International Journal on Advanced Science Engineering Information Technology

Vol.12 (2022) No. 5
ISSN: 2088-5334

The Evolution of Cyberattack Motives

Sirapat Boonkrong [a,b,*], Kaewrattana Prompunjai [a], Suwitchayagon Watcharawongbodee [a], Supisara Chueachantuek [a]

[a] School of Information Technology, Suranaree University of Technology, 111 University Ave., Nakhon Ratchasima, 30000, Thailand
[b] DIGITECH, Suranaree University of Technology, 111 University Ave., Nakhon Ratchasima, 30000, Thailand
Corresponding author: *sirapat@g.sut.ac.th

Abstract— **A cyberattack can be defined as an action aiming to cause damages and losses to computer networks, information systems, and even personal devices and data. Many professionals and organizations have put a lot of effort and resources into preventing cyberattacks based on how they occur, their targets, and what damages they can cause. However, one of the aspects that are often overlooked and one of the reasons that cyberattacks are successfully carried out is the fact that the nature of attackers' motivations is not fully understood. Therefore, this research examines the main reasons for cyberattacks to be carried out by adversaries and the motives behind cyberattacks. Specifically, we studied over 7,700 cyber records and events between 2006 and 2018, including data breaches, privacy violations, and cyber incidents, to learn how attack motives have evolved over the years. The analyses of the data were mainly carried out using descriptive analysis. Our study found that the early cyberattacks were mainly financially motivated. However, in the later years, the cyberattack motives included espionage, ideology, and skill and knowledge testing. This implies that the motives behind cyberattacks became more varied in terms of types, proportions, and correlations between them. It is hoped and expected that the results of the analyses will be helpful to various stakeholders in such a way that they will better understand the reasons and motivations for cyberattacks.**

Keywords— **Attack motive; cyberattack; cybersecurity; evolution.**

Manuscript received 10 Oct. 2021; revised 23 Apr. 2022; accepted 6 Jun. 2022. Date of publication 31 Oct. 2022.

I. INTRODUCTION

Cybersecurity [1] is defined as technologies, practices and processes used to protect information systems, namely software, hardware, people, data, procedures and networks, from being attacked. It is also considered as a process for reducing risks and mitigating vulnerabilities in information systems. Therefore, many cybersecurity frameworks have been introduced as the sources of cybersecurity good practices. These frameworks include the NIST cybersecurity framework [2] and the ISO27001 standard [3]. No matter which framework is applied, the main objective is to reduce the risk of information systems being compromised.

Although cybersecurity frameworks exist and can be said to be widely accepted and applied by many organizations in various industries, cyberattacks still occur on a daily basis. The recent high-profile examples of cyberattacks include a ransomware attack on a US fuel pipelines [4], [5] which resulted in the company not being able to supply fuel to the US households, and a data breach on a popular social network platform [6]–[8], namely Facebook, which resulted in personal data of over five hundred million users leaking publicly online.

The usual process after an attack has occurred is to find causes of the attack. The result of such investigation normally comes down to such reasons as misconfiguration of a system, software errors, lack of awareness on the human side, and lack of preparation [9][10]. A working group called the Open Web Application Security Project or OWASP (https://owasp.org) is just one of many that have put a lot of effort into finding the main vulnerabilities which in turn lead to cyberattacks. They have pointed out that both Web and mobile applications do have similar vulnerabilities [11], [12] that are frequently overlooked. The examples are insecure authentication, insecure data storage and transmission and insecure software development. All of them are technical causes that can allow adversaries to attack the system.

A. Research Objective

This research takes another perspective to look at another dimension of why cyberattacks occur. We investigated the main motives behind cyberattacks and examine how these

motives have evolved over the years. In order to accomplish this goal, a dataset of over 7,700 cyber incident records between the years 2006 and 2018 were thoroughly studied and analyzed.

It is expected that the results of the analysis would be helpful to various stakeholders, both private sector and government agencies. At least, they will understand better why attackers carry out the attacks. Researchers from Michigan State University [13] even went so far as saying "knowing the motives is key to stopping hackers." This appears to be related to a famous quote by Sun Tzu who said in "The Art of War" that "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." The keywords are *you* (or yourself) and *enemy*. In the context of information technology, the "you" or "yourself" is when an organization knows about its own information assets and environment completely, while the "enemy" means knowing what an organization is facing whether it is the cyberattacks themselves or the people behind the attacks. We investigated the previous data to see what the main motives behind the cyberattacks were so that preventing or at least reducing the risk of being attacked will be more feasible.

B. Related Work

A cyber threat can be defined as a harmful event or incident that has the potential to occur. That is, if there is a chance for it to occur and cause damage to information systems or assets, we can call it a threat. However, whenever that potential incident actually takes place, it will transform from a threat to an attack or a cyberattack. Several researchers [14]–[16] have studied the impact of cyberattacks in terms of both physical damage and economic consequences. Many have categorized these cyber threats based on how they could occur, such as unintentional and intentional threats, natural disasters, software and hardware failure as well as internal and external threats. Some have taken another approach in categorizing them by their characteristics, which include harmonized characteristic (the synchronization of steps involved to compromise a system), organized characteristic (the use of logical steps leading to more efficient attack methods), enormous characteristic (a large scale attack affecting a large number of systems), regimented characteristic (a perfectly sequenced attack resulting in a severe damage), ad hoc characteristic (a carefully planned attack to cause maximum damage), and resource characteristic (an attack requiring a lot of time and money to be carried out) [17]

In addition to many researchers having studied the impacts and characteristics of cyberattacks, there are other researchers that have specifically focused on and attempted to characterized the motives behind the attacks.

Bhuyan *et al.* [18] mentioned that a researcher called Goderdzishvili recognized that the main targets of cyberattacks are data and information. This was especially the case with governmental Web sites, financial Web sites, social media and news Web sites. However, he did not explain the real motives behind the cyberattacks as such. Consequently, Uma and Padmavathi [17] attempted to provide the detail of the purposes of the processes behind the attacks. In other words, to carry out a cyberattack, there would be many steps involved. Uma and Padmavathi, therefore, summarized seven purposes of the cyberattack steps.

