Journal of Business and Economics, ISSN 2155-7950, USA
July 2016, Volume 7, No. 7, pp. 1118-1124
DOI: 10.15341/jbe(2155-7950)/07.07.2016/007

http://www.academicstar.us

Modeling Cybercrime Revenue Losses*

Thomas Fink, David A. Walker
(Georgetown University, USA)

Abstract: A dynamic model is developed to represent revenue losses where a firm is a cybercrime victim after a period of strong revenue growth. The firm's goal is assumed to be revenue maximization. An application illustrates that it will require a long time before the firm reestablishes strong revenue growth after cybercrime. The continuing costs Target and Home Depot incur are examples. The model portrays dynamic stages of revenue growth for a victimized firm. The model can be extended to a wide range of other business and economic losses for public institutions, assuming a different utility function.

Key words: dynamic economic loss; cybercrime
JEL code: D21

1. Background

Models to portray economic losses often imply a philosophical approach. Some models are based on *pro forma* assumptions that mostly depend on dynamic projections. Other approaches depend on sophisticated mathematical theories or treatments that often originate with the physical sciences and chaos theory.

This paper provides a dynamic model for the revenue maximizing firm to portray revenue losses for a catastrophic event such as having credit files hacked. The event is not expected to reoccur but causes continuing revenue losses that can only be recouped over many future periods, if ever. Firms whose credit files have been hacked invest considerable resources to insure that files are protected in the future and to assure customers they will be protected. This is above and beyond legal settlements that may be necessary to satisfy customers or clients.

Section II provides a brief literature review from which a dynamic revenue growth model is developed for a victimized firm in Section III. In Section IV, the model is applied to a cybercrime case, like the one that faced two large US retailers — Home Depot and Target. The Conclusions follow.

2. Literature

2.1 Framework

Forensic business loss models and applications have often been projections of *pro forma* cases. The cases

* An earlier version of this paper was presented to the 22nd Annual Conference of the American Society of Business and Behavior Sciences, Las Vegas, Nevada where it received a Best Paper Award.

The views in this paper are the authors' and do not represent opinions or views of TREPP, LLC.

Thomas Fink, BA degree, Georgetown University; research areas/interests: securitized assets and CMOs. E-mail: tom_fink@trepp.com.

David A. Walker, Ph.D., Iowa State University, Professor, School of Business, Georgetown University; research areas/interests: financial services and entrepreneurship. E-mail: walkerd@georgetown.edu.

presented by Pratt and Niculita (2008) are classic examples.

An alternative is to develop dynamic conditions from chaos theory and differential equations (Murphy, 1996; Hirsch et al., 2013). Werndl (2009) discusses the unpredictability and uncertainty of chaos losses. Alligood and Yorke (2008, p. 41) discuss stability conditions related to the model in this paper. They define a "chaotic trajectory" to be an unstable, oscillating time path.

Beinhocker (2006) and Meyer et al. (2002) have applied chaos theory to corporate cases. Beinhocker draws upon the network phenomenon of *complexity catastroph*e to explain corporations' inability to adapt to change. Meyer and his co-authors analyze project areas where project managers did not distinguish between project risk and uncertainty. They discuss predictable plan variations to unforeseeable effects that might include earthquakes, hurricanes, external forces and terrorist attacks.

The impacts of cybercrime extend across every industry and the public sector. The IRS and US Office of Personnel Management have experienced recent major invasions. Benardo and Weatherby (2015) offer "A Framework of Cyber Security" from a public sector perspective.

2.2 Recent Experience

Recent incidences and surveys demonstrate the need for a theoretical framework to analyze short-term and to project long-term revenue losses for a corporate cybercrime victim. A Net Diligence Cyber Claims Study (2014) analyzes a sample of 117 insurance claims from 2013 and estimates the average payout for a large, hacked company to be almost $3 million, plus an average legal defense cost of almost $700,000. These claims represent only 5-10 percent of 2013 cyber claims, since the sample includes only insurance claims.

A McAfee Intel Security study (2014) for the Center for Strategic and International Studies estimates that annual global cybercrime direct plus indirect costs may reach $575 billion. They indicate US cybercrime costs could be $115 billion, 0.64 percent of US GDP, and more than twice the percentage for Germany. "Cybercrime damages trade, competitiveness, innovation, and global economic growth" (McAfee, p. 3), which is the basis for revenue deterioration that is assumed in this study. Krebs on Security (2014) claims Target's loss for their December 2013 hacking is $420 million, almost 0.60 percent of the firm's annual 2014 sales ($72.3 billion).

