer stores where hackers gained access to hundreds of Point of Sale machines and systematically stole credit card numbers from thousands of customers fits this category (Krebs 2016). Other examples include illicit acquisition of technical, customer, personal, or organizational data from CCTV cameras, smart TVs, or baby monitors.

Exploitation of End Hosts. Hackers often are interested in the data stored on user's desktop computers, laptops, or mobile devices. When data is stolen through illicit access to devices used directly by employees of an organization or by private individuals it is categorized as an Exploitation of End Host cyber event. Tactics used in this type of attack include sending a malicious link for a user to click or leveraging compromised user credentials to log in to an account.

Exploitation of Network Infrastructure. When data is compromised through direct access to networking equipment such as routers, switches, and modems, the attack is classified as an Exploitation of Network Infrastructure event. These types of events involve a hacker who, through use of an exploit or credential compromise, gains direct access to the underlying infrastructure. For example, a malicious actor who used a vulnerability in the CISCO IOS operating system to steal configuration information from an organization's core routing infrastructure would engineer an Exploitation Network Infrastructure cyber event.

Exploitation of Application Server. Malicious actors who, through misconfiguration or vulnerability, gain access to data contained in a server-side application (e.g. database) or on the server itself would generate an Exploitation of Application Server event. A hacker using a SQL injection to access millions of customer records or the direct access of an e-mail server with all organizational correspondence would fit into this category. For instance, the compromise of data in the Office of Personnel Management was the result of access by a malicious actor to a database hosted on a server (Koerner 2016). Stealing the data required several steps and months of work, but the event is classified by its ultimate outcome—loss of sensitive information from central servers hosting large database applications.

Exploitation of Data in Transit. Hackers who acquire data as it is being transmitted between devices cause Exploitation of Data in Transit events. Examples of this type of event include the acquisition of unencrypted data as it is sent from a PoS device to a database or moved from an end-user device through an unsecured wireless hotspot at a local coffee shop.

Testing the Taxomony on Cyber Events 2014-2016

The best way to assess how well this classification system meets the criteria for a well-defined taxonomy is to see whether it can be easily and unambiguously used to categorize all the events in an extensive data set.

Unfortunately, there are no public datasets of cyber attacks that include a variety of cyber events with a range of both exploitive and disruptive effects. Most public data repositories focus on some types of events to the exclusion of others. The Privacy Rights Clearinghouse, for example, has a dataset focused on domestic exploitive attacks, while the blog H-zone.org has a dataset focused on website defacement attacks (a subset of Message Manipulation). Other datasets are on privately maintained blogs and webpages. Some do not use a repeatable process to classify or categorize by sector thereby limiting the range of analysis that can be applied. Others are compiled from proprietary data or are only available for a steep fee.

To create a dataset that had the information needed to test the CISSM taxonomy, the author used systematic web searches to identify cyber events that could be characterized by their effects. Initial searches for generalized references to cyber attacks yielded 3,355 possible events that were referenced by blogs, security vendor portals, or other English-language news sources from January 2014 through December 2016.

Of the initial 3,355 candidate cyber events initially discovered, 2,431 were included in the dataset (72%). Media reports about 909 of the candidate events were broad discussions of malware campaigns or generalized discussions about threat actor plans and tactics. These were excluded because they did not provide information on the primary effect to a specific victim. Media reports about an additional 15 events specifically spoke to the tactics used by the threat actor independent of the effect to the primary victim, so they were also discarded. For example, one source discussed the use of compromised Amazon Web services credentials to access a system but did not talk about what types of actions took place once in the target network.

In complex cases where the victim suffered multiple effects (e.g. website defacement and DDoS), the dataset counts each effect as a separate, but overlapping, event registered to the victim. Cyber events were coded to include date, event type, organization type (using the North American Industrial Classification System (NAICS), a description of the event, and a link to the source.

This dataset is not an exhaustive accounting of all cyber events during this period. It only includes events for which there was a direct news source that was verifiable and that provided some insight into the methods of the attack. The true population of malign cyber activity is unknown because some significant events are kept secret and many other cyber incidents are too trivial to warrant media attention. Nevertheless, this dataset includes a large enough number of events for it to be useful for testing the taxonomy and making rough generalizations about relative frequencies of different types of events in different sectors.