The first purpose was the obstruction of information, which was blocking the access of information [19] required by organizations or governmental offices. The second purpose was to counter cybersecurity measures, which was to challenge and defeat the protection mechanisms put in place by the data owners. The third purpose was the retardation of decision-making process, which was to cause delays in decision making processes. The fourth was to create disruption of public services [20], which basically meant that authorized users would not be able to access and use any public services. The fifth and sixth purposes were closely related in that the aim of the attacks was to damage the confidence of users and reputation of organizations. Finally, the seventh purpose as mentioned by Uma and Padmavathi was to break laws.

Even though there were researches that put an effort into understanding the purposes of cyberattacks, it was still unclear what the real motivations were. As a result, Gandhi *et al.* thoroughly study past cyberattack events in order to understand the nature and motivations behind these attacks. They began their study by first giving the definition of a cyberattack as "any act by an insider or an outsider that compromises the security expectations of an individual, organization or nation" [15]. Gandhi *et al.* then analyzed some of the major cyberattacks that occurred between 1995 and 2009. With the emphasis on the cyberattacks across cultural, social, economic and political dimensions, it was not surprising that they found three main categories of motivations. They consisted of the cyberattacks that were politically motivated, socio-culturally motivated and economically motivated.

Gandhi *et al.* [15] explained that politically motivated cyberattacks were usually carried out by those who were members of extremist groups. Their aim was to spread propaganda, deface Web sites and attack networks of their political enemies. The politically motivated cyberattacks could also be further divided into the followings.

The first group was the protests against political and governmental actions. Examples of a protest against political action were the 1998 attack on an atomic research center in India and the 1999 cyberattack to protest against the G8 summit in Germany. The second group was the protest against laws or public documents. Examples include the 1995 attack on the French Government Web sites and the 2001 attack on the Japanese Ministry of Education's Web site. The third group in the politically motivated cyberattack category was the outrage against acts of physical violence. Examples include the 2000 attack by the Israelis and Palestinians on a private technology company and the 2007 Estonia and Russia DDoS attack as a result from the conflict of the World War II monument.

For the socio-culturally motivated cyberattacks, Gandhi *et al.* justified that they were related to conflicts between individuals or groups usually over objectives, resources and even the denial of being controlled by others. This group of cyberattacks could be over land disputes such as the 2000 attack on Indian Web sites by the "Pakistani hackers" over the Kashmir conflict.

Finally, the economically motivated cyberattacks were basically personal or organizational greed. It was not difficult to find that these were frequently carried out by organized cybercriminals. Examples of the economically motivated cyberattacks include the 2009 attack on health records in the USA and the 2009 attacks between the USA and China to steal strategic information.

What Gandhi *et al.* presented appeared to be the start of the study and analysis of the motives behind cyberattacks. Unfortunately, they only focused on the cultural, social, economic and political issues, which was precisely the reason that they obtained three broad categories of cyberattack motives. Many researchers, including us, believed that this was too broadly specified. Maasberg *et al.* [21], therefore, led a way with a detailed analysis of motivations associated with a type of attack known as insider cyberattacks.

An insider attack occurs when an individual working in an organization commits an act that could negatively affect or damage that organization and its information systems. Maasberg *et al.* claimed that there were a few motives that could influence an insider attack. They included revenge, personal conflicts and financial gain [21].

We have now seen that there have been a few studies attempting to find purposes and motives behind cyberattacks. However, most of them appeared to look at some specific sectors of attacks only. Moreover, there have not been any that show how the motivations have evolved over the years. This is what we tried to achieve in this paper.

II. Material and Method

A dataset of cyber incidents was acquired from data.world (https://data.world), a US-based company that is claimed to be "the largest open data community in the world" [22]. The data on data.world were collaboratively collected, shared and sometimes sold to corporate that would like to use them for research or solving business problems.

Even though data.world is a with-profit organization whose products include cataloguing data, curating data and even analyzing data, for this research we only used the cyber incident data that were gathered by data.world and their community. In details, the data acquired from data.world for this research included, as mentioned, cyber incident data, which also contained such information as the actions of the attacks, i.e., whether they were malware, social engineering, data misuse or error, and the sectors in which cyber incidents occurred. However, what we were interested in this research was the motivations behind those attacks, which were also parts of the acquired data.

There were also other data sources that were related to cyberattacks. One of those was Kaggle (https://www.kaggle.com) who provided cyber incident data. However, they were not relevant to our research objective in trying to study and analyze the evolution of cyberattack motives. What these other data sources provided were simply the records and observations of attack sources and destinations of cyber incidents that occurred over the years. Moreover, there are other researches such as [23][24][25] that also used data from data.world in their research. The main reason that differentiates it from other sources is the fact that it offers the ability to join and match different datasets, and also the ability for users to collectively share their data, which would make them more complete [25].

It should be understood that there are usually certain conditions of cyberattack data collection [14]. In other words, when a cyber incident or a cyberattack occurs, it is either detected or not detected, which means that it is not possible to collect all cyber events. Secondly, in the case where the cyber incident is detected, it does not mean that it will always be disclosed to the public. It is either due to legal limitations or organization's own policy. This implies that what data collectors such as data.world and their community end up with will be the data or cyber events that can be detected, disclosed and recorded only. This brings us to the description of the dataset used in this research.

The data used in the research consisted of 7,792 cyber incidents which were recorded between the year 2006 and the year 2018. The number of recorded cyber incidents in this particular dataset appeared to increase steadily from 2006 to 2009, but began to exponentially increase from 2010 to 2013. The number of cyber incidents in the dataset went down from 2014 onwards and was believed to be due to the non-disclosure reasons, which suggested that companies appeared to under-report their cyber incidents during that period, especially between 2016 and 2018 [26]. Table 1 summarizes the number of recorded cyber incidents within the dataset used in the study.

TABLE I
AMOUNT OF RECORDED CYBER INCIDENTS

Year	Number of Cyber Incidents
2006	20
2007	48
2008	80
2009	89
2010	586
2011	534
2012	1,240
2013	1,795
2014	932
2015	883
2016	807
2017	526
2018	252

It has to be noted that the number of incidents shown in Table 1 is not the number of all cyber incidents that occurred all over the world in the specified period. It is simply the number of cyberattacks recorded by data.world. Having said that, we believed that the acquired dataset was adequate for what we tried to accomplish, namely the analysis of the evolution of cyberattack motives which can be explained in the subsequent sections.