2.3 Foundations

The foundations for the model are the classic Friedman and Savage (1948) utility perspective under uncertainty and Baumol's (1967) revenue maximization hypothesis. The firm maximizes its utility as a function of revenue, $U = U(R)$, under uncertainty, as Friedman and Savage represented for consumers. The firm takes precautions against cybercrime, CC, but cannot predict how, when (t), or to what extent crime may occur. An extension would be to introduce a cost and/or profit constraint to include cybercrime and operations' costs.

Let r represent the firm's normal revenue growth rate, t is the time period, and CC represents the potential but uncertain cybercrime. $U = U(R)$ and $R = R(r, t, CC)$ and, $dr/dt > 0$ when $CC = 0$. When a crime occurs, $CC \neq 0$ and $dr/dt < 0$ or at least the growth rate is smaller than when there is no crime.

3. Revenue Loss Model

Revenue losses from cybercrime can be analyzed within the framework of a dynamic loss model. The model represents the victimized firm's income. The firm is assumed to be sufficiently large and geographically diverse that it operates in continuous time in a multitude of markets. The cyber catastrophe is assumed to disrupt the firm's revenue stream and cause dramatic revenue deterioration, with declining sales as a result of the cybercrime.

Restoring public confidence and reestablishing normal revenue growth will require significant company resources and the passage of time.

3.1 Four Periods

Consider four distinct time periods: (1) a normal business period before the cybercrime; (2) the time, t = t1, when the catastrophic crime occurs; (3) the period beginning with t1 + Δt when revenue impacts are recognized through the end of the period when the negative economic impacts have dissipated and most revenue deterioration ends; and (4) the time when the hacked firm begins rebuilding its revenue growth. (The notation {t = a:b} defines continuous time t such that $a \leq t \leq b$.)

After a normal period of revenue growth {t = 0:t1} at a rate r_1, the firm encounters the catastrophe at t = t1. Significant revenue losses and revenue deterioration at a rate of r_2 continue until t = t2 {t = t1:t2}, the end of period 3. In period 3, revenues are assumed to deteriorate, or to grow at a much slower rate than in period 1; $r_2 < r_1$ is a sufficient condition. It is assumed, however, that revenues decline throughout period 2, in which case $r_2 < 0$.

Beginning in the third period (at t = t2) for an unspecified time {t = t2:t3}, the firm is assumed to begin recapturing its revenue growth at a rate of r_3. This growth rate is likely to be smaller than it had been in the normal growth period before credit files were hacked at t1. Therefore, $0 < r_3 < r_1$ is expected.

3.2 Models for Three Intervals

Revenues for the distinct periods with the time intervals {0:t1}; {t1:t2}; and {t2:t3} are represented by simple growth models. The catastrophe occurs at the end of period 1 at t = t1, the boundary between the first and second periods.

Let the firm's credit sales at time t be represented by R(t). Let Rt represent credit sales across the range of time t, and assume that all sales are credit sales.

Period 1 {0:t1}: At time, t, within {0:t1}, revenues R(1) are represented by $f_1(t)$ and approximated by $f_1(t) = A_1\exp(r_1 t)$ with a sales growth rate of r_1. Aggregate credit sales for period 1 are.

$$R1 = \int_0^{t1} f_1(t)dt = \int_0^{t1} [A_1 \exp(r_1 t)dt = [A_1/r_1][\exp(r_1 t1) - 1] \quad (1)$$

r_1 is assumed to be a constant, but it could be a function of exogenous factors, such as the competitive industry environment or economic policy changes, depending on the firm's market and the magnitude of the cybercrime.

For this or any period, the simple model might include cyclical revenues assuming $f_1(t) = A_{11}\exp(r_{11}t) + A_{12}\exp(r_{12}t)$ with some restrictions on r_{11} and r_{12}.

$f_1(t)$ could be a much more complex, continuous function.

Period 1 – Period 2 Border: The crime is assumed to occur at the border between periods 1 and 2, at t = t1. Credit revenues are assumed to decline immediately at t1+ Δt to only a percentage of credit sales at t = t1 - Δt. Let k_1 be the percentage of credit sales that continue into period 2 at t1+Δt in contrast to the credit sales at t = t1 - Δt. (If, for example, 30 percent of sales were lost immediately at t1, $k_1 = 0.70$ and $(1 - k_1) = 0.30$ represents the immediate hacking revenue loss.)

