Fall 2018

Cyber Security Classification Model Evaluation and Comparison

Wade Scholten
Iowa State University

Cyber Security Classification Model Evaluation and Comparison

A qualitative evaluation of cyber security models and their application

by

Wade G. Scholten

A creative component submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Information Systems

Program of Study Committee:
James Davis, Major Professor
Russell Laczniak

Iowa State University

Ames, Iowa

2018

Table of Contents

Introduction

Cyber incidents can be defined as violations of explicit or implied policies that can include unauthorized access, disruption, unauthorized use, or changes to systems, networks, hardware, and software (US Cert, 2018). This description does not account for all possibilities and cyber incidents continue to evolve and increase in visibility for organizations (Pescatore, 2017). Cyber incidents can have real costs associated with them to governments, companies, and individuals. For instance, in December of 2013 Target Corp. reported a data breach of 40 million credit card accounts (Krebs, 2013). According to their 2016 SEC filings, it cost the company $291 million and hurt their reputation in the market (Herberger, 2016). Another great example would be the StuxNet attack where a worm was able to physically damage lab equipment required to develop nuclear weapons in Iran. The costs of lost national security, development time, and cost of the equipment were huge, but are not easily calculated (Kushner, 2013). Further the recent cyber incident at Equifax, where on September 7th of 2017 an estimated 143 million U.S. consumers' data was breached at Equifax. While this is costly to the organization it had larger implications for consumers and the economy (DeMarco, 2018).

Problem Statement

To combat these cyber incidents organizations, governments, and professionals should to be able to identify these incidents and describe them effectively to better protect against them. As Peter Denning stated in 2010, "It is not possible to build strong defenses without acquiring and maintaining a solid understanding of how attacks work and how effective they might be." (Denning, 2010). To identify and learn more about these cyber-attacks and incidents we need a solid foundation of evaluation and method of classification to be able to share information about attacks and their characteristics. Classification models and taxonomies have been proposed for cyber-attacks dating back from 1984 (Igure, 2008). The challenge with the numerous taxonomies and models is determining which to use and how to use them. This research focuses on evaluating cyber incident models and to determine which cyber incident model is best at answering the following questions through a qualitative investigation.

1. How easy is the model to understand and communicate?
2. Does the model give insight on how to defend in the future?
3. Does it account for all areas of attacks and does the classification give meaningful information?
4. Is it flexible to adapt to changes in cyber incidents?

The analysis and evaluation of the models will be conducted through the classification process and thorough comparison of the final classifications of two separate cyber incidents. When looking at the first question the analysis hinges on whether a person with no knowledge of the attack is able to understand and describe the cyber incident. The second question will be evaluated on how well the categorization gives direction on how to take defensive measures

into the future. The third question looks at whether the model captures the full breadth of the incident and if it leaves out any obvious factors or elements that exist in cyber incidents. The last question's analysis relies on the ease of adding elements or factors to the model and how well the model captures uncertainty. Due to the qualitative nature of the questions, the evaluation of the models relies on judgment developed through the application and final result of the categorization of the cyber incidents in this study.

Background & Previous Research

There has been extensive research on security models, but few have focused on cyber incidents and evaluating which would be suitable for wide adoption of security professionals. Cyber incident taxonomies date back to 1984 with the Perry and Walich developing a two dimensional model where one dimension described the actor in the attack and the second dimension was aimed at the type of cyber incident (Perry, 1984). The largest weakness however was that the actor dimension was specific and showed little value in categorization and the incident was categorized by the impact and did not consider the incident's details as stated by Igure and Williams (Igure, 2008). Late Brinkley and Shell presented another model focused on "misuse", but the events can be considered attacks or incidents. Their model is hierarchical and is designed as a method of listing the possible misuse in computer systems (Brinkley, 1995). Due to this fact, it is only effective for classification and not security action. In 1997, Fred Cohen developed a taxonomy to inform security assessment, with the goal of fitting all attacks into one taxonomy (Cohen, 1997). It essentially created a list of cyber incidents, 94 different incident classifications. With a specific list of incidents, it is static and shows no way to be flexible and grow with technological advances (Igure, 2008). Neumann worked for many years to develop a classification system and ultimately in 1995 published a classification system including 26 incidents or attacks into 9 categories (Igure, 2008, Neumann, 1995). The classifications are hard to link and not fully refined, if able to pinpoint the area of the flaw it could have been informative to security assessment (Igure, 2008). Lindquist and Jonsson built upon Neumann and Parker's classification and further divided three categories to add another layer to the taxonomy and better describe the classification (Igure, 2008; Lindquist, 1997). They were the first to introduce the idea of dimension of classification (Lindquist, 1997). Thus, leading to hierarchical taxonomies with each level further describing the factors involved and better describing the vulnerabilities that allowed the attack.

