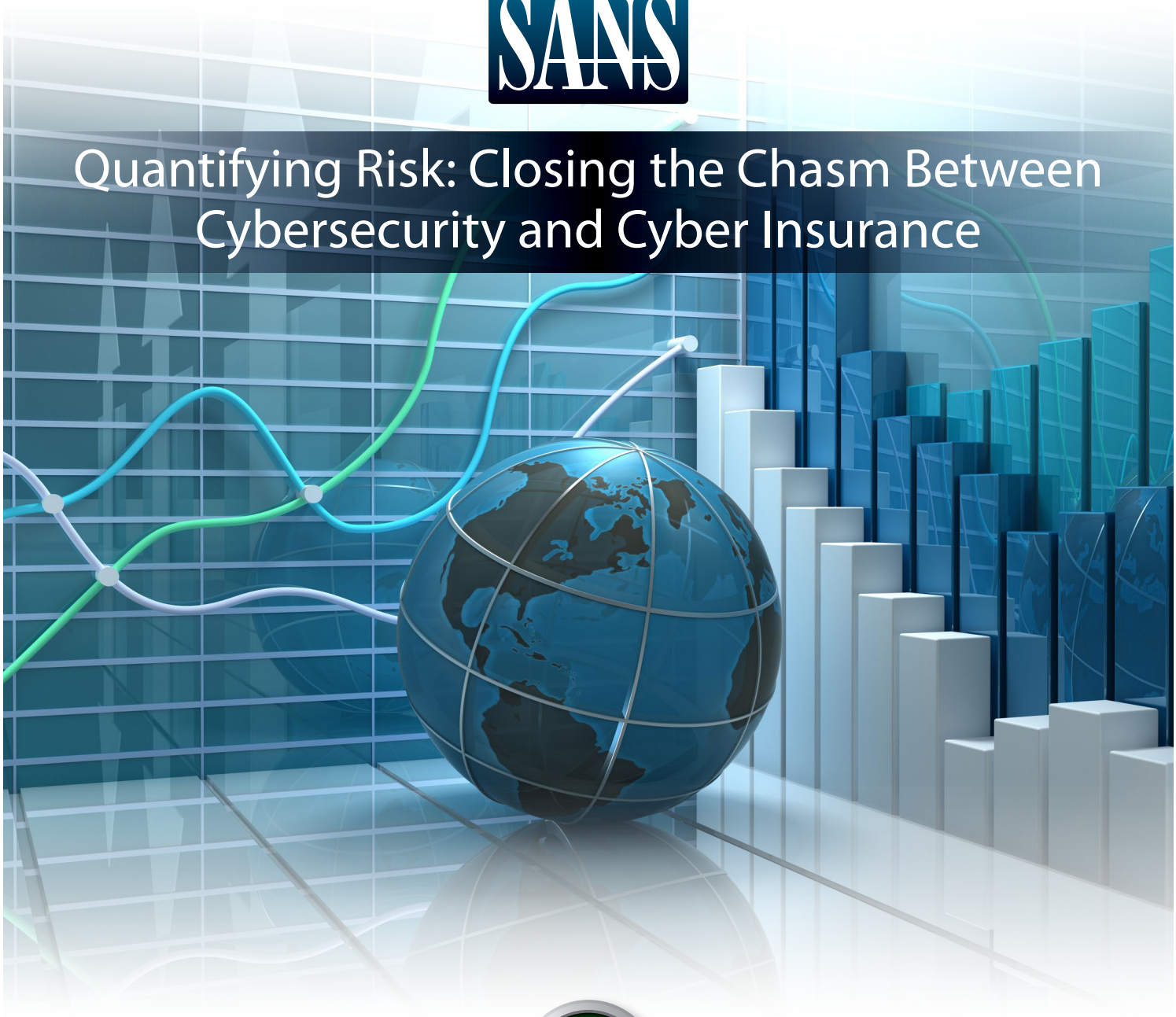
Quantifying Risk: Closing the Chasm Between Cybersecurity and Cyber Insurance

Sponsored by PivotPoint Risk Analytics, in conjunction with Advisen.