Period 2 {t1:t2}: The revenue in period 2 is represented by

$$R(2) = f_2(t) = A_2\exp(r_2 t) \quad \text{and} \quad R2 = \int_{t1}^{t2} A_2\exp(r_2 t)dt \quad (2)$$

At the beginning of period 2, initial revenues are

$$A_2\exp(r_2 t1)=k_1 A_1\exp(r_1 t1) \text{ and } k_1 = [A_2/A_1]\exp((r_2-r_1)t1)$$

The initial decline of credit sales in period 2 is represented by $k_1 < 1.0$ and $r_2 < 0$, the deterioration of credit sales throughout {t1:t2}. Credit sales deteriorate throughout the second period {t1:t2}, while the short-term cyber losses continue. Some consumers may substitute cash for credit sales from the "hacked" firm and others switch to competitor firms.

To link periods 1 and 2, let $k_2 = r_2/r_1$ ($r_1 > 0$ and $r_2 < 0$). $k_2 < 0$ represents the relative magnitude of the revenue deterioration rate within period 2 compared to revenue growth rate in period 1.

Substituting for A_2 and r_2, the revenue path in period 2 can be represented by

$$R2 = \int_{t1}^{t2} f_2(t)dt = \int_{t1}^{t2} A_2\exp(r_2 t) = \int_{t1}^{t2} k_1 A_1\exp(k_2 r_1 t),\ 0<k_1<1,\ k_2<0,\ r_1>0,\ r_2<0 \quad (3)$$

Integrating (3) and then substituting $k_1 = [A_2 / A_1]\exp((r_2 - r_1)t1)$ for k_1 provides

$$R2=[A_2/(k_2 r_1)]\exp((r_2-r_1)t1)[\exp(k_2 r_1 t2)-\exp(k_2 r_1 t1)] \quad (4)$$

where $[A_2/(k_2 r_1)] < 0$ and k_1, k_2, r_1 and r_2 reflect the possibilities between $A_2\exp(r_2 t)$ and $A_1\exp(r_1 t)$; $r_1 > 0$, $r_2 < 0$, $0 < k_1 < 1$, $k_2 < 0$, and $r_2 = k_2$, $r_1 < 0$ delineate the deteriorating revenues throughout period 2.

3.3 Measuring Catastrophe

If no cybercrime or catastrophe had occurred at t1 and the firm's revenues continued to grow in period 2 as they had in period 1, r_1, the revenue in period 2 would be

$$R2a=\int_{t1}^{t2} A_1\exp(r_1 t)dt=[A_1/r_1][\exp(r_1 t2)-\exp(r_1 t1)] \quad (5)$$

As a result of the crime, the firm's revenue in period 2 is represented by (4).

3.4 Period 2 Loss

The revenue loss in period 2 is the revenue that would have been earned "but for" the hacking — equation (5), minus the revenue earned in period 2, equation (4).

$$R2LOSS=[A_1/r_1][\exp(r_1 t2)-\exp(r_1 t1)]-[A_2/k_2 r_1][\exp(r_2-r_1)t1][\exp(k_2 r_1 t2)-\exp(k_2 r_1 t1)] \quad (6)$$

Since $k_2 r_1$ is negative and $t2 > t1$, each term in brackets in equation (6) is positive.

Period 3 {t2:t3}: Beginning at t2, the initial hacking effect is assumed to have passed and the firm enters a positive revenue growth stream. Within period 3, {t2:t3} $R3 = f_3(t)$ is represented by $A_3\exp(r_3 t)$. Across period 3, credit sales are

$$R3=\int_{t2}^{t3} f_3(t)dt=\int_{t2}^{t3}[A_3\exp(r_3 t)]dt=[A_3/r_3][\exp(r_3 t3)-\exp(r_3 t2)] \quad (7)$$

Revenues in period 3 are assumed to grow, but the growth rate, r_3, is likely to be smaller than r_1, as residual damage from the cybercrime continues. Moreover, it may be a long time into the future before r_3 becomes as large as r_1. R3 will be less than R1, unless the period {t2:t3} is considerable longer than {0:t1}. It may take a long time for many credit customers to have confidence that their data are protected.

3.5 Aggregate Revenues across Three Periods: {0:t3}

The expected conditions across the three periods are:

$$r_1 > 0;\ r_3 > 0;\ r_1 > r_3;\ r_2 < 0,\ r_2 = k_2 r_1 < 0;\ |r_1| > |r_2| \text{ and } -1 < k_2 < 0,\ 0 < k_1 < 1.$$

The expected permanent damage to the revenue stream as a result of the catastrophe is reflected by these characteristics and assumptions about r_1, r_2, r_3, k_1 and k_2.

