Exploring the cybersecurity landscape

Insurance Governance Leadership Network

April 2014

EY
Building a better
working world

Tapestry
Networks

Insurance Governance Leadership Network
ViewPoints

April 23, 2014

TAPESTRY NETWORKS, INC · WWW.TAPESTRYNETWORKS.COM · +1 781 290 2270

Exploring the cybersecurity landscape: growing risk and opportunity

"We know we are not bulletproof. Our thinking has gone from 'if' to 'when.' We are just trying to ensure we are staying on top of new developments."

– Director, global insurer

Cybersecurity has frequently come up as a risk topic within the Insurance Governance Leadership Network (IGLN) since the network's inception in 2012. As the economic and reputational damage caused by security breaches has grown, the IGLN's discussions – which have included security experts and guests from supervisory and regulatory authorities – have grown more intense.

By most accounts, cybersecurity continues to ascend board agendas, though opinions differ as to the magnitude of the risk. Some insurance leaders and experts warn that attacks could represent a threat to a company's survival, while others assign a much lower importance to the threat. Although IGLN participants hold a range of views on the severity and immediacy of the risk, almost all agreed that cybersecurity is a matter for the boardroom and that insurers urgently need to catch up with other industries in monitoring and managing cybersecurity risks.

On March 4 and 20, IGLN participants gathered in London and New York, respectively, to discuss cybersecurity. Dialogue centered on the evolving threat, the risks posed to individual firms, the possible systemic risk, and how boards can best address cybersecurity issues. Participants also discussed innovative tactics for improving insurer defenses. For a list of participants, see Appendix 1, on page 13.

This *ViewPoints*[1] captures the essence of those conversations, centering on six key themes:

- Understanding the risks
- Establishing protective measures for internal systems
- Focusing on people, not just technology
- Moving beyond prevention to response
- Strengthening risk governance
- Realizing opportunities

Understanding the risks

The cybersecurity risk landscape is much more complex than many other risk areas. One director led the IGLN discussion by asking, *"Why is cybersecurity risk so different? Why can't we identify the problem and apply solutions?"* A risk chair noted, *"If it were simply a new form of fraud, it would be easier to address. It*

[1] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby names of network participants and their corporate or institutional affiliations are a matter of public record, but comments are not attributed to individuals, corporations, or institutions. Network participants' comments appear in italics.

can be [fraud], but in many cases you don't know what to expect, can't assess the damage, and don't know what the cost is." Participants identified the following complexities in the cybersecurity landscape:

Firms are not clear or consistent in their assessment of threat severity

When asked to describe the threat, some directors believed *"it could destroy the company,"* while others dismissed it as no more than *"low-grade problems that are embarrassing and [possibly] expensive,"* but nothing that would sink a company. Several participants noted that no major insurer had suffered a significant event such as has happened in banking and other industries. Participants at the two meetings differed significantly in their responses. In one meeting, the majority of insurers were of the opinion that their intellectual property was not vulnerable and that they could withstand service interruptions since they were not banks. In contrast, participants in the other meeting largely believed that the risk to their informational assets, including intellectual property and personal identifying information, was severe.

Threats vary considerably, but some are sophisticated and evolve rapidly

One expert noted, *"Anyone with a $500 laptop and an Internet connection is a potential adversary."* The most common sources of threat include organized crime, state actors, employees, vendors, and activists. Many actors are motivated by financial gain; others have political agendas. Most directors agreed with an expert who observed, *"In order to understand the threats, you need to understand the motivations and the actors."* Characterizing the greatest threat, one director said, *"[It] is not a solitary hacker at a terminal somewhere … These are sophisticated criminal operations with structures and serious budgets. They are looking for significant return on investment."* A recent report noted a disturbing trend: although there were fewer breaches reported in the first half of 2013 than in the same period in 2012, the amount of data lost was far greater.[2] This suggests that improvements in security may be succeeding in repelling the less advanced threats, but attackers continue to increase their sophistication. As the highly publicized and damaging breach at the US retailer Target shows,[3] attackers may use a combination of methods repeatedly to attack entities that offer the greatest payoff.

Emerging threats in the digital world

While cybersecurity risk as a whole is no longer considered an emerging risk, new threats continue to develop in the digital ecosystem. IGLN participants identified the following developing threat areas:

continued overleaf

[2] Risk Based Security, "More Than 462 Million Records Already Compromised in 2013," October 2, 2013.