Quantifying Risk: Closing the Chasm Between Cybersecurity and Cyber Insurance



Written by Barbara Filkins

March 2016

Sponsored by
PivotPoint Risk Analytics

In conjunction with
Advisen

Cyberattacks may be the biggest risk that global businesses are unprepared for.[1] Record numbers of data breaches have driven large organizations to increase spending on security at twice the rate of other information technology during the past several years, according to market-growth studies by Gartner, IDC and others that predict growth of between 4.7 percent and 9.9 percent during the next five to seven years.[2]

While that growth is significant, it is dwarfed by annual increases of between 25 percent and 35 percent in the cyber insurance market. This sector, worth less than a billion dollars worldwide during 2012, topped $2 billion during 2015 and could triple by 2020, according to Moody's. This explosive growth is a result of executives trying to protect their organizations' financial health in an ever-hostile cyber landscape, as well as carriers seeing profits in a new business segment.[3]

Unlike auto theft or fire insurance, cyber insurance is an emerging form of coverage. Predicting risks for the online environment cannot be based on retrospective analysis, since lack of historical data presents a tremendous challenge. The data simply does not exist to develop the models used by underwriters to calculate risk and set rates related to predictable expectations of loss and exposure. In addition, trying to gain even a toehold is difficult because the data, the technology, and the harmful incidents are growing and evolving so rapidly.[4]

"Without historical data, actuaries cannot drive using the rearview mirror."[5]
–Annmarie Geddes Baribeau

The result is a fragmented and volatile situation for both business and carriers. Carriers must essentially guess at their exposure, reflected in a market that is highly variable in both policy terms and prices. Business leaders, unable to comprehend coverage limits and reimbursement requirements, elect to bear the risk when faced with high costs, high deductibles and outright denial of coverage.

The SANS report "Cleaning Up After a Breach—Post-Breach Impact: A Cost Compendium" predicts that the evolving insurance market will have a strong influence on the ways organizations will approach their risk assessment and management activities, as well as how they will handle their investment in defending against escalating post-breach costs and total financial loss.[6] This will require CEOs/CISOs and insurance underwriters/agents to achieve a common understanding about the meaning of risk and how both sides must work together to achieve a realistic floor from which cyber insurance makes solid business sense.

[1] www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

[2] http://cybersecurityventures.com/cybersecurity-market-report

[3] http://usa.marsh.com/Portals/9/Documents/BenchmarkingTrendsCyber8094.pdf

[4] Nigel Pearson, Global Head of Fidelity, AGCS and one of the authors of a seminal January, 2014, report on the cyber insurance conundrum

[5] http://annmariecommunicatesinsurance.com/2015/01/02/cyber-coverage-and-the-actuarial-challenge-2

[6] www.sans.org/reading-room/whitepapers/analyst/cleaning-breach-post-breach-impact-cost-compendium-36517

The Meaning of Risk: You Say Risk Loss, I Say Risk Uncertainty

Security professionals view risk as "the possibility of suffering harm or loss,"[7] the product of threats and vulnerabilities. We concentrate on our critical assets, first assessing and then continually managing to limit potential harm or loss. Risk management entails first determining an appropriate course of action: avoidance (i.e., ignore entirely or withdraw); mitigation (i.e., reduce the risk); transference (e.g., obtain insurance); or acceptance. From here, we develop the organizational risk posture or profile—the documented "types, amounts and priority of information risk that an organization finds acceptable and unacceptable."[8]

For the InfoSec community, a risk profile identifies problems to be fixed—the open doorway attackers might use to penetrate the organization itself. The fewer the problems, the better the risk profile of the organization.

The insurance industry, on the other hand, defines risk as "uncertainty arising from the possible occurrence of given events."[9] By itself, this risk is not a direct measure of harm or loss, but a tool to gauge the probability of events, both downside (leading to loss) and upside (leading to gain). Risk management, the practice of appraising and controlling risk, has evolved as a discrete field of study and practice, ultimately resulting in what we consider the core of an insurance policy—premiums, deductibles, exclusions, and the conditions and circumstances under which the insured will be financially compensated.

A "risk profile" is "a measure of expected losses for a finite time period based on various items of historical data such as total losses, number of losses, average loss size, and payout patterns."[10] In general, a risk profile is based on a set of calculations to predict, broadly, how many disasters will befall a given set of customers, without knowing specifically which ones will be affected. The actual process is complex; one might say that it overlaps what security practitioners do in quantitative risk assessment—but on steroids.

To date, the information industry has been unable to come up with a standardized, broad approach to estimating costs related to breaches or loss of sensitive data. The current state of knowledge about data incidents or breaches in information security is so variable that leading analysis firms all use different approaches to estimating what a data breach actually costs, resulting in estimates that can differ widely. Actuaries face the same challenge on perhaps an even greater scale—the need to create models that can accurately capture and simulate the effects of rapidly developing technology; actors—whether political, military, or citizen—that are not limited by region or country; and the growth and priorities of a largely invisible, global environment of digital crime and espionage.

[7] Alberts, C., & Dorofee, A. (2003). Managing Information Security Risks: The OCTAVE Approach. Addison Wesley (2002), p. 8.