As discussed earlier, a well-designed taxonomy should, among other things, account for all the items to be classified, clearly differentiate among categories, ensure that each item has a unique classification, and have clear rules that can be consistently applied. The CISSM cyber event taxomony easily passed each test.

Each of the 2,431 events in the dataset could be coded as either Exploitive or Disruptive and assigned to one of ten effect-based sub-categories in the CISSM taxonomy. This fulfills the exhaustiveness requirement. Treating complex attacks in which multiple effects were achieved by the hacker as a set of separate but overlapping events made it possible to apply the taxonomy in a consistent manner, to differentiate between categories of effect, and to maintain clear differentiation between the categorized effects. This analysis did not assess the taxonomy's currency, ascertainability, or affinity, because these standards should be judged by individual users rather than the creator of the taxonomy.

Many cyber classification systems run into the same three major problems: Their inability to distinguish between tactics and effects; their difficulty remaining relevant as threat actors change and hacking techniques evolve; and their applicability to some types of IT systems, but not others. The CISSM taxonomy disentangles stable categories of effects from the rapidly advancing tactics employed by an ever-changing set of state and non-state hackers in a way that can be applied to all IT systems in use today or envisioned for the future.

Using the Taxonomy to Analyze Cyber Events

Categorizing cyber events according to their effects rather than treating them as an indistinguishable, but ever increasing, mass of "cyberattacks" yields a number of useful insights. Of the 2,431 cyber events during the three-year period reviewed, over 70 percent (1,700) were exploitive, whereas 30 percent (725) were disruptive. This ratio appears to relatively stable when examining events on a yearly basis, too. Of the 633 events recorded in 2014, 67 percent (423) were exploitive, and 33 percent (210) were disruptive. Of the 843 cyber events in 2015, 67 percent (563) were exploitive and 33 percent (280) were disruptive. And of the 955 events recorded in 2016, 75 percent (714) were exploitive events, compared with 25 percent (241) that were disruptive.

Of the 1,700 exploitative events, the two most common sub-categories are Exploitation of Application Server events and Exploitation of End Host events. Ninety percent of all exploitive events in the dataset fall into one of these two categories. This reflects the current popularity of SQL injection attacks against web applications, and the heavy use of spearphising campaigns against end users.

A much smaller percentage of exploitative attacks fall into the other three categories, most likely because these types of events often require internal access, are inherently more difficult to pull off, are not as well monitored, or are not as well publicized. Exploitation of Sensor events represent only 5 percent of the exploitive events sample, probably because the value of data from many of the devices in this category, like smart thermostats and baby monitors, might not be as large as records from other sources. Whereas a ready market exists on the Dark Web for customer data stolen from POS devices, most types of sensor data will not be of broad interest.

The remaining 5 percent (90) of cyber events were divided between Exploitation of Network Infrastructure (70 events) and Exploitation of Data in Transit (20 events). These events often reflected the efforts of more skilled hackers who can leverage toeholds in networks to expand internal access and acquire information either from network infrastructure such as file shares or from unencrypted data passed internally through the network.

The 725 disruptive cyber events in the dataset follow a similar pattern with most activity falling into categories that are generally less problematic. Ninety-six percent of all disruptive events are either Message Manipulation (60 percent, 433) or External Denial of Service (36 percent, 263) events. This events reflect efforts by malign actors using less sophisticated techniques to deface websites that are vulnerable to external access and manipulation, weak passwords surrounding social media accounts, or high levels of DDoS activity applied by actors against identified targets.

The remaining 5 percent (29 events), are split between Internal Denial of Service (2 percent, 11 events), Data Attack (2 percent, 14 events), or Physical Attack (1 percent, 4 events). These types of events involved internal networks, so they required more sophisticated access techniques or malware leveraged to engineer the intended disruptive effects.