[3] See, for example, Paul Ziobro and Danny Yadron, "Target Now Says 70 Million People Hit in Data Breach," *Wall Street Journal*, January 10, 2014.

Emerging threats in the digital world *continued*

- **The cloud.** *"What exactly is the cloud, and when do 'cloud risks' come into play?"* one non-executive asked. Cloud computing refers to the outsourcing of data and applications to third-party Internet servers and can be used for storage or computing purposes. In addition, third-party employees, who are not subject to the same standards as the insurer's own employees, may review, manipulate, and analyze the information. Data that is stored in the cloud is typically not housed in physical locations controlled by the insurer. Cloud facilities may change over time, and cloud providers may, in turn, outsource information and services to other providers or locations.

  For insurers, the cloud may represent a means to achieve greater efficiency, flexibility, time to market, and cost savings for core processing functions (e.g., policy, claims, and billing) as well as a means to explore data analytics and growth in new markets. However, when firms transfer services and confidential data to vendors, they lose some control over information security. Insurers need to structure contracts to ensure providers comply with legal requirements and privacy rules, account for physical, cyber, and other risks facing the provider, and address the potential for data loss.

- **The Internet of Things**. Defense against cybersecurity risks demands protection of an ever-widening perimeter as the sources of potential threats grow. "The Internet of Things" refers to products within the physical world, such as cars, thermostats, and healthcare devices, that are connected to the Internet and to each other. Frequently these devices can communicate, transfer, or control other connected devices. In January 2014, a security company confirmed what may be the first known phishing[4] attack featuring home routers, televisions, and at least one refrigerator.[5]

- **Fragmentation**. Some experts warn that growing fears about interconnectivity, as well as revelations about government spying, could provoke greater isolationism and fragmentation of the digital world. German chancellor Angela Merkel has recently called for a European Internet, walled off from the United States.[6] *"What if the European Central Bank decided all data had to be stored in Europe? What would that do to commerce?"* one director asked. Likewise, protectionist or poorly coordinated policy development could damage operations and lead to lost opportunities.

Risks manifest directly and indirectly

For insurers, cybersecurity risks can manifest as direct threats to the enterprise, as unknown or poorly defined sources of risks within existing policies, or as risk to the broader financial system. One director said, *"They attack us for information or money, and they attack our clients, and we may be in the liability chain.*

[4] Phishing is the act of attempting to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

[5] "Spam in the Fridge: When the Internet of Things Misbehaves," *Economist*, January 23, 2014.

[6] Jeevan Vasagar and James Fontanella-Khan, "Angela Merkel Backs EU Internet to Deter US Spying," *Financial Times*, February 16, 2014.

How well do we really understand the direct and indirect threats?" A chief risk officer (CRO) agreed: *"I do think there is liability in existing books of business that is not well understood, particularly in the reinsurance and commercial-lines space. Insurers may not know or clearly understand the risks already on the books."*

While most directors were focused on the threats to the company, several recognized the threats inherent in being part of the broader financial system. One CRO said, *"Insurers are linked to banks via the clearing functions, so we also have to be concerned about potential service interruptions for our own customers. The supply chain is important."* While many insurers do not believe they will be targeted as banks have been, the financial system is highly interconnected and therefore vulnerable. Governments have increased investment in cybersecurity for the financial system because it is viewed as critical infrastructure. Insurers are an integral part of that system and stand to be adversely affected if vulnerabilities elsewhere in the system are exploited.

Sources of vulnerability will increase over time

The increasing digitization of insurance continues to extend the borders that must be defended, with one expert observing, *"Today anything of value is pushed onto the corporate network."* This intensifies information security problems, as ways to access these networks are increasing exponentially – for example, through employees' personal devices, which can connect to company systems, creating additional vulnerabilities. This heightened vulnerability makes it harder to protect customer data. One director asked, *"Can we ensure anything the customer shares with us is safe? That is our obligation; it is also what many regulators seem focused on."*

Cybersecurity challenges defy simple quantification

Many executives and boards want to quantify and measure the risk posed by cybersecurity threats. How often do attacks materialize? What is the financial impact? *"What is the value of intellectual property? Lost productivity? None of this is clear,"* said one expert. These things are very difficult to measure accurately, though several participants noted that insurers are in the business of measuring difficult risks and should be well positioned to do so. Even for insurers, accounting for less tangible hazards, such as reputational damage, can be exceedingly difficult, and there is a risk of undervaluing assets or underestimating the cost of an attack.