There are many additional taxonomies that focus on specialized areas such as web specific attacks (Alvarez, 2003), denial of service (DoS) attacks (Gerber, 2000; Kumar, 2006; Kumar 2005; Mirkovic, 2004), and intrusion detection methods (Kumar, 1995; Killourhy, 2004). However, these models are narrow focused and do not encompass the goal of an overarching taxonomy that can capture all cyber attack areas.

Further there are several models that were created to assist in security evaluation that are effective at capturing facets that are present in all cyber incidents. For instance, Lough developed a taxonomy that attempted to build a taxonomy that included all common factors

across attacks (Lough, 2001). Lough put all attacks into four categories, the categories are determined by the cause of the attack however, due to the general nature of this taxonomy and the blending of cause and vulnerabilities Lough's model is not particularly effective for a security evaluation. One interesting application of a security evaluation focused taxonomy is Mostow et all's attempt at building an attack simulator and using a taxonomy to get proper coverage of attacks within the simulation (Mostow, 2000). The simulator was devised to better measure security postures and be able to measure the security of a system. The limitation of the taxonomy used was there was only a single level developed and was not the focus of the research. Delooze went on to build upon Mostow's taxonomy which created a tree diagram and ended up with 25 different leaf's that covered many known internet attacks or incidents (Delooze, 2004). The attacks from the CVE list were classified to show usage of the taxonomy. While further developed than Mostow's model, Delooze's taxonomy was not all encompassing and left certain factors out such as effect of attack and categorized attacks on a single basis. Hansman and Hunt in 2004 determined that developing a single tree taxonomy was not appropriate and decided to propose four separate taxonomies to better describe cyber incidents (Hansman, 2005). The four taxonomies focused on attack vector, attack target, vulnerabilities and exploits, and attacks with payloads. All of the taxonomies had a hierarchy with further detail described as the level increased. While each taxonomy is able to capture the element of an attack it tries to capture it is cumbersome to use all four to classify each attack.

As Igure and Williams aptly stated most if not all taxonomies try to capture four elements of cyber incidents, impact of attack, cause of attack (vulnerability exploited), target of the attack, and the scope of the attack (Igure, 2008). These taxonomies all have weaknesses and strengths in their implementation and design, but all grapple with the same issues of best describing and categorizing the factors and elements of cyber incidents.

The following taxonomies and models are recent and influential models being considered today. In 2006, Nong Ye et all proposed a framework to classify cyber attacks or incidents focusing on separating cause and effect of the attack (Ye, 2006). They leaned on system engineering, fault modeling, and risk assessment theories to create a model with seven areas of categorization; objective, propagation, attack origin, action, vulnerability, asset, state effects, and performance effects. Their model allows for further description in each category and flexibility to evolve as the nature of cyber attacks do. While the model is effective in modeling the factors in an attack it does not account for multiple step attacks or incidents and does not allow for a hierarchical segmentation of attacks. Then in 2011, Eric Hutchins et all published a model known as the cyber kill chain in partnership with Lockheed Martin (Hutchins, 2011). The attack classification model focuses on advanced persistent threats (APT's) or "well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information." (Hutchins, 2011). The model's goal is to define the series of steps in successful attacks and the counter measures available at each step. The model has seven steps and they are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. This model gives

great insight into all attacks and can direct efforts against future and current attacks on security. However, this model is not a true classification model and focuses on countermeasures to attacks and how to better implement them. In 2014, Simmons et all proposed a new taxonomy for cyber attacks and incidents, AVOIDIT (Simmons, 2014). The model proposed builds off of previous models from Lough, Howard, and Hansman. The model classifies attack factors by attack vector, operational impact, defense, informational impact, and target. Further, the model allows a single attack to have multiple attack vectors to better describe multi step attacks. This is accomplished through their CADAT process and tree structures. AVOIDIT was applied at the IRS to classify attacks and the results of the testing is not clear. AVOIDIT gives thorough information in its classification, but does not account for physical attacks and the defense factor gives little insight on how to implement the defense.

Methods

There are few examples of extensive taxonomy review and prove effective for understanding the differences and relative strengths and weaknesses of each model (Igure, 2008; Joshi, 2015). Some proposed models compare themselves against similar models to show they are able to improve upon their predecessors (Simmons, 2014). Few attempts have been made to capture the breadth of taxonomies and models available. Thus, computer security world has no definitive model to classify cyber incidents. Evaluation of the current models available gives insight as to the best option and can drive further innovation towards an ideal classification system.

This evaluation will look at the previous stated qualitative measures to determine the most effective model. To measure each category intuition of the final categorization and the process of fitting each cyber incident to the model will be used.

1. How easy is the model to understand and communicate?
2. Does the model give insight on how to defend in the future?
3. Does it account for all areas of attacks and does the classification give meaningful information?
4. Is it flexible to adapt to changes in cyber incidents?

Selection of Models

The models selected include Howard & Longstaff's Computer and Network Incident Taxonomy , Simmons' et al AVOIDIT Cyber Attack Taxonomy, and the Lockheed Martin Cyber Kill Chain (Howard, 1998; Simmons, 2014; Hutchins 2011). Each model is able to capture different elements of a cyber incident and all capture the elements of a cyber incident differently. Howard & Longstaff's model focuses on the attacker and the event, while the AVOID it model focuses on the attack vector and the operational impact of the incident. Finally, the cyber kill chain focuses on defense and the steps involved in the attack. These models give a breadth of categorizations that give further insight on what types of models are most effective.

Selection of Cyber Incidents

To best measure the models being evaluated, the cyber incidents need to be diverse in size and scope. Unfortunately, there is limited detail information on smaller attacks as they are not reported as often or thoroughly. To best fit each model details on attackers, the attack vector, targets, and objectives are needed to provide the information necessary for categorization into each respective model. Many attacks have multiple facets to the total event and to best measure how a model captures that information, both attacks selected have multiple steps in their attack profile.

Two cyber incidents were selected based upon available detailed information. The two attacks are as follows:

1. Target Breach, Between November 27th and December 18th 2013
2. Equifax Breach, Announced September 7th 2017

Target Breach

In November of 2013 Target Corporation's network was breached and 40 million credit card details and 70 million personal records were stolen (Shu, 2017). It appears the initial incident occurred when a third party's computer was compromised, likely though an email attachment, which gave the attackers access to Target's internal network. Once the attackers gained access to the internal network they were able to leverage default passwords to install malware on the point of sale terminals which was able to pull credit card information from the RAM in the machine when cards were scanned. After collecting the credit card information the attackers were then able to transfer the data out of the network through Target's own FTP servers using valid user name and password combinations during the peak times of the day. The diagram below displays the order of events of the attack (Shu, 2017).

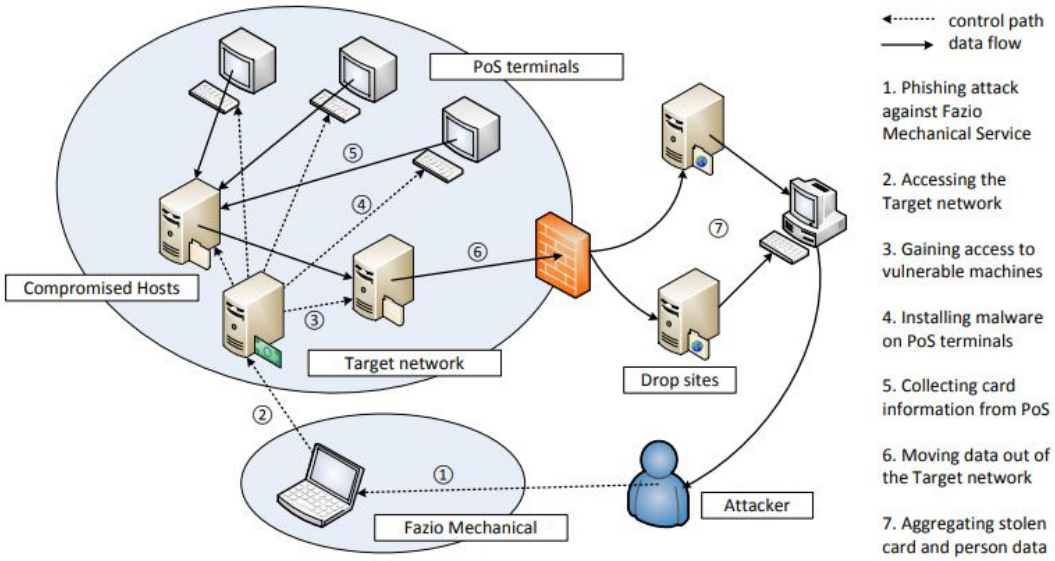
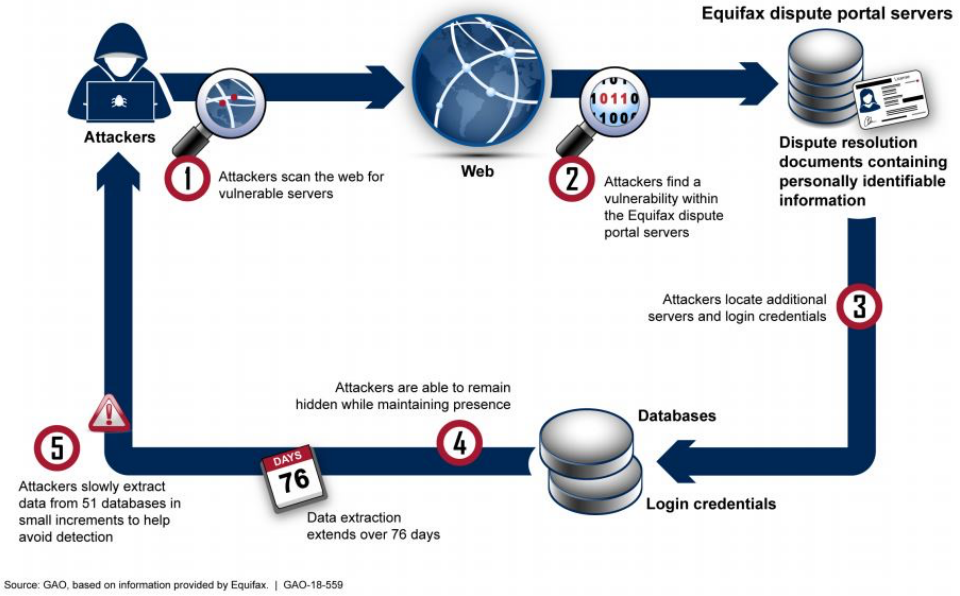


Fig. 2. Attack steps of the Target breach.

Equifax Breach

The Equifax breach was announced on September 7th and the initial breach occurred on March 10th (Krebs, 2018). The breach included the disclosure of an estimated 143 million U.S. consumers information. This information included credit card numbers, names, social security numbers, addresses, birthdates, and driver license numbers (Marinos, 2018). Further the breach greatly affected the reputation and standing of the credit agency to the general public. According to the congressional report it appears that the initial breach was due to a vulnerability in the Apache Struts running on a web server at Equifax, CVE-2017-5638 (Marinos, 2018; Krebs 2017). Then once the attackers had access through the vulnerability they were able to use a variety of tools to leverage and gain access to databases holding the information ultimately stolen. They were then able to extract the data slowly over 76 days to an offsite location. Please refer to the diagram below outlining the attack (Marinos, 2018).



Modeling the Incidents

When fitting each cyber incident or attack into the models there is room for judgement decisions to determine how the elements should be categorized. When determining the best categorization multiple sources of the attack were consulted and the definitions from the model itself. Both Howard and Longstaff's model and the AVOIDIT model give clear insight on the categorization of each element and in most cases give clear definitions of each of the classifications (Howard 1998, Simmons 2014). Both attempting to meet each of the six criteria Howard and Longstaff state; mutual exclusivity, exhaustive, unambiguous, repeatable, accepted, and useful. However the Cyber Kill Chain model is more fluid in its categorization as it was not designed as a classification model, but a mapping of the process of advanced

persistent threats (Hutchins, 2011). Ultimately best judgement and comparison to other sources determined the best categorization for each element within each model.

In the AVOIDIT model, the authors give insight on how to apply incidents to the model, using their CADAT process. Using this method I found that the model was unclear on how to capture multiple actions in the incident (Simmons, 2014). Further, Howard and Longstaff's model did give some insight in their model that with the attackers and objectives staying constant you can categorize an incident with different tools, vulnerabilities, actions, targets, and unauthorized results (Howard, 1998). Using these insights, the AVOIDIT model was slightly altered to include multiple actions over the course of the incident.

The Cyber Kill Chain model required the most use of judgement to best describe the incidents in the appropriate manner. In an ideal setup, the Cyber Kill chain works best in a report format where details can be better highlighted in each phase of the "kill chain". This is best represented in the congressional report "A "Kill Chain" Analysis of the 2013 Target Data Breach" created to explain the process of the attack to congressional members on the committee on commerce, science, and transportation (US Congress, 2014). Thus the pertinent details are captured in the Cyber Kill Chain model, but in a few words or less.

Findings

The following section begins with the classifications in table form, beginning with the Target Breach and then the Equifax Breach, followed by general findings from each model. Then evaluations of each question and final comments on the models as a whole.

Target Breach Model Categorization

Howard and Longstaff's Computer and Network Incident Taxonomy							
Target Breach	**Attackers**	**Tool**	**Vulnerability**	**Action**	**Target**	**Unauthorized Result**	**Objectives**
Phase 1	Hackers/Professional Criminals	Information Exchange	Configuration	Modify	Computer	Increased Access	Financial Gain
Phase 2	Hackers/Professional Criminals	User Command	Implementation	Authenticate	Network	Increased Access	Financial Gain
Phase 3	Hackers/Professional Criminals	Script or Program / Data Tap	Configuration	Read	Data	Disclosure of Information	Financial Gain
Phase 4	Hackers/Professional Criminals	Script or Program	Implementation	Steal	Data	Theft of Resources	Financial Gain

AVOIDIT Cyber Attack Taxonomy					
Target Breach	**Attack Vector**	**Operational Impact**	**Defense**	**Informational Impact**	**Target**
Phase 1	Social Engineering	User Compromise	Mitigation(remove from network)	Discover	Client
Phase 2	Insufficient Authentication Validation: BA	Web Compromise	Mitigation(remove from network)	Discover	Network
Phase 3	Misconfiguration	Installed Malware (Spyware)	Mitigation(whitelisting)	Discover	Application / Client
Phase 4	Misconfiguration / Design Flaws	Misuse of Resources	Mitigation(whitelisting FTP Sites)	Disclose	Network

Lockheed Martin Cyber Kill Chain						
Reconnaissance	**Weaponization**	**Delivery**	**Exploitation**	**Installation**	**Command & Control**	**Actions/Objectives**
Web Research on 3rd Party and Target	PDF or Microsoft Office Document	Spearphishing Email led to Credentials on Target Internal Network	Using Stolen Credentials to Install RAM Scraping Malware	Installed on POS Machines using Default Account Name	Continued use of Stolen Credentials & Installation of Malware	FTP transfer of Data to Off Network Server.

Equifax Breach Model Categorization

Howard and Longstaff's Computer and Network Incident Taxonomy							
Equifax Breach	**Attackers**	**Tool**	**Vulnerability**	**Action**	**Target**	**Unauthorized Result**	**Objectives**
Phase 1	Hackers	Script or Program	Implementation	Bypass	Process	Increased Access	Financial Gain
Phase 2	Hackers	User Command	Configuration	Read	Data	Disclosure of Information	Financial Gain
Phase 3	Hackers	User Command	Configuration	Steal	Data	Theft of Resources	Financial Gain

AVOIDIT Cyber Attack Taxonomy					
Equifax Breach	**Attack Vector**	**Operational Impact**	**Defense**	**Informational Impact**	**Target**
Phase 1	Insufficient Input Validation: XSS	Web Compromise	Mitigation (CVE-2017-5638)	Discover	Network
Phase 2	Design Flaws	Misuse of Resources	Mitigation (remove from network)	Disclose	Application

Lockheed Martin Cyber Kill Chain						
Reconnaissance	**Weaponization**	**Delivery**	**Exploitation**	**Installation**	**Command & Control**	**Actions/Objectives**
Scanning of Apache Struts Web Sites	Crafting URL for Apache Struts Vulnerability	HTTP Request to Vulnerable Server	Exploit Struts Vulnerability for network access	Install Malicious Code to Create Backdoor Access	Collect Sensitive Information and Prepare for FTP Transfer	Exfiltration over 76 days using FTP Server

Overall, the models capture different details of the attack and when looking through them it is apparent that no model was able to categorize the incidents fully.