III. Results and Discussion

This section explains what was found after the analyses on the data. This section is divided into four parts, which are number of cyberattack motives, types of cyberattack motives, proportions of cyberattack motives, cyberattack motive rankings and correlation analysis.

A. Number of Cyberattack Motives

Table 1, as mentioned earlier, shows the number of cyberattacks that were recorded in the dataset. The figures in the table reflect the data captured over a thirteen-year period from 2006 to 2018.

From the data, the first piece of information that we extracted was the amount of different cyberattack motives in each year. It should be made clear that the cyberattack motives were already specified as an attribute in the dataset. The data source explained that the way the motives were specified was first by looking at the cyberattack target of the cyber incidents. For example, if a cyberattack occurred in the financial sector, the attack would likely be financially motivated. However, as the dataset suggested, this was not always the case. The identification of cyberattack motives was made possible as a result of the application of honeypots [27], which was actually how some of the incidents were recorded. Overall, Fig. 1 displays how the number motives increased from the earlier years.

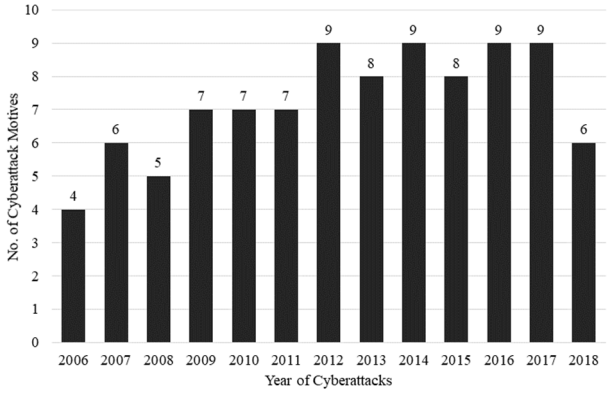

Fig. 1 Number of Cyberattack Motives Comparison

Fig. 1 shows that in 2006, there were only four different cyberattack motives. The number appeared to go up from the year 2007 to the year 2011 which contained between five and seven attack motives. Further, the number of cyberattack motives went up from seven to nine and remained at that number between 2012 and 2017. In 2018, however, the number of motives decreased a little, which we believed was due to the number of cyber incidents captured that year.

B. Types of Cyberattack Motives over the Years

It is necessary to explain different types of cyberattack motives prior to illustrating how the cyber incidents evolved over the years with respect to these motives. The cyber incident data recorded between 2006 and 2018 contained nine different types of cyberattack motives. They were (in alphabetical order) convenience, espionage, fear, finance, fun, grudge, ideology, multi-motives and others. They can be explained as follows.

The convenience motive (it could also be known as simplicity) means that the cyberattacks that occurred were simple to proceed by attackers. That is, the attacks could be done with little effort. It could be because the targets were hosting databases or applications with well-known vulnerabilities. Therefore, they could be attacked with ease and became the reason for adversaries to attack the systems.

The espionage motive in this context is defined as the act of stealing sensitive, classified or secret information for either business advantage or even political reasons. The third motive was fear. This did not mean that adversaries were afraid of something. What this motive meant was the fact that cyberattacks were done with an aim to generate fears to the targets. In more detail, attackers knew that if an attack were successful and damages were done to a target, this would create and spread an atmosphere of fear, which in turn could cause a panic in wide areas.

The fourth cyberattack motive was, of course, finance. Financially motivated cyberattacks simply had an aim of financial gain. This included stealing money directly from financial accounts, stealing credit card information and demanding ransom. The next cause of cyberattack was just attackers having fun. Many attackers simply enjoyed testing their knowledge and skills. For this reason, the attackers with this motive tended not to have any intent to cause any harm, since most of the time they only wanted to gain some experience and have some fun.

The next cause of cyberattacks was grudge. This usually occurred when the attackers had the desire to take revenge against individuals or organizations. For example, an employee who felt unfairly treated might steal or delete valuable data from their organization's database. Ideology was the next attack motive that we were able to extract from the captured data. This type of motive was when attackers wanted to express their opinions or criticisms over political, social or any current affairs. For ideology, the attack targets would be mostly government or organization's Web sites.

The final two cyberattack motives were called multi-motives and others. The multi-motives were the cyberattacks that were carried out because of more than one of the previously stated reasons, while others meant anything other than what we had already stated.

Now that we have seen what the different types of motives were, it is possible to illustrate what cyberattack motives each year contained. Fig. 2 summarizes the cyberattack motives that were the causes of the incidents between 2006 and 2018.

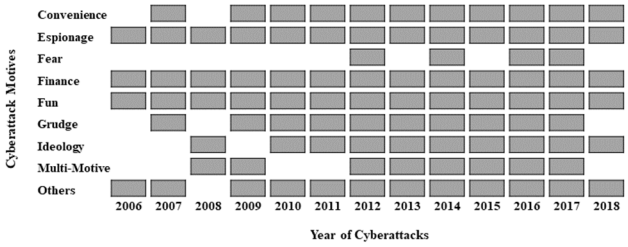

Fig. 2 Cyberattack Motives between 2006 and 2018

From the data shown in Fig. 2, we examine the cyberattack motives that were thought to be the causes of cyber incidents from 2006 to 2018. The results show that in 2006, there were only three main attack motives (excluding others), which were espionage, finance and fun. In 2007, two motives were added to the list, namely convenience and grudge. Interestingly, in 2008, the convenience and grudge attack motives were replaced by ideology and multi-motive. That said, the number of attack motives in the first three years that the data was collected lied between three and five.

In 2009, the count of motives increased to six with convenience and grudge brought back to the main causes of cyberattacks, along with espionage, finance, fun and multi-motive. The main cyberattack motives in 2010 and 2011 were exactly the same. They included convenience, espionage, finance, fun, grudge and ideology.

The year 2012 showed that the number of attack motives increased from the previous years and appeared to remain that way until 2017. Overall, the motives that caused cyber incidents were convenience, espionage, fear, finance, fun, grudge, ideology and multi-motive. It should be noted that 2012 was the first time that fear became one of the attack motives.

Let us look at the data and Fig. 2 in more detail. What the data shows is that there were only three cyberattack motives out of nine that stayed throughout the years 2006 to 2018. They were espionage, finance and fun. Ideology only came into the scene in 2008 and appeared to remain one of the major motives until 2018. Moreover, the fear motive began to play a role in 2012. This particular motive seemed to come and go but was still one of the major ones to be taken into account.

Finally, 2012 was the very first time that the cyberattacks were caused by all the major motives. This was also the case in 2014, 2016 and 2017, while the number of different motives dropped in 2018. This might be because of the number of records or incidents collected that year.

On the whole, what can be summarized regarding the types of cyberattack motives and how they evolved over the years, at least in the space of thirteen years from 2006 and 2018, is as follows. In the earlier years, the causes of the attacks were simply the acts of stealing information, financial gain and reputation seeking in the espionage, finance and fun motives, respectively. The count of motives increased in the later years to include grudge, fear, convenience, and especially ideology. This implies that as we went further through the years, we should understand that there are many different motives behind the attacks. This means that preventing attackers from attempting to steal information or money may not be enough. It is necessary to put some thoughts into other causes and motives such as employee's revenge and ideology, too.

C. Proportions of Cyberattack Motives

What we have seen in the previous section is how new motives entered the attack space as the years progressed. This section takes a different perspective in the data analysis by examining the proportion of each type of motives that occurred between 2006 and 2018. In other words, Fig. 3 shows the percentage of the motives that were the causes of cyberattacks each year.

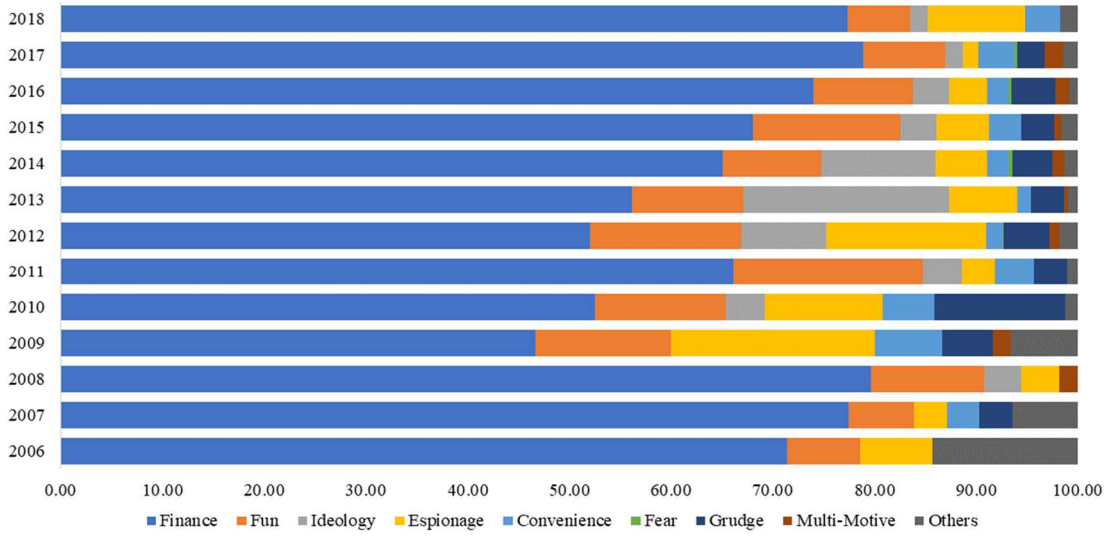

Fig. 3 Proportion of Cyber Attacks between 2016 and 2018

The data in Fig. 3 shows that the largest proportion of cyberattack motive was the finance motive throughout the studied period. Between 2006 and 2008, the cyberattacks that were financially motivated accounted for over 70%. The proportion dropped to approximately 47% in 2009 but went up again to over 66% in 2011. The number of financially motivated attacks appeared to decrease again in 2012. Since then, the proportion steadily climbed up to almost 80% in 2018. This data, therefore, tells us that although there were many different motives to carry out cyberattacks, finance was still the reason for the majority of the attacks that occurred between 2006 and 2018, with the average of approximately 63.66%.

The second motive that we looked at is the fun motive since it constituted the second highest proportion and appeared throughout the years. Although this particular motivation represented the second largest in proportion, it was

still a large distance behind the top motivation. The fun motivation appeared to steadily increase in value from 2006 to 2011 rising from 7.14% to 18.58%. From 2012, the proportion seemed to fluctuate a little throughout, ranging between 6.00% and 14.86%. Overall, the cyberattacks that were motivated by attackers having fun or testing their knowledge accounted for approximately 11.69%.

The motive that gave the third highest number in proportion was surprisingly ideology. We said surprisingly because from the data, ideology only became the motivation of any note in 2008, two years later than finance, fun and espionage motivations. Since it came into the scene as a cause of cyberattacks, the number of attacks motivated by ideology was consistent in its first three years. The number of ideology

motivated cyberattacks increased sharply in 2013 with it taking over 20% of all cyberattacks and over 11% in the following year. However, the number of cyberattacks caused by ideology had decreased to around 1.74% in 2018. In general, ideology accounted for 9.09% of all cyberattacks between 2006 and 2018 according to our data.

The next motivation that we looked at is espionage. The amount of espionage motivation between 2006 and 2018 appeared to fluctuate. That is, in 2006, the proportion of this type of motivation was 7.14%. The value went down in the next two years to just over 3%. However, the number suddenly shot up to twenty per cent in 2009 and went down again in 2010 and 2011. In 2012, the number of attacks with espionage motivation increased to its highest at 15.67%. The number of attacks occurred due to this motivation decreased steadily from 6.72% in 2013 to just 1.48% of all attacks collected in 2017. Finally, in 2018, the proportion of espionage was at 9.57%. This gave the overall average of the espionage motivated attacks at 7.08% of all cyberattacks recorded between 2006 and 2018.

Other motivations, namely convenience, fear, grudge, multi-motive and others, completed the recorded cyberattack motivations. On average, they made up smaller proportions of all motivations at 2.34%, 0.13%, 3.68%, 0.85% and 1.47%, respectively. This means that altogether these five motivations only had approximately 8.65% of all motivations behind the attacks that occurred from 2006 to 2018.

D. Cyberattack Motive Rankings

We have now seen that there were many different motivations behind cyberattacks, and what their proportions were compared with others. It would be interesting to see how each motivation ranked each year as well as how the rankings changed over the years. This is so that we would be able to see how the motivations evolved, in terms of the number of attacks caused by them. The rankings can be seen in Fig. 4.

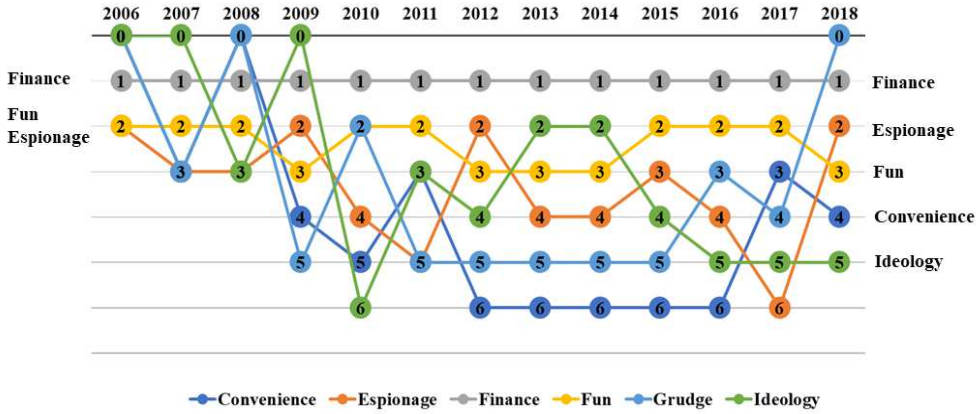

Fig. 4 How Cyberattack Motivations were Ranked between 2006 and 2018

Note that fear motivation, multi-motive motivation and others were left out from the figure because it would make the figure clearer, and more importantly, they contributed to just over two per cent of all cyberattacks.

The data in Fig. 4 shows that finance was always the top motivation for cyberattacks as it was consistently ranked number one. The fun or skill testing motivation only varied between second and third throughout the studied period. In other words, the motivation was ranked second between 2006 and 2008. It dropped to number three in 2009 and went back to number two again in the next two years in 2010 and 2011. From 2012 and 2014, the fun motivation was at number three before it went up to the second highest ranked motivation between 2015 and 2017. In 2018, it was overtaken by espionage which made the fun motivation drop to third.

Espionage motivated cyberattacks appeared to oscillate throughout the years. Between 2006 and 2009, espionage was ranked between second and third, in terms of the number of attacks motivated by it. There was a drop in its rank to number four and five in 2010 and 2011, respectively. Espionage motivation sharply went up to number two in 2012. Over the next four years, it seemed to be more consistent in its proportion ranking by remaining between third and fourth. Interestingly, espionage dropped to sixth in 2017 before going back to the number two spot in 2018.

The next motivation to be discussed is ideology, which was the cause of the third highest number of cyberattacks according to our data in the previous section. Ideology first came to be one of the motivations behind cyberattacks in 2008 at number three. In 2010, ideology was not as popular as other motivations as it dropped to number six in the rankings. However, between 2011 and 2015, ideology became one of the notable motivations, placing itself between number two and number four in the rankings. In the final three years, it was ranked fifth, meaning that although still a noteworthy motivation, it was not as outstanding as the others.

There was a cause of cyberattack, namely convenience, which was not ranked as highly as we first thought. Convenience or simplicity, as explained earlier, means that it would not take a lot of effort from the attackers to compromise a system. This might be because there was a known vulnerability or there was an easy-to-use tool to assist in attacking the system. Although this was the case, the convenience motivation was only ranked between third and sixth. In fact, it started off at the number three spot in 2007. In 2008, it was not even considered one of the top motivations in our dataset. The convenience motivation appeared in the rankings again in 2009 at the number four spot before gaining its popularity in 2010 to rise to the third position. However, that was as high as it got. After that, convenience dropped to

the number sixth position and remained there between 2012 and 2016. In 2017 and 2018, this motivation was sought after again at rank number three and four, respectively.

Even though grudge or revenge was an intriguing motivation, it only performed similarly to the convenience motivation. In other words, grudge first appeared in the dataset in 2007 at the number three position. In 2008, it did not make the rankings at all 2008 before appearing at number five in 2009. Grudge went to its highest position in 2010 at number two. However, from 2012 to 2015, the grudge was ranked number five, meaning that it was not one of the bigger causes of cyberattacks during that period. In 2016 and 2017, it became more popular, which showed in our dataset at positions three and four, respectively. In 2018, this motivation disappeared altogether, indicating that grudge was no longer considered a real motivation behind cyberattacks.

What we learned from the ranking analysis, on the whole, is that finance had always been at the number one position for cyberattack motivation, and it never left the top position over the studied period at all. Secondly, the fun or skill testing motivation performed consistently throughout the years, ranking in the second and third positions according to our dataset. Espionage and ideology appeared to vary the most, with their positions ranging from number two to number six between 2006 and 2018. Fourthly, convenience started in 2006 at the number three position before trailing off to rank number six and ending at the fourth in 2018. Finally, grudge entered the cyberattack motivation scene at the third position, lost its strength, and remained at number five. In 2018, grudge or revenge was not even a cyberattack motivation recorded in the dataset.

E. Correlation Analysis

We have now seen how cyberattack motives evolved in the context of variety, types, and proportions. It would be necessary to go deeper in the analysis to see the changes throughout the studied period. Correlation analysis, specifically the Pearson correlation coefficient, was the statistical test applied so that the development or evolution of relationships between cyberattack motives could be studied.

As we already know, correlation is a statistical method that is used to test the relationship between variables [28]. In this case, the variables were the cyberattack motives. A correlation coefficient was applied to measure how strongly or weakly the cyberattack motives were related. The Pearson correlation coefficient was calculated through the number of cyber incidents that occurred due to each cyberattack motive. Table 2 displays the correlations between the cyberattack motives.