One director described the risk of a cyberattack as *"like a chronic disease. You manage it; you can't ever cure it. We need to learn to live with it."*

Establishing protective measures for internal systems

Board members acknowledged the need to establish basic practices and processes to prevent cybersecurity breaches and to mitigate them when they occur. Insurers' legacy systems, typically a patchwork resulting from numerous mergers and acquisitions, are difficult to protect. For many participants, an important step has been accepting that systems will ultimately be breached and moving from a sole focus on prevention to mitigation and response. Practically, this means that insurers need to prevent the data that matters most from leaving their systems and develop a defensive plan for dealing with intrusions.

IGLN discussions identified a number of practices insurers view as necessary, though not sufficient, to establish an effective cybersecurity defense strategy:

Identify and protect key assets

Experts refer to these assets as *"crown jewels"* or *"trophies."* One CRO noted, *"You can't lock down systems entirely. [What] is essential?"* Having acknowledged that some data will ultimately be taken or manipulated, it is most important to concentrate security efforts on core assets and systems. *"The trophies are money, personally identifiable information, and business intelligence,"* said one expert. Companies must also identify their unique assets. Internal systems related to underwriting, claims, or models could contain important intellectual property. When identifying assets, one expert challenged directors to think beyond simple theft. What consequences will data corruption have? What if human resources, payment, or claims systems are rendered inoperable or otherwise compromised? One executive acknowledged, *"We have to have a clear understanding of which applications carry customer data and how data is carried. Inventorying our systems for this kind of information is a monumental task."* Appendix 2, on page 15, provides a more thorough list of targets, threat actions, and actors and motivations.

Ensure rigorous IT hygiene

Are insurers successfully maintaining basic practices such as updating patches and enforcing controls? One chairman observed, *"Most risks are self-inflicted. There is a lack of clean-desk regulations and policies on encryption and transportation of data. What are the rules on hardware, data sticks, use of equipment? Maybe the policies are there, but they are not enforced; procedures are lax."* One CRO remarked, *"Within the product environment, serious mistakes can be made. For example, what if an individual gets a view of someone else's account information?"* Increasing reliance on technology and the complexity and interconnectedness of financial-sector systems raise the probability of mistakes and lapses. Notably for insurers, supervisors are very focused on this issue as well: *"Insurance does not have a great record for IT excellence. The industry creates its own problems. We are conscious of that,"* remarked one supervisor.

Use "smarter" security measures

One expert said, *"Defense in depth is a baseline. That is a defensive posture that is layered."* Systems should be partitioned, so that if they are penetrated, they are difficult to navigate and difficult to exit. One participant likened it to building a maze, rather than a higher wall. The expert continued, *"More advanced companies are also looking into behavior-based security rather than permission-based."* Behavior-based security requires analysis of system usage: *"A person may have legitimate access to a system, but are they using that access inappropriately? Others may not have access to the system, but strange usage patterns or behavioral patterns can alert you to problems."*

Though it is tempting to focus on the latest technologies, smarter security may also involve simplification. One director reported, *"We are consolidating data centers. There will be fewer scattered parts. It will improve security and cost."*

Regularly test system vulnerability

Most participants indicated that their organizations used third parties to test system integrity through penetration testing. These tests can be straightforward penetration attempts, with the results reported to management and the board, or they may be elaborate war games that engage employees in active defense and response. One director asserted, *"If you are not doing cyber war games, you are not competitive."*

Be alert to changes in your risk profile

Several IGLN participants pointed out that major events, such as mergers, acquisitions, new market entry, organizational changes, or other headline-grabbing episodes, can increase cybersecurity risks. *"We are going through tremendous change within the organization. We have structural changes and significant systems changes ahead in the next 18 to 24 months. Obviously that puts us at greater risk,"* noted one director. A CRO highlighted how a high-profile sponsorship was causing the company to rethink how it might be targeted. An EY report outlines points of vulnerability throughout the business life cycle.[7]

Focusing on people, not just technology

"Fundamentally, cybersecurity is a people problem. People create the problem. People will fix it. Without good people, your technology doesn't matter," said one expert. As cybersecurity practices mature, insurers are increasingly focused on the human elements of security. These include the threats posed by employees and vendors, the importance of internal and external capabilities and expertise, and the role of intelligence sharing.

