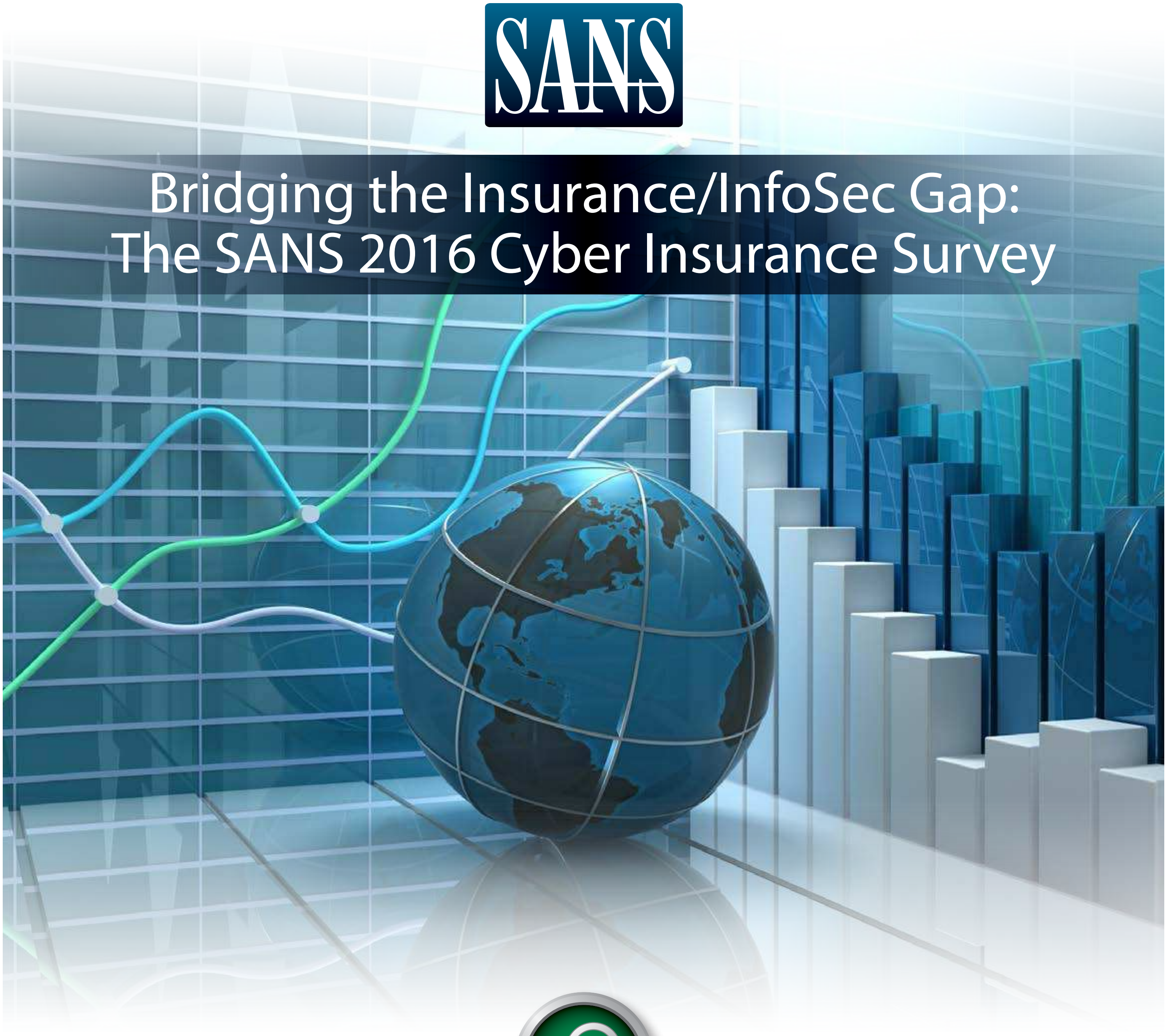
Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey

Results of this survey, conducted in conjunction with Advisen, Ltd., make it clear that the effort to achieve a common understanding of cyber insurance and derive value from it will require focused attention from all sides. This study also sets a direction toward a common, achievable goal: reducing the risk of financial loss from a cyber incident. The gaps identified in this survey come together to form the building blocks needed to achieve this goal.

Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey



A SANS Survey

conducted in conjunction with Advisen, Ltd.

Written by Barbara Filkins

with contributions by Benjamin Wright and David Bradford

June 2016

Sponsored by
PivotPoint Risk Analytics

Executive Summary

Cyber security insurance has become increasingly popular as significant data breaches have become more common. Unlike other information security (InfoSec) preparations, however, the purpose of cyber insurance is not defense; rather, it is the "transfer of financial risk associated with network and computer incidents to a third party."[1] The field is young, dynamic and multifaceted. InfoSec professionals, underwriters and brokers each have different roles in negotiating or implementing policies, as well as different metrics with which to gauge the value of a cyber insurance contract.

In a recent report, "Quantifying Risk: Closing the Chasm Between Cybersecurity and Cyber Insurance,"[2] SANS highlighted conceptual gaps that often make it difficult for members of the cyber security and cyber insurance communities to find a common basis on which to develop reasonable standards of security and insurability. This study, conducted in conjunction with insurance-industry research firm Advisen, Ltd., seeks to further quantify and resolve these gaps, making cyber insurance an integral and highly valued part of a comprehensive InfoSec program.

The results make it clear that the effort to achieve a common understanding of cyber insurance and derive value from it will require focused attention from all sides. This study also sets a direction toward a common, achievable goal: reducing the risk of financial loss from a cyber incident. The gaps identified in this survey come together to form the building blocks needed to achieve this goal. There are four primary areas of disagreement:

1. **The Terminology Gap.** InfoSec and insurance professionals acknowledge they do not speak the same language when defining and quantifying risk, leading to different expectations, actions and justification for outcomes. The terminology gap actually begins within each community, between members that have common, or at least complementary, objectives. Within an organization, the InfoSec professional must reach out to the risk manager. Within the insurance community, underwriters and brokers must develop a common vocabulary to describe the cyber risk profile of an organization.

2. **The Assessment/Framework Gap.** A framework establishes standard actions, practices, plans, metrics and, ultimately, costs related to cyber risk management. Setting transparent standards for minimal acceptable levels of cyber hygiene and incorporating these standards into a risk management framework that bridges the concerns of the two communities establishes the common ground between the two communities and helps create an effective organizational risk management program acceptable to both.

[1] www.econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme.pdf

[2] "Quantifying Risk: Closing the Chasm Between Cybersecurity and Cyber Insurance," www.sans.org/reading-room/whitepapers/analyst/quantifying-risk-closing-chasm-cybersecurity-cyber-insurance-36770

3. **The Communication Gap.** A common vocabulary and framework can inform the needed steps to ensure closure among all involved stakeholders. Without communication to educate and inform all involved stakeholders, the business decisions leading to the evaluation, recommendation and purchase of cyber insurance coverage and its impact on the organization's security program may cause the coverage to fall short of expectations. InfoSec and enterprise risk management activities need to be aligned, to understand the threats facing an organization and its readiness to deal with them, as well as the final decisions about what a policy should cover, what kinds of coverage the company needs and what the policy should cost.

4. **The Investment Gap.** Organizations seeking cyber insurance should aim for alignment between their InfoSec investments and the underwriting criteria. The environment, however, is too dynamic: Underwriters are not always transparent in how they establish criteria, leading to consternation for both the brokers and the buyers. An organization needs to determine its return on investment as it prepares for cyber security insurance coverage.

The next set of challenges is how to narrow those conceptual gaps. To evolve freely, the cyber security and insurance markets need a flexible standard that can serve as a directional indicator. Strict measures encoded in legislation can quickly become obsolete. A flexible road map must address aspects of organizational governance, risk and compliance, but the real challenge may not lie there.

While breaches of sensitive information capture current headlines, catastrophic possibilities loom as the Internet of Things (IoT) and interconnected control grids have now become a reality. Who is liable when a car or an airplane malfunctions because of defects in its software design? What happens when the energy grid is hacked and people die? What forms of insurance will or should respond? These may be the questions for the future, but the risk vocabulary, framework and investment elements must adapt now—and quickly—to these evolving threats.

Executive Summary: The Insurance Industry Perspective

Times are good for the cyber insurance market. Competition has increased rapidly, but so has the size of the market: Premiums increased about 25% between 2014 and 2015 and may double by 2020 if current projections hold true. Organizations of all types and sizes are now purchasing cyber insurance. Purchase decisions often come from the top—the C-suite and the board of directors. According to the 2016 SANS Cyber Insurance Survey of InfoSec professionals, executive management makes the purchase decision 50% of the time and the board 25% of the time.

While more organizations are purchasing cyber insurance, only 48% of the chief information security officers (CISOs) and other InfoSec professionals surveyed find cyber insurance at least "adequate" when addressing the consequence of a data breach. Regardless of how the value of insurance is perceived, it is now part of the InfoSec strategy of many organizations, and interaction between InfoSec professionals and cyber insurance brokers and underwriters is becoming far more common. With this state of affairs, a number of critical issues have surfaced, including the following:

- How much influence do (or should) underwriters have over an organization's InfoSec strategy?
- Do underwriters and InfoSec professionals largely concur on best practices? Where are the gaps and the sources of friction?
- Are underwriters and InfoSec professionals speaking the same language when discussing cyber risk? Where are the disconnects? What are the consequences?
- What can be done to further improve communication, coordination and cooperation?
- What role should the CISO play in the insurance procurement process?
- What can be done to ensure that insurance is valued as an integral part of an organization's overall InfoSec strategy?

This report, the outcome of a joint study by the SANS Institute and Advisen, Ltd., highlights the significance of many of these issues and offers insights into a productive path forward for both the InfoSec and cyber insurance communities. Key takeaways include the following:

- Communication gaps and differences in priorities may be hindering a unified approach to resolving an agreed-upon need to reduce the financial impact of a data breach.