TABLE II
PEARSON CORRELATION COEFFICIENT BETWEEN CYBERATTACK MOTIVES FROM 2006 TO 2018

Motive	1	2	3	4	5	6
1 Convenience	1					
2 Espionage	0.444	1				
3 Finance	-0.428	-0.795	1			
4 Fun	0.265	0.263	-0.569	1		
5 Grudge	0.569	0.352	-0.626	0.374	1	
6 Ideology	-0.324	-0.033	-0.368	0.176	0.089	1

The values of the correlations in Table 2 were calculated using the data from 2006 to 2018 so that we could first see the overall picture. We should also note that we omitted the fear, multi-motive, and other motives since they only contributed to a very small number of cyberattacks.

In general, between 2006 and 2018, there appeared to be moderate positive relationships between convenience and espionage and convenience and grudge with the values of Pearson correlation coefficients of 0.444 and 0.569, respectively. There were also moderate to high negative correlations between several pairs of motives. The first was between finance and espionage, with a value of -0.795. The second moderate negative relation was between fun and finance, with a magnitude of -0.569. The third was -0.626 coefficient between grudge and finance. Other cyberattack motives did not seem to have much correlation. Although Table 2 provided information regarding whether or not there were any correlations between motives, it was not the exact aim of the research to look at this directly. Having said that, we learn from Table 2 that for positive relationships, in the case of knowing that a cyberattack with a particular motive occurs, one could foresee that a motive with a positive relationship might be increasing side, too. This implies that preparation could be in place to reduce the risk. What we did next, though, would be more closely connected to the research objective in analyzing how the correlations developed or evolved through time.

The method we adopted to see the evolution of relationships was to divide the data into two halves. The first was to compute the correlation coefficients between cyberattack motives in the first six years of the dataset from 2006 to 2011. This is shown in Table 3. The second half was the computation of the correlations from 2012 to 2018. This is displayed in Table 4.

TABLE III
PEARSON CORRELATION COEFFICIENT BETWEEN CYBERATTACK MOTIVES FROM 2006 TO 2011

Motive	1	2	3	4	5	6
1 Convenience	1					
2 Espionage	0.689	1				
3 Finance	-0.847	-0.892	1			
4 Fun	0.470	0.153	-0.463	1		
5 Grudge	0.713	0.451	-0.703	0.296	1	
6 Ideology	-0.048	-0.319	0.023	0.645	0.321	1

TABLE IV
PEARSON CORRELATION COEFFICIENT BETWEEN CYBERATTACK MOTIVES FROM 2012 TO 2018

Motive	1	2	3	4	5	6
1 Convenience	1					
2 Espionage	-0.407	1				
3 Finance	0.859	-0.644	1			
4 Fun	-0.485	0.408	-0.719	1		
5 Grudge	-0.663	0.011	-0.545	0.688	1	
6 Ideology	-0.814	0.177	-0.756	0.246	0.320	1

The data in Table 3 and Table 4 show a few notable developments in the correlations between cyberattack motives. They can be described as follows. First, the convenience and espionage motives appeared to have a moderately strong positive relationship with a coefficient of 0.689 between 2006

and 2011. However, the relationship turned opposite between 2012 and 2018, with a coefficient of -0.407.

The second and most obvious development was the relationship between finance and convenience attack motivations. In the first six years of the dataset, it can be seen from Table 3 that the correlation coefficient was -0.847, which indicated a very strong negative relationship between the two motives. In the final seven years, however, the value was 0.859, which indicated a very strong positive relationship. We would like to point out that correlation did not intend to mean causation [28]. We did the analysis to illustrate how each pair of cyberattack motives was related and evolved throughout the studied period. In this case, it was obvious in the evolution that the relationship between finance and convenience changed completely as time passed.

The relationships between espionage and convenience as well as finance and convenience, were not the only ones that ultimately flipped from one direction to another. There were two other pairs of cyberattack motives whose relationship reversed: convenience and fun and convenience and grudge. For the convenience and fun correlation, from 2006 to 2011, the relationship was positive and moderate, while from 2012 to 2018, it became moderately negative. For the convenience and grudge correlation, from 2006 to 2011, the relationship was strongly positive with a 0.713 coefficient, but the relationship turned moderately negative during the 2012 and 2018 period with a coefficient value of -0.663.

Ideology and finance correlation could not be overlooked at all. This was because, during the 2006 to 2011 period, their relationship was on the positive side, albeit very weak. However, during the 2012 to 2018 period, the correlation turned negative, and on the strong side of negative, too, with the correlation coefficient of -0.756.

Another dimension that appeared to be interesting regarding the development of correlations between cyberattack motives was that some relationships got stronger or weaker as time passed. The first obvious example was the convenience and ideology pair. During the first half of the studied period, the correlation coefficient was only slightly negative at -0.048. During the second half, though still negative, the correlation became approximately seventeen times stronger at -0.814.

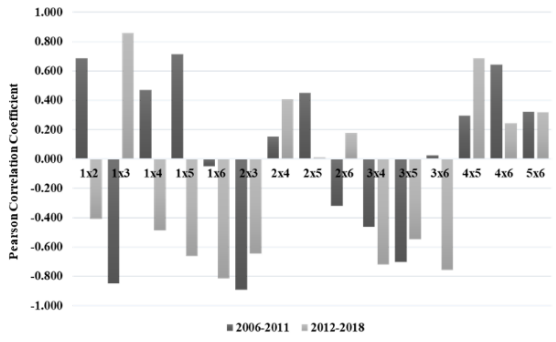

Fig. 5 How the Correlations between Cyberattack Motivations Evolved

There was one other relationship whose correlation coefficient got higher in the second half. The grudge and fun's correlation coefficient went from 0.296 to 0.688 or around 2.33 times higher. On the other hand, the ideology and fun's correlation coefficient decreased in value from 0.645 to 0.246 or approximately 2.62 times weaker. This part, we analyzed the data to see whether there were any changes in the correlations between cyberattack motives over the 2006 and 2018 period. It was found that several pairs of the attack motives evolved from having a negative correlation to a positive one and vice versa. In addition, a few relationships became notably stronger, both positively and negatively, as the years went by. This is summarized in Fig 5.