[8] www.isaca.org/Journal/archives/2013/Volume-4/Pages/Key-Elements-of-an-Information-Risk-Profile.aspx

[9] www.irmi.com/online/insurance-glossary/terms/r/risk.aspx

[10] www.irmi.com/online/insurance-glossary/terms/r/risk-profile.aspx

In the Short Term: The Current Situation

Independent of cyber-related issues, the problem is that insurance is multifaceted and depends on whether and how a policy's details conform to a business's specific threat and risk profile. The business needs to understand how to draw the necessary boundaries, define the terrain to be navigated, and then determine how the insurance and the policy fit together. If a business struggles to determine the impact of a potential breach, despite rigorous quantitative calculations and statistical analysis, its management may question whether cyber insurance is worth the cost.

Top Cyber Insurance Considerations:

1. Establish the correct level of coverage you might need. While quantifying cyber risk in financial terms may still be more art than science, one starting point is through an internal audit to determine the total value of your company's data as well as the aggregate cost of a possible breach.
2. Carefully check definitions of terms such as "hackers," "attacks" or "incidents," and "breach" to make sure they fit the situation(s) and the associated possibilities. Know what situations will trigger your coverage.
3. Make sure that policies (and situations) meet your needs. Be certain that a policy isn't geared only toward compromises from external sources, thereby excluding threats from the inside, which may be far more likely and just as, or more, damaging. Keep in mind that your business might also need specific coverages such as extortion, intellectual property infringement and advertising injury.
4. Consider that many cyber insurance policies do not cover nontechnical attacks, such as an authorized person stealing confidential data. Know which business insurance policy covers that contingency.
5. Make sure that one policy does not negate another. Insurance is a complicated area, and overlaps exist among policies. Resist the temptation to stack multiple cyber insurance policies in the hope that, collectively, they will provide you with a level of protection.
6. Ensure that policies cover more than just the immediate damage and any possible losses from litigation following a breach. The ideal level of cyber insurance protection should cover a business for all costs associated with an incident—discovery, investigation and remediation, as well as any court costs, judgments or penalties.
7. When you're talking to underwriters, find out how much weight they put on the security controls you already have in place. Judgments about the degree to which those controls reduce your company's risk, and therefore its cyber insurance premiums, can be made based on your company's history or the underwriter's own data and calculations.
8. Work closely with a broker you trust, who can guide your company toward a cyber insurance policy that matches the company's specific needs. Ask the broker to compare your costs to those of companies with similar budgets and risk profiles. If the premiums differ significantly, find out what the other company did to raise or lower its exposure in the judgment of underwriters who probably evaluated both companies.

In the Long Term: Toward an Improved Framework to Manage Risk

Until recently, the variability, high premiums, excessive deductibles and exclusions of current cyber insurance policies meant that this type of insurance did not make business sense for most organizations. As the number and intensity of cyber incidents has increased, however, so has the threat to the financial stability of victimized organizations. It is also more likely that managers will turn to IT and information security staffs for advice about the viability and structure of insurance policies that could provide financial protection for the consequences of attacks technological protections could not prevent.

However, security professionals gauge risk by evaluating the types of attacks likely to take place and the ability of InfoSec staffs to identify and repel them (threat × vulnerabilities).

Cyber insurance providers calculate risk by estimating the likelihood of attack, the costs of recovery and the potential cost to underwriters of paying claims resulting from successful attacks.

The risk involved and the cost and variability of cyber insurance policies can therefore logically be reduced by organizations with a strong security stance—whether that stance is established independently or by following effective procedures established by underwriters as a prerequisite for coverage.

Risk-Management Issues To Be Considered

The framework to establish an acceptable level of protection must include the most important items from the priority lists of both underwriters and security organizations. Specific requirements for such a framework are beyond the scope of this paper. Below, however, we ask some of what we think are the right questions.

1. How could this unification between insurance and security expertise influence the development or maturation of the science behind cyber risk assessment? The cyber environment is dynamic, diverse and full of unimaginable threat. Academia, industry and computational actuarial scientists struggle to perfect the data and the algorithms needed to assess cyber risk. With so little historical data available, it may be necessary to gauge risk using data that reflect only the present and project the future. How can collaboration with security professionals help the insurance industry in gauging the potential for disaster and the positive impact of innovative technology? How should the detailed methods used mainly for retrospective analysis influence the education of security professionals?

2. How can we transform this science into an operational asset for both the insurance and security communities? Can an international, structured data breach repository, built using both actual events and model scenarios, help better shape both insurance and security vendors' products and offerings? Should existing sources be used for this purpose?

3. What would a robust risk governance framework based on a unified approach include? Would fundamental risk management definitions, such as threat, vulnerability and risk, shift in their meaning? Should there be a common taxonomy of terms related to risk? How would this affect the evaluation and algorithms used by security professionals? How should this affect privacy and security frameworks (e.g., NIST 800-53rev4) that support regulatory compliance? How does risk factor into the cost/benefit determination of cyber insurance coverage?