- Cyber security investments made by companies being insured do not always align with the criteria and priorities of underwriters. Although the priorities of underwriters probably should not be the driving force behind decisions about information security, InfoSec professionals should consider the consequences of security decisions on insurance cost and availability.
- Only 14% of brokers surveyed by Advisen said that CISOs understand the role and value of insurance "very well." This suggests that underwriters, and especially brokers, should be doing more to educate and communicate with CISOs.
- CISOs are widely involved in the insurance procurement process, but rarely do they have a decision-making role. There are signs, however, that this will change in the future as insurance becomes more widely viewed as a key element in an end-to-end security strategy.

Communication was a theme that was repeated throughout the survey findings. It is clear that underwriters and InfoSec professionals would benefit from communicating more and communicating better with a common language of risk. Additionally, while CISOs, risk managers and underwriters all have different metrics for assessing risk, different tactics for managing risk and different understandings of what is at risk, all would benefit from a common framework to support a robust and meaningful dialogue.

Methodology and Scope

SANS conducted this survey during early 2016 in conjunction with Advisen, a New York-based firm that provides data, research, quantitative analysis and other services to commercial insurance brokers, underwriters and risk analysis firms. The goal of this collaboration was to provide a deeper understanding of the barriers encountered in establishing appropriate levels of cyber insurance coverage and the impact on the security posture of those organizations.

Advisen concurrently conducted two surveys designed to elicit responses from brokers and underwriters separately, as insurance industry counterparts for cyber coverage. Questions and selection criteria were adjusted to accurately reflect the population and outlook of each industry and were matched as closely as possible to ensure that each data set would complement the other, as well as the results from the SANS survey of InfoSec professionals.

While the intended audience for this paper is the InfoSec professional, SANS has included results and insights from the insurance surveys, where relevant, to expand the security community's understanding of cyber insurance. These results are included in the report and often appear in sidebars.

Legal considerations can be critical in determining cyber insurance coverage. Project advisor Benjamin Wright has written Appendix A: "Cyber Insurance Policy Words and Negotiation," which describes the role and concerns of attorneys during cyber security insurance negotiations, to help InfoSec staff use their legal resources most effectively.

Risk managers in most organizations have been slow to integrate into the InfoSec environment. Yet, the interaction of the risk manager and security professionals is vital to enabling insurance coverages that meet organizational needs. David Bradford, chief strategy officer for Advisen, wrote Appendix B: "Information Security and the Corporate Risk Manager" to outline how risk managers can integrate with InfoSec professionals.

Who Responded

The SANS survey, conducted in early 2016, includes a total of 203 respondents who consider themselves involved in helping establish the security risk profile of their organization or customers, especially in terms of developing a strategy for cyber insurance. A total of 194 insurance professionals responded to the Advisen surveys.

Insurance Respondents

66
Number of Underwriters

128
Number of Brokers

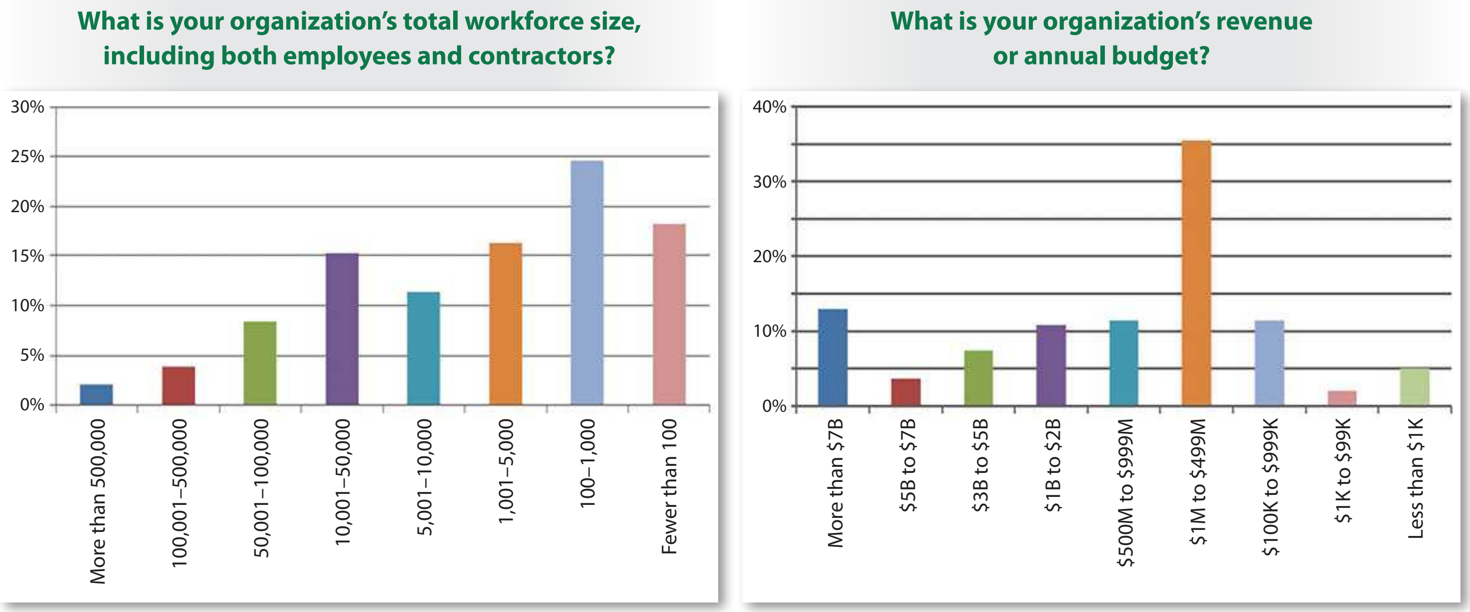
Respondents representing the view of security professionals were close to evenly split between security analysts and administrators (30%) and security management (29%), with senior security (CSO, CISO) management comprising about 45% of security management.

The top industries represented in the SANS survey are shown in Table 1.

Table 1.
Top Industries Represented

Industry	% Response
Financial services/Banking/Insurance	26.6%
Government	15.8%
High tech	13.7%
Education	6.9%
Healthcare	6.9%
Manufacturing	4.4%

Respondent organizations were oriented toward medium-sized organizations, with 59% having workforces under 5,000 and financial worth (as reported by revenue or annual budget) of $1M to $499M, as illustrated in Figure 1.



What is your organization's total workforce size, including both employees and contractors?

What is your organization's revenue or annual budget?

Figure 1. Size of Respondent Organizations by Workforce and Revenue/Budget

Where Risks Lie: Perception Versus Reality

Survey results exposed an interesting dichotomy between where respondents expected risks to exist and where they actually appeared. Based on their risk assessments, respondents said they are most concerned about risks involving the organization's data and information, followed by the applications and databases that interact with and manage that data and information. Risks related to the workforce, both employees and contractors, rank third overall among the major categories of concern.

However, workforce-related issues are the leading category where risks have been realized. (See purple bar, second graph in Figure 2.) Overall, this category also comes close to eclipsing the category of data and information.