F. Discussion

When it comes to minimizing the risk of cyberattacks, many people and organizations focus on security tools, processes, and mechanisms, from installing anti-virus software to configuring firewalls. Although these defenses can be helpful, we believe that knowing the reasons or motives can create a strong defense against cyberattacks. Therefore, this study examined the motivations behind the cyberattacks recorded between 2006 and 2018.

The results provided insight into how the motives changed or evolved over the years. First, the number of recorded cyberattack motives started off in 2006 with only three notable types of motives (excluding others) espionage, finance, and fun. The number steadily increased to eight different types (also excluding others) in 2017. During the studied period, the motives that appeared and stayed for good, specifically from 2010 onwards, were grudge and ideology. This implies that the attacks began with a clear motivation, whether to steal information, make a profit, or have fun. However, as time passed, the cyberattacks appeared to be more sophisticated in attackers wanting to express their opinions or carry out an act of revenge.

Second, it can be seen from our analysis that finance had always been, and will always be the primary motive behind cyberattacks, with it having the largest proportion of all cyberattacks recorded between 2006 and 2018. Over thirteen years, financially motivated attacks accounted for approximately 63.66% of all attacks. A motive closely related to finance was espionage [21], which was the act of stealing information from individuals or organizations. The espionage motive was the one that surprised us the most. This was because we had expected the proportion to be close to finance. On the contrary, only seven percent of all attacks were motivated by espionage. 2010 was the only year that the amount of espionage went above the 10% mark. Saying that 2018 presented an interesting trend. It was the first time that financially motivated attacks, together with espionage, were recorded at almost 87% of all cyberattacks. This seemed to have set the trend for the present day's attacks, of which over ninety percent were financially motivated [14], [21].

In the middle of the studied period, specifically between 2008 and 2015, fun appeared to contribute to the second largest proportion of the cause of cyberattacks, with the highest value in 2011 at over eighteen percent. However, the amount dropped off a little bit towards the end where fun accounted for around 6% in 2018. Interestingly, one study suggested that attackers motivated by the desire to have fun were more likely to use known vulnerabilities as their channel of attack [13]. This led us to look at another motivation known as a convenience.

There should be some relationship between fun and convenience [13]. However, our finding was not consistent with the suggestion by Holt *et al.* By calculating the correlation value between the fun and convenience motives, we obtained the overall resultant value of 0.265, which meant that the two were not as closely related as mentioned by Holt *et al.* [13]. Furthermore, the correlation coefficient represented a negative relationship between these two motivations with a value of -0.485 in the period towards the end of our study.

Ideology was a cyberattack motivation that was discussed in a few works of literature as one of the main causes of cyberattacks. Holt *et al.* [13] went so far as to suggest that ideology was strongly correlated to cyberattacks. Our study partly agreed with this suggestion because, on average, ideology accounted for almost 10% of all the causes of cyberattacks between 2006 and 2018. We used the phrase "partly agreed" because if we looked at the data more closely, we would see that the amount of ideologically motivated cyberattacks peaked in 2010 and 2011 at 20.26% and 11.26%, respectively.

Another motivation that entered the cyberattack scene but trailed off towards the end of the study period was a grudge. A grudge or an act of revenge was usually carried out by an insider or someone who worked within an organization. Maasberg *et al.* [21], [29] showed several possible motivations behind insider attacks. However, the one that was more significant than the others was revenge.

IV. Conclusion

Attackers are people who aim to compromise information systems. At the same time, one of the goals of the owners of those information systems is to reduce the risk of being attacked by applying various means such as detection, identification, and threat prevention. In order to achieve the required objective, it is vital to understand the motivations behind cyberattacks [30].

Our research looked at the different attack motivations and analyzed how the motivations developed and evolved over the years. Specifically, we studied over 7,700 cyber incidents recorded between 2006 and 2018 and analyzed the evolution of cyberattack motives five folds.

Firstly, it was clear that the number of cyberattack motives increased as the years went by. Secondly, in 2006, there were only three main motivations behind the attacks: espionage, finance, and fun. Towards the end of the studied period, a few more motives were added to the existing ones: convenience, fear, grudge, and ideology.

The third and fourth aspects that we studied were the proportions and ranks of the cyberattack motives. It was found that cyberattacks that were financially motivated took the largest proportion and were ranked first throughout the thirteen years of our data. The second-ranked motivation based on the amount was the fun motive when attackers want to test their skills and knowledge to see whether they could attack their targets. For other motives, the proportions and ranks varied over the study period, with espionage seemingly varied the most by going from second to sixth to back. Ideology was another interesting motive because it only became something of a note in 2008 at rank number three, fluctuated to all the positions (except the top motive), and ended up at the number five attack motive in 2018.

Finally, the correlation between the motivations behind the cyberattacks was analyzed. This was when the development and changes could be very clearly spotted. In other words, it was apparent that in the first half of the period of the recorded incidents, some pairs of attack motives such as convenience and espionage and convenience and grudge had a positive relationship. However, negative correlations were obtained in the second half or from 2012 to 2018. On the other hand, some motives had a negative correlation in the first six years, but the correlation turned positive later. Examples of such motivations were espionage and ideology. Moreover, there were other pairs of cyberattack motives whose relationships got stronger or weaker in both the positive and negative directions as the years went on. An example of the correlation that got stronger positively was the fun and grudge motivations, whereas the one that got stronger in the negative direction included the finance and fun motivations.

Even though it is believed that our analysis provided insight into how cyberattack motives evolved or developed over the years, there were still a couple of limitations to our study. The first was the data used in the analysis. Although the number of recorded cyber incidents was impressively over 7,700, they only came from one data aggregator that collected them from various sources, meaning that cyber incidents would be missing from the dataset. Secondly, despite the comprehensive analysis of the data, the cyber incidents only ranged from 2006 to 2018, which may not truly reflect the evolution up to the present day in 2021. It is believed that the thirteen-year period should still provide an adequate indication of how the motivations developed and evolved.