Howard and Longstaff's model is able to capture the attacker and the motivations through the objectives category that help to better understand the attack as a whole. Although it is difficult to determine the motivations of an attacker, and in many cases can only be inferred. This model captures events quite well in that it can be quickly understood and read. For instance, in the Equifax breach phase 1, the hackers used a script or program to bypass a process to increase their access. The model creates almost a sentence structure that is intuitive. In doing so the categories become quite general and the details become less apparent. One of the biggest weaknesses for this model is the general vulnerability category where it only captures implementation, design, or configuration vulnerabilities. This general category is sometimes difficult to differentiate between design and implementation and gives no insight on what element was the source of the vulnerability.

The AVOIDIT captured the technical details of attacks better than Howard and Longstaff's model, but failed to describe intent or the actor in the attack. This makes sense as the AVOIDIT model focuses in on vulnerabilities. One confusing aspect of the AVOIDIT's model is the "informational impact" category. Divided into distort, disrupt, destruct, disclose, and discover, the category is not always obvious as to what that means. Distort and disrupt are quite similar

as well as disclose and discover. The AVOIDIT model's defense category is general and gives little insight on how to implement the defense. It points to either the CVE or general strategies such as remove from network, which can be implemented in countless ways. Finally, the AVOIDIT model fails to take into account physical attacks (Simmons, 2014).

Lockheed Martin's Cyber Kill Chain gives ample details on the attack and individual actions that progress that attack. However, when looking at multiple attacks it becomes hard to compare them to each other without detailed analysis. This model excels at looking at a single incident and how to defend oneself from the actions that occurred in the incident.

How easy is the model to understand and communicate?

Howard and Longstaff Computer and Network Incident Taxonomy	AVOIDIT Cyber Attack Taxonomy	Lockheed Martin Cyber Kill Chain
• Reads like a sentence and quickly understood • Includes actors and motivations	• Clearly states vulnerabilities that led to incident • Difficult to determine impact to organization	• Detail oriented with clear steps of actor and incident • Difficult to compare multiple incidents • Each step difficult to categorize

The model that stands out as easy to understand and communicate is Howard & Longstaff's model. It also is quite easy for a person with no knowledge of the cyber incident to quickly read the table and understand the steps and the outcomes of the cyber incident. While the Cyber Kill Chain model gives many details and has clear steps, it requires more in depth reading to get a full grasp of the incident. As for the AVOIDIT model, the actors and actions are difficult to understand quickly and require additional knowledge of the incident to fully understand the incident.

Does the model give insight on how to defend in the future?

Howard and Longstaff Computer and Network Incident Taxonomy	AVOIDIT Cyber Attack Taxonomy	Lockheed Martin Cyber Kill Chain
• General description of vulnerability provides almost no insight • Motivation and attacker allow organization to prioritize defense	• Specific vulnerability details and CVE's • Difficult to determine the impact of the vulnerability • Defense category gives no insight on implementation	• Specifies the steps involved in the attack and the weaknesses • Gives insight on the steps to mitigate the attack at each phase

The two models that excelled in this area were the AVOIDIT model and the Cyber Kill Chain. The AVOIDIT model clearly defines the vulnerability involved in the incident, although does not give insight on implementation of the defense necessary. The Cyber Kill Chain model clearly defines the actions in each stage and gives direction on the actions necessary to stop the incident at each stage. Howard and Longstaff's model is too general to give effective information in how to defend into the future beyond the attackers, motivations, and if the vulnerability a design, implementation or configuration flaw. The Cyber Kill Chain is the most effective at giving defensive insights.

Does the model account for all areas of attacks and does the classification give meaningful information?

Howard and Longstaff Computer and Network Incident Taxonomy	AVOIDIT Cyber Attack Taxonomy	Lockheed Martin Cyber Kill Chain
• Covers all aspects of incidents • Categorization is general and doesn't give meaningful distinction	• Fails to capture attacker, motivation, and physical attacks • Gives meaningful information on vulnerability	• Captures all the steps in an incident in detail • Gives meaningful information to better understand the incident

For the question on whether the model accounts for all areas there was one model that had obvious factors not accounted for, AVOIDIT model. The factors missing from the AVOIDIT model include the attacker, motivations, and physical attacks. Both the Cyber Kill Chain and Howard and Longstaff's model appear to capture all of the factors in cyber incidents. They are able to capture them in different ways, but both are sufficiently broad in their categorizations to include the obvious elements.

Is the model flexible enough to adapt to changes in cyber incidents?

