MAY 7, 2015

Updated: January 11, 2016

AND THEN THE ACCOUNTANTS SHOWED UP

HOW THE INSURANCE INDUSTRY WILL DRIVE CYBERSECURITY

CHIP BLOCK
EVOLVER, INC
Reston, VA

Technology and the Cyber Insurance Industry – An Update

In May 2015, Evolver released a research paper on the impact the insurance industry will have on the cyber technology market. The paper, titled "And Then the Accountants Showed Up…How the Insurance Industry Will Drive CyberSecurity," presents ideas on how the growing cyber insurance industry is changing and how companies are addressing cyber challenges.

In the paper, Evolver predicted two main concepts:

- a rapid growth in cyber insurance adoption
- associated use of quantitative cyber risk calculations

Both of these predictions have come true, possibly even faster than anticipated.

The following is an update to the May 2015 paper. It highlights what has happened in the seven months since its release.

Trends in Cyber Insurance that Occurred as Predicted

Cyber Insurance Growth

The paper predicted a rapid growth in cyber insurance across multiple segments. In 2015, there was a major increase in insurance offerings and market expansion. Advisen's *Cyber Liability Insurance Market Trends: Survey of October 2015* indicates that the "cyber insurance market has grown to over $2B in gross written premiums with industry prognosticators forecasting it to double by 2020". [1]

Quantification of Cyber Risk

The Evolver paper predicted that the growth of insurance and overall risk programs would create the adoption of quantifiable risk calculations processes and technologies. New products are hitting the market for the quantification of cyber risk such as RiskLens (www.risklens.com). Likewise, major accounting and consulting firms such as Deloitte have started practices in the formal quantification of cyber risks.

Other Trends in the Market

Law Firm Leadership

The research paper mentioned briefly that the legal community would have an increased involvement in the cyber technology area. What has occurred (at a much greater rate than predicted) has been the rise of market leadership out of law firms.

Many law firms, such as Lewis Brisbois Bisgaard & Smith and Wilson Elser Moskowitz Edelman & Dicker, have formed partnerships with insurance companies to provide a variety of services from breach response to risk evaluation. Additionally, law firms are taking the lead in establishing cybersecurity programs for major corporations.

Insurance and Tech Firm Partnerships

Another trend that is moving significantly faster than anticipated has been technology companies aligning with insurance companies for cyber offerings. The best example of this acceleration is the CyberEdge offering from AIG. The CyberEdge program has IBM, RSA, Verizon, K2 Intelligence and others as technical companies that provide a set of preventive tools that can be procured under an AIG umbrella. Other insurance companies are putting together similar portfolios of packaged insurance and preventive tools from third party technology companies.

Resource

[1] Cyber Liability Insurance Market Trends: Survey, Advisen Ltd. October 2015

AND THEN THE ACCOUNTANTS SHOWED UP

How the Insurance Industry Will Drive CyberSecurity
May 7, 2015

For those of us that have been involved in the information technology business since we were writing our own software programs on Radio Shack TRS-80 computers in the 1970's, there are some trends that you can just feel. During the 80's, we had computers but sharing was difficult and the stovepiped capabilities such as Novell were too limiting and the norm. Then the internet arrived and sharing of information took off. During the internet boom of the late 1990's, stocks were flying high but there was an obvious missing element—customers. Thus the crash of 2000.

Now we are at another nexus, the cybersecurity crisis. Every day another story arises about a major breach at a major company or Government agency. The debacles of Target and Sony are still fresh in our minds. Companies are springing up everywhere to try and attack this very real threat to our economic and physical well-being. So who will rise to put some order into this morass? The insurance industry.

Over the past few years, the view of cybersecurity has changed from a checkbox process for protecting networks to a risk-based view that assumes that some level of attack will be successful. As FBI Director James Comey stated, "There are two kinds of big companies in the United States. There are those that have been hacked…and those who don't know they've been hacked."