In summary, we learned from the analysis that not all cyberattack motives were equal, no matter in what dimension. Organizations or information system owners should not only focus on protecting what would be the targets of attackers, they should also learn the motivations behind the attacks so that it will be possible to at least understand better what the attackers are after. As a result, this would help defend against cyberattacks better, too.

References

[1] S. Boonkrong, *Authentication and Access Control: Practical Cryptography Methods and Tools*, Apress, 2021.

[2] National Institute of Standards and Technology, "Security Requirements for Cryptographic Modules," National Institute of Standards and Technology, Washington, D.C., 2001.

[3] International Organization for Standardization, "ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems," International Organization for Standardization, Vernier, Geneva, Switzerland, 2018.

[4] R. Mei, H. B. Yan and Z. H. Han, "RansomLens: Understanding Ransomware via Causality Analysis on System Provenance Graph," *Lecture Notes in CompSci, SceSec2021*, 13 - 5 Aug 2021.

[5] L. Huang and Q. Zhu, "Duplicity Games for Deception Design with an Application to Insider Threat Mitigation," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 4843 - 4856, 2021.

[6] R. Chen, D. J. Kim and R. H. Rao, "A study of social networking site use from a three-pronged security and privacy threat assessment perspective," *Inf. Mang.,* vol. 58, no. 5, July 2021.

[7] A.Altalbe and F. Kateb, "Assuring enhanced privacy violation detection model for social networks," *Int. J. Intell. Comput.*, vol.15, no. 1, pp. 75 - 91, 2022.

[8] M. Mahapatra, N. Gupta and R. Kushwaha, "Data Breach in Social Networks Using Machine Learning," *Commun. Comput. Inf. Sci., IACC 2021*, 18 - 19 December 2021.

[9] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Rep.,* vol. 7, pp. 8176-8186, September 2021.
[10] T. Oyinloye, T. Eze and L. Speakman, "Towards Cyber-User Awareness: Design and Evaluation," in *Proc. of Eur. Conf. Inf. Warf. Secur.*, Reading, UK, 2020.
[11] H. Hamam and D. Abdelouahid, "An OWASP top ten driven survey on web application protection methods," *LNCS*, pp. 235-252, 2021.
[12] N. K. Singh, P. Gupta, V. Singh and R. Ranjan, "Attacks on Vulnerable Web Applications," *CONIT 2021*, 25 - 27 June 2021.
[13] T. J. Holt and S. v. d. Weijer, "An Examination of Motivation and Routine Activity Theory to Account for Cyberattacks Against Dutch Web Sites," *Crim Justice Behav,* vol. 47, no. 4, pp. 487-505, January 2020.
[14] J.W. Welburn and A.M. Strong, "Systemic Cyber Risk and Aggregate Impacts", *Risk Anal.*, In Press, 2021.
[15] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu and P. Laplante, "Dimensions of cyber-attacks: Cultural, social, economic, and political," *IEEE Technol. Soc. Mag.*, vol. 30, no. 1, pp. 28-38, Spring 2011.
[16] S.K. Srivastava, S. Das, G.J. Udo and K. Bagchi, "Determinants of Cybercrime Originating within a Nation: A Cross-country Study," *J. Glob. Inf. Technol.*, vol. 23, no. 2, pp. 112 - 137, April 2020.
[17] M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and their Classification," International Journal of Network Security, vol. 15, no. 5, pp. 390-396, 2013.
[18] S.S. Bhuyan, U.Y. Kabir, J.M. Escareno, K. Ector, S. Palakodeti, D. Wyant, S. Kumar, M. Levy, S. Kedia, D. Dasgupta and A. Dobolian, "Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations," *J. Med. Syst.*, vol. 44, no. 5, May 2020.
[19] V.-L. Nguyen, P.-C. Lin and R.-H. Hwang, "Web attacks: defeating monetisation attempts," *Netw. Secur.,* vol. 2019, no. 5, pp. 11-19, May 2019.
[20] A. Jawad and J. Jaskolka, "Modeling and Simulation Approaches for Cybersecurity Impact Analysis: State-of-the-Art," in *Proc of ANNSIM 2021*, Virtual Fairfax, 19-22 July 2021.
[21] M. Maasberg, X. Zhang, M. Ko, S. R. Miller and N. L. Beebe, "An Analysis of Motive and Observable Behavioral Indicators Associated With Insider Cyber-Sabotage and Other Attacks," *IEEE Eng. Manag. Rev.,* vol. 48, no. 2, pp. 151-165, June 2020.
[22] M. J. Pappaterra, F. Flammini, V. Vittorini and N. Besinovic, "A Systematic Review of Artificial Intelligence Public Datasets for Railway Applications," *Infrastructures,* vol. 6, no. 10, pp. 1-28, October 2021.
[23] P. Silva, C. Macas, E. Polisciuc and P. Machado, "Visualisation Tool to Support Fraud Detection," in *Proc. of IV*, Sydney, 5-9 July 2021.
[24] F. Fong, Z. Qin, L. Xue, J. Zhang, X. Lin and X. Shen, "Privacy-Preserving Keyword Similarity Search over Encrypted Spatial Data in Cloud Computing," *IEEE Internet Things J.*, in Press, 2021.
[25] J. Lu, "Data Analytics Research-Informed Teaching in a Digital Technologies Curriculum," *ITE*, vol. 20, no. 2, pp. 57-72, 2020.
[26] Barclays, "IoD Policy Report - Cyber Security Underpinning the Digital Economy," Barclays, London, UK, 2016.
[27] J. Franco, A. Aris, B. Canberk and A.S. Uluagac, "A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 4, pp. 2351-2383, 2021.
[28] R. Aggarwal and P. Ranganathan, "Common pitfalls in statistical analysis: The use of correlation techniques," *Perspect Clin Res.*, vol. 7, no. 4, p. 187, October - December 2016.
[29] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K.-K. R. Choo and P. Burnap, "Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses," *Elec.*, vol. 9, no. 9, pp. 1-29, 2020.
[30] P. Chapman, "Defending against insider threats with network security's eighth layer," *Comput. Fraud Secur.*, vol. 2021, no. 3, pp. 8 - 13, March 2021.