4. How can this framework achieve an *insurable* cyberposture and a higher level of security assurance? What metrics can evaluate the resulting risk profile to the underlying goals and objectives of the business? What services and tools can measure and continuously assess cybersecurity risk and the effectiveness of controls?

5. How can the maturing cyber insurance market benefit organizations that become its customers? A business needs to consider some of the other values it derives from a cyber insurance partner in addition to the potential of a paid claim. Insurance companies typically have both in-house and outsourced resources, such as lawyers to help fight class-action lawsuits, security vendors at negotiated rates to help advise both pre-breach on protection strategies and post-breach on incident response support, and credit monitoring services to help consumers after a breach.

The answers to these questions won't directly lower the risk or cost of cyber insurance or cyber attack. They will, however, allow information security departments to effectively support decisions made by business managers. The answers may also provide visibility into how cyber incidents work, how they affect the business, and how those effects can be translated into financial protection that is effective and sustainable for both underwriters and the organizations whose financial stability they insure.

About the Author

Barbara Filkins, a senior SANS analyst who holds the CISSP and SANS GSEC (Gold), GCH (Gold), GSLC (Gold), and GCPM (Silver) certifications, has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. She is deeply involved with HIPAA security issues in the health and human services industry, with clients ranging from federal agencies (Department of Defense and Department of Veterans Affairs) to municipalities and commercial businesses. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, as well as the legal aspects of enforcing information security in today's mobile and cloud environments.

Sponsor

SANS would like to thank this paper's sponsor:

PIVOTPOINT RISK ANALYTICS

In conjunction with

Advisen Transforming • Insurance™

Last Updated: March 3rd, 2016

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS 2016	**Orlando, FLUS**	**Mar 12, 2016 - Mar 21, 2016**	**Live Event**
ICS410 Dubai 2016	**Dubai, AE**	**Mar 13, 2016 - Mar 17, 2016**	**Live Event**
NetWars @ NSM Conference '16	**Oslo, NO**	**Mar 16, 2016 - Mar 17, 2016**	**Live Event**
SANS Secure Singapore 2016	**Singapore, SG**	**Mar 28, 2016 - Apr 09, 2016**	**Live Event**
SANS Atlanta 2016	**Atlanta, GAUS**	**Apr 04, 2016 - Apr 09, 2016**	**Live Event**
SANS Northern Virginia - Reston 2016	**Reston, VAUS**	**Apr 04, 2016 - Apr 09, 2016**	**Live Event**
SANS Secure Europe 2016	**Amsterdam, NL**	**Apr 04, 2016 - Apr 16, 2016**	**Live Event**
Threat Hunting and Incident Response Summit	**New Orleans, LAUS**	**Apr 12, 2016 - Apr 19, 2016**	**Live Event**
SANS Secure Canberra 2016	**Canberra, AU**	**Apr 18, 2016 - Apr 23, 2016**	**Live Event**
ICS Amsterdam 2016	**Amsterdam, NL**	**Apr 18, 2016 - Apr 23, 2016**	**Live Event**
SANS Pen Test Austin	**Austin, TXUS**	**Apr 18, 2016 - Apr 23, 2016**	**Live Event**
SANS Copenhagen 2016	**Copenhagen, DK**	**Apr 25, 2016 - Apr 30, 2016**	**Live Event**
SANS Security West 2016	**San Diego, CAUS**	**Apr 29, 2016 - May 06, 2016**	**Live Event**
SANS SEC542 Budapest	**Budapest, HU**	**May 02, 2016 - May 07, 2016**	**Live Event**
SANS FOR508 Hamburg in German	**Hamburg, DE**	**May 09, 2016 - May 14, 2016**	**Live Event**
SANS Stockholm 2016	**Stockholm, SE**	**May 09, 2016 - May 14, 2016**	**Live Event**
SANS Houston 2016	**Houston, TXUS**	**May 09, 2016 - May 14, 2016**	**Live Event**
SANS Baltimore Spring 2016	**Baltimore, MDUS**	**May 09, 2016 - May 14, 2016**	**Live Event**
SANS Prague 2016	**Prague, CZ**	**May 09, 2016 - May 14, 2016**	**Live Event**
SANS Melbourne 2016	**Melbourne, AU**	**May 16, 2016 - May 21, 2016**	**Live Event**
Beta 2 Cincinnati - ICS456	**Covington, KYUS**	**May 16, 2016 - May 20, 2016**	**Live Event**
Security Operations Center Summit & Training	**Crystal City, VAUS**	**May 19, 2016 - May 26, 2016**	**Live Event**
SANS SEC401 Luxembourg en francais	**Luxembourg, LU**	**May 30, 2016 - Jun 04, 2016**	**Live Event**
SANS Abu Dhabi 2016	**OnlineAE**	**Mar 05, 2016 - Mar 10, 2016**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**