Employees are creating new cybersecurity risks

Employees can present a threat both through simple negligence and through deliberate malicious action. One audit chair remarked, *"I suspect most firms are aware of the danger of the insider threat. I think it is viewed as high severity, low probability – at least you hope it is low probability."* Insider threats can originate with disgruntled or opportunistic employees, or even with criminals placed within organizations. One subject matter expert acknowledged how difficult it is to address the threat: *"The insider threat is a real problem. You need to use [human resources], psychology, and tech [to monitor]."*

While malicious insiders may be the most sinister threat, most participants agreed that simple negligence or lack of awareness contributes to the majority of employee-related problems. Despite education, many employees remain unaware of the dangers of opening a phishing email or suspicious attachment. One director remarked, *"We are providing more education – be careful with emails, attachments, transmitting files, etc."*

The growth of third-party vendors increases risks exponentially

As heavy users of third parties for a variety of functions throughout the activity chain, insurers absolutely must develop robust protection against third-party threats. One chairman noted, *"If you sign a contract*

[7] See EY, *Under Cyber Attack: EY's Global Information Security Survey 2013* (London: EYGM Limited, 2013).

[with a vendor] without securing full access for your internal auditor or IT to review protocols, you are creating the problem." A director observed, *"We need to understand that we are dependent on the third parties we know, as well as the ones we don't, but that have a relationship with our customers. If AT&T is a customer's mobile provider, we have a relationship with AT&T."* One expert challenged, *"Do you ever think about whether you represent a vulnerability to others? Are you part of a bancassurance model? Can criminals get to the bank through you?"*

Insurers must balance reliance on internal and external security resources

"Are companies better off relying on ourselves or relying on outsourcing for protection?" asked an executive. Most participating insurers use some combination of both. Security personnel need to understand both cybersecurity and the business, which means a strong internal team needs to be in place, even if a company outsources heavily. However, building sufficient in-house expertise outside of the organization's core competencies is difficult and expensive. One director asked, *"Do the best and brightest go into security in an insurance company – especially smaller companies? How do you get the talent you need?"* An executive echoed this concern noting, *"Most insurers are in the same boat. When it comes to IT, you need programmers desperately, so you hire anyone qualified."*

One director came out strongly in favor of outsourcers:

> *I've certainly done security both ways. Outsourcers are constantly training and trying to stay ahead. They coordinate well with the various sectors and information sharing and analysis centers. Most of the outsourcers are large enough that they could put feet on the ground to deal with most issues, or could source the right people. If you do it yourself, it typically starts off well, and five or six years later your people are stale. How much are you willing to spend on training? Can you provide continual training and move employees up fast enough to keep them sharp?*

Intelligence sharing across organizations is important but constrained

Although banking and other sectors rely on intelligence sharing as a means to combat attacks, IGLN participants questioned the degree to which insurers will follow suit. Most participants representing US-based insurers noted their organizations participate in the Financial Services Information Sharing and Analysis Center, a formal organization that promotes intelligence sharing within the financial sector and with the public sector.

One director spoke for several when he said, *"I wonder how successful we could be at information sharing. Our natural instinct in the sector is to not talk about problems. How do you change that attitude?"* Numerous participants acknowledged the challenge in building robust exchanges, specifically the legal barriers to information sharing, government agencies' inability to share classified information, and sensitivities around proprietary client information. Furthermore, when intelligence is shared, communication tends to happen ad hoc via email, and may not be shared in real-time or in an automated fashion.

Moving beyond prevention to response

Given that no defenses are perfect, *"it is important that a company have a process in place to quickly identify that a breach has occurred and have effective recovery plans in place."* Defining an appropriate response to an unknown event poses significant challenges. Even so, participants agreed that insurers should have a basic and adaptable strategy in place so they are not in the position of having to create a plan in the midst of an unfolding crisis. In that regard, several directors noted the importance of scenario exercises that test and evaluate a company's ability to respond. Participants identified the following elements of a proactive incident response strategy:

- **Quickly define loses.** Though cybercrimes often defy easy accounting, participants stressed the importance of defining and understanding the losses as quickly as possible. Referencing a recent US event with a major retailer, one director noted, *"What we don't want to do is say it is 40 million records lost this week, and come back in two weeks with a bigger estimate."*

- **Understand legal requirements.** Legal disclosure and breach notification requirements vary significantly by jurisdiction. In the United States, there is no federal standard for loss of personal information, but companies may face Securities and Exchange Commission filing requirements as well as requirements from the individual states and territories.[8] The European Parliament and EU Council are currently negotiating more stringent data-protection regulation, which would require notification of authorities "without undue delay."[9] Any incident response plan should anticipate different legal requirements.