Total revenue (TR) over the whole period 0 to t3 is represented by R1 + R2 + R3, the sum of equations (1), (4), and (7):

$$TR = \int_0^{t1} A_1 \exp(r_1 t)dt + \int_{t1}^{t2} A_2 \exp(r_2 t)dt + \int_{t2}^{t3} A_3 \exp(r_3 t)dt$$

$$=[A_1/r_1][\exp(r_1 t1)-1]+[A_2/(k_2 r_1)][\exp((r_2-r_1)t1][\exp(k_2 r_1 t2)-\exp(k_2 r_1 t1)]+[A_3/r_3][\exp(r_3 t3)-\exp(r_3 t2)] \quad (8)$$

The loss from the crime is given by equation (6) plus the slower revenue growth in period 3. The various coefficients also reflect the hacking losses to the firm's revenue stream through $t1 \leq t \leq t3$. The relative sizes of the coefficients determine the loss and recovery from the crime.

Figure 1 portrays the revenue growth in the first period; deteriorating revenue in period 2 beginning at t1 and continuing through t2 ($r_2 < 0$); and the expected recovery through period 3 ($0 < r_3 < r_1$).

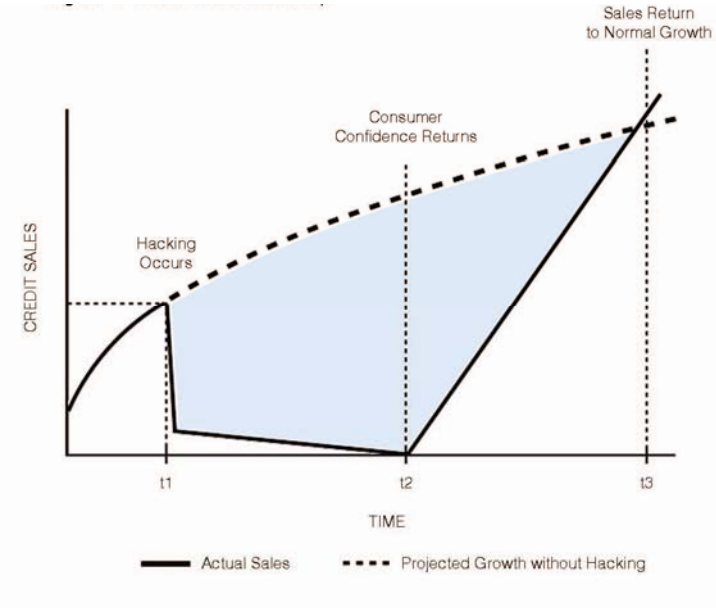

Figure 1 Credit Sales Catch Up

The revenue losses are the difference between the dotted and solid lines beginning at t1. To overcome the cybercrime losses in period 3, the revenue growth rate beginning at t2 (r_3) would need to be considerable larger than the growth rate in period 1 (r_1), unless the period t2 to t3 were considerably longer than the period 0 to t1. The revenue growth rate would have to be greater in period 3 ([t2:t3]) than period 1 to reach the level that the firm would have been expected by t3 if hacking had not occurred.

4. Losses for the Bullet Company: A Cybercrime Victim

Suppose the Bullet Company experienced the credit sales portrayed in Table 1 and hacking occurred at the end of its 14th month (the end of period 1).

Table 1 Bullet Company Monthly Revenues

	Period 1		Period 2			Period 3
months	[0:t1]	months	[t1:t2]	no hacking	months	[t2:t3]
1	5000000	15	3592276	5388414	27	3055390
2	5050125	16	3583295	5415356	28	3065574
3	5075376	17	3565401	5442433	29	3086045
4	5100753	18	3538727	5469645	30	3117009
5	5126256	19	3503473	5496993	31	3158777
6	5151888	20	3459898	5524478	32	3211776
7	5177647	21	3408322	5552100	33	3276549
8	5203535	22	3349122	5579861	34	3353771
9	5229553	23	3282723	5607760	35	3444255
10	5255701	24	3209596	5635799	36	3548971
11	5281979	25	3130253	5663978	37	3669060
12	5308389	26	3045239	5692298	38	3805857
13	5334931				39	3960914
14	5361606				40	4136028
15					41	4333281
16					42	4555075
18					43	4804181
19					44	5100746
20					45	5433670
21					46	5807619
22					47	6227993
23					48	6701059
24					49	7234091
Rate	r1 = 0.5%	Rate	r2 = -0.25%		Rate	r3 = 0.33%
Loss = 25,800,789.00						

If revenues for the first month were $5 million (month 1 of period [0:t1]) and monthly revenues increased by 0.50 (r_1) percent (6 percent per annum) for the next 13 months (months 2-14), monthly revenues would have reached $5,361,606. Hacking occurs at t = t1 = 14 and the immediate revenue loss for the first month of the hacking is assumed to be 33 percent (k_1). For the first month of period 2, revenue declines to $3,592,276.

