https://doi.org/10.48009/4_iis_2018_176-186

Issues in Information Systems
Volume 19, Issue 4, pp. 176-186, 2018

ANALYSIS OF THE GROWTH OF SECURITY BREACHES: A MULTI-GROWTH MODEL APPROACH

Godwin Udo, University of Texas, El Paso, gudo@utep.edu
Kallol Bagchi, University of Texas, El Paso, kbgachi@utep.edu
Peeter Kirs, University of Texas, El Paso, pkirs@utep.edu

ABSTRACT

We compare the performance of three growth models – Gompertz, Logistics, and Exponential -using security breaches data from the fifteenth annual report of the Computer Security Institute. Unlike other studies, multiple components (frequency of attacks and dollar loss value) are utilized to model the growth of security breaches thereby providing a balanced understanding of the undesirable phenomenon. The findings indicate that multiple-dimensional approach to modeling security breach approach seems more rigorous than the single-dimension found in the literature. The two components seem to be different and each explains an aspect of security breach growth rate. Frequency of attacks provides a slightly better fit than dollar loss value in all three models.

Keywords: Security Breaches, Frequency of Attacks, Dollar Loss Value, Gompertz Model, Logistics Model, Exponential Model

INTRODUCTION

Cybercrime affects everyone including individuals, states, corporations, national governments, and even not-for-profit organizations. With the explosive growth in the use of the Internet by individuals, businesses, and academia, there is a promising new market in security break-ins which exploits the weaknesses of the Internet. McAfee Inc., a security software company, estimates the annual cost of cybercrime at one trillion dollars (Hyman, 2013). Internet-related crimes show no signs of abatement. From 2013 to present there has been a flurry of data security breaches involving social media (e.g. Facebook, LinkedIn, Twitter, Google, Yahoo, etc.); Target store (with over 40 million customers' credit and debit cards number stolen); Adobe (more than 150 million Adobe username and password were compromised); Evernote (about 50 million account passwords reset after data breach); and the U.S. Federal Reserve Bank (whose website was hacked) just to name a few. The annual study by the Ponemon Institute (2014) reports that in 2014, the average annualized cost of cybercrime experienced by the U.S. firms was $12.7 million which is a 96% surge in five years (Rawlinson, 2014). The report also indicates that attacks are occurring more frequently and that it takes the firms 33% longer time to resolve the attacks with the average cost per attack being over $1.6 million. Some of the report's main findings are: cybercrimes impact all industries; cybercrimes are becoming more costly than ever; cybercrimes are intrusive and common; and information theft is the most costly among all cybercrimes. In 2014, eBay (about 145 million customers), JP Morgan Chase (about 76 million customers), and Home Depot (about 56 million customers) have suffered great losses because of attacks on their business data. According to Rob Lever (2018), report by McAfee indicated that cyberattacks are growing at a rapid pace in 2017 with intellectual property theft accounting for one-fourth of cybercrime in that year.

Table 1 below shows some of the large-scale data and security breaches in recent years thereby confirming the severity of the problem.

Table 1. Large-Scale Data Breaches

Victim	Year	# Affected (in millions)
Adobe	2013	152
eBay	2014	145
Heartland	2009	130
T.J. Maxx	2007	94
AOL	2005	92
Anthem	2015	80
Sony PSN	2011	77
US Military	2009	76
Target	2014	70
Evernote	2013	50
Living Social	2014	50

According to Markets and Markets, AlixPartners (2018), the global cybersecurity market is expected to reach $224.48 billion by 2022 growing at a rate of 14.84% from 2015 to 2022. Another practitioner source (Javelin Strategy Research, 2011) compares the dollar values losses between 2003 and 2010 with the conclusion that the total losses rise and fall from one year to another without any clear trend. For example, comparing 2003 ($59 billion) to 2004 ($70 billion) and 2009 ($56 billion) to 2010 ($36 billion) show no clear trend. This type of finding begs for a more systematic analysis of how dollar value loss can be used to understand the growth of data breach diffusion. The present study attempts this analysis.

