Global Cybercrime Risk Rankings

Paper 7

By Alan Buttars

Global Cybercrime Risk Rankings

During the past two decades, the use of computers and the World Wide Web has risen from obscurity to a vital and integral part of everyday life. But although the web revolutionized global communication, the stock market, and the economy, it brought with it the potential for a new, unprecedented brand of crime. This unforeseen advent, labeled "cybercrime," was to be defined as any criminal act involving the use of a computer or a network[3].

With the threat acknowledged, the government of the United States moved to protect its own critical information in the Comprehensive National Cybersecurity Initiative of 2008[1]. With such a massive and growing financial burden placed on private and public corporations across the world, the U.S. was joined by numerous nations in creating cybercrime investigation organizations. Digital attack had clearly become a serious concern to 21st century government. South Korea established the Cyber Terror Response Center[5], Germany the National Cyberdefence Centre[4], and Estonia the *Küberkaitse Kompetentsikeskus*[4 5 11]. In 2004, one of the first transnational cybersecurity organizations was created in the European Network and Information Security Agency[6].

Unfortunately, these institutions have failed to match the efforts of an exponentially growing field of cybercriminals. According to the Office of Management and Budget in its release of the United States' 2011 budget plan, the National Cyber Security Division[10] was allocated $364 million during the last calendar year[14]. This pales in comparison, however, to the actual financial cost of cybercrime. According to a study conducted during 2011, computer crimes cost the United States nearly $140 billion last year, and almost $400 billion globally[2].

Given these unfortunate indications, it might be useful to develop a solid framework for understanding the global characteristics of cybercrime. The mathematical model we examine will attempt to complete just such a task.

1. The Model

For the purposes of this model, we will examine ten countries historically rated as those most prevalent in cybercrime by the Symantec Corporation, as determined by annual Internet Security Threat Reports from 2006 to 2011[8].

Nations (Set *S*)

c_1: Brazil
c_2: Canada
c_3: China
c_4: France
c_5: Germany
c_6: India
c_7: Italy
c_8: Russia
c_9: United Kingdom
c_{10}: United States

With our nations identified, it would now be appropriate to determine the precise model we will use. For this purpose we will use three major factors:

*F*1: **Damage**
Identified as any monetary loss incurred either by the use of stolen information or the costs associated with correcting such effects. All figures will be in United States dollars.

*F*2: **Prevalence**
We will represent prevalence in two ways. The first, by the relative global frequency of certain computer attacks, and second, by the frequency of online adults who suffer negative effects from a cybercrime attack.

*F*3: **Growth Potential**
As determined by the global growth characteristics of certain types of cyber attacks from 2006 to 2011.

Further, we identify several other sub-factors that will be used in both $F2$ and $F3$. Here, our sub-factors will be the five major types of computer attacks, described below:

f_1: **Bot-infected computer attacks**
Bots are programs installed on a compromised machine to allow an attacker to remotely control it via a communication channel and orchestrate other attacks.

f_2: **Hacking**
Hacking is any attack aimed at gaining access to computer systems or networks for the purpose of data mining and system manipulation. Those who use this method are greatly aided by currently-available "hacker software" such as L0phtCrack, which is used for password cracking.

f_3: **Malicious code**
Malicious code samples, or vandals, are auto-executable applications that are used to attack network drives. Their behavior is dependent on the code itself, but common methods are the lifting of data and passwords or gaining access to email for the use of spamming.

f_4: **Phishing website hosting**
Phishing attacks occur when an attacker attempts to gain confidential information (credit card numbers, banking information, etc.) from victims by mimicking a specific company or brand.

f_5: **Spam zombies**
Spamming is the delivering of unsolicited email, which may contain Trojans, viruses, and phishing attempts. Spam zombies, similar to bot-infected computers, are machines remotely controlled by an attacker, who uses it to distribute spam without the victim's knowledge.

$F3$ adds another factor, to be used as a multiplicand:

f_6: **Adult victims**
The prevalence of adult victims is identified as the percentage of online adults in each country who have suffered some detrimental effect at the result of a cybercrime in 2011.

Therefore, Figure 1 below shows a visual representation of the model we will use:

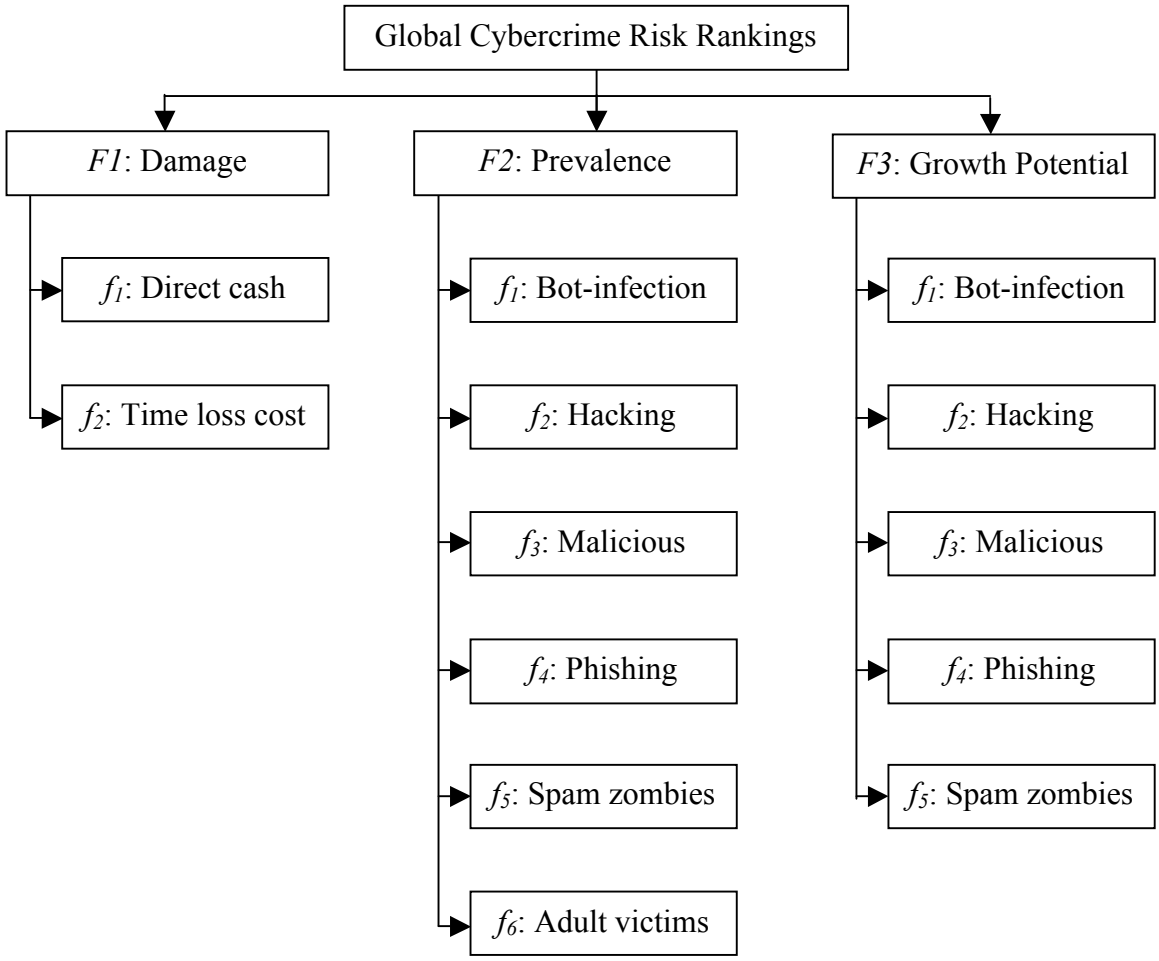

Figure 1. Mathematical model to be used in describing the rankings of global cybercrime risk

2. Expert Opinion

The ratings of the above factors were determined via ratings made by Creighton University faculty and staff with expertise in security technology. Their responses indicated the relative importance of the above factors and sub-factors in comprising the overall goal *G,* the relative risk of cybercrime for each country in set *S*.

A. Importance of Three Major Factors

We will use three different methods to achieve our goal. These methods are the Analytical Hierarchy Process (AHP)[12 13], Guiasu[7], and Yen[15]. Using our expert opinions, we find

the equations for each method below in matrix *W*, which depicts expert ratings of major factors *F*i, where i = 1, 2, 3:

$$W = \begin{array}{c} \\ F1 \\ F2 \\ F3 \end{array} \begin{array}{c} \begin{array}{cccc} E1 & E2 & E3 & E4 \end{array} \\ \begin{bmatrix} .3 & .9 & .5 & .3 \\ .5 & .7 & .8 & .6 \\ .5 & .8 & .7 & .8 \end{bmatrix} \end{array} \begin{array}{c} \text{Row Average} \\ \begin{bmatrix} 0.5 \\ 0.65 \\ 0.7 \end{bmatrix} \end{array}$$

AHP: $G = .2703F1 + .3514F2 + .3784F3$

Guiasu: $G = .2581F1 + .3573F2 + .3846F3$

Yen: $G = .2628F1 + .3566F2 + .3805F3$

B. Importance of Sub-factors on Damage

The data from each sub-factor of *F*2 is in terms of monetary U.S. dollars. As dollars are inherently equal to each other, we will not assign differing weight values to f_1 and f_2. Therefore:

AHP: $F1 = 12f1 + 12f2$
Guiasu: $F1 = 12f1 + 12f2$
Yen: $F1 = 12f1 + 12f2$

We will also examine *F*1 as an ordinal factor among countries, so that the country which suffered the highest monetary damage in 2011 will be given a rank of 1 and the country with the lowest monetary damage will receive a rank of 10.