This view of cybersecurity as a risk management issue is prevalent across most industries. The Federal Government has moved to a Risk Management Framework for the security of its information technology systems. Companies are assigning their Chief Information Security Officer (CISO) under their Corporate Risk Manager Officer. Cyber-attacks and data breaches are now viewed like the weather, natural disasters and corporate malfeasance. The Sony breach emphasized how a major attack could affect almost every part of a company. Cybersecurity is no longer just the domain of the geeky guys in the back room, it is now a major risk that has the CEO and board of directors' attention.

So how does corporate America address risk? Insurance. Since, like a natural disaster, a company cannot completely avoid a cyber-attack, the next best option is to mitigate the impact an attack can have. Additionally, since the range of impact from cyber-attacks can be as minor as an embarrassing picture of an employee to as critical as the total draining of the corporate bank accounts, there is no way to effectively prepare for all outcomes. The insurance model, therefore, fits the cybersecurity challenge very well. As with all insurance, it is a gamble. The insurance company is betting that the cost of incidents is significantly lower than the premiums collected by its customers. Likewise, the business is hoping that the regular premiums paid will protect the company from catastrophic failure.

Cyber insurance is growing rapidly, with most major insurance providers offering some level of coverage. A recent study by Advisen Insurance Intelligence[1] shows close to a 50% increase in demand for cyber insurance. The increase in demand varies by market with retail, financial and healthcare leading the way. The high profile events of Target, Home Depot, Anthem and Sony are adding to the interest at the C-Level of companies for cyber insurance.

So why would a cybersecurity engineer care about insurance? In the end, technology is driven by business. Who, what, where and how products and services are purchased are driven by the economic conditions of the buyers and the sellers. Today, cyber products and services are within the purview of the IT departments of corporations, usually under the control of the Chief Information Officer (CIO). Expenditures are part of IT budgets and capital expenditures for the company. Most CEOs could not give a detailed description of their cyber budget for the previous quarter.

Additionally, the cost of a cyber-attack is something the CEO and other executives are just hoping doesn't happen to them but is not quantified in any meaningful spreadsheet. To most C-level executives, cybersecurity is an ethereal concept involving unknown threats trying to steal unknown assets that can cause unknown damage. Executives know they should do something, but what they should do is difficult to define.

Here come the accountants – the codification of cyber

As cyber insurance becomes a common element across the business landscape, the accountants and actuaries will define the risks and assign financial value to these risks. This is what insurance companies do. They determine how much the risk of a weather disaster is to a region of a country, the value of personal property, the likely cost of medical expenses and even estimate the cost of death.

This process, called codification, identifies risks and estimates an underwriter's exposure for different type of events. As the insurance industry codifies cyber risks, they will also assign pricing based on these risks and those activities that mitigate these risks. No longer will C-Level executives be faced with the ethereal concepts. They will have costs and expenditures defined in monthly premiums, deductibles and all the other elements of insurance we are all familiar with. As this occurs, the technology that corporations purchase will align with these codified insurance elements. The sales process for products and services will also align as there will be a basis for evaluation. In other words, the market will move to the insurance company's direction.

For those that think the codification of cyber threats is years away, think again. Last year the Chief Risk Officer's (CRO) Forum released a report titled *"Cyber resilience – The cyber risk challenge and the role of*

insurance"[2]. The CRO Forum is a high level discussion group formed and attended by Chief Risk Officers of major European insurance companies.

In the CRO Forum report, a detailed description of the cyber insurance market is presented from an insurance company perspective. After this review, the report breaks the cyber market into risk areas and provides a summary statement of what would be covered under each area. The risk categories and described by the CRO Forum Report are:

First Party Costs [2]

1 Business interruption	A computer system failure or breach of network security leading to income loss and expenses incurred during the period of interruption.
2 Restoration costs	Expenses to restore information/data after a failure of the computer system or network leading to destruction, corruption or loss of electronic information assets and/or data.
3 Regulatory defence costs	Defence costs of regulatory action due to breach of privacy regulation. Cover may include fines and penalties due to breach of privacy regulation.
4 Security and privacy	Investigation costs to determine cause and extent of security failure. Cover may include fines and penalties due to breach of privacy regulation.
5 Cyber extortion	Costs and expenses related to threats or extortion after the release of confidential information or breach of computer security.
6 Intellectual property	Value of trade secrets stolen through a cyber attack.