In another field study by Javelin Strategy Research (2015), there is a clear indication that an increase in the number of attack incidents does not always imply an increase in the value of dollar loss. For example, the study shows that between 2010 and 2011, the attack incidents increased from 10.2 million (2010) to 11.6 million (2011) whereas the dollar value losses decreased from $20 billion (2010) to $18 billion (2011). In the same study, the difference is even clearer if 2012 is compared to 2014 which indicates an increase in attack incidents (12.6 to 12.7 million attacks) but the dollar value loss decreased significantly ($21 billion to $16 billion).

According to a research firm (AlixPartners, 2018, Ponemon Report, 2016), the following items have been identified as the fastest growing spending items: security analytics, threat intelligence, mobile security, and cloud security. The reason for the continued increase in security budget is cybercrime. The more the growth of data and security breaches, the more the organizations spend in an attempt to deter it. Some of the factors driving the continued growth in security spending are: regulatory compliance, business continuity, company reputation, internal policy compliance, among others. A lion share of security budget goes to the technologies used as countermeasures. Firms resort to countermeasure technologies as a means of protecting their data and systems. Some of the technologies fall into the following categories: monitoring and assessment, policies and control, software, firewalls, authentication/access, and encryption. We believe that how well a firm is prepared for the next data breach incidence can be measured by the sheer number of countermeasure technologies the firm employs.

The 2016 Ponemon Report (2016) reveals that healthcare organizations are attacked on monthly basis with over half of the healthcare organizations surveyed indicating that they experienced one or more cyberattacks in the last 12 months with 20% of them experiencing over 10 attacks. The report also shows that about 50% of the participants experienced losses or exposure of patient data during the last 12-month period. As already predicted by Expedia in its 2016 data breach projection report (2016), 2016 is the year healthcare industry will experience the most incidences of cybercrimes in its entire history so far. The industry has been said to be ill prepared for the new trend of attacks aimed at them. Ponemon states “Despite frequent cyberattacks, our survey shows that the healthcare sector is not consistently prepared with incident response processes to deal with them.”

Data security practitioners often indicate that the growth of data and security breaches can best be modeled in multiple dimensions such as frequency of attacks or cybersecurity budget. However, most of the empirical studies model the phenomenon with a single component which may not fully reveal the extent of the growth. Empirical studies dealing with cyber-attacks are scanty. Bagchi and Udo (2003) is one of the few studies that use the modified Gompertz model to analyze various cybercrimes. The present paper deals with understanding the various facets of data and security breaches by exploring it in two dimensions. It is no longer sufficient to measure security breaches with one-dimensional approach (Rawlison, 2014). We believe that more insight would be gain if multi-dimensional approach is used to study the growth of this undesirable phenomenon. The growth of data and security breaches can be measured in many ways including frequency of (number) attacks, dollar value of such attacks, the number of countermeasures deployed by the firms (number of technologies used by the firms), etc. Specifically, we intend to use two components to model cyber security breaches, namely: (a) the frequency of attacks; and (b) the dollar loss value of such attacks.

Using multi-dimension modeling, a few natural questions arise: Are these elements of attack analysis the same or are they different dimensions of a cyber-attack? Can the number of attacks be equivalent to the dollar loss value of such attacks? In a 2007 CSI (CSI, 2007) report, it was noted that “Even though average losses are up markedly this year, computer security incidents apparently occur with less frequency within organizations (page 11)”. This statement emphasizes the need for research that explores how these trends affect the growth of data and security. The role of countermeasure should be part of any security program (Straub and Wilke, 1998). According to co-diffusion framework (Rogers, 2003), innovations adoptions are interdependent in the same systems. Thus, the relationship between total number of security technology used and the frequency of various types of attacks needs to be empirically explored. Empirical studies are needed to explore various such relationships. This paper is an effort in this direction. It includes a time-series empirical analysis of the two elements of breaches using three popular diffusion models and compares the results obtained.

The objective of the present study is to test whether the two components are similar. The components data will be fitted with the three growth models— logistic, Gompertz and exponential. If the same model say logistic failed to model best the two sets of data, then it can be concluded that the components are different though each model has its own strengths. Thus the research question follows:
Research Question 1 (RQ1). Which of the three growth models best explain the growth of security breach?
Research Question 2 (RQ2) Are the two components of security breach (Frequency of Attacks and Dollar Loss Value) similar?