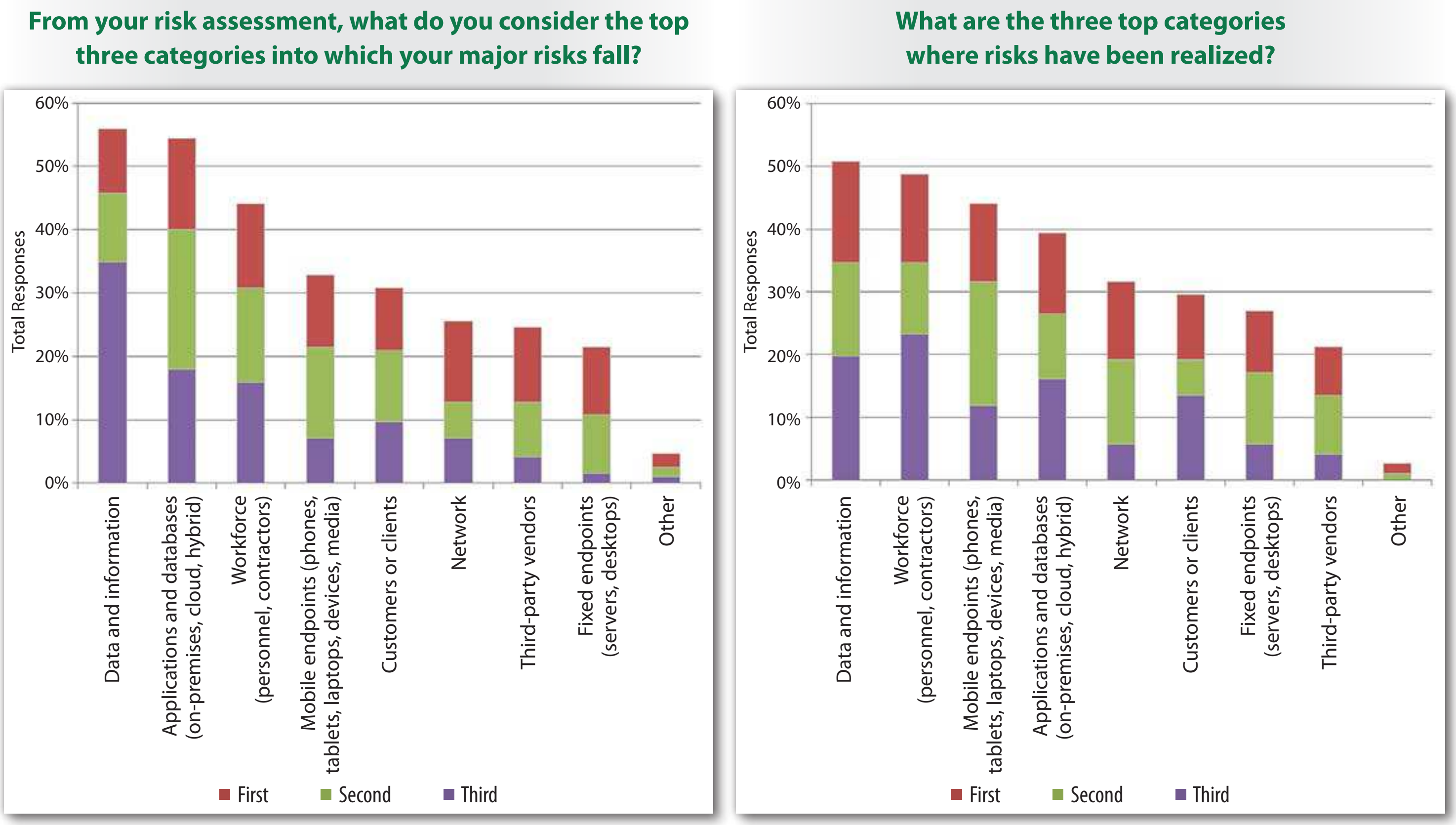


Figure 2. Where Risks Fall Versus Where They Have Been Realized

Risk is managed through three general actions: accept, transfer or mitigate. InfoSec professionals feel most comfortable mitigating risk for those assets they know the best, over which they have ownership or control. Respondents primarily manage risk through mitigation for most technical categories: network, fixed endpoints (servers and desktops), applications, data and information, and mobile endpoints. Acceptance of risk rises dramatically with respect to human elements (workforce, customers or clients, and third-party vendors) as does transferring the risk through insurance. Respondents appear to view transferring risk via insurance as an effective way to mitigate vendor-related risks, most likely through contractual requirements that require a vendor to be insured. See Figure 3.

TAKEAWAY:

Consider insurance, along with appropriate contractual and service level terms and conditions, as useful techniques to manage those people-related risks (workforce, customers, third parties) that might fall outside your ability, as an InfoSec professional, to directly influence, mitigate or remediate.

For each, how do you manage the majority of your risks?

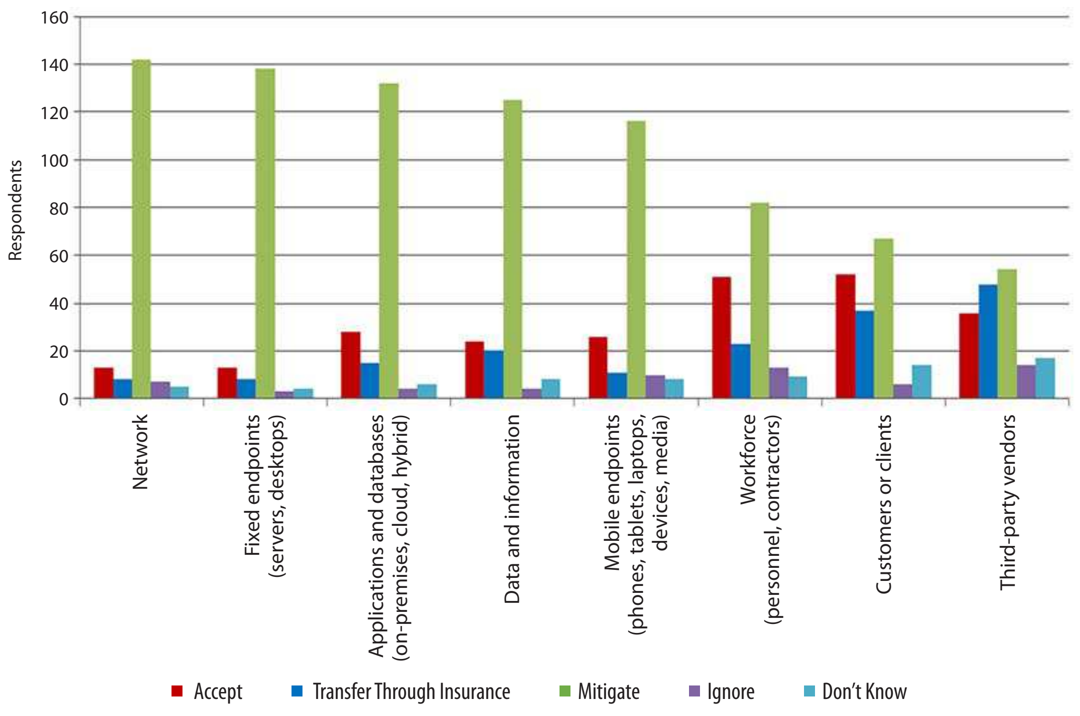


Figure 3. Approach Used to Manage Risk

Frameworks: Formalizing Risk Assessment

Risk assessment is the process by which risks are identified and the impact of those risks determined.[3] Approaches are either *qualitative*, where risk is measured against a relative scale (high/medium/low) to determine the probability of a threat exploiting a vulnerability, or *quantitative*, which allows a financial value to be assigned to loss associated with vulnerability.

Qualitative approaches are used because InfoSec professionals "just don't have enough accurate historical data to calculate the probabilities and magnitude of risks [the way] an insurance activity would," whereas *quantitative* approaches must provide a mathematical basis that "relies heavily on having accurate historical data about previous breaches."[4]

Insurers traditionally rely on a quantitative approach to assess risk, assuming that past claims experience is predictive of the future. However, comparatively little historical cyber insurance claims data exists for underwriting and pricing purposes. As a result, actuaries and other model builders are turning to nontraditional, external sources of cyber event data, and some insurers are in the early phases of developing and deploying underwriting and pricing tools that look very different from traditional actuarial models. While some underwriters are actively using these tools, the underwriting process typically has a significant qualitative aspect as well. According to the Advisen underwriters survey, nearly 60% of respondents said they primarily "rely on [their] underwriters' experience and judgment" to quantify risk for underwriting purposes.

InfoSec survey respondents (57%) approach risk assessment largely from qualitative or not very detailed quantitative methods, as shown in Figure 4.

Does your company develop a quantitative model for assessing and managing cyber risk? ***Select the best answer.***

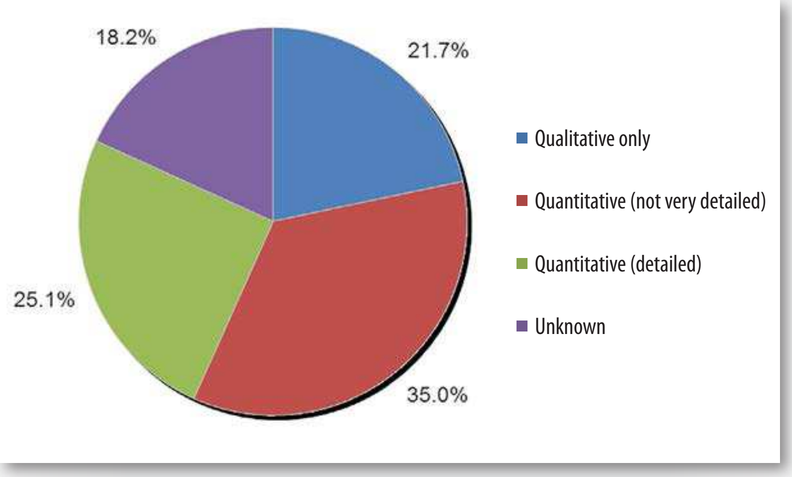


Figure 4. Risk Modeling Approach Used by Respondents

[3] "Glossary of Security Terms," SANS, www.sans.org/security-resources/glossary-of-terms

[4] SANS MGT512 course

An *InfoSec framework* is "a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of InfoSec controls in an enterprise environment." A *framework* provides the set of plans to support the orderly construction of an InfoSec program, similar to blueprints in the construction industry. Well-known examples of frameworks include NIST SP 800-53, FISMA, CIS Critical Security Controls, COBIT, ISO 27000 and HIPAA.[5] All of these address the need for risk assessment and management.

Organizational risk is defined in terms of assumptions, constraints, tolerances and priorities that interact with each other. For this reason, specialized risk frameworks have emerged that are complementary to the security frameworks used by InfoSec, such as the relationship between NIST SP 800-53 and NIST SP 800-30. A framework specific to risk establishes the standards for assessing the components listed and the plans for the subsequent risk management process. It also establishes expectations for external relationships with organizations that will accept the transfer of risk, such as insurance carriers, as well as suppliers, clients and business partners.[6]

A framework should establish criteria (or the basis for such criteria) that address the top reasons why underwriters decline application submission for insurance coverage, clearly establishing the boundaries around "inadequate." See Table 2.

Table 2. Underwriter Reasons for Rejection[7]

Reason for Rejection	% Response
Inadequate cyber security testing procedures and audits	44.7%
Inadequate processes to stay current on new releases and patches	40.4%
Inadequate cyber incident response plan	38.3%
Inadequate backup processes and recovery	34.0%
Structure, size and configuration of network	31.9%
Inadequate policies concerning the security of vendors and business partners	31.9%
Quality of security software	25.5%
Quality of employee training on security issues	23.4%
Lack of adherence to a published security standard (e.g., ISO 27000)	17.0%
Lack of CISO or similar role	14.9%
Inadequate security score provided by third-party service	14.9%
Other	14.9%
Physical security of data center	8.5%

[5] "A Plan for How to Get There and What to Do When You Arrive:
Practical Advice on Establishing a Security Information Management Program within Healthcare,"
www.sans.org/reading-room/whitepapers/leadership/plan-arrive-practical-advice-establishing-secu-35707

[6] http://searchsecurity.techtarget.com/feature/Risk-Management-Framework

[7] Data from the 2016 Advisen Underwriter Survey conducted in conjunction with the SANS Survey

Interestingly, the "other" reasons included the lack of basic controls, such as firewalls, antivirus and intrusion detection; personally identifiable information on portable devices with no encryption; inadequate access controls/monitoring; as well as a general lack of concern about IT security and lack of understanding of the risks.