C. Importance of Five Sub-factors on Prevalence

Our equation for *F*2 will include both a weighted and constant component. In this case, the weighted component is determined by expert opinion. This will be multiplied directly by f_6, which is a constant, non-arbitrary factor which describes the prevalence of online adult victims in each country.

$$\begin{array}{c} \\ f1 \\ f2 \\ f3 \\ f4 \\ f5 \end{array} \begin{array}{c} \begin{array}{cccc} E1 & E2 & E3 & E4 \end{array} \\ \begin{bmatrix} .3 & .8 & .7 & .3 \\ .5 & .5 & .7 & .4 \\ .4 & .6 & .6 & .2 \\ .2 & .8 & .4 & .6 \\ .1 & .3 & .4 & .7 \end{bmatrix} \end{array} \begin{array}{c} \text{Row Average} \\ \begin{bmatrix} .525 \\ .525 \\ .45 \\ .5 \\ .375 \end{bmatrix} \end{array}$$

AHP: $F2 = .2211f1 + .2211f2 + .1895f3 + .2105f4 + .1579f5 \times f6$

Guiasu: $F2=.2133f1+.2329f2+.1930f3+.2039f4+.1569f5\times f6$
Yen: $F2=.2180f1+.2301f2+.1938f3+.2036f4+.1545f5\times f6$

D. Importance of Five Sub-factors on Growth Potential

*F*3 will again be calculated by using expert opinion, but without the constant multiplicand used in *F*2.

	*E*1	*E*2	*E*3	*E*4	*Row average*
*f*1	.2	.7	.9	.3	.525
*f*2	.5	.5	1.0	.6	.65
*f*3	.2	.6	.7	.7	.55
*f*4	.2	.6	.5	.3	.4
*f*5	.2	.3	.1	.3	.225

AHP: $F3=.2234f1+.2766f2+.2340f3+.1702f4+.0957f5$
Guiasu: $F3=.2077f1+.2887f2+.2283f3+.1671f4+.1082f5$
Yen: $F3=.2132f1+.2790f2+.2310f3+.1708f4+.1060f5$

To determine *F*3 data, we will use linear regression on each country in set *S.* We will use linear regression on the rankings of countries c_i where $i = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ from 2006 to 2011 on each of sub-factors f_i where $i = 1, 2, 3, 4, 5$. In essence, those countries with the most negative slope — meaning they are ascending from a low rank to a high rank, i.e. 10th to 1st over the course of six years — will be granted the highest rankings and those with the most positive slopes will be given the lowest rankings. Findings are in Table 1 below:

	f_1 *m* (Rank)	f_2 *m* (Rank)	f_3 *m* (Rank)	f_4 *m* (Rank)	f_5 *m* (Rank)
c_1	-0.86 (1)	-0.77 (2)	-0.94 (2)	-0.31 (1)	-1.23 (2)
c_2	+0.31 (8)	-0.11 (4)	+0.71 (9)	-0.29 (2)	-0.34 (3)
c_3	+0.77 (9)	+0.00 (5)	+0.26 (6)	-0.06 (5)	+0.54 (7)
c_4	+0.86 (10)	-2.42 (1)	+0.37 (7)	+0.66 (10)	-1.77 (1)
c_5	-0.17 (4)	-0.29 (3)	+0.60 (8)	+0.00 (6)	+1.06 (9)
c_6	-0.14 (5)	1.00 (9)	-1.63 (1)	-0.14 (3)	+0.77 (8)
c_7	-0.29 (3)	+0.71 (8)	+1.11 (10)	+0.20 (9)	+0.00 (6)
c_8	-0.37 (2)	1.00 (9)	-0.86 (3)	+0.09 (8)	-0.06 (5)
c_9	-0.09 (6)	+0.14 (7)	+0.23 (5)	-0.14 (3)	+1.11 (10)
c_{10}	-0.03 (7)	+0.00 (5)	+0.14 (4)	+0.00 (6)	-0.09 (4)

Table 1. Linear regression of set *S* in *F*3

Note. In some rare instances, empirical rankings were not obtained. These ranks were estimated after a thorough review of available country data.

In our longitudinal analysis, we will keep *F*3 constant while adjusting *F*2 for each successive year. Above, we used linear regression; but as many cyber attack trends do not follow a linear progression, we will instead find use multiple regression to find the most appropriate formula for each sub-factor; this we do to predict the ranks of each sub-factor of *F*2 in 2012, 2013, and 2014 (Table 10). Any prediction beyond this would be inappropriate given the vast shifts that may occur in any technological arena.

3. Degree of Expert Consensus

We will use fuzzy preference relations to examine the degree to which each major factor is preferred over other factors[9].