The remainder of this paper is grouped into the following sections. Section 2 presents the relevant literature while Section 3 presents the two security breach components and Section 4 the growth models. In Section 5 we discuss the data and method used while in Section 6 we present the results. The last section is for the discussions and conclusions.

RELEVANT LITERATURE

Kannan et al. (2007) mention that the costs of cybercrime are difficult to measure; however, these costs are reasonably substantial and growing rapidly. Garg et al. (2003) attempted to quantify the financial impact of IT security breaches by using event-study methodology. They came to the same conclusion that IT breaches are extremely costly. Lukasik (2000) claims that cybercrime costs are essentially doubling each year. The problem becomes even more complicated when one considers that these crimes are underreported. Ullman and Ferrera (1998) mention that, according to FBI estimates, only 17 percent of computer crimes are reported to government authorities.

Previous studies on internet security are lacking in empirical results on how different factors affect (retard or accelerate) internet attack growth. There are two major factors that influence growth of attack incidents: attacks and countermeasures. Growth models such as the one introduced in this paper are explanatory and based on theory. Such models can also be used to produce reliable forecasting of such attacks. By relating the model to fundamental factors that drive the attack growth process, it is possible to explain how the attack process is evolving over time. Relative contributions of each factor can be noted and changes over time can be examined.
A number of previous studies and reports (Harrington, 1996; Straub and Welke, 1998; D'Arcy, et al., 2009; Higgins, et al., 2005; Siponen and Vance, 2010) on computer/information systems security and related issues are found in the literature. Harrington (1996) observed that company codes of ethics may clarify responsibility and reduce rationalizations for some people. Unlike company codes, IS-specific codes of ethics had a direct effect on computer sabotage judgments and intentions, and responsibility denial was directly related to all computer abuse judgments and intentions studied. This has relevance to harmful computer activities within a firm. Straub and Welke (1998) advocated a theory-based security program for firms that included (1) use of a security risk planning model, (2) education/training in security awareness, and (3) countermeasure matrix analysis. Security losses can be managed or reduced when managers are aware of the full range of controls available and implement the most effective controls. Straub (1990) did an exhaustive work on security improvements in organizations. Based on Straub's observation that digital abuse growth is also dependent on security countermeasures, it is imperative that any explanatory model should include not only attack but also deterrence efforts. Such an explanatory model can show the relative strengths of attack and deterrence efforts over time and thus help in evaluating the status of attack growth and deterrence efforts. Research on causes of attacks should take into account the time-related social learning processes that mediate the impact of these factors. The interactive nature of attacks should be appropriately modeled. Existing security literature does not address this issue which is the motivation and contribution of the current study.

Commonly, past studies identify two main types of factors behind attacks: instigation and inhibition efforts. Hackers are one of the prime motivators of attacks. With the increase in size of the Internet, the hacker community has also grown in size. This community consists of "free thinkers," talented software developers who think software should be free, at the one extreme, and "crackers," who just like to break into systems with malicious motives, at the other extreme. The second factor in the equation, an inhibition factor, leads to preventive actions such as the installation of preventive infrastructures (firewalls, intruder detection, and timely introduction of security patches), the presence of security providers of a firm, as well as security advisories on the Internet and government regulations (Panko, 2002). The security infrastructure and security providers no doubt act as a deterrent to attempts of breaches. Growth models are needed that can capture both deterrence as well as imitation activities to model the attack incidents. It is important to compare growth models in order to determine how such a growth model performs. However, traditional diffusion models do not provide the necessary explanatory power to analyze the attack phenomenon adequately (Mahajan and Peterson, 1987). It is therefore necessary to explore a growth model that is theory-based as called for by Straub and Welke (1998).

The growth of cyber security breaches can be studied from an innovation diffusion perspective (Rogers, 2003). Innovation diffusion literature is usually concerned with good innovations and thus biased towards good innovations. The study of bad innovations such as internet security attacks can alert readers to the fact that innovations are not always good and what actions need to be taken to prevent such bad innovations. The present study therefore contributes to the literature by investigating the diffusion of undesirable or negative innovation namely cyber security breaches. Many previous studies have used diffusion models to explain or analyze patterns of diffusion of innovations over a period of time. These models usually result on fairly accurate forecast of the level of penetration and saturation (Bagchi and Udo, 2003). Functions such as the logistic, Gompertz, exponential, or mixed are the most common in the literature and they have been shown to follow an s-curve pattern.