Both InfoSec professionals and underwriters already depend on the use of risk frameworks. A framework, in general, allows an organization to measure and benchmark itself internally or against other organizations. SANS survey respondents favor (29%) the Risk Management Framework (RMF), as defined by NIST SP 800-37 and NIST SP 800-30, with another 22% using their own internal framework followed by 20% using ISO 27000. The majority of respondents in the Advisen Underwriter Survey concur that the NIST and ISO 27000 frameworks are at least "somewhat helpful," with 63% saying that internally developed frameworks are "very helpful" or "essential."

Standards such as the RMF provide an initial starting point but can be limiting, especially for an organization with a mature understanding of its business processes. Organizations often turn to tailoring their risk framework based on their approach to risk modeling and their internal business model or needs. The RMF is the most popular for those who performed quantitative risk modeling, but it is matched by internally developed frameworks for those who depend upon qualitative risk methods (see Figure 5).

Risk Modeling Approach Versus Framework Used

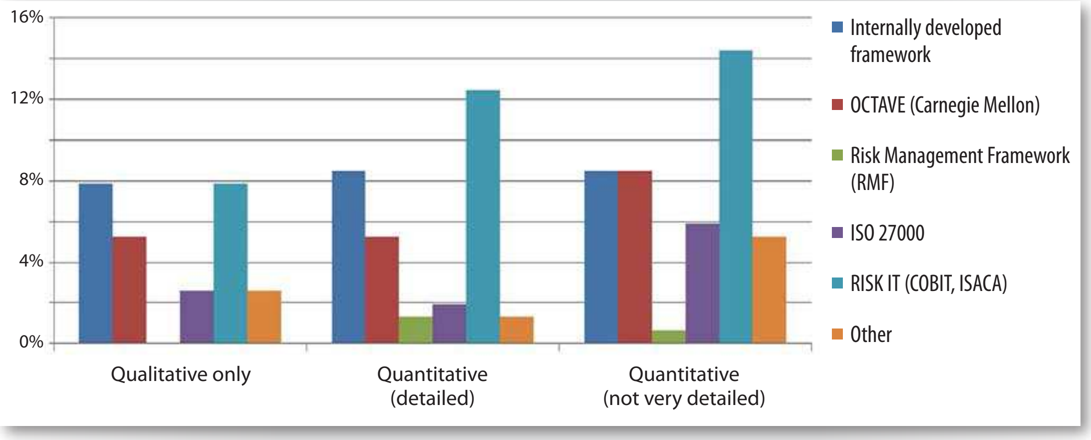


Figure 5. Risk Modeling Approach Versus Framework Used

The Assessment/Framework Gap

The absence of common cyber security standards, best practices and metrics is cited as a barrier to a robust cyber insurance market. Members of the InfoSec and insurance industries would benefit from a common framework that supports understanding, realistic modeling, and justifiable and affordable actions.

Investment: The Haves and Have Nots

Despite the almost daily release of information about new cyber breaches, only 34% of respondents have cyber insurance, with another 12% reporting they are self-insured. See Figure 6.

Do you have cyber insurance coverage?

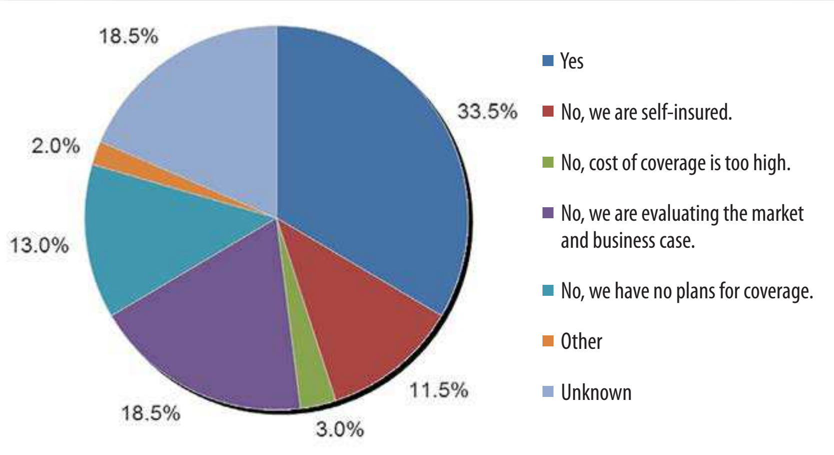


Figure 6. Cyber Insurance Coverage

Reviewing the demographics of our respondent population with respect to whether they have cyber insurance, we found that, although the overall leading industry of our respondents is the combination of financial services, banking and insurance, government replaces that sector as the leading industry sector for the 12% that self-insure.

Financial size of the organization, measured either by its budget or revenue, did not appear to correlate with whether or not the organization had obtained cyber insurance, although there was an observable trend showing that organizations with larger workforces tend to be self-insured, while those with smaller headcounts are less likely to have obtained coverage.

Organizations large enough to fund their own expected cyber claims are increasingly turning to a *captive insurance company*, an insurer owned by the entity being insured. "Captives" have most often been used to underwrite property damage, workers' compensation and third-party liability risks, but a growing number of companies are now using their captives to insure their cyber risks as well.[8]

[8] "2016 Global Risk Management Survey," www.aon.com/risk-services/2016-captive-cyber-survey.jsp

Knowing What You Have

Only 64% of respondents that are covered either by third-party coverage or are self-insured know how their organization obtains that coverage. Figure 7 shows the distribution of where they choose to get coverage.

Brokers surveyed by Advisen have a generally high opinion of the insurance knowledge level of CISOs and other security professionals. More than 70% said that, on average, CISOs and other security professionals understand the role and value of cyber insurance "somewhat well" or "very well."

How have you chosen to obtain your cyber insurance coverage?
Select the best answer.

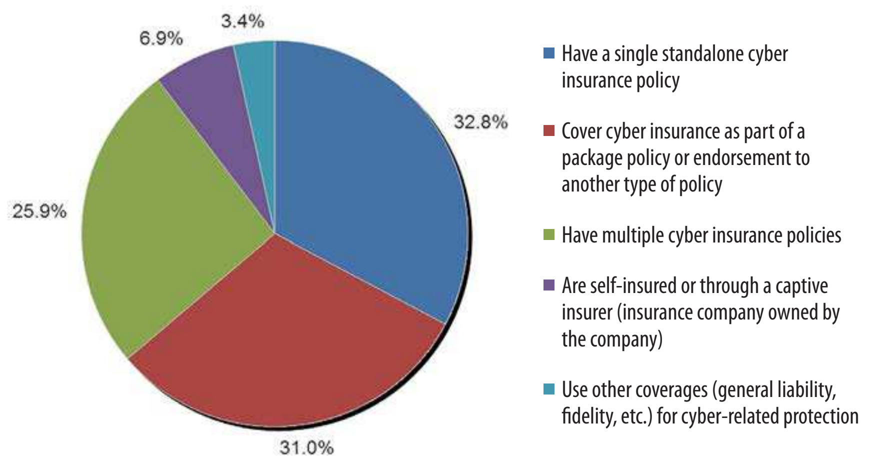


Figure 7. How Cyber Insurance Coverage Is Obtained

For those respondents that either have cyber insurance or are self-insured, SANS wanted to dig a little deeper. Only 60% of this population indicated that they actually understand the characteristics and limits of their insurance coverage. For organizations that actually had obtained cyber insurance (as opposed to those that are self-insured), the leading respondent role was security management in general, including managers, supervisors and senior management (CISO, CSO), perhaps indicating that people in these roles are knowledgeable about the cyber security practices of their organization.

For the purposes of this survey, SANS used the following definitions to describe the elements normally covered by cyber insurance:

- **Data breach/Privacy crisis management**—includes expenses related to the management of an incident, the investigation, the remediation, data subject notification, call management, credit checking for data subjects, legal costs, court attendance and regulatory fines
- **Multimedia/Media liability**—covers third-party damages, such as specific defacement of a website and infringement of intellectual property rights
- **Extortion liability**—covers losses due to a threat of extortion and professional fees related to dealing with the extortion
- **Network security liability**—covers third-party damages that result from denial of access, costs related to data on third-party suppliers, and costs related to the theft of data on third-party systems

Respondents who that know what elements are included in their coverage indicated that, by far, data breach/privacy crisis management services are the most frequently covered, as shown in Figure 8.

What elements does your cyber insurance cover?
Consider all sources of insurance. Select all categories that apply.

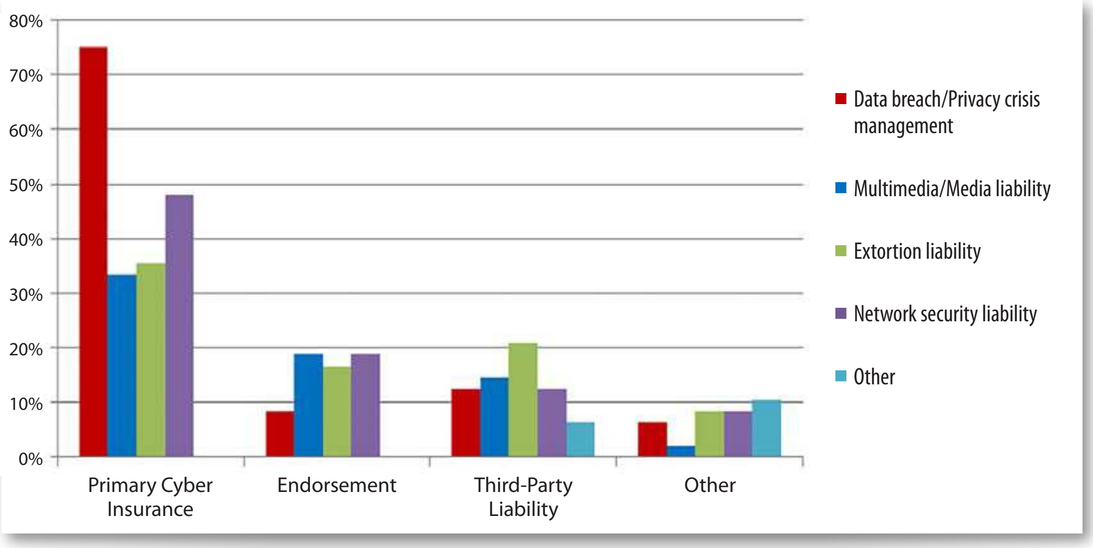


Figure 8. Cyber Insurance Coverage Preferences

Cyber insurance is a comparatively new and rapidly evolving product. As such, there is little standardization among policies, with coverage terms varying substantially from policy to policy. A recent study of 26 cyber insurance policies found that "almost no two products have exactly the same number and types of coverage in their offering."[9] Nonetheless, the gap between, for example, those claiming their organization's policy covers data breach/privacy crisis management (74%) and those saying their policy covers network security liability (48%) is surprising, because both are typically covered under cyber policies, regardless of the insurer.