Sector Analysis for Cyber Events

While looking at a general breakdown of cyber event type is useful, further analysis by sector reveals interesting variation of effect between industries. To conduct this analysis, the author coded the 2,431 cyber events collected using the North American Industrial Classification System (NAICS), a hierarchical classification system commonly used by the U.S. government and industry to collect, analyze, and publish information on the U.S. economy. The data set likely reflects over or under sampling in some industries and event types with specific state and federal laws requiring the publication of cyber-attacks with others not requiring the same notification. For example, the State of Maryland's Personal Information Protection Act imposes a 45-day notification requirement for businesses to notify residents when their personal data has been compromised, yet there is no such requirement when a business' website has been defaced.

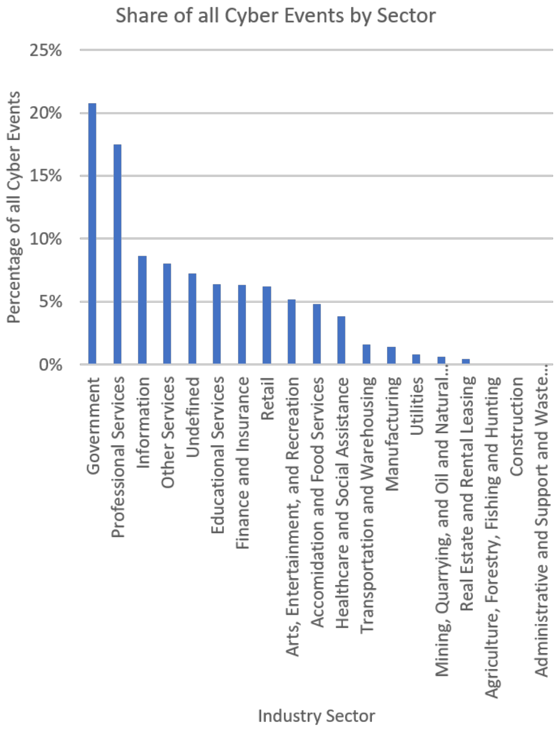


Figure 2: Share of all Cyber Events by Sector

An analysis of cyber event activity by sector reveals three interesting themes. First, while most industry sectors are represented in the data, some appear to be targeted by malicious actors more frequently. Second, the distribution between exploitive and disruptive event types varies by sector, with some sector's distribution diverging significantly from the overall average. Finally, industrial sectors experience a range of event types, with some industries experiencing very specific categories of effect while others being targeted for a broad range of effects.

In Figure 2, the level of cyber event activity in different sectors is ranked into three tiers—High, medium, and low—to identify which sectors are currently most prone to the types of cyberattacks that make it into the public record. Sectors that experience more than 15 percent of all cyber events in our dataset fit into the highest tier. Government services and professional services fall into this category; together, they account for 38 percent of all events recorded.

Medium-activity sectors include those that see at least 3.8 percent, but less than 15 percent, of the events in the full dataset. Sectors falling into this tier include information services, education, healthcare, finance, retail, entertainment, and accommodation services. The nine sectors in this category experienced approximately 56.7 percent of the total number of cyber events, suggesting that a larger breadth of industries is affected by significant numbers of cyber events.

The lowest activity tier includes sectors that had fewer than 3.8 percent of the total events. This tier includes traditional industries that are less dependent on information technology than other sectors of the modern economy, such as agriculture, mining, real estate, and construction. Two sectors considered critical infrastructure—transportation and utilities—also fell into this tier.

In addition to the frequency of event activity, the nature of those effects is also an important factor in assessing risk to specific sectors. In Figure 3, the percentage of total cyber events characterized as exploitive is plotted versus the percentage that are disruptive in nature. Only the ten sectors with the highest frequencies of cyber events are represented in the figure, as many of the low tier sectors have too few observations to draw meaningful conclusions.