- **Identify and engage necessary partners.** Depending on the nature of the event, companies may need to engage multiple partners in a response. Insurers may need to secure vendors to implement crisis control plans, analyze breaches, implement new security measures, provide additional services, such as credit monitoring, to customers, or rebuild compromised systems. Identifying crisis services and providers in advance of incidents will improve response time and effectiveness.

- **Develop a clear communications strategy.** Notifying authorities may be an appropriate first step, but an effective response requires ongoing communication with a variety of stakeholders. Boards must determine the content of the communications and methods for disclosing information to investors, regulators, customers, and the public.

Strengthening risk governance

Only a small number of IGLN director participants have had experience with cybersecurity breaches. Limited experience, combined with a lack of consistent frameworks or expectations for board involvement, could worsen the impact of a breach. IGLN conversations highlighted several areas for improvement.

[8] National Conference of State Legislatures, "State Security Breach Notification Laws," January 21, 2014.

[9] European Parliament, *Report on the Proposal ... Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union* (Brussels: European Parliament, 2014), 53.

- **Ensuring sufficient time and attention is paid to cybersecurity risk.** Directors agreed that boards need to devote time and resources to understanding the cybersecurity challenges, but practices differ widely across the industry. They recommended that one committee, typically audit, risk, or information technology, own cybersecurity risk to ensure due attention and focus. Most insurers also use a shared reporting structure, which spans multiple committees, to address areas of overlapping responsibility such as internal controls. Participants reported increasing attention to cybersecurity risk among committees and the board in the last 18 months, estimating that committees are discussing cybersecurity between three and six times per year, and full board discussion often twice a year.

- **Providing effective challenge to management.** Since most directors do not have direct experience with information technology or security, effectively challenging management can be difficult. One director noted, *"We've thought about bringing more IT experience into the board for security and for strategy."* Some boards have begun to use board recruitment to enhance governance in this area. Others have focused on board training. Appendix 3, on page 17, provides a short list of key questions for directors to consider.

- **Coordinating the approach to controls.** Many insurers have not yet determined the best approach to managing cybersecurity risk across IT, internal audit, risk, and compliance functions. Since cybersecurity risks can involve vendors, employees, and customers, other key functions, such as human resources, legal, and underwriting, may also need to be involved in a coordinated control effort.

- **Embedding cybersecurity risks into enterprise risk management frameworks.** A recent EY report noted that 62% of surveyed organizations have not aligned their information security strategy with their risk appetite or risk tolerance. As a result, "too few organizations consider the cyber risks they are prepared to accept or must defend against at all costs."[10] One director said, *"We should be able to say, 'Here's my risk appetite. Here's how I justify spending.' How do we help management make rational decisions? It seems to me that there isn't the same discipline yet around this risk as there is for others."* Most large firms have a single point of accountability – increasingly the chief information security officer (CISO), but sometimes the chief information officer or CRO. That individual is usually highly positioned within the organization, often reporting to the CEO. One expert said, *"The CISO needs to be at a high enough level to communicate important information to the right people. I've seen a variety of models. I'd suggest that burying the CISO [or other responsible officer] five levels down is not the right approach."* One executive stressed, *"Cybersecurity requires an enterprise solution. People need to see it as their job, not someone else's."* An expert agreed, saying, *"In a major event, everyone will fail, not just the CISO."*

- **Developing more effective performance measures.** As with other operational risks, the challenge for management is how best to quantify cybersecurity risks and responses. Increasingly, board members are challenging management to produce better metrics and benchmarks that demonstrate improvement in

[10] EY, *Under Cyber Attack: EY's Global Information Security Survey 2013,* 7.

security programs. They also seek a more robust quantitative basis for decision making and resource allocation.