$$W = \begin{matrix} & E1 & E2 & E3 & E4 \\ F1 & .3 & .9 & .5 & .3 \\ F2 & .5 & .7 & .8 & .6 \\ F3 & .5 & .8 & .7 & .8 \end{matrix}$$

$$PkFi, Fj = eik - ejk + 0.5 \wedge 1 \text{ if } eik \geq ejk \; 1 - ejk - eik + 1.0 - 0.5 \wedge 1] \text{ if } ejk > eik$$

$$\text{where } i, j = 1, 2, 3 \text{ and } k = 1, 2, 3, 4$$

Let Rk=rijk, k=1, 2, 3, 4

$$R1 = \begin{matrix} & F1 & F2 & F3 \\ F1 & .5 & .3 & .3 \\ F2 & .7 & .5 & .5 \\ F3 & .7 & .5 & .5 \end{matrix} \qquad R2 = \begin{matrix} & F1 & F2 & F3 \\ F1 & .5 & .7 & .6 \\ F2 & .3 & .5 & .4 \\ F3 & .4 & .6 & .5 \end{matrix}$$

$$R3 = \begin{matrix} & F1 & F2 & F3 \\ F1 & .5 & .2 & .3 \\ F2 & .8 & .5 & .6 \\ F3 & .7 & .4 & .5 \end{matrix} \qquad R4 = \begin{matrix} & F1 & F2 & F3 \\ F1 & .5 & .20 & .0 \\ F2 & .8 & .5 & .3 \\ F3 & 1.0 & .7 & .5 \end{matrix}$$

Let Ak=aijk, k=1, 2, 3, 4 where aijk= 1 if rijk >0.50 otherwise

$$A1 = \begin{matrix} & F1 & F2 & F3 \\ F1 & 0 & 0 & 0 \\ F2 & 1 & 0 & 0 \\ F3 & 1 & 0 & 0 \end{matrix} \qquad A2 = \begin{matrix} & F1 & F2 & F3 \\ F1 & 0 & 1 & 1 \\ F2 & 0 & 0 & 0 \\ F3 & 0 & 0 & 0 \end{matrix}$$

$$A3 = \begin{matrix} & F1 & F2 & F3 \\ F1 & 0 & 0 & 0 \\ F2 & 1 & 0 & 0 \\ F3 & 1 & 0 & 0 \end{matrix} \qquad A4 = \begin{matrix} & F1 & F2 & F3 \\ F1 & 0 & 0 & 0 \\ F2 & 1 & 0 & 0 \\ F3 & 1 & 0 & 0 \end{matrix}$$

Let Rk=rij = 14k=13aijk if i ≠j where i, j=1, 2, 30 otherwise

$$R = \begin{array}{c} \\ F1 \\ F2 \\ F3 \end{array} \begin{array}{c} \begin{array}{ccc} F1 & F2 & F3 \end{array} \\ \begin{array}{ccc} 0 & 1 & 4 \\ 3 & 4 & 0 \\ 1 & 4 & 3 \end{array} \end{array}$$

Let G =gij = 1 if rij >0.50 otherwise

$$G = \begin{array}{c} \\ F1 \\ F2 \\ F3 \end{array} \begin{array}{c} \begin{array}{ccc} F1 & F2 & F3 \end{array} \\ \begin{array}{ccc} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{array} \end{array}$$

g1= 12j=13gij= 120+0+0=0
g2= 12j=23gij= 121+0+0=12
g3= 12j=33gij= 121+0+0=12

*Let zQi= μQgi for i=1, 2, 3 is the extent to which Fi is preferred to Q other Fi, j=1, 2, 3.We will define Q=*most *[of the Fj]*
If Q denotes most,*then ∀x∈0, 1.*

$$\mu Qx = \begin{cases} 1 & \text{if } .8 \le x \le 1.0 \\ 2x - .6 & \text{if } .3 < x < .8 \\ 0 & \text{if } 0 \le x \le .3 \end{cases}$$

The fuzzy Q−consensus is defined to be the fuzzy subset wQFi= zQi, i=1, 2, 3 as the fuzzy subset of the set of Fi that is preferred to Q other Fj

zQ1= μQg1= μQ0=0
zQ2= μQg2= μQ12=212− .6= .4
zQ3= μQg3= μQ12=212− .6= .4
Therefore:
wQF1= 0 wQF2= .4 wQF3= .4

Definition: *Let S, I, ≻, R, ~ be relations on X having the following meaning.*
S:Outranking relation:xSy means x is not worse than y
I:Indifference relation:xIy means x and y are indifferent
≻:Preference relation:x≻y means x is preferred to y
R:Incomparability relation:xRy means x and y are incomparable
~:Outranking relation:x~y means x and y cannot be discriminated

Definition: *Define the following indices from S: ∀x,y ∈X*
Indifference index: ISx,y=Sx,y S(y,x)
Incomparability index: RSx,y=(1−Sx,y) (1−S(y,x))
Preference index: ≻Sx,y=Sx,y (1−Sy,x)
Nonpreference index: ~Sx,y=IS R(S)