COMPONENTS OF SECURITY BREACH GROWTH

Previous studies have identified categories of factors: instigation and inhibition efforts that can be used as indicators of security breaches diffusion. In this study we do not only consider the two categories but we have added a third category namely: the extent of damage done by breaches as measured by dollar loss value. First, let us discuss instigation efforts. Therefore, the first component to be considered is frequency (or number) of attacks.

Hackers play a significant role in cyber security breaches and with the increase in size of the uses, competition among hackers has increased in recent years making poorly designed systems of many famous businesses and government agencies easy targets. The more successful the earlier attackers are, the more aggressive the behavior of the next attacker becomes. Each such incident is an imitation of previous behavior and a behavioral model for others to imitate. In our present study we refer to this category of factor as the number of breaches experiences over a time and is measured by the sheer number of attack incidents.

The second factor - dollar loss value - can be a good indicator of security breaches growth. Is the loss due to these attacks increasing or declining in value? Neumann (1999) mentions that the costs of cybercrime are difficult to measure, however, they are reasonably substantial and growing exponentially. Example of loss resulting from security breaches includes losses due to interruption in business operations, lost sales, reduced volume due to dissatisfied or frightened customers, cost of restoring the systems, etc. (Garg et al., 2003; Lukasik, 2000).

GROWTH MODELS

We use three primary growth models to observe, which one best represented the attack-incidence growth. These were:
1. Exponential model
2. Logistic model
3. Gompertz' model (Pitcher *et al.*, 1978, Mahajan and Peterson 1987)

These diffusion models are time-dependent and not spatial (Mahajan and Peterson, 1987). Prior research has also shown that internet growth is more of an exponential one, not showing any sign of decreasing (Rai *et al.*, 1998). It could therefore be argued that, consistent with internet growth, attack incidents grow exponentially without any deterrence activities. The logistic model is based on a contagion hypothesis, which triggers an activator part and also contains an inhibitor part. The model is symmetric in nature. Gompertz model assumes that the probable causes for the outbreak of attack incidents are imitative as well as inhibitive in nature. The imitative aspect is said to be based on incident news spread via the internet as well as by word-of-mouth; the inhibitive aspects can also be spread via internet/websites and related stories. People engage in security attacks when they feel threatened or are motivated by some economic or other gain and have observed the success of earlier attackers (Bandura, 1986). According to experts, hackers do it for the sheer intellectual challenge rather than any criminal intent. Of course, other types of challenges come, for instance, from making money or taking economic or political advantage. On the other hand, the increase of security activities and success stories about preventing such attacks could reduce the number of attacks. Thus, a combination of imitation and inhibition as assumed by an asymmetric model could provide a realistic background in modelling such incidents.

Table 1 shows the functional form of each of these three models. Linear and nonlinear regression analyses were performed to derive estimates of the various parameters.

Table 1. Functional forms of four models

Model	Model expression
Exponential model	$N(t) = f \cdot e^{gt}$
Logistic model	$n(t) = \dfrac{K}{1 + Ka \cdot b^{t}}$
Gompertz model	$\dfrac{dN(t)}{dt} = c \cdot e^{-qt} \cdot N(t)$

Note: t = time; N(t)= cumulative number of attack incidents at time t; n(t) = number of attack incidents at time t; ε(t) = error term; a, b, c, f, g, q, K: parameters of the models.

DATA ANALYSIS AND METHOD

The fifteenth Annual Report of the Computer Security Institute (CSI) which Richard Power (2011) directs is the 2010/2011 survey of computer crimes and security practices. The institute has been gathering data on some aspects of cybercrimes since 1997 using a survey questionnaire distributed to information security personnel in organizations in the U.S. The 2011 survey was distributed to 5412 individuals with response rate of 6.4% or 351 individuals responding. The statistical rigor of the survey findings is sound (Richardson, 2011). The same survey has been used for all years and the respondents are mostly security professionals with firms who are better-informed about the attacks than others. This data set is used for the present study. We used total annual loss data which was available in US$ value. We decided to use the annual financial loss data as it would reflect the most accurate situation in terms of extent of financial damages incurred by firms by such attacks. The financial loss data were converted to 1996 US$ value by dividing by the price deflator for each year.