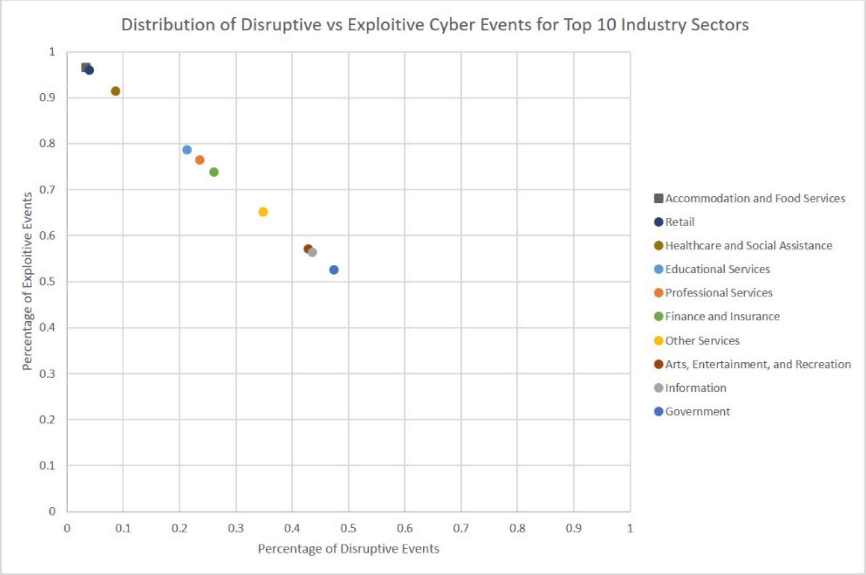


Figure 3: Exploitive vs Disruptive as a Share of Total Events for Top 10 Industry Sectors

Among the industries that are represented, there appears to be significant differences in the relative frequencies of exploitative versus disruptive events. For instance, the Retail and Accommodation and Food Services sectors predominately experience exploitation events (>95 percent Exploitive) whereas the Government Services sector faces a broader mix of exploitation and disruptive events (53 percent Exploitive, 47 percent Disruptive).

The only sectoral category where the relative frequency of exploitative and disruptive events is roughly the same as in the entire data set (70 percent Exploitive, 30 percent Disruptive) is the "other" category. The relative frequency within most sectors is significantly different from the average distribution. This highlights the importance of assessing risks on a per industry basis instead of applying general guidance about what types of cyber events are most common.

Lastly, the categories of cyber events are also found to vary between sectors. Table 1 highlights all cyber events, by share, drawing out some interesting differences. For example, while Accommodation and Food Services represent only 4.8 percent of all cyber events in the dataset, that sector accounts for over 36 percent of all Exploitation of Sensor events, well above the average rate of 3.8 percent. This observation draws attention to the heavy targeting by hackers of PoS devices used by fast food restaurants and hotels. The same sector is under-represented for Message Manipulation events. Only 3.4 percent of the events it experienced fell in this category, compared to the average of 17.9 percent for all sectors.

Differences between sectors in the frequencies of different types of cyber events likely reflect differences in attacker motivations, vulnerabilities, and benefits that can be obtained through different types of exploitation of data disruption of key organizational services. For example, Government Services suffers more Message Manipulation and External Denial of Service event types, whereas it does not see many Application Server events. A review of specific incidents in the dataset reveals a large number of attacks against websites aimed at promoting a political message. These attacks are often exploiting misconfigurations and can be automated thereby promoting larger numbers of events, whereas exploitation of applications might not occur as often if the information exploited requires greater effort by the hacker to achieve their goals.