Revenues continue to decline each month in period 2 by 0.25 (r_2) percent per month (-3.0 percent per annum). Period 2 is assumed to last 12 months (months 15-26). The monthly revenues would decline to $3,045,239 for the final month of period 2. For period 2, the losses are the revenues that would have been earned for the months in period 2, if revenues had continued to grow at 0.50 percent per month, **minus** the assumed revenues for period 2. The total loss for period 2 is $25,800,789.

The column for period 3 shows monthly revenue assuming growth at a rate of 0.33 (r_3) percent per month (4.0 percent per annum) from the beginning of period 3 (month 27), having declined to $3,045,239 for month 26. It requires 20 months (months 27-46) in period 3 until the revenues exceed the revenues the last month of period 1

(month 14). The lost credit sales from the hacking may never be fully recaptured. That would require the revenue growth rate in period 3 (r_3) to exceed the revenue growth rate in period 1 (r_1).

5. Conclusion

Numerous firms have incurred significant revenue losses from cybercrime. This paper provides a dynamic model to portray catastrophic revenue loss for the victimized firm after a successful revenue growth period. The application illustrates the potential losses and lengthy period before the firm is likely to reestablish revenue growth. The firm is unlikely to regain all of the lost revenue and it is likely to be a long-time, and maybe forever, before the firm's revenue growth rate returns to the growth rate before the crime occurred.

References

Alligood Kathleen T. and James A. Yorke (1989). "Fractal basin boundaries and chaotic attractors", in: *Chaos and Fractals: The Mathematics Behind the Computer Graphics.*

Bank Info Security (2015). "Banks suing target make new demands", July 29, available online at: http://www.bankifosecurity.com/banks-suing-target-make-new-demands-a-8438.

Baumol William J. (1967). *Business Behavior, Value and Growth* (rev. ed.), Harcourt, Brace & World Inc. New York, NY.

Beinhocker Eric D. (2006). "The adaptable corporation", *McKinsey Quarterly*, No. 2, pp. 50-67.

Benardo Michael B. and Kathryn M. Weatherby (2015). "A framework for cyber security", *Supervisory Insights Federal Deposit Insurance Corporation*, Washington, DC, winter.

Brock W. A., Hsieh D. and Le Baron B. (1991). *Nonlinear Dynamics, Chaos, and Instability*, MIT Press, Cambridge, MA.

Friedman Milton and Leonard Savage (1948). "The utility analysis of choices involving risks", *The Journal of Political Economy*, August, pp. 279-304.

Hirsch Morris W., Stephen Smale and Robert L. Devaney (2013). *Differential Equations, Dynamic Systems and an Introduction to Chaos* (3rd ed.), Academic Press, Waltham, MA.

Krebs on Security (2014). "Inside target corp., days after 2013 breach", September 15, available online at: http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach.

Meyer Aroud De, Christoph H. Loch and Michael T. Pich (2002). "Managing project uncertainty: From variation to chaos," *MIT Sloan Management Review*, Winter.

McAfee Intel Security (2014). "Net losses estimating the global cost of cybercrime", contracted by the Center for Strategic and International Studies, Washington, DC, June.

Murphy Priscila (1996). "Chaos theory as a model for managing issues and crises", *Public Relations Review*, Vol. 22, No. 2, pp. 95-113.

Netdiligence (2014). "Cyber claims study", Net Dilengenc, available online at: http://www.netdiligence.com.

Page Alfred N. (1968). *Utility theory: A Book of Readings*, John Wiley & Sons, Inc. New York, NY.

Penrose Edith (1995). *The Theory of the Growth of the Firm*, Oxford University Press, Oxford, England.

Pratt Shannon P. and Alina V. Niculita (2008). *Valuing A Business* (5th ed.), McGraw Hill. New York, NY.

"Target announces settlement agreement with MasterCard: Estimated costs already reflected in previously reported results", April 15, 2015, available online at: http://www.pressroom.target.com.

SmartBrief (2015). "Ace to underwrite cyberinsurance policies with coverage up to $100M", September 25.

Werndl Charlotte (2009). "What are the new implications of chaos for unpredictability?", *The British Journal for the Philosophy of Science*, Vol. 60, No. 1, pp. 195-220.