RESULTS

Table 2 shows the job titles, annual revenues, industry sectors, and number of employees of the participating organizations. As expected, security officer was the largest category (20%) followed by CEOs (12.6%); systems administrators (10.9%); CISOs (10.6%); and CIOs (4.9%). The other job titles jointly made up 41.2%. Annual revenue of over one billion dollars made up 28.1% while under 10 million dollars made up 38.2% of the participating organizations. Over 31% of the organizations employed 99 or less workers, 13.2% of them employed 499 or less; 10.3% employed 1499 or less while 34.5 % employed 1500 or more employees. The largest industry section was consulting (21.5%), followed by financial services (10.6%), information technology (10.9%), and education (8.9%). Other sectors included federal government (7.4%), health services (6.6%), manufacturing (6.0%), retail (3.2%), and others (25.0%).

Table 2. About the Respondents

Job Tiles of Respondents		Annual Revenue (Dollars)	
Security Officer	20%	Over 1 billion	28.1%
CEO	12.6%	100 million – 1 billion	13.3%
Systems Administrator	10.9%	10 million – 99 million	20.4%
CISO	10.6%	Under 10 million	38.2%
CIO	4.9%		
CSO	2.9%		
Others	38.3%		

Number of Employees		Industry Sectors	
1 – 99	31.3%	Consulting	21.5%
100 – 499	13.2%	Financial Services	10.6%
500 – 1,499	10.3%	Education	8.9%
1,500 – 9,999	22.4%	Federal Government	7.4%
10,000 – 49,999	12.1%	Health Services	6.6%
50,000 or more	10.6%	Information Tech	10.9%
		Manufacturing	6.0%
		Retail	3.2%
		Others	25.0%

The performance indicator for the growth models is R-Square. The R-Square indicates the explanatory power of the model. As shown in Table 3, Gompertz models yields R-Square of .998 in the case of frequency of attacks and R-Sq of .983 in the case dollar loss value. These result means that Gompertz model performs well in both the frequency of attacks and the dollar loss value as indicated by the R-Square.

Table 3. Gompertz Model Performance

Component		**Gompertz Model**	
Frequency of Attacks	Parameter	Estimate	t-Value
	Log K	8.537	316.18
	Log A	-2.968	-43.65
	B	.681	56.75
	R-Sq.	.998	
Dollars Lost	Log K	9.155	132.68
	Log A	-4.718	-11.10
	B	.551	13.78
	R-Sq.	.983	

Table 4 displays the results from logistic model which yields R-Sq of .997 in the case of frequency of attacks and R-Sq of .996 in the case dollar loss value. Logistic model also seems to perform well in predicting both the frequency of attack and the dollar loss value.

As shown in Table 5, exponential model yields R-Sq of .952 in the case of frequency of attacks; and R-Sq of .943 in the case dollar loss value. Compared with Gompertz and logistic models, exponential model registers the lowest performance in both components (frequency of attacks and dollars loss value). It is worth noting that all three growth models perform acceptably well in both components of security breach. Based on the R-Squares generated by the three models on the two breach components, we cannot safely state that the two components are different. If anything, the results of the present study call for further studies.

Table 4. Logistic Model Performance

Component		**Logistic Model**	
Frequency of Attacks	Parameter	Estimate	t-Value
	Log K	.000	
	Log A	.003	
	B	.447	23.53
	R-Sq.	.997	
Dollars Lost	Log K	.000	
	Log A	.003	
	B	.352	16.78
	R-Sq.	.996	

Table 5. Exponential Model Performance

Component		**Exponential Model**	
	Parameter	Estimate	t-Value
Frequency of Attacks	A	8.582	110.03
	B	2.268	11.45
	R-Sq.	.952	
Dollars Lost	A	9.452	101.63
	B	2.983	12.59
	R-Sq.	.943	

Figures 1 and 2 are the graphical display of the three growth models on the two components of security breaches. The Gompertz model slightly outperforms the other models in terms of frequency of attacks while logistics model records the best performance in terms of dollars loss value. The graphs also reveal the fact that security breach growth is not uniform over the years and that no single growth model is superior over the years. The implication here is that all three models (and even more) should be used to study the growth rate of security breaches for the period of interest before managers decide which results to act upon.