Third Party Costs

7 Data breach	Compensation of third party liability claims related to the disclosure of confidential commercial and/or personal information (privacy), as well as economic harm suffered by others from a failure of network security.
8 Crisis management	Costs and expenses associated with managing a cyber event (e.g. a privacy breach), which may include forensic investigation expenses, call centre costs, credit monitoring costs and public relations costs.

The CRO Forum goes on to provide recommendations on how Chief Risk Officers should properly code cyber risks to effectively control the exposure of the insurer. The coding of cyber risks will have more impact than just providing insurance companies with exposure data for the setting of premiums and paying claims by companies. This coding will set cost parameters for cyber events. There will likely be great discussion among engineers, accountants, lawyers and insurance actuators as to the accuracy of this coding but the establishment of cyber event estimates by any viable group will impact the market.

Currently, the sales routine for cyber products, whether it be new firewalls, malware detection, vulnerability assessments or identity management, is for engineers to scare senior staff into buying products and services because the cyber threat is new, real and the top story on the news. What is not part of the current sales routine is a financial quantification of how spending more money on a product or service reduces the risk of a particular business area. The coding by the insurance industry will

provide the financial basis that will become part of the sales cycle as executives will want vendors to present their offerings in terms of financial risk protection.

Technology Follows the Money

This move toward a codified, risk-based cyber environment is already beginning to take shape. New products and services are already hitting the market. For example, CXOWARE, a software company out of Spokane, WA, has released a product called Risk Calibrator that provides a quantifiable risk assessment of a business. The tool uses the Factor Analysis of Information Risk (FAIR) industry standard risk model to calculate the quantifiable cost of areas such as business interruption, capital asset replacement, etc. The insurance industry's codification of risks will be incorporated into tools similar to this which will provide the quantifiable risks that companies can use to calculate what type, and how much, cyber investment is needed for each area.

Likewise, Carnegie Mellon Software Engineering Institute (SEI) has developed a CERT® Resilience Management Model that provides a maturity model of an organization's cyber operations. This model acts similar to the Capability Maturity Model Integration (CMMI) that is used in the software industry to measure an organizations maturity level in developing and managing software. Many of the students attending the SEI courses are Chief Information Security Officers (CISO) for major companies and organizations.

This type of maturity modeling will allow insurers the ability to assess a company's cyber capabilities against the calculated financial risk. CISOs are being trained at places such as Carnegie Mellon to approach cyber from a risk based approach versus the formal, checklist driven compliance methodology that has been employed in the past. This risk-based approach aligns with the objectives of the insurance industry.

And don't forget the lawyers….

As with most businesses, the three legs of the stool are operations, accounting and legal. The cyber world is no different. The Target breach has resulted in numerous class action suits and these cases will have an impact, and expense, for years to come. As the quantification of risk becomes more defined, so will the liability calculations. This again will drive technology.

Take, for example, the financial community. The Securities and Exchange Commission released a Risk Alert under the National Exam Program[3] for the Office of Compliance Inspections and Examinations (OCIE) Cybersecurity Initiative. This document describes 28 areas where the OCIE could evaluate companies under the SEC auspices. A logical legal defense against a hack of a securities firm would be that firms that followed this guideline followed commercially reasonable efforts for protecting their environment. Companies will buy technologies that provide the regular reporting requirements to meet this SEC standard.

Similarly, companies that follow the National Institute of Standards and Technology (NIST) Framework[4] and associated standards will claim commercially reasonable efforts toward cyber protection. There will be a growth in technologies that support legal actions from breach notification, from e-discovery to forensics tools that can be used to defend or prosecute companies that have had a breach.