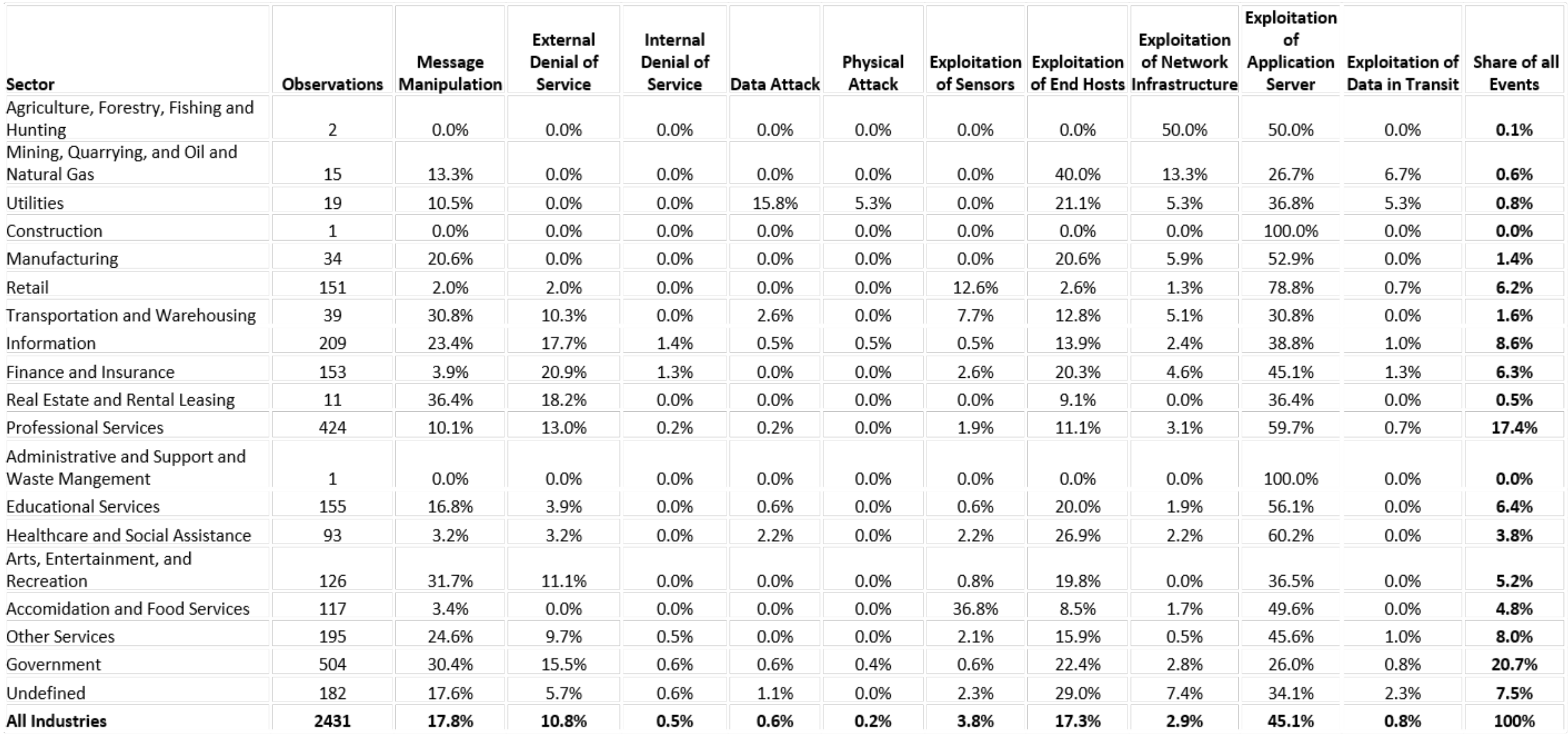
Conclusion

Having an easy-to-use taxonomy that provides an exclusive, exhaustive, and consistent way to differentiate the primary effects of cyber activity will help organizational leaders and policy makers have more sophisticated discussions about the different types of threats they face, and the appropriate risk mitigation strategies. The taxonomy presented in this paper and the analysis of three years of publicized cyber event data highlights variance in scale, effects, and method. Differences in the types of disruptive or exploitive attacks directly inform organizational leaders on both the range as well as concentration of effects they might face. By disentangling tactics from effect this classification provides a first step in creating a framework by which organizational leaders can categorize and assess the most consequential forms of cyber attack they might face. Additional work to measure the impact of specific attacks would allow organizations and governments to adequately plan for the types of threats they are most likely to face, and invest in the technology, training, and processes needed to defend against the most consequential forms of attack.

Understanding the variation of effect by industry allows organizational leaders to be more focused on defensive strategies, resiliency measures, or training programs that address specific effects they are likely to face, rather than interpreting vague guidance by experts or by purchasing technical solutions that might not be as useful for the threats they face.

About the author

Charles Harry is a senior leader, practitioner, and researcher with over 20 years of experience in intelligence and cyber operations. Dr. Harry is the Director of Operations at the Maryland Global Initiative in Cybersecurity (MaGIC), an Associate Research Professor in the School of Public Policy, and a Senior Research Associate at CISSM.