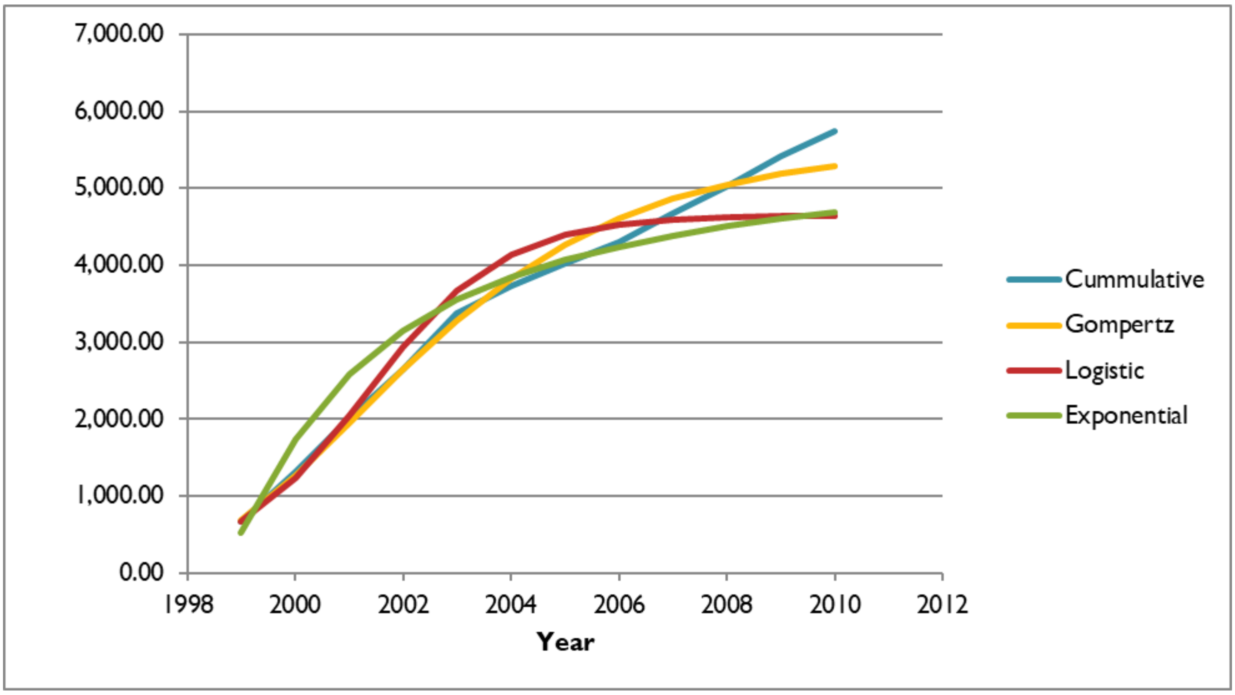

Figure1. Models Performance – Frequency of Attacks

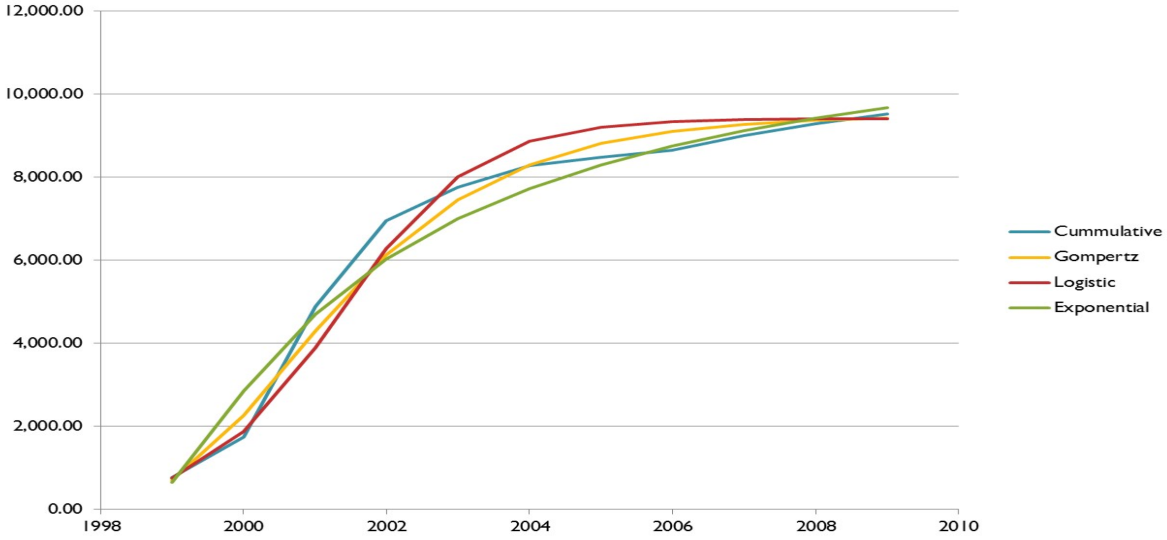

Figure 2. Model Performance – Dollar Loss Value

DISCUSSION AND CONCLUSION

In this study we propose that to fully understand the growth rate of security breaches over time, it is more appropriate to consider several elements or components of security breaches instead of depending on a single component as is the case in some previous studies. To that effect, we have used frequency of attacks and dollar loss values to investigate the growth rate of security breaches for a period ranging from 1998 to 2009. We also use three well-known growth models in modeling the phenomenon. The results provide the answers to the research questions and hence understanding in this critical area.

Our initial conclusions are as follows:

- Multiple-dimension approach to modeling breach approach seems more rigorous than single-dimension found in the literature.
- The two components considered (number of attacks, amount of dollars lost) are different and so each explains an aspect of breach growth rate.
- Number of Attacks seems to be a more effective component than dollars loss value.
- It is a more complete approach to compare a number of growth models.
- Gompertz model seems to produce the best result in the case of frequency of attacks while Logistics model performs the best in the case of dollar loss value. Exponential model performs relatively poorer in both cases.
- Frequency of attacks provides a slightly better fit than dollar loss value in all three models.