And finally, the expansion of risk with the Internet of Things (IoT)…

The insurance trend mentioned above is based on the current information environment where the loss to a company is primarily in business interruption, personal/financial data release, reputation attacks and similar events. This will change rapidly as the Internet of Things (IoT) becomes part of our daily lives. From driverless cars to the control of critical facility systems such as heating and security, the risks jump from the information domain to the physical domain. Risks then include the loss and damage of property and the health and safety of people.

This increased risk will further involve insurance companies in the day-to-day cyber operations of everything from medical devices to home security. A cost of doing business will include protection from cyber-attacks that could cause serious harm.

Furthermore, the interpretation of attacks will become a critical item. For example, many insurance policies do not cover "terrorism or acts of war". If the Government states that a cyber-attack could be the action of a foreign state, this could affect the recovery of insurance claims. The combination of the insurance and legal factions into the cyber marketplace will dramatically change the lexicon of how cyber-attacks are described and attributed.

Fear, Uncertainty and Doubt…The Cyber Sales Model

The current sales model for cyber products and services is striking fear into senior executives to make a purchase to avoid the disaster that could be a cyber-event. The successful sales person sows enough fear into the buyer that they will either buy a new product or upgrade their existing capability. Products will point out some type of attack their competition can't address. This sales model can only last for a limited amount of time until the market begins to look for more quantitative approaches. This is where the insurance industry will become a key player.

The logical change in the sales model will be the separation of different products by capabilities and cost. Right now, the fear model makes it difficult to determine how much to spend on a product to protect some indeterminate risk. To quote a CISO from Texas, "you don't put a hundred dollar fence around a ten dollar horse." As risks are quantified, and the associated threats to those risks are refined, determining if a large scale, enterprise security solution is needed or a localized, endpoint protection fits the bill will become evident. This will likewise change the sales model. The starting point for this shift will be the codification of risks by the insurance industry.

The Timing of Insurance Industry Influence

Determining how quickly the insurance industry will gain influence over the cyber technology market is directly related to the speed by which companies begin to purchase cyber insurance. According to a Los Angeles Times article of February 19, 2015[5], the purchase of insurance is growing rapidly. The article states insurance purchased doubled between 2013 and 2014 and that, after the major breaches of last year, many insurance providers are swamped with applications this year.

Also, the benefit of insurance is being realized as Target is expected to recover $90M from their insurance in the wake of their breach, according to the article. The other factor that will be drive

adoption is the insurance industry's willingness to provide insurance to an area where there is still relatively little data on the frequency and impact of a cyber attack. Though Target will receive funds from their cyber insurance, the estimated loss is over $250M, according to the L.A. Times.

Even with this uncertainty, the increase in cyber insurance is assured to grow. This growth will drive the C-Level thought processes, which will drive the sales model which, inevitably will drive the technical direction of the cyber market. A major factor in this speed will be the availability of data for the insurance industry to use in their codification process. The availability is growing rapidly. Major reports, such as the Verizon Data Breach Investigation Report[6] which breaks down attacks by type, industry and frequency. With this data and the market changes, the insurance industry's influence could become evident within the next twelve to eighteen months.

Resources

[1] Cyber Liability Insurance Market Trends: Survey, Advisen Insurance Intelligence, October 2014
2 Cyber resilience – The cyber risk challenge and the role of insurance, CRO Forum, December 2014
3 National Exam Program Risk Alert, Volume IV, Issue 2, April 15, 2014
4 National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, February 12, 2014
5 Los Angeles Times, Spending on Cyberattack Insurance Soars as Hacks Become More Common, February 9, 2015
6 Verizon 2015 Data Breach Investigations Report, April 2015

About the Author

Chip Block is Vice President of Evolver, Inc. (www.evolverinc.com) a major supplier of cybersecurity and infrastructure services to the commercial and public sectors. Mr. Block has worked extensively in the cyber research, development and operations field for over fifteen years and been awarded several high level honors for his advanced technological achievements. He is a frequent speaker at technology conferences on cybersecurity, cyber risk and cyber insurance. His email is chip.block@evolverinc.com.