Let S = R, where R=
$$\begin{array}{c} \\ F1 \\ F2 \\ F3 \end{array} \begin{array}{c} \begin{array}{ccc} F1 & F2 & F3 \end{array} \\ \begin{array}{ccc} 0 & 1 & 4 \\ 3 & 4 & 0 \\ 1 & 4 & 3 \end{array} \end{array}$$

$$F1 \quad F2 \quad F3 \quad F1 \quad F2 \quad F3$$
$$I(S) = F1\ F2\ F3\ 0\wedge 014\wedge 3414\wedge 3434\wedge 140\wedge 014\wedge 2434\wedge 1424\wedge 140\wedge 0 = F1\ F2\ F3\ 014141401414140$$

$$F1 \quad F2 \quad F3 \quad F1 \quad F2 \quad F3$$
$$R(S) = F1\ F2\ F3\ 1\wedge 134\wedge 1434\wedge 1414\wedge 341\wedge 134\wedge 2414\wedge 3424\wedge 341\wedge 1 = F1\ F2\ F3\ 114141412414241$$

$$F1 \quad F2 \quad F3 \quad F1 \quad F2 \quad F3$$
$$\succ(S) = F1\ F2\ F3\ 0\wedge 114\wedge 1414\wedge 1434\wedge 340\wedge 114\wedge 2434\wedge 3424\wedge 340\wedge 1 = F1\ F2\ F3\ 014143401434240$$

$$F1 \quad F2 \quad F3 \quad F1 \quad F2 \quad F3$$
$$\sim(S) = F1\ F2\ F3\ 0V114V1414V1414V140V114V2414V1414V240V1 = F1\ F2\ F3\ 114141412414241$$

We consider the degree of agreement between the experts m, n=1, 2, 3, 4

Define Vijm, n= 1 if rijm− rijn ≤1−.94= .060 otherwise

$$F1\ F2\ F3 \qquad F1\ F2\ F3$$
$$R1 = F1\ F2\ F3\ .5.3.3.7.5.5.7.5.5 \quad R2 = F1\ F2\ F3\ .5.7.6.3.5.4.4.6.5$$

$$F1\ F2\ F3 \qquad F1\ F2\ F3$$
$$R3 = F1\ F2\ F3\ .5.2.3.8.5.6.7.4.5 \quad R4 = F1\ F2\ F3\ .5.20.0.8.5.31.0.7.5$$

$$F1\ F2\ F3 \qquad F1\ F2\ F3 \qquad F1\ F2\ F3$$
$$Vij12 = F1\ F2\ F3\ 100010001 \quad Vij13 = F1\ F2\ F3\ 101010101 \quad Vij14 = F1\ F2\ F3\ 100010001$$

$$F1\ F2\ F3 \qquad F1\ F2\ F3 \qquad F1\ F2\ F3$$
$$Vij23 = F1\ F2\ F3\ 100010001 \quad Vij24 = F1\ F2\ F3\ 100010001 \quad Vij34 = F1\ F2\ F3\ 110110001$$

The degree of agreement between experts m, n as to their preference is:
vBm, n= 13i=12j=i+13vij(m, n) where m, n=1, 2, 3, 4

We have:

vB1, 2= 130=0
vB1, 3= 131=13
vB1, 4= 130=0
vB2, 4= 130=0
vB2, 4= 130=0
vB3, 4= 131=13

The degree of agreement of all pairs of experts m, n is given by the formula:

$$VB= 16n=12m=n+13vB(m, n)= 160+ 13+0+0+0+ 13= 19$$

4. Country Data

The relevant data we will use comes from the Symantec Corporation[8], the world's largest vendor of computer security software packages. Their annual Internet Security Threat Reports summarize the trends and characteristics of cybercrime, and a 2011 study conducted by Norton — a Symantec brand — adds survey data on the costs and prevalence of cyber crime. For a full summary of data, see Tables 4 to 9 below (*Note.* The 2011 Norton survey study defines cybercrime as the appearance of a computer virus or malware, successful phishing or smishing request, online harassment, social network profile hacking, sexual predation, response to online scams, online credit card fraud, identity theft, or otherwise unspecified mobile device or computer attack on a respondent).

Given that the data, ε, for each major factor is ordinal on a scale from 1 to 10, we will define the data in terms: $vi=1.1-(\varepsilon i\times 0.1)$ so that a rank of 10th produces a score of 0.1 and a rank of 1st produces a score of 1.0. Using our equations displayed above, we find:

	Method	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}
G_{2011}	AHP	.630	.469	.445	.469	.616	.409	.213	.359	.435	.658
	Guiasu	.623	.470	.438	.473	.612	.401	.212	.356	.435	.651
	Yen	.623	.468	.440	.468	.612	.404	.212	.356	.435	.652
G_{2012}	AHP	.616	.510	.443	.571	.585	.411	.236	.332	.427	.619
	Guiasu	.608	.512	.435	.577	.582	.403	.234	.328	.426	.611
	Yen	.609	.510	.437	.573	.582	.406	.234	.327	.427	.613
G_{2013}	AHP	.607	.528	.444	.561	.613	.408	.245	.332	.432	.599
	Guiasu	.600	.532	.437	.567	.609	.400	.244	.328	.431	.591
	Yen	.600	.529	.439	.563	.610	.403	.243	.328	.432	.592
G_{2014}	AHP	.603	.528	.444	.568	.598	.409	.245	.332	.426	.599
	Guiasu	.596	.532	.437	.574	.595	.401	.244	.328	.425	.591
	Yen	.596	.529	.439	.570	.595	.404	.243	.328	.425	.592

Table 3. Final findings for major factors of *G* and *G* for 2011, 2012, 2013, and 2014

5. Conclusion

Final calculation results are found in Table 3 above. There is a great degree of consistency regarding country rankings, especially among countries $c_6 \ldots c_{10}$. The only substantial change in ratings occurred with c_{10} (United States), which is predicted to descend from first to third in overall cybercrime ranking over the next three years. Given the derived growth patterns in each type of cyberattack, countries c_1 (Brazil), c_4 (France), and c_5 (Germany) are expected to rise one value in rankings by 2014, while c_2 (Canada) and c_{10} (United States) are expected to drop. Brazil is expected to regain the top-ranked position in cybercrime by the end of 2012 and retain that rank through 2014.