Caution should be used when applying these findings given the fact that this is an initial study which of course has some limitations. One of such limitations is the absence of the impact of price. Price adjustment should be considered in order to properly account for present value of dollar and the dropping cost of the countermeasure technologies.

REFERENCES

Bagchi, K. and Udo, G. (2003). An analysis of the growth of computer and internet security breaches. *Communications of the Association for Information Systems*, *12*, 684-700.

Bandura, A. (1986). *Social Foundations of Thought and Action*, Prentice-Hall, Engelwood Cliffs, NJ: Prentice-Hall.

D'Arcy, J., Hovav, A., and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20(1)*, 79 – 98.

Garg, A., Curtis, J. and Halper, H. (2003). Quantifying the financial impact of IT security breaches" *Information Management & Security, (11)2*, 74-83.

Harrington, S.J. (1996), The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*, *20(3)*, 257–268.

Higgins, G.E., Wilson, A.L., and Fell, B.D. (2005). An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture*, *12(3)*, 166 – 184.

Hyman, P. (2013). Cybercrime: It's serious, but exactly how serious? *Communications of the ACM*, *56(3)*, 18-20.

Kankanhalli, A., H.-H. Teo, B. C. Y. Tan, K.-K.Wei (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23(2)* 139–154.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. International Journal of Electronic Commerce, 12(1), 69-91. doi:10.2753/JEC1086-4415120103.

Karine, E., Frank, L., & Laine, K. (2004). Effect of price on the diffusion of cellular subscriptions in Finland. *Journal of Product& Brand Management, 13*(3), 192–199.

Lee, S. M., Lee, S.-G. & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information Management, 41*(6), 707-718.