Howard and Longstaff Computer and Network Incident Taxonomy	AVOIDIT Cyber Attack Taxonomy	Lockheed Martin Cyber Kill Chain
• Model is general enough to capture any changes in cyber incidents • Categories could be altered to capture any unforeseen change	• Detailed and rigid structure of attack vector may need changes over time • Defense strategies and targets may change and require model changes	• Fluid nature of model allows flexibility in interpretation and application • Phases of incidents unlikely to change

Flexibility is difficult to measure and it is also unclear as to how cyber incidents could change in the future. Thus generalities and the ability to alter a category without compromising the larger model are best to measure the flexibility of a model. The AVOIDIT model appeared to be rigid and resistant to change. This is evident in the attack vector category. Attack vectors are carefully prescribed and as cyber incidents continue to evolve they may cover multiple attack vectors which would make previous categorizations less effective. Both the Cyber Kill Chain and Howard and Longstaff model appear flexible in that they are general enough or customizable to the individual incident that they are categorizing. The AVOIDIT model is the least flexible of the three models with the other two being nearly equal in flexibility.

Final Impressions of the Models

All the models excel in one area or another and it is unfortunately impossible to determine a "best" model for cyber incident classification. Perhaps a combination of the classifications and ideas of these models would produce an industry accepted best fit, but would prove challenging. Ultimately, the determination of which classification model to analyze cyber incidents is up to the analyst themselves and what information they find most beneficial for their analysis.

Conclusion

This paper concludes with the idea that classification of cyber incidents is a difficult problem that does not have a clear solution. Without a clear solution cyber incident classification will continue to be done in fragmented ways that add complexity to analyzing them as a whole. On an individual level, models have benefits and detractions and knowing those elements assists in the individuals' evaluation of cyber incidents in the future.

Howard and Longstaff's Computer and Network Incident Taxonomy allows quick and easy understanding of the events, motivations, attackers, and the outcomes. While AVOIDIT focuses on the vulnerabilities used in the incident to give insight on the sources of insecurity and Lockheed Martin's Cyber Kill Chain focuses on the detailed steps taken by the attacker and how to stop each step in the chain. Applying these models to cyber incidents gives understanding and a better vision of the incident as a whole. Choosing the correct model to apply relies on the motivations and information needed.

Hopefully professionals will determine a standard for cyber incident classification, but until that day knowing the differences between models is paramount for analysis of current and past cyber incidents. We all strive for better security and understanding what has happened leads to better security policies into the future.

Future Work

As cyber incidents evolve the research of how those incidents relate to one another will continue to be important. As Howard and Longstaff attempted, it is important that cyber security professionals can communicate using a "common language for computer security incidents" and a clear classification of incidents helps all in the industry. Thus research on how to combine the detail of a Cyber Kill Chain analysis with the vulnerabilities of the AVOIDIT taxonomy, with the flexible and easily read nature of Howard and Longstaff's would be beneficial and quite powerful in describing, categorizing, and fundamental in defending against these incidents in the future.

Bibliography

[1] United States Computer Emergency Readiness Team, US Cert, (2018). “Incident Definition” Retrieved From: https://www.us-cert.gov/government-users/compliance-and-reporting/incident-definition”

[2] Pescatore J. (2017). “Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017” SANS Institute InfoSec Reading Room.

[3] Krebs B. (2013). “Inside Target Corp., Days After 2013 Breach”, Retrieved from: https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/ .

[4] Hersberger P. & Northcutt S. (2016). “Data Breach Impact Estimation” , SANS Institute InfoSec Reading Room.

[5] Kushner D. (2013). “The Real Story of StuxNet”, Spectrum.IEE.org March 2013

[6] DeMarco, Edward J., Jr., & Bernard Mason. (2018) "THE EQUIFAX DATA BREACH AND ITS CONSEQUENCES." The RMA Journal Nov. 2017: 80+. Business Insights: Essentials.

[7] Denning P. J., & Denning D. E. (2010). The profession of IT: Discussing cyber attack. (Viewpoints)(information technology). Communications of the ACM, 53(9), 29.

[8] Igure, V., & Williams, R. (2008). Taxonomies of attacks and vulnerabilities in computer systems. IEEE Communications Surveys & Tutorials, 10(1), 6-19.

[9] Perry T. S., & Wallich P. (1984) “Can Computer Crime Be Stopped?” IEEE Spectrum, vol. 21, no. 5, pp. 34–45.