Table 4

$F1$ and $F2_{2011}$ for set S

	$F1$: Damage		$F2$: Prevalence	
c_i	Net cost	(Rank)	Victims	(Rank)
c_1	63300	(3)	.74	(3)
c_2	5700	(6)	.61	(7)
c_3	85100	(2)	.86	(1)
c_4	2400	(7)	.57	(9)
c_5	33800	(4)	.50	(10)
c_6	7600	(5)	.81	(2)
c_7	9	(10)	.67	(4)
c_8	1800	(9)	.63	(6)
c_9	1800	(8)	.61	(8)
c_{10}	107600	(1)	.66	(5)

Note. Net cost = 2011 net cost of cybercrime in millions of US dollars; Victims = 2011 percent of online adult victims

Table 5

Bot-infected computer attack rankings for set S

	Global ranks						Relative Ranks					
c_i	2006	2007	2008	2009	2010	2011	2006	2007	2008	2009	2010	2011
c_1		6	5	3	3	5	8	5	4	3	2	4
c_2	8	13	14		17		7	8	8	9	8	9
c_3	1	3	1	2	6	6	1	3	1	2	5	5
c_4	5	8	10			12	4	6	7	10	10	7
c_5	3	2	4	5	4	2	3	2	3	4	3	1
c_6			20	20	20		10	10	10	8	9	10
c_7	6	5	6	6	5	4	5	4	5	5	4	3
c_8			17	19	16		9	9	9	7	7	8
c_9	7	9	9	14	9	7	6	7	6	6	6	6
c_{10}	2	1	2	1	2	3	2	1	2	1	1	2

Table 6

Hacking computer attack rankings for set *S*

	Global ranks						Relative Ranks					
c_i	2006	2007	2008	2009	2010	2011	2006	2007	2008	2009	2010	2011
c_1		9	9	6	3		10	8	7	5	3	8
c_2	7	7	10		12	2	6	6	8	10	9	3
c_3	2	2	2	2	2	2	2	2	2	2	2	2
c_4	4	6	5			5	4	5	5	9	10	6
c_5	3	3	4	3	7	3	3	3	4	3	7	4
c_6			19	18	8		9	10	10	8	8	10
c_7	8	8	8	8	6		7	7	6	6	6	9
c_8			14	10	5	8	8	9	9	7	5	7
c_9	5	5	3	4	4	4	5	4	3	4	4	5
c_{10}	1	1	1	1	1	1	1	1	1	1	1	1

Table 7

Malicious code computer attack rankings for set *S*

	Global ranks						Relative Ranks					
c_i	2006	2007	2008	2009	2010	2011	2006	2007	2008	2009	2010	2011
c_1		21	16	5	6	9	9	8	9	5	5	5
c_2	6	4	5		8		5	4	5	9	6	8
c_3	2	2	2	3	3	4	2	2	2	3	3	3
c_4	9	11	8			19	7	7	6	10	10	7
c_5	7	7	12	21	11		6	5	8	8	7	9
c_6			3	2	2	1	8	9	3	2	2	1
c_7	5	10	11	16	21		4	6	7	7	9	10
c_8			18	12	15	10	10	10	10	6	8	6
c_9	3	3	4	4	4	5	3	3	4	4	4	4
c_{10}	1	1	1	1	1	2	1	1	1	1	1	2

Table 8

Phishing computer attack rankings for set *S*

	Global ranks						Relative Ranks					
c_i	2006	2007	2008	2009	2010	2011	2006	2007	2008	2009	2010	2011
c_1		13	16	12	10	10	9	8	9	6	7	8
c_2	7	5	3		2	4	6	4	3	9	2	4
c_3	9	2	6	6	7	5	7	2	5	4	5	5
c_4	6	6	9			7	5	5	7	10	10	6
c_5	2	3	2	2	3	2	2	3	2	2	3	2
c_6			22	21	30		10	10	10	8	9	10
c_7	12	11	14	18	11	12	8	7	8	7	8	9
c_8	5		7	5	8	8	4	9	6	3	6	7
c_9	3	7	5	7	4	3	3	6	4	5	4	3
c_{10}	1	1	1	1	1	1	1	1	1	1	1	1

