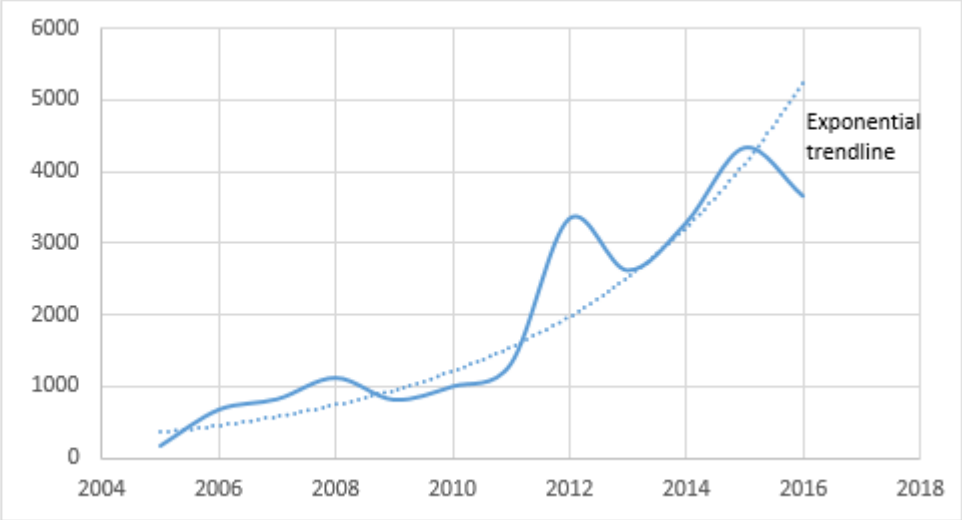
Risk Assessment Mechanisms for Cybersecurity Breaches: Facilitating Risk Management & Underwriting for the Insurance Industry

(by Daniel Minoli)

Unfortunately, in today's world a single day does not go by without reading about a cybersecurity breach somewhere around the globe, whether related to commercial operations, industry, government units, healthcare institutions, financial entities, political parties, and personal data. See Table below. The number of known computer threats such as viruses, worms, trojans, exploits, backdoors, password stealers, spyware, botnet and other variations of potentially unwanted software is estimated to range into the millions. Companies of all types are at constant risk of being penetrated and subject to data breaches. The number of actual breaches is growing exponentially based on data from Risk Based Securities Inc.

Year	Breaches
2005	158
2006	663
2007	810
2008	1108
2009	802
2010	987
2011	1302
2012	3333
2013	2610
2014	3274
2015	4324
2016	3650



Just in 2016 there were 3,650 incidents and 2.9 billion customer records compromised. Organizations impacted include but are not limited to Centene, ADP, Federal Bureau of Investigation - Department of Homeland Security, Seagate, Internal Revenue Service, LinkedIn, MySpace, 21st Century Oncology, Office of Child Support Enforcement, Federal Deposit Insurance Corporation, and Verizon Enterprise Services (also see Table below). According to a 2016 report published by IBM, attacked businesses on average incur data breach costs of $158 per compromised record, and the response costs to a data breach average $4 million. The study also notes that biggest financial consequence to organizations that experienced a data breach is lost business. Following a data breach, organizations need to take steps to retain customers' trust to reduce the long-term financial impact.

Cybersecurity infractions have negative business effects on the targeted firms; therefore, many firms are beginning to seek the protection of an insurance policy; i.e., cybersecurity insurance, which aims at mitigating losses from a variety of cyber infractions, including data breaches, business interruption, and network damage.

Insurance service providers in turn, need security threat, security trends, and breach data analytics to formulate policies and premiums that are commensurate with the exposures facing their policy holders and members.

Researchers at DVI Communications (New York, NY) and CoffyLaw (Freehold, NJ) have developed a **patent-pending objective method** and a defined one-dimensional cybersecurity risk score, **MESERI (MEasure of SEcurity RIsk),** which is a measure of the enterprise's architecture robustness to security threats and infractions. While a handful of industry techniques have been developed to address cybersecurity risks, they tend to be complex and "multi (dimensionally)-valued". MESERI provides a uniform method of attaching a single-valued metric (a scalar) that captures in a rather simple way the complexity of the security situation. MESERI is intended to provide a uniform, cross-entity comparative measure of the enterprise cybersecurity robustness.

This uniform objective measure can be viewed as a Key Performance Indicator (KPI) value. Before- and after- assessments can be made when remedial strategies are undertaken or need to be compared. Because the issue is multidimensional, it is difficult to make comparisons based on vector values in n-th space. Similar multidimensionality issues exist in other disciplines, for example in risk assessment for the financial dependability of a consumer – to address such needs the one-dimensional FICO® score has been introduced and is routinely employed.

The methodology we have developed is described in great details in our patent pending application. Insurance firms can use the score to assess risk of a firm they wish to ensure. In the future, the CEO, CRO (Chief Risk Officer), Board, or Investors may require that each company publish its score. A security certification agency could establish the score for the firm, or it can be estimated by the CISO (Chief Information Security Officer) prior to an infraction by empirically postulating scenarios.

Table: Example of data breaches taking place in early December 2016 – simply Illustrative

Recent Data Breach	Organization
43,000 patient names, addresses, dates of birth, and blood test results exposed on the Internet due to misconfigured database	Hsppl Healthcare Solutions
3,000 user names, email addresses, and phone numbers stolen by hackers and dumped onto the Internet	Caja de Ahorros de la Tropa Profesional del Ejercito Bolivariano Venezolano (CATROPAEJ)
421,313 customer names, addresses, genders, dates of birth, ages, occupations, phone numbers, email addresses, passwords, purchase records, and credit or debit card numbers with expiration dates stolen by hackers through undisclosed means	Shiseido Company Limited
Unknown number of employee names, access card numbers, email addresses, Social Security numbers, phone numbers, dates of birth, driver's license numbers, and explosives handling licenses exposed on the Internet due to misconfigured database	Allied-Horizontal Wireline Services
26,500 customer names, contact details, transaction histories, dates of birth, bank sort codes, partial bank account numbers, and partial credit or debit card numbers with expiration dates accessed by hackers using stolen login credentials	Camelot
Unknown number of suspected criminal names and phone numbers, as well as police investigation information exposed to others after being inappropriately put on an unencrypted hard drive that was connected to the Internet	Europol
Unknown amount and type of confidential business information stolen by two employees and given to rival business	Zynga, Inc.
Unknown number of customer names, addresses, and credit or debit card numbers with expiration dates and security codes stolen by hackers employing malware	The LANG Companies
An unknown amount of customer debit card details captured by skimming device discovered on an ATM	Simplicity Credit Union

For further information, please contact Emmanuel Coffy, Esq. at (973) 375-1804 or Email questions/inquiries to emmanuel.coffy@coffylaw.com