Sector	Observations	Message Manipulation	External Denial of Service	Internal Denial of Service	Data Attack	Physical Attack	Exploitation of Sensors	Exploitation of End Hosts	Exploitation of Network Infrastructure	Exploitation of Application Server	Exploitation of Data in Transit	Share of all Events
Agriculture, Forestry, Fishing and Hunting	2	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	50.0%	50.0%	0.0%	**0.1%**
Mining, Quarrying, and Oil and Natural Gas	15	13.3%	0.0%	0.0%	0.0%	0.0%	0.0%	40.0%	13.3%	26.7%	6.7%	**0.6%**
Utilities	19	10.5%	0.0%	0.0%	15.8%	5.3%	0.0%	21.1%	5.3%	36.8%	5.3%	**0.8%**
Construction	1	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	100.0%	0.0%	**0.0%**
Manufacturing	34	20.6%	0.0%	0.0%	0.0%	0.0%	0.0%	20.6%	5.9%	52.9%	0.0%	**1.4%**
Retail	151	2.0%	2.0%	0.0%	0.0%	0.0%	12.6%	2.6%	1.3%	78.8%	0.7%	**6.2%**
Transportation and Warehousing	39	30.8%	10.3%	0.0%	2.6%	0.0%	7.7%	12.8%	5.1%	30.8%	0.0%	**1.6%**
Information	209	23.4%	17.7%	1.4%	0.5%	0.5%	0.5%	13.9%	2.4%	38.8%	1.0%	**8.6%**
Finance and Insurance	153	3.9%	20.9%	1.3%	0.0%	0.0%	2.6%	20.3%	4.6%	45.1%	1.3%	**6.3%**
Real Estate and Rental Leasing	11	36.4%	18.2%	0.0%	0.0%	0.0%	0.0%	9.1%	0.0%	36.4%	0.0%	**0.5%**
Professional Services	424	10.1%	13.0%	0.2%	0.2%	0.0%	1.9%	11.1%	3.1%	59.7%	0.7%	**17.4%**
Administrative and Support and Waste Mangement	1	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	100.0%	0.0%	**0.0%**
Educational Services	155	16.8%	3.9%	0.0%	0.6%	0.0%	0.6%	20.0%	1.9%	56.1%	0.0%	**6.4%**
Healthcare and Social Assistance	93	3.2%	3.2%	0.0%	2.2%	0.0%	2.2%	26.9%	2.2%	60.2%	0.0%	**3.8%**
Arts, Entertainment, and Recreation	126	31.7%	11.1%	0.0%	0.0%	0.0%	0.8%	19.8%	0.0%	36.5%	0.0%	**5.2%**
Accomidation and Food Services	117	3.4%	0.0%	0.0%	0.0%	0.0%	36.8%	8.5%	1.7%	49.6%	0.0%	**4.8%**
Other Services	195	24.6%	9.7%	0.5%	0.0%	0.0%	2.1%	15.9%	0.5%	45.6%	1.0%	**8.0%**
Government	504	30.4%	15.5%	0.6%	0.6%	0.4%	0.6%	22.4%	2.8%	26.0%	0.8%	**20.7%**
Undefined	182	17.6%	5.7%	0.6%	1.1%	0.0%	2.3%	29.0%	7.4%	34.1%	2.3%	**7.5%**
All Industries	**2431**	**17.8%**	**10.8%**	**0.5%**	**0.6%**	**0.2%**	**3.8%**	**17.3%**	**2.9%**	**45.1%**	**0.8%**	**100%**

Table 1: Cyber Events by Type and Industry Sector

References

Bedford, D. (2013) “Evaluating Classification Schema and Classification Decisions”. *Bulletin of the American Society for Information Science & Technology*, Vol. 39 Issue 2, p13-21

Cimpanu C. (2016) “Iranian Hacker Defaces IWF Website Following Controversial Rio Olympics Decision” Softpedia News http://news.softpedia.com/news/iranian-hackers-deface-iwf-website-following-controversial-rio-olympics-decision-507436.shtml

Choo, K. (2011). “The cyber threat landscape: Challenges and future research directions” *Computers & Security, 30*(8), 719-731. doi: http://dx.doi.org/10.1016/j.cose.2011.08.004

de Bruijne, M., van Eeten M., Ganan, C., Pieters, W. (2017). “Towards a New Cyber Threat actor Topology: A Hybrid Method for the NCSC Cyber Security Assessment” Delft University of Technology https://www.wodc.nl/binaries/2740_Volledige_Tekst_tcm28-273243.pdf