Table 9

Spamming computer attack rankings for set *S*

	Global ranks						Relative Ranks					
c_i	2006	2007	2008	2009	2010	2011	2006	2007	2008	2009	2010	2011
c_1			7	2	9	3	9	9	6	2	6	3
c_2		7	14			13	10	6	9	10	10	5
c_3	15	2	2	7	5		5	2	2	5	4	7
c_4			11	3	1	2	8	10	8	3	1	2
c_5	6	35	40		41		3	8	10	9	9	10
c_6	2	1	3	6	3		2	1	3	4	3	6
c_7	31	12	10	19	7		7	7	7	8	5	8
c_8	20	6	6	9	11	10	6	5	5	7	7	4
c_9	7	4	4	8	28		4	4	4	6	8	9
c_{10}	1	3	1	1	2	1	1	3	1	1	2	1

Table 10

Ranking predictions for sub-factors for 2012, 2013, and 2014

				$F2_{2012}$		$F2_{2013}$		$F2_{2014}$	
f_i	c_i	Regression gx where x is years after 2005	R^2	*g(2012)*	(*Rank*)	*g(2013)*	(*Rank*)	*g(2014)*	(*Rank*)
f_1	c_1	.046x3−.04x2−2.515x+10.333	.958	6.55	(5)	11.21	(7)	17.99	(8)
	c_2	*.306x3−2.655x2+ 5.04x+7*	.903	17.14	(10)	34.07	(10)	60.38	(10)
	c_3	*.019x3−.016x2+ .108x+1.33*	.691	7.82	(7)	10.90	(6)	14.86	(6)
	c_4	*−.231x3+ 1.913x2−2.856x+5.333*	.964	-0.16	(2)	-13.36	(2)	-33.82	(1)
	c_5	*−.194x3+1.81x2−4.71x+6*	.933	4.82	(4)	-15.17	(1)	-31.21	(2)
	c_6	*.139x3−1.298x2+ 3.135x+8*	.735	14.02	(9)	21.18	(9)	32.41	(9)
	c_7	*−.093x3+ .829x2−2.221x+6.333*	.824	-0.49	(1)	-6.00	(3)	-14.30	(3)
	c_8	*.157x3−1.563x2+ 3.993x+6.333*	.893	11.55	(8)	18.63	(8)	30.12	(8)
	c_9	*.065x3−.698x2+ 2.094x+4.667*	.495	7.42	(6)	10.03	(5)	14.36	(5)
	c_{10}	*.037x3−.282x2+ .396x+1.667*	.354	3.31	(3)	5.73	(4)	9.36	(4)
f_2	c_1	*.306x3−2.655x2+ 5.04x+7*	.903	17.14	(10)	34.07	(10)	60.38	(10)
	c_2	*−.407x3+ 3.528x2−7.779x+10.667*	1.00	-10.52	(1)	-34.16	(1)	-70.28	(1)
	c_3	2	1.00	2.00	(5)	2.00	(6)	2.00	(6)
	c_4	*−.380x3+ 3.611x2−8.581x+9.667*	.902	-3.80	(2)	-22.44	(2)	-52.09	(2)
	c_5	*−.176x3+ 1.794x2−4.745x+6.333*	.481	0.66	(3)	-6.92	(4)	-19.36	(4)
	c_6	*.25x3−2.536x2+7.214x+4*	.926	15.98	(9)	27.41	(9)	45.76	(9)
	c_7	*−.38x3+ 3.611x2−8.581x+9.667*	.966	3.80	(6)	-22.44	(2)	-52.09	(2)
	c_8	*.287x3−3.067x2+8.931x+1.667*	.902	12.34	(8)	23.77	(8)	42.84	(8)
	c_9	*−.037x3+ .639x2−2.896x+7.333*	.860	5.68	(7)	6.12	(7)	6.06	(8)
	c_{10}	1	1.00	1.00	(4)	1.00	(5)	1.00	(5)
f_3	c_1	*.157x3−1.635x2+3.922x+6.333*	.824	7.52	(7)	13.45	(8)	23.65	(8)
	c_2	*−.139x3+ 1.44x2−3.563x+7*	.541	4.94	(6)	-0.51	(2)	-9.76	(2)
	c_3	*−.056x3+ .583x2−1.504x+3*	.905	1.83	(3)	-0.39	(3)	-4.14	(3)
	c_4	*−.343x3+ 3.401x2−9.114x+13.333*	.773	-1.47	(1)	-17.53	(1)	-43.26	(1)
	c_5	*.009x3−.115x2+1.019x+4.667*	.583	9.25	(8)	10.07	(7)	11.08	(8)
	c_6	*14.274×(1−.646)x*	.906	0.01	(2)	0.00	(4)	0.00	(4)

	c_7	*.083x3−.893x2+3.881x+1*	.972	12.88	(9)	17.39	(9)	24.10	(9)
	c_8	*.093x3−.036x2−.607x+8.667*	.696	34.55	(10)	49.12	(10)	68.09	(10)
	c_9	*−.019x3+ .123x2+.142x+2.667*	.845	3.17	(4)	1.95	(5)	0.06	(5)
	c_{10}	*.046x3−.397x2+.985x+.333*	.952	3.55	(5)	6.36	(6)	10.58	(6)
f_4	c_1	*.13x3−1.183x2+2.545x+7.333*	.587	11.77	(8)	18.54	(8)	29.19	(8)
	c_2	*−.185x3+1.873x2−5.656x+9.667*	.123	-1.60	(2)	-10.43	(2)	-24.39	(2)
	c_3	*−.25x3+2.929x2−10.107x+14*	.566	1.02	(4)	-7.40	(3)	-21.96	(3)
	c_4	*−.389x3+3.583x2−8.171x+10*	.995	-5.06	(1)	-25.22	(1)	-56.90	(1)
	c_5	*−.036x2+ .25x+2*	.036	1.99	(5)	1.70	(5)	1.33	(5)
	c_6	*.139x3−1.298x2+3.135x+8*	.735	14.02	(9)	21.18	(9)	32.41	(9)
	c_7	*.019x3−.016x2−.463x+8.333*	.675	10.83	(7)	13.33	(7)	16.72	(7)
	c_8	*.444x3−4.595x2+13.675x−5*	.575	17.86	(10)	37.65	(10)	69.56	(10)
	c_9	*.093x3−1.258x2+4.792x−.333*	.580	3.47	(6)	5.11	(6)	8.69	(6)
	c_{10}	1	1.00	1.00	(3)	1.00	(4)	1.00	(4)
f_5	c_1	*.065x3−.448x2−.799x+10.667*	.670	5.42	(5)	8.88	(6)	14.57	(7)
	c_2	*−.528x3+5.238x2−14.948x+20*	.930	-9.08	(1)	-34.69	(1)	-75.17	(1)
	c_3	*−.148x3+2.02x2−7.403x+10.333*	.777	6.73	(6)	4.61	(4)	-0.57	(4)
	c_4	*.491x3−5.242x2+14.41x−1.667*	.993	10.76	(8)	29.52	(10)	61.36	(10)
	c_5	*.296x3−3.611x2+13.95x−7.667*	.993	14.57	(10)	24.38	(9)	41.18	(9)
	c_6	*.019x3−.052x2+.358x+1.333*	.755	7.81	(7)	10.60	(7)	14.19	(6)
	c_7	*.139x3−1.405x2+4.028x+4*	.226	11.03	(9)	17.47	(8)	27.78	(8)
	c_8	*−.29x3+2.933x2−8.2x+11.667*	.946	-1.49	(2)	-14.70	(2)	-35.97	(2)
	c_9	*−.102x3+1.302x2−3.739x+.667*	.983	3.31	(4)	1.86	(3)	-1.88	(3)
	c_{10}	*.065x3−.734x2+2.344x−.333*	.145	2.40	(3)	4.72	(5)	8.69	(5)

Note. All regression equations calculated using SPSS software.

References

1. Comprehensive national cybersecurity initiative, *National Security Council Web.* <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative >.

2. Cybercrime report 2011, *Symantec Corporation,* <http://www.symantec.com/content/en/us/home_homeoffice/html/ncr/>.

3. Cyber crime, *Federal Bureau of Investigation* <http://www.fbi.gov/aboutus/investigate/cyber/cyber>.

4. Cyber defence, *Cooperative Cyber Defence Centre of Excellence*. <http://www.ccdcoe.org/>.

5. Cyber terror response center, The. *Cyber Cop Netan*. <http://www.ctrc.go.kr/eng/about/aboutus.jsp>.

6. ENISA – Securing Europe's information society, *European Network and Information Security Agency*, < http://www.enisa.europa.eu/>.

7. S. Guiasu, Reaching a verdict by weighted evidence, in Advances in Fuzzy Set Theory and Technology, ed. Paul Wang Vol. II Bookwright, Druham, 1994 167-189.

8. Internet security threat report archive*, Symantec Corporation*. <http://www.symantec.com/threatreport/archive.jsp>.

9. J. Kacprzyk, M. Fredricci, and H. Nurmi, Group decision making and consensus under fuzzy preferences and fuzzy majority, *Fuzzy Sets and Systems* 49 (1992) 31-32.

10. National cyber security division, *Department of Homeland Security*. <http://www.dhs.gov/xabout/structure/editorial_0839.shtm>.

11. Privacy and information security law blog, *Hunton & Williams LLP*. <http://www.huntonprivacyblog.com/2011/07/articles/germany-launches-national-cyber-defense-center/>.

12. T. L. Saaty, Relative Measurement and Its Generalization in Decision Making: Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors: The Analytic Hierarchy Process, RACSAM (Review of the Royal Spanish Academy of Sciences), series A, Mathematics, 102.2 (2008) 252-319.

13. T. L. Saaty and L. G. Vargas, Models, Methods, Concepts, and Applications of the Analytic Hierarchy Process, International Series in Operations Research and Management Science, Kluwer Academic Publishers, Boston/Dordrecht/London, 2001.

14. United States. Office of management and budget. in *The Budget of the United States Government:Fiscal Year 2011* (2010).

15. J. Yen, Generalizing the Dempster-Shafer theory of fuzzy sets, In Z. Wang and G. J. Klir, Fuzzy Measure Theory, Plenum (1992) 257-283