[10] Brinkley D.L. and R. R. Schell. (1995). “What Is There to Worry About? An Introduction to the Computer Security Problem,” Information Security: An Integrated Collection of Essays, pp. 11–39, IEEE Comp. Soc. Press.

[11] Cohen F. (1997). “Information System Attacks: A Preliminary Classification Scheme,” Comp. & Sec., vol. 16, no. 1, pp. 29–46.

[12] Neumann P. G. (1995). Computer Related Risks, ACM Press.

[13] Lindquist U., & Jonsson E. (1997). “How to Systematically Classify Computer Security Intrusions,” Proc. IEEE Symp. Sec. and Privacy, pp.154–63.

[14] Lindquist U., & Jonsson E. (1998). “A Map of Security Risks Associated with Using COTS,” IEEE Computer, vol. 31 no. 6, pp. 60–66.

[15] Lough D. L. (2001). “A Taxonomy of Computer Attacks with Applications to Wireless Networks,” Ph.D. dissertation, Virginia Tech.

[16] Alvarez G. & Petrovic S. (2003). “A Taxonomy of Web Attacks Suitable for Efficient Encoding,” Comp. & Sec., vol. 22, no. 5, pp. 435–49.

[17] Gerber L. (2000). “Denial of Service Attacks Rip the Internet,” IEEE Computer, vol. 33, no. 4, pp. 12–17.

[18] Kumar S. (2006). “PING Attack — How Bad Is It?” Comp. & Sec. J., vol. 25, issue 5, pp. 332–37.

[19] Kumar S. (2005). “On Impact of Distributed Denial of Service (DDoS) Attack due to ARP Storm,” Lecture Notes in Comp. Sci., vol. LNCS-3421, Springer-Verlag.

[20] Mirkovic J. & Reiher P. (2004). “A Taxonomy of DDoS Attack and DDoS Defense Mechanisms,” ACM SIGCOMM Comp. Commun. Rev., vol. 34, no. 2, pp. 39–53.

[21] Kumar S. (1995), “Classification and Detection of Computer Intrusions,” Ph.D. thesis, Purdue Univ.

[22] Killourhy K. S., Maxion R. A., & Tan K. M. C. (2004). “A Defense-Centric Taxonomy Based on Attack Manifestations,” Proc. Int’l. Conf. Dependable Sys. and Networks, pp. 91–100.

[23] DeLooze L. L. (2004). “Classification of Computer Attacks Using a Self-Organizing Map,” Proc. 5th Annual IEEE Sys. Man and Cybernetics Info. Assurance Wksp., pp. 365–69.

[24] Hansman S. & Hunt R. (2005). “A Taxonomy of Network and Computer Attacks,” Comp. & Sec., vol. 24, no. 1, Feb. 2005, pp. 31–43.

[25] Mostow J. R., Roberts J. D., & Bott J. (2000). “Integration of an Internet Attack Simulator in an HLA Environment,” Proc. IEEE Wksp. Info. Assurance and Sec., West Point, NY, June 6–7, 2000.

[26] Ye, Nong & Newman, Clark & Farley, Toni. (2005). A System-Fault-Risk Framework for cyber attack classification. Information Knowledge Systems Management. 5. 135-151.

[27] Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1(1), 80.

[28] Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2014). AVOIDIT: A cyber attack taxonomy. In Proc. of 9th Annual Symposium On Information Assurance-ASIA (Vol. 14).

[29] Joshi, C., Singh, U. K., & Tarey, K. (2015). A review on taxonomies of attacks and vulnerability in computer and network system. International Journal, 5(1).

[30] Howard, J. D., Longstaff, T. A. (1998). A Common Language for Computer Security Incidents. Report, October 1, 1998.

[31] Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017). Breaking the Target: An Analysis of Target Data Breach and Lessons Learned.

[32] Marinos, N., Clements, M., (2018). Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. United State Government Accountability Office, Report to Congressional Requestors.

[33] Krebs, B. (2017). Equifax Hackers Stole 200k Credit Card Accounts in One Fell Swoop. Retrieved from: https://krebsonsecurity.com/2017/09/equifax-hackers-stole-200k-credit-card-accounts-in-one-fell-swoop/#more-40773

[34] United States Congressional Committee on Commerce, Science, and Transportation. (2014). A “Kill Chain” Analysis of the 2013 Target Data Breach. Majority Staff Report for Chairman Rockefeller, March 26, 2014.