Lever, R. (2018). Global cybercrime costs $600 bn annually, Retrieved from: https://phys.org/news/2018-02-global-cybercrime-bn-annually.html

Liang, H. G., & Xue, Y. J. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly,* 33(1), 71-90.

Loh, L. & Venkatraman, N. (1992). Diffusion of IT Outsourcing: Influence Sources and Kodak Effect. *Information Systems Research*, 3, 334-358.

Lukasik, S. J. (2000). Protecting the Global Information Commons. Telecommunication Policy, (24)6-7, 519-531.

Mahajan, V. & Peterson, R. (1987). *Models for Innovation Diffusion, Sage University Paper series on Quantitative Applications in the Social Science.,* (2nd Ed.), Beverly Hills and London: SAGE Publications.

Martino, J. P. (1972). The Effect of Errors in Estimating the Upper Limit of a Growth Curve. *Technological Forecasting and Social Change,* (4), 77-84.

Markets and Markets Cyber Security - Global Market Outlook (2016-2022) https://www.researchandmarkets.com/reports/4335716/cyber-security-global-market-outlook-2016-2022#pos-2

Niculescu, M. F. & Whang, S. (2012). Codiffusion of wireless voice and data services: An empirical analysis of the Japanese mobile telecommunications market. *Information Systems Research, 23*(1), 260-279.

Norton, J. A. & Bass, F. M. (1987). A diffusion theory model of adoption and substitution for successive generations of high-technology products. *Management Science, 33(*9), 1069-1086.

Panko, R. (2002). *Business Data Networks and Telecommunications*, 4th edition, Prentice-Hall, New Jersey.

Peterson, R. A. & Mahajan, V. (1978). Multi-product growth models. In J. Sheth (ed.) *Research in Marketing* Greenwich, CT: JAI Press, pp. 201-231.

Pitcher, B., Hamblin, R. & Miller, J. (1978). The Diffusion of Collective Violence. *American Sociological Review*, 43, 23-35.

Ponemon Institute (2014). Cost of Cyber Crime Study: United States, Ponemon Institute, October 2014. Based on internal analysis of the results from the 2010-2014. Cost of Cyber Crime Study: United States reports from Ponemon Institute.

Ponemon, L. (2016). *A Report on Cybercrime and Healthcar.,* Ponemon Institute, March.

Rai, A., Ravichandran, T., & Samaddar, S. (1998). How to Anticipate the Internet's Global Diffusion, *Communications of the ACM, 41,* 97-106.

Rawlison, K. (2014) Annual Study Reveals Average Cost of Cyber Crime Escalates 96 Percent to $12.7 Million per Organization. Retrieved from: http://www8.hp.com/us/en/hp-news/press-release.html?id=1815969#.VHN70tLOOSo

Richardson, R. (2003) *The 2003 CSI/FBI Computer Crime and Security Survey*. San Francisco**:** Computer Security Institute Inc., 1-20.

Roberds, W., & Schreft, S. L. (2009). Data Breaches and Identity Theft. *Journal of Monetary Economics, 56*(7), 918-929.

Rogers, E. M. (2003) *The Diffusion of Innovation*. New York: Free Press.

Rogers, E. M. (1962). *The Diffusion of Innovation*. New York: Free Press.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do Data Breach Disclosure Laws Reduce Identity Theft? *Journal of Policy Analysis and Management, 30*(2), 256-286.

Siponen, M. & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violation. *MIS Quarterly, 34*(3), 487 – 502.

SPSS 11 Syntax Reference Guide, 2003. SPSS Publication Sales, 233 South Wacker Drive, Chicago IL, 6060-6307.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research, 1*(3), 255-276.

Straub, D. & Welke, R. (1998). Coping with Systems Risk: Security Planning Models for Management Decision-Making. *MIS Quarterly*, 22(4), 441-469.

Shankar, V. & Bayus, B. L. (2003). Network Effects and Competition: An Empirical Analysis of the Home Video Game Industry. *Strategic Management Journal, 24*(4), 375-384.

Theoharidou, M, Kokolakis, S. Karyda, M. & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computer Security, 24*(6), 472-484.

Ullman, R. & Ferrera, D. (1998). Crime on the Internet. *Boston Bar Journal, 6,* Nov./Dec.