Adequacy of Coverage

Looking again at those respondents who have insurance or are self-insured, only 4% feel that cyber insurance is "totally useless." The majority (41%) feel that coverage is "somewhat adequate," with 48% considering their coverage to be "adequate" or above. See Figure 9. Respondents to the Advisen Broker and Underwriter surveys concur that InfoSec professionals see the insurance industry as doing a slightly better than average job in addressing the financial consequences of InfoSec exposures.

How adequate do you believe insurance is in addressing the financial consequences of your organization's cyber security exposure?

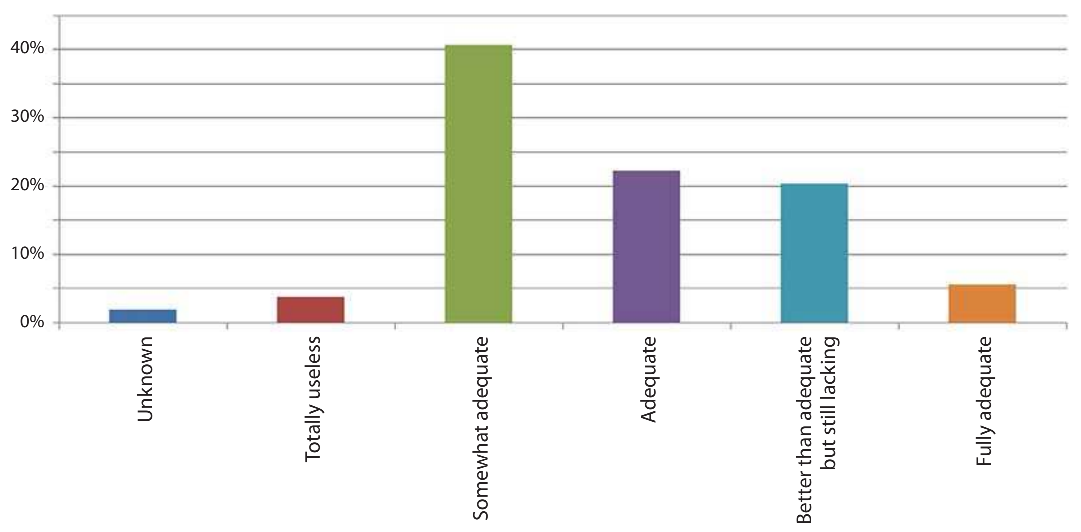


Figure 9. Adequacy of Coverage

[9] Cambridge University Centre for Risk Studies, "Managing Cyber Insurance Accumulation Risk," http://cambridgeriskframework.com/getdocument/39

TAKEAWAY:

Carefully consider the value of pre- and post-breach services packaged with indemnification. They may lower your overall pre- or post-breach costs, improve your coverage and reduce the chances that your submitted claim will be denied.

However, there is no quantifiable definition, based on experience, of what is "adequate coverage." More than 70% of these respondents have never recovered losses through cyber insurance, whether they ever submitted a claim or not, yet they believe their coverage is adequate.

On the other hand, this perception of adequacy may be due to other factors, such as the value provided by the pre- and post-breach services packaged with indemnification. Most respondents (63%) value these services, with 30% having obtained these services and an additional 17% exploring the possibility, findings that, although demonstrating less enthusiasm, match broker and underwriter perceptions. According to 73% of underwriters and 55% of brokers, CISOs frequently or always value pre- and post-breach services packaged with indemnification.

Meeting Coverage Demands

One thing is certain. Most respondents had to adjust their security profile to obtain satisfactory cyber insurance coverage. Only 9% reported having to make no adjustments (as write-in responses captured in the "Other" category), while 41% of this set of respondents had to implement or update policies or processes, as shown in Figure 10.

What adjustments (if any) did you have to make to your security profile in order to obtain satisfactory cyber insurance coverage? ***Select all that apply.***

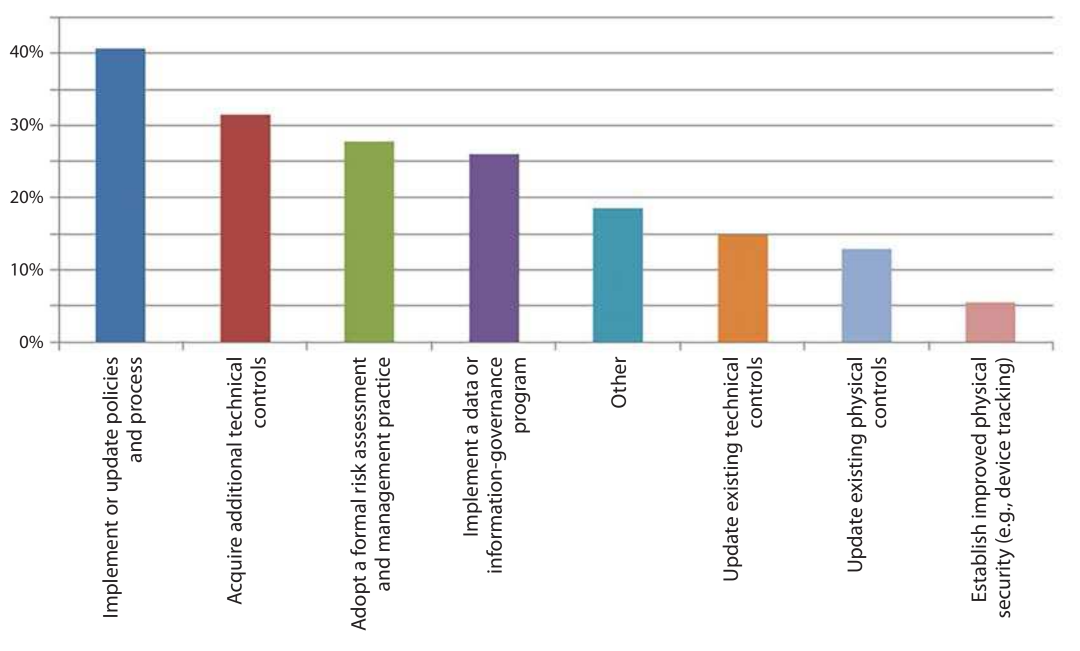


Figure 10. Changes to Security Profile to Obtain Cyber Insurance

What is still unknown is the extent to which these changes actually reduce cyber risk or make cyber insurance cost-effective. One respondent to the Advisen Broker Survey stated, "The cost of a policy is directly impacted by the security policies of an organization. Clients have said that spending money on the security measures is more cost-effective because of concerns with exclusions in the policy."

The cyber insurance industry suffers from a lack of transparency, starting with the concerns, standards and expectations of underwriters. Research from Advisen shows that insurance brokers are frustrated by divergent and sometimes conflicting expectations from underwriters, due to the market's rapid state of flux and a wide variation in understanding of the criteria to be used to assessing an organization's cyber risk posture. According to some brokers surveyed, underwriters often decline to insure a company not because of its specific InfoSec practices, but simply because it is in an industry ("class of business") the underwriter prefers to avoid.

"Underwriting criteria for cyber liability [are] changing in real time. Underwriters are as transparent as they can be at any given point, but there is something new from month to month."

—Respondent, Advisen Broker Survey

But before underwriters and InfoSec professionals can share a common set of expectations, the insurance industry must develop its own set of standard expectations.

On the InfoSec side, organizations struggle to implement and document best practices that should ultimately afford them the best premium. Information systems can be complex assemblies of components provided by vendors and service providers who might not even be aware of each other, and the systems might be installed on virtual and physical servers anywhere in the world. The terms for coverage and the resulting costs can be difficult to establish and understand.

For example, the coverage effective date for a cyber insurance policy is more critical and less clear-cut than that for health or property coverage. In contrast to storm or fire damage, cyber incidents can go undetected for more than a year. Given the time it can take to discover and patch critical vulnerabilities, years may pass before the real effects from an incident are felt. An overall strategy is needed—one driven by transparency in terms of standards and expectations.

The Investment Gap

Framing cyber risk in a standardized manner lays the foundation for understanding how developing new processes and tools or improving existing ones can or should affect the decision and/or actions to buy insurance. Both underwriters and InfoSec professionals need to get their bearings on common cost elements—the investment (from the InfoSec side), and the cost and coverage limits and sublimits (from the cyber insurance side)—so that organizations can evaluate the potential return on their investment in cyber insurance.

Decision Makers: To Buy or Not to Buy

A decision to purchase cyber insurance is rapidly becoming a de facto business decision. Executive management and boards of directors are highly motivated to buy cyber insurance, given U.S. Security and Exchange Commission (SEC) guidance for public companies (as well as creating a standard for private companies) and high-profile breaches resulting in executive shake-ups and shareholder suits against directors and officers. Thirty-six percent of respondents are involved in purchasing cyber insurance. Of these, 47% were either executives (CEO, CFO) or senior management from both security (CSO, CISO) and IT (CTO, CIO). The majority (88%) of brokers report that their clients engage senior security management (CISOs) in insurance purchasing decisions, but only 15% report that CISOs have "much" influence over those decisions.