Realizing opportunities

Insurers want to capitalize on opportunities as well as focus on risks. One audit chair spoke for several directors when he said, *"My first observation is, this is the biggest new risk opportunity to emerge in decades. I take the view that it is an opportunity, and it is underserved."*

Cyberinsurance is a relatively new and evolving product area. Early insurers began selling policies 10 to 15 years ago. Since that time, the number of carriers, insureds, and the amount of premium volume, has continued to grow steadily. Approximately 70 insurers sell coverage today.[11] The existence of persistent residual risk has led to increasing demand for risk transfer solutions. Insurers made the following observations about the market:

- **The current market is small compared to estimates of risk.** Best estimates of the size of the global marketplace range from $600 million to $1.3 billion in gross written premiums in 2013, though many experts believe total volume to be higher.[12] In recent years, new insurers have entered the market, and pricing has become more competitive. Given the variety of risk types, policies tend to be highly specialized.[13] Underwriting often requires customers to demonstrate certain risk management standards and controls are in place. In a recent study, only 31% of respondents indicated their organization had a cybersecurity insurance policy.[14] However, among those companies that do not have a policy, 57% say they plan to purchase one in the future.[15]
- **Recent events highlight the need for coverage.** The high-profile attacks on leading US retailers Target and Neiman Marcus may be driving interest in coverage. One insurance industry lawyer likened the Target breach to "10 free Super Bowl ads"[16] for insurance, and leading brokers such as Marsh & McLennan and Aon have noted increased demand in recent months.[17]
- **Insurers want to address challenges in the market to capitalize on the opportunity.** To increase uptake, insurers will need to address several challenges in the market. One director observed, *"Understanding how to sell and price cyberpolicies is an issue within the industry. We have a ways to go yet."* Participants identified the following challenge areas:

[11] Leslie Scism, *"Cyberattacks Give Lift to Insurance,"* Wall Street Journal, March 26, 2014.

[12] Estimates vary considerably. See for example, Ibid.; Guy Carpenter, *Tomorrow Never Knows* (New York: Guy Carpenter, 2013), 10; and Betterly Risk Consultants, *Cyber/Privacy Insurance Market Survey*, Betterly Report (Sterling, MA: Betterly Risk Consultants, 2013), 6.

[13] Commercial policies typically cover four main types of exposure: property and theft, liability, remediation or reputation, and fees and fines.

[14] Ponemon Institute, *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age* (Traverse City, MI: Ponemon Institute, 2013), 4.

[15] Ibid.

[16] Leslie Scism, "Cyberattacks Give Lift to Insurance."

[17] Ibid.

- **Pricing.** A recent study revealed that among the 43% of respondents who do not plan to purchase coverage, price, exclusions, and uninsurable risks were the primary barriers.[18] Insurers noted that coverage levels are very high among the largest companies, but as they try to broaden coverage to small and mid-sized companies, pricing could become a more significant hurdle.
- **Coverage for less tangible assets.** Insurers noted that existing policies have become proficient at providing for direct and more predictable exposures such as investigations, legal costs, and credit protection, but observed that the market does not have as sophisticated solutions for indirect and less quantifiable exposures, such as lost future revenue or intellectual property theft. Estimates suggest that for leading economies, between 41% and 68% of the per capita breach costs are indirect.[19] As cyberinsurance matures, policies will need to adapt to address these costs.
- **Underwriting.** According to one director, *"Demand is still an issue, but getting the underwriting right, with some degree of confidence, also limits supply."* Several directors observed that effective underwriting remains in development, with one noting, *"The big concern is that you are writing policies and don't know the actual risk. In that case, how confident can you be in your pricing? There is limited history and not sufficient science around this."* Another agreed: *"It's a very difficult risk for insurers because it aggregates globally. It's very likely to affect many clients across the world at the same time. How do you diversify to accommodate that? This keeps limits lower."*
- **Communication.** Participants and industry experts have observed that the complexities of cyberinsurance necessitate a high degree of clarity in negotiations. To date, many purchasers have been sophisticated consumers. However, insurers have experienced negative publicity and lawsuits from clients who believed they had appropriate coverage and discovered they did not after an event. Additionally, as one director noted, *"You rarely hear about this kind of insurance working as it should. No one wants to admit they couldn't fend off an attack."*

★ ★ ★

Insurance company boards and directors have a critical role to play in creating institutions that are resilient in the face of cybersecurity risks, especially as insurers are a part of, and dependent on, the broader banking and financial systems, which are the sectors most targeted by cybercriminals.

While progress has been made since the IGLN started discussing these issues more than 18 months ago, much remains to be done. Several directors were concerned that their boards do not yet demonstrate best-practice governance. As boards further define roles and responsibilities for cybersecurity risk, directors are demanding better metrics. Outside the insurance sector, this same process is driving increased interest in cyberinsurance policies as a logical part of any security strategy. Leading insurers should be well placed both to protect their own enterprises and to partner with other companies to provide increasingly important risk transfer products.

[18] Ponemon Institute, *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age,* 4.

[19] Ponemon Institute, *2013 Cost of Data Breach Study: Global Analysis* (Traverse City, MI: Ponemon Institute, 2013), 18.

Insurance Governance Leadership Network
ViewPoints

About the Insurance Governance Leadership Network (IGLN)

The IGLN addresses key issues facing complex global insurers. Its primary focus is the non-executive director, but it also engages members of senior management, policymakers, supervisors, and other key stakeholders committed to outstanding governance and supervision in support of building strong, enduring, and trustworthy insurance institutions. The IGLN is organized and led by Tapestry Networks, with the support of EY. *ViewPoints* is produced by Tapestry Networks and aims to capture the essence of the IGLN discussion and associated research. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, members of senior management, advisers, and stakeholders who become engaged in this leading edge dialogue, the more value will be created for all.

About Tapestry Networks

Tapestry Networks is a privately held professional services firm. Its mission is to advance society's ability to govern and lead across the borders of sector, geography, and constituency. To do this, Tapestry forms multistakeholder collaborations that embrace the public and private sector, as well as civil society. The participants in these initiatives are leaders drawn from key stakeholder organizations who realize the status quo is neither desirable nor sustainable, and are seeking a goal that transcends their own interests and benefits everyone. Tapestry has used this approach to address critical and complex challenges in corporate governance, financial services, and healthcare.

About EY

EY is a global leader in assurance, tax, transaction, and advisory services to the insurance industry. The insights and quality services it delivers help build trust and confidence in the capital markets and in economies the world over. EY develops outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, EY plays a critical role in building a better working world for its people, for its clients, and for its communities. EY supports the IGLN as part of its continuing commitment to board effectiveness and good governance in the financial services sector.

The perspectives presented in this document are the sole responsibility of Tapestry Networks and do not necessarily reflect the views of any individual financial institution, its directors or executives, regulators or supervisors, or EY. Please consult your counselors for specific advice. EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. This material is prepared and copyrighted by Tapestry Networks with all rights reserved. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends. Tapestry Networks and the associated logos are trademarks of Tapestry Networks, Inc., and EY and the associated logos are trademarks of EYGM Ltd.

Appendix 1: Meeting participants

- Mr Mike Arnold, Risk Committee Chair, Audit Committee Member, Nomination Committee Member, Old Mutual
- Mr Alastair Barbour, Audit Committee Chair, Investment Committee Member, RSA
- Mr Mark Chaplin, Group Enterprise Risk Director, Aviva
- Mr Tom de Swaan, Chairman, Governance and Nominations Committee Chair, Remuneration Committee Member, Zurich Insurance Group
- Mr John Fitzpatrick, Finance and Risk Committee Chair, Audit Committee Member, American International Group
- Ms Kirstin Gould, Executive Vice President, General Counsel, and Secretary, XL Group
- Ms Jane Hanson, Risk Committee Chair, Corporate and Social Responsibility Committee Chair, Direct Line Insurance Group
- Mr Simon Harris, Managing Director, Financial Institutions Group, Moody's Investors Service
- Mr Shawn Henry, President, CrowdStrike
- Ms Sue Kean, Chief Risk Officer, Old Mutual
- Ms Joan Lamm-Tennant, Chief Economist and Risk Strategist, Guy Carpenter
- Mr Michael Losh, Audit Committee Chair, Aon
- Mr Patrick Montagner, Director, Insurance Supervisory Department, Autorité de contrôle prudentiel et de resolution, Banque de France
- Mr Carlos Montalvo, Executive Director, European Insurance and Occupational Pensions Authority
- Mr Chris Moulder, Head of Department, London Markets, Prudential Regulation Authority
- Mr Andrew Palmer, Audit Committee Chair, Investment Committee Member, Risk Committee Member, Nomination Committee Member, Remuneration Committee Member, Direct Line Insurance Group
- Mr Ronald Rittenmeyer, Technology Committee Chair, Audit Committee Member, Compensation and Management Resources