Filipkowski, W. (2008). “Cyber Laundering: An Analysis of Typology and Techniques” *International Journal of Criminal Justice Sciences, Vol 3*, pgs 15-27

Gruschka, N., & Jensen, M. (2010). “Attack Surfaces: A Taxonomy for Attacks on Cloud Services” Paper presented at the IEEE CLOUD

Hansman, S., Hunt R., (2005) “A taxonomy of network and computer attacks”. *Computers and Security,* Vo.l 24 Issue 1, p 31-43

Harry, C. (2015) “A Framework for Characterizing Disruptive Cyber Activity and Assessing its Impact”, Working Paper, Center for International and Security Studies at Maryland (CISSM), University of Maryland

Harry C. & Gallagher N. (2017) “Categorizing and Assessing Severity of Disruptive Cyber Events” Policy Brief, Center for International and Security Studies at Maryland (CISSM), University of Maryland

Howard, J. and Longstaff, T. (1998) “A Common Language for Computer Security Incidents,” Technical Report, Sandia National Laboratories

Jiankun H., Hemanshu R., and Song G. (2014) “Taxonomy of Attacks for Agent-Based Smart Grids” IEEE Transactions on Parallel and Distributed Systems, Vol 25, No 7

Kjaerland, M., (2005) “A taxonomy and comparison of computer security incidents from the commercial and government sectors”. Computers and Security, Vol 25 pgs 522–538.

Kjaerland M. (2005) “A classification of computer security incidents based on reported attack data” *Journal of Investigative Psychology and Offender Profiling*. Vol 2, Issue 2 pgs 69-146

Koerner, B. (2016) “Inside the Cyberattack that Shocked the US Government”, Wired, October 2016. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

Krebs, B. (2016) “Malware Infected All Eddie Bauer Stores in US and Canada”, *Krebs on Security*, https://krebsonsecurity.com/2016/08/malware-infected-all-eddie-bauer-stores-in-u-s-canada/

Lamothe, D “U.S military social media accounts apparently hacked by Islamic State sympathizers” , http://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-statesympathizers/, Washington Post, January 2015.

Lee, R., Assante, M., Conway, T. (2016) “Analysis of the Cyber Attack on the Ukrainian Power Grid”, *Sans Institute*,. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Lough, D. (2001) “A Taxonomy of Computer Attacks with Applications to Wireless Networks,” PhD thesis, Virginia Polytechnic Institute and State University

Matthews, L. (2017) “NotPeyta Ransomware Attack Cost Shipping Giant Maersk Over $200 Million”, *Forbes* https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#40970b504f9a

Mirkovic, J., and Reiher, P. (2004) “A taxonomy of DDoS attack and DDoS defense mechanisms” *SIGCOMM Comput. Commun. Rev., Vol 34*(2), pgs 39-53

Ranganathan, S. R. (1957). *Prolegomena to library classification.* London: The Library Association

Rege-Patwardan, A. (2009). “Cybercrimes against critical infrastructures: a study of online criminal organization and techniques”. *Criminal Justice Studies,* Vol 22(3), pgs 261-271.

Reza, Ali (2016) “Anti-DDoS firm Staminus hacked, private data posted on line” , *Hack Read*, https://www.hackread.com/anti-ddos-firm-staminus-hacked-private-data-posted-online/

Saini, A. Gaur M.S, Laxmi V.S (2015) “A Taxonomy of Browser Attacks”, *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* 2015 p. 291-313

Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q (2009). “*AVOIDIT: A cyber attack taxonomy"*. University of Memphis.

Woolf, N (2016) “DDoS attack that disrupted internet was the largest of its kind in history, experts say.” *Guardian* https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Zetter, K. (2016) “Inside the Cunning Unprecedented Hack of Ukraine’s Power Grid”, *Wired*, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zhu, B. and Sastry, S. (2017) “SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy”, Department of Electrical Computer and Security Engineering, University of California at Berkeley. Berkeley, CA