TAKEAWAY:

Make sure the CSO or CISO is engaged in the recommendation for buying cyber insurance and an assessment of how this coverage may affect your organization's cyber security posture, which includes both the enablers (e.g., pre- and post-breach services) and the possible barriers (e.g., unnecessary investments in new technology or processes).

According to one Advisen Broker Survey respondent, "The more sophisticated clients engage the CISO in the renewal process. Usually, if the CISO is involved, it indicates the client has a better handle on cyber risk."

The roles involved in making the recommendation to buy cyber insurances, as well as those making the final decision, are shown in Table 3. Executive management is the dominant role for both recommending and buying cyber insurance. The risk manager, senior security management (CISO or CSO) and legal counsel all play a significant role in developing recommendations for cyber insurance but, as Table 3 shows, individuals in the C-suite make the ultimate decision on buying a policy.

Table 3. Roles in Decisions About Buying Cyber Insurance

Role	Recommend	Decide
Executive management (CEO, CFO, COO, President, VP, AVP)	63.3%	50.0%
Risk manager	36.7%	1.7%
Board of Directors	33.3%	25.0%
Legal (internal or external counsel)	30.0%	8.3%
Senior security management (CSO, CISO, director)	30.0%	5.0%
Compliance officer or auditor	23.3%	3.3%
Senior technical management (CTO, CIO, director)	18.3%	1.7%

InfoSec professionals have a substantial influence on how the insurance industry assesses risk. Most underwriters (71%) said their company has InfoSec professionals on staff or a contract with an InfoSec firm to provide technical expertise.

—Advisen Underwriter Survey

However, the majority (72%) still do involve security professionals in the decision-making process leading to the purchase of cyber insurance. Of these, 42% engage their CSO/CISO and internal security team in the decision-making process, with another 22% augmenting their internal staff with external consultants as needed (See Figure 11).

Does your company engage the services of security professionals in making the decision to buy cyber insurance?

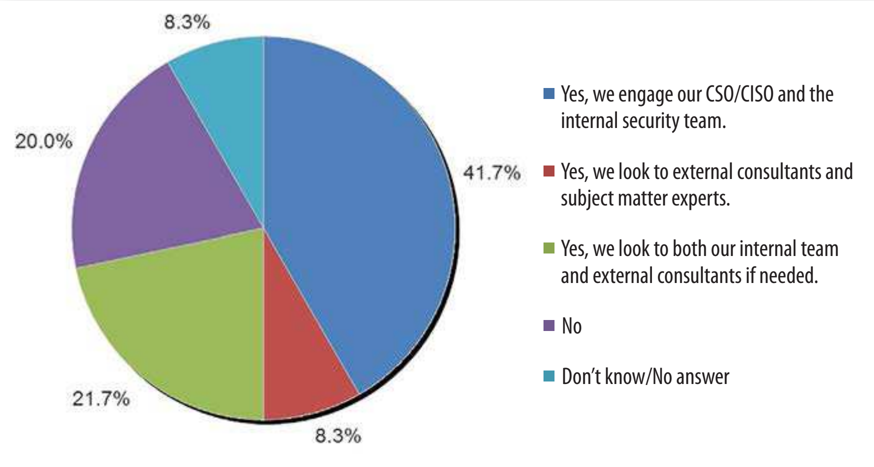


Figure 11. Engagement of Security Professional in Cyber Insurance Procurement

The Communication Gap

Communication is key to understanding the challenges associated with cyber insurance. Two key gaps exist:

- **Between information security and enterprise risk management.** Many organizations have been slow to include IT as part of the risk management process. Risk managers typically do not understand InfoSec, and senior security managers, such as CISOs, may not understand what insurance covers, its purpose or how it works. The risk manager should be a member of any enterprise InfoSec team. The CISO should be on any team charged with evaluating and purchasing cyber insurance.
- **Between information security and the C-suite.** Senior security management must play a key role in effectively communicating to the C-suite concerning threats, attacks, defensive technologies and risk-mitigation strategies. Does the board understand the threats that target the business? Do the executives understand the factors that increase the potential attack surface for a specific threat, either through a technology decision (e.g., adoption of social networking) or a change in business strategy (e.g., acquisitions and mergers)?

Toward Better Understanding: Common Terminology

Only 38% of respondents involved in the decision to purchase cyber insurance believe there is a common language of cyber risk between themselves and their insurance representative, and 55% say they lack a common language with which to communicate about cyber insurance.

Interestingly, most respondents (62%) think that they, personally, understand the role of cyber insurance well or very well—in fact better than their management team, where only 42% are believed to understand the role! Although the majority (64%) is not involved in the process of purchasing insurance, their executive management is involved in the recommendation process.

A Starting Point: The Definition of Risk by Two Communities

Information Security Community: Risk is "the possibility of suffering harm or loss,"[10] the product of threats and vulnerabilities.

Insurance Community: Risk is "uncertainty arising from the possible occurrence of given events.[11] 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)."[12]

Understanding and Quantifying Risk

There are vast differences in the way InfoSec and insurance professionals approach risk, starting with its definition. The insurance industry tends to focus on uncertainty or probabilities, as illustrated in the results from the Advisen Underwriter Survey in Figure 12.

Which of the statements below comes closest to your definition of "risk?"

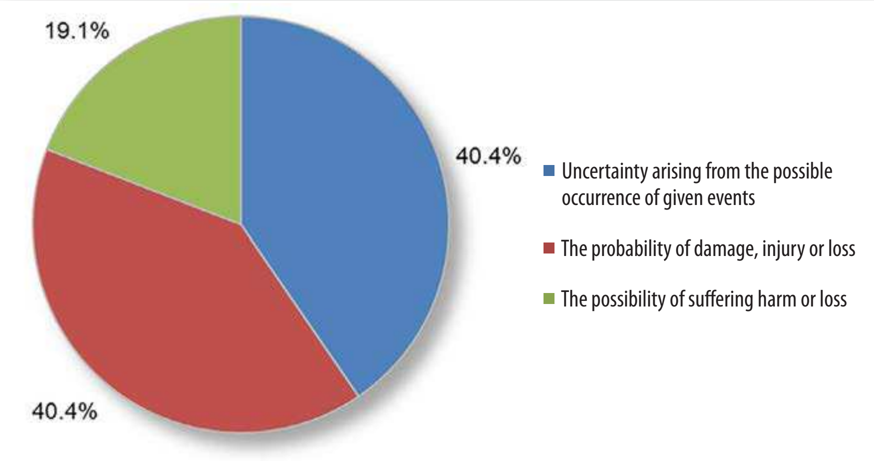


Figure 12. Underwriter Definitions of Risk

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

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

[12] "Quantifying Risk: Closing the Chasm Between Cybersecurity and Cyber Insurance," www.sans.org/reading-room/whitepapers/analyst/quantifying-risk-closing-chasm-cybersecurity-cyber-insurance-36770

We asked InfoSec respondents for their definition of risk using open-ended responses. We found that the answers reflect the time-honored InfoSec definition of risk as "risk equals threat times vulnerability." A word cloud created from the InfoSec open-ended responses in the survey, shown in Figure 13, reflects this definition. The word *financial* appears relatively fewer times than words such as *risk*, *threat*, *vulnerability* and *loss*.

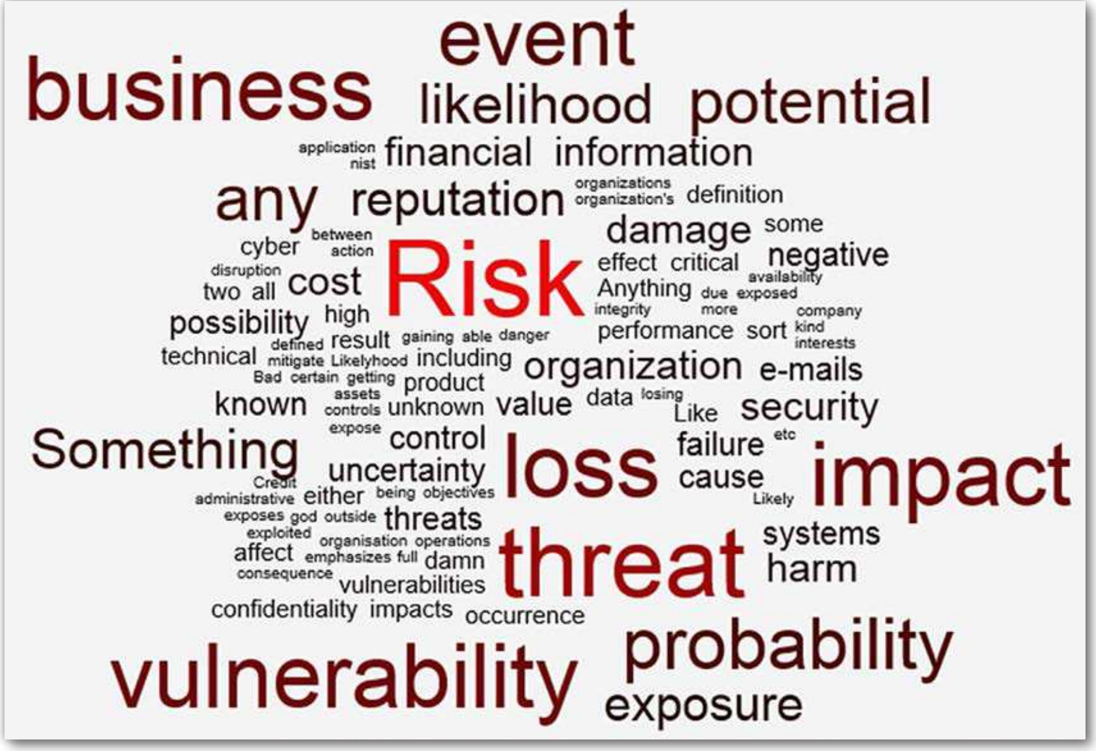


Figure 13. Word Cloud of Open-Ended Responses Defining Risk

While all respondents said it is a priority to manage "risk," the meaning of the term can be very different for underwriting managers, desk underwriters, corporate risk managers and InfoSec professionals. From an insurance management perspective, risk has little to do with whether any specific insured organization experiences an InfoSec event; it is a certainty that many will. Instead, risk is about whether the aggregate premium charged for all insureds is adequate.

InfoSec is the province of senior security management—the *CISO*. Insurance is the province of the *risk manager*. Each role represents a different necessary perspective on how risk is defined. The common denominator linking the two viewpoints is the organization's financial loss or, more specifically, its likelihood.

The role of the CISO is to reduce InfoSec risks, focusing on reduction of vulnerabilities and management of threats, which, in turn, reduces the likelihood of a breach. Ultimately, this reduces an organization's potential financial loss, from both quantifiable (i.e., dollar value) and qualitative (i.e., reputational) perspectives.

TAKEAWAY:

Strive to achieve a common understanding of cyber risk and the language used to express key concepts among your InfoSec team, your corporate risk manager, your insurance broker and your cyber insurance underwriter.

The risk manager, on the other hand, has a much broader role. This individual specializes in identifying any potential risks to the profitability or existence of an organization. The risk manager identifies and assesses potential causes of accidents or loss, recommends and implements preventive measures, and devises plans to minimize damage if things go wrong, including obtaining insurance coverage. Purchasing insurance transfers the risk of financial loss from the organization to the insurer in exchange for payment of a premium.

The need for a common language is echoed by both the Advisen Broker and Underwriter surveys. The insurance industry sees room for improvement in communicating with InfoSec professionals about cyber risk. Only 19% of brokers and 30% of underwriters said there is a common language of cyber risk.

This, in itself, is not too surprising, because the cyber insurance sector lacks a common language of cyber risk. Cyber insurance is comparatively new, fast-growing and rapidly changing, leading different insurers to use language inconsistently from policy to policy. The Centre for Risk Studies at Cambridge University has taken on the task of trying to sort out the language confusion in the cyber insurance sector, publishing the *Cyber Insurance Exposure Data Schema v1.0*, which was developed in conjunction with various insurance organizations (though with no apparent InfoSec input) with a stated goal to "provide a [schema] framework for exposure-related dialogues for risk managers, brokers, consultants, and analysts."[13] Note: Those dialogues also should involve InfoSec professionals.

The Terminology Gap

A common risk framework must rely on a consistent vocabulary that allows the in-depth conversations needed to establish cyber risk profiles that will underlie any cyber insurance policy.

The definition of risk is fundamental to how each stakeholder approaches the problem. A security professional will attempt to manage the risks he or she can control at almost any cost, while a risk manager will accept a negative outcome if the cost is within expected parameters. Insurers expect to pay claims and are primarily concerned about the consequences of not charging adequate premiums across their entire portfolio of policyholders.

The first step in closing this gap must be to establish a common terminology that allows the two communities' various stakeholders to communicate clearly and accurately about their expectations and actions, especially as they relate to possible regulatory and legal actions.

[13] Centre for Risk Studies at Cambridge University, "Cyber Insurance Exposure Data Schema v1.0," http://cambridgeriskframework.com/getdocument/38

Where to Go from Here?

To bring some transparency to the issues surrounding cyber insurance, SANS wondered whether respondents would view state and federal involvement as helpful. Only 29% of respondents felt a market-driven approach was desirable. Respondents asked for regulators to step in to define due diligence and standards as well as to clarify existing regulations, although they were more reluctant to have regulators actually require procurement of insurance or provide a common floor as they do with the National Flood Insurance Program. See in Figure 14.

In what areas should state and federal regulators get involved with cyber security insurance?
Select all that apply.

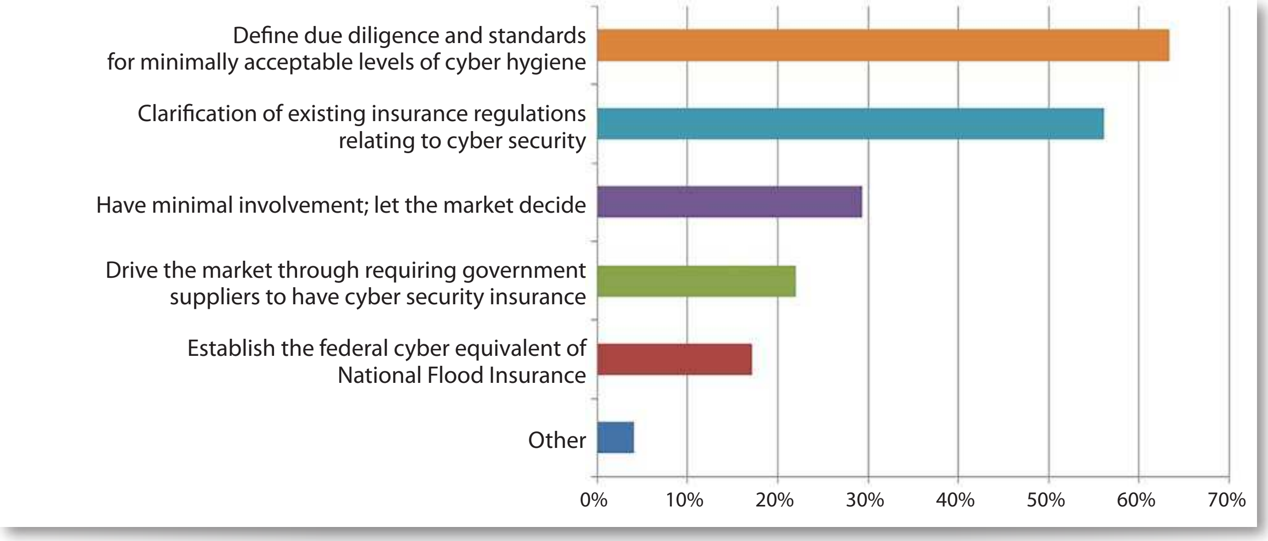


Figure 14. Involvement of Regulators in Cyber Security Insurance

Insurance is regulated at the state level, so we have little reason to expect much guidance from the federal government on standards for cyber insurance. In fact, the federal government has looked to the insurance industry to set and enforce standards for cyber security. According to the U.S. Department of Homeland Security, "A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection."[14]

[14] "Cybersecurity Insurance," www.dhs.gov/cybersecurity-insurance

So far, state regulators, who generally are more concerned about protecting consumers than businesses, are taking a wait-and-see approach as the market develops. It seems likely that the courts will be the governmental bodies that will shape the cyber insurance industry. In practice, the actual definition of risk assumed under an insurance policy depends on the language in the policy. Each cyber insurer tends to use different policy language. Two different insurers may think they are covering the same risk, but they may not be because they use different words to describe the risk. As relatively few claims have been made against cyber insurance, we know very little about how the actual interpretation of the words affects the recovery of loss. But we do know that differences in expectations and interpretations between insurers and customers inevitably lead to disputes and litigation. For more on this topic, see Appendix A: "Cyber Insurance Policy Words and Negotiation."

Setting the due diligence and minimally acceptable levels of cyber hygiene, as the California attorney general did in her February 2016 "California Data Breach Report,"[15] may be the practical way to proceed. As security professionals, we strive to deal in "clear and measurable" requirements that realistically reflect what can be considered securable (and therefore, in our minds, insurable) in as transparent a manner as possible. The concern expressed by one respondent is that "because governments are only responding to compliance requirements, we need basic hygiene requirements; else we'll likely never get there," meaning being able to actively prevent and protect against the threat.

Governmental or regulatory policy can set the basic floor by focusing on flexible standards that allow the cyber security and insurance markets to evolve, rather than legislating strict measures that can quickly become outmoded. Both the cyber security and insurance communities need to have breathing space that allows them to mature in the light of constantly evolving threats and the increasing potential for widespread catastrophic damage. The viewpoint needs to be broad rather than narrow, focusing on adaptable methods to close existing gaps and address new ones, rather than thinking that the work is done after the first bridge across the present chasm has been built.

[15] https://oag.ca.gov/breachreport2016

Appendix A
Cyber Insurance Policy Words and Negotiation

Cyber insurance is not a commodity. It is a custom-tailored service, shaped by both legal and business practices—practices that can be hard to evaluate. In any given instance, the outcome of these practices reflects complex negotiations that span many months or years. There is the negotiation of the words of the policy contract itself. And there is also the negotiation of the business relationship among the broker, the insurer and the customer.

Immature Market

Today, these negotiations are transpiring in a nascent market. The market is confused about what risks should and should not be covered under a cyber policy. Unlike the risks of fire and flood that apply to physical property, cyber risks are evolving very rapidly. A lawyer can try to define in the words of a policy which risks are covered, but technology can quickly render those words obsolete.

So, for example, the words written into a policy can appear to cover unauthorized electronic funds transfers, but when hackers concoct a new way to cause an unauthorized transfer—such as executive email spoofing—the insurer interprets the words of the policy as not covering that kind of unauthorized transfer. See the currently pending lawsuit *Medidata Solutions Inc. v. Federal Insurance Co*.

Words of Policy Ambiguous

By definition, insurance covers risk in the future. But in InfoSec the future is hard to predict and articulate in the words of a written policy. Technology changes constantly, the threats change and the perceptions for minimum cyber security standards change. Moreover, all of this change causes confusion over when a customer possesses enough evidence of a cyber incident that it is required under the wording of a cyber policy to notify the insurer about the incident.

Court cases interpreting the words in cyber policies are few. As a consequence, virtually any claim under a cyber policy can be disputed and litigated—for years and at great expense—through the court system.

Risks to Negotiate

Insurers must put limits around coverage. They can't just cover "all loss or damage related to unauthorized performance of computers." That would embrace far more risk than can be underwritten.

Yet it is hard for customers, even with the help of experienced insurance coverage lawyers, to articulate what they want the cyber policy to cover. They want the risk of loss or damage covered, but it is hard to see far enough ahead to realize they want to cover (for example) an email spoofing attack that causes an unauthorized funds transfer. At the time the policy is written, such an attack may be rare or nonexistent.

Granted, a good insurance coverage lawyer can help a customer understand gaps in coverage offered in a proposed policy. But typically the lawyer does this by comparing policies that have been written in the *past* to identify what is not covered in the proposed policy. Anticipating *future* risks and changes in technology is much harder for the lawyer to do.

If the customer cannot see far enough into the future to know what coverage to ask for, the customer is unlikely to get that coverage written into the policy.

Effectiveness, Relationships and Reputation

Given these difficulties, the actual outcome of a particular policy often depends on subjective business practices. For example, during the term of the policy a claim might arise that is not clearly covered by the words in the policy. The broker may lobby the insurer to cover the claim anyway because the broker wants to maintain the customer's trust. For its part, the insurer may decide to pay the claim—even though it could avoid coverage if the topic were disputed and litigated—because the insurer wants to maintain its relationship with the broker, or because the insurer wants to project a good reputation in the marketplace.

Accordingly, for the customer, negotiation of an effective policy entails more than employing a good lawyer to negotiate for and write the best wording into the policy. It also entails cultivating and maintaining good relationships with the broker and the insurer.

Conclusion and Takeaways

Cyber insurance is an imperfect tool for managing risk. But it can be useful. A cyber policy is more likely to be useful to a customer that follows these steps:

- Strive to develop and maintain strong relationships with a broker and an insurer that have excellent reputations and qualifications.
- Retain the services of a qualified insurance coverage lawyer who can help to explain and negotiate the words written into the policy.
- Educate senior management and the board of directors about two things: 1) cyber insurance is, in fact, imperfect; and 2) therefore, management and the board should allocate more resources for substantive security (that is, InfoSec staff, training, tools and services).

Appendix B
Information Security and the Corporate Risk Manager

Risk managers are the insurance buyers in larger organizations. For some risk managers, conducting risk assessments, buying insurance and managing insurance programs comprise the majority of their day-to-day activities. Other people with the risk manager title have broader risk mitigation responsibilities, such as implementing health and safety measures, and creating and maintaining business continuity plans.

To better understand the role of risk managers in InfoSec programs and their perceptions of cyber insurance, Advisen, with the sponsorship of Zurich Insurance, has interviewed risk managers annually since 2011. Some of the key findings of the most recent survey (2015)[16] include:

- In 2011, cyber insurance was still a novelty to many risk managers, and relatively few companies bought cyber policies. In 2015, more than 60% of companies participating in the survey were insured.
- Not all risk managers are in favor of buying cyber insurance. Price, breadth of coverage and low exposure to cyber risk were considerations noted by respondents who did not buy policies.
- More companies are viewing cyber security as an enterprisewide issue that requires a multidepartmental approach. In 2015, 57% of respondents claimed their organization has a multidepartment InfoSec risk management team or committee.
- Of the companies that have cross-departmental teams, 78% include a representative from the risk management department on the team.
- In 12% of organizations, the risk management department has primary responsibility for spearheading the InfoSec risk management effort.
- Boards of directors now view cyber risks more seriously. The boards of 68% of respondents viewed the cyber environment as a serious concern in 2015, 4 percentage points higher than in 2014 and 23 percentage points higher than the first survey in 2011.

[16] "2015 Information Security and Cyber Liability Risk Management," www.advisenltd.com/2015/10/16/information-security-cyber-liability-risk-management

Cyber-related insurance coverages have been in the marketplace since the late 1990s, but cyber insurance remains a challenging topic for many risk managers. This is, in part, a result of complex cyber insurance policies with coverage features that are materially different from other types of insurance policies. "We have cyber liability insurance coverage, but I am not sure what it covers," confessed one survey respondent. To add to the confusion, policy language and specific terms and conditions vary substantially from policy to policy.

Cyber insurance also is challenging to risk managers because few have a solid grounding in information security. This lack of InfoSec knowledge makes it "difficult to get your hands around what a potential loss may be in order to make informed decisions around the purchase of coverage," according to a survey respondent. Another risk manager lamented, "I feel inadequately knowledgeable to understand the specific cyber risks my company could experience."

By necessity, risk managers rarely operate alone when purchasing cyber insurance. At the very least, they need to engage the IT department and corporate InfoSec professionals to fill out often complex and detailed application forms and to meet with underwriters. Risk managers complain, however, that it can be difficult to get the willing cooperation of InfoSec professionals who don't always see value in cyber insurance.

As cyber insurance gains acceptance and comes to be widely viewed as an essential component of an organization's security strategy, CISOs and other InfoSec professionals will be increasingly engaged throughout the insurance procurement process. It is, therefore, essential that risk managers and CISOs communicate through a common language of risk, and that their priorities and objectives are aligned. Risk management participation in an organization's InfoSec initiatives throughout the year can help facilitate this process and can create opportunities to blend complementary areas of expertise, resulting in a cohesive and more comprehensive, end-to-end InfoSec strategy.

About the Authoring Team

Barbara Filkins, a senior SANS analyst who holds the CISSP and SANS GSEC (Gold), GCIH (Gold), GSLC (Gold), GCCC (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.

Benjamin Wright, a SANS senior instructor, practicing attorney and author of several technology law books, including *Business Law and Computer Security*, teaches the Law of Data Security and Investigations course for the SANS Institute. This unique five-day course trains security, forensic and legal professionals to cope with the risks surrounding data breaches, digital investigations, electronic discovery and technology contracts. With 26 years in private law practice, he has advised many organizations, large and small, on privacy, e-commerce, computer security, and email discovery. He has been quoted in publications around the globe, from the Wall Street Journal to the Sydney (Australia) Morning Herald. Benjamin maintains a popular blog at http://hack-igations.blogspot.com.

David Bradford, contributing author, is co-founder and chief strategy officer of insurance industry analytics provider Advisen, Ltd. Prior to co-founding Advisen in 2000, Dave spent 20 years in the reinsurance industry in underwriting, marketing and strategy-development roles. He was most recently a senior vice president with Swiss Re, where he led the Global & National Division of Swiss Re America, a $500 million profit center. Prior to Swiss Re, Dave was a senior vice president at Reliance Reinsurance Corp., where he founded and managed the special programs department. Dave began his career as an actuarial analyst and treaty underwriter with Allstate's Assumed Reinsurance Division.

Sponsor

SANS would like to thank this survey's sponsor:

PIVOTPOINT
RISK ANALYTICS

and our research partner:

Advisen
Transforming • Insurance℠

Last Updated: June 21st, 2016

Upcoming SANS Training

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

SANS Salt Lake City 2016	Salt Lake City, UTUS	Jun 27, 2016 - Jul 02, 2016	Live Event
SANS Cyber Defence Canberra 2016	Canberra, AU	Jun 27, 2016 - Jul 09, 2016	Live Event
MGT433 at SANS London Summer 2016	London, GB	Jul 07, 2016 - Jul 08, 2016	Live Event
SANS London Summer 2016	London, GB	Jul 09, 2016 - Jul 18, 2016	Live Event
SANS Rocky Mountain 2016	Denver, COUS	Jul 11, 2016 - Jul 16, 2016	Live Event
SANS Delhi 2016	Delhi, IN	Jul 18, 2016 - Jul 30, 2016	Live Event
SANS San Antonio 2016	San Antonio, TXUS	Jul 18, 2016 - Jul 23, 2016	Live Event
SANS Minneapolis 2016	Minneapolis, MNUS	Jul 18, 2016 - Jul 23, 2016	Live Event
SANS San Jose 2016	San Jose, CAUS	Jul 25, 2016 - Jul 30, 2016	Live Event
Industrial Control Systems Security Training	Houston, TXUS	Jul 25, 2016 - Jul 30, 2016	Live Event
SANS Vienna	Vienna, AT	Aug 01, 2016 - Aug 06, 2016	Live Event
SANS Boston 2016	Boston, MAUS	Aug 01, 2016 - Aug 06, 2016	Live Event
Security Awareness Summit & Training	San Francisco, CAUS	Aug 01, 2016 - Aug 10, 2016	Live Event
DEV531: Defending Mobile Apps	San Francisco, CAUS	Aug 08, 2016 - Aug 09, 2016	Live Event
SANS Portland 2016	Portland, ORUS	Aug 08, 2016 - Aug 13, 2016	Live Event
SANS Dallas 2016	Dallas, TXUS	Aug 08, 2016 - Aug 13, 2016	Live Event
DEV534: Secure DevOps	San Francisco, CAUS	Aug 10, 2016 - Aug 11, 2016	Live Event
Data Breach Summit	Chicago, ILUS	Aug 18, 2016 - Aug 18, 2016	Live Event
SANS Alaska 2016	Anchorage, AKUS	Aug 22, 2016 - Aug 27, 2016	Live Event
SANS Bangalore 2016	Bangalore, IN	Aug 22, 2016 - Sep 03, 2016	Live Event
SANS Chicago 2016	Chicago, ILUS	Aug 22, 2016 - Aug 27, 2016	Live Event
SANS Virginia Beach 2016	Virginia Beach, VAUS	Aug 22, 2016 - Sep 02, 2016	Live Event
SANS Brussels Autumn 2016	Brussels, BE	Sep 05, 2016 - Sep 10, 2016	Live Event
SANS Adelaide 2016	Adelaide, AU	Sep 05, 2016 - Sep 10, 2016	Live Event
SANS Northern Virginia - Crystal City 2016	Crystal City, VAUS	Sep 06, 2016 - Sep 11, 2016	Live Event
SANS Network Security 2016	Las Vegas, NVUS	Sep 10, 2016 - Sep 19, 2016	Live Event
SANS London Autumn	London, GB	Sep 19, 2016 - Sep 24, 2016	Live Event
SANS ICS London 2016	London, GB	Sep 19, 2016 - Sep 25, 2016	Live Event
Digital Forensics & Incident Response Summit	OnlineTXUS	Jun 23, 2016 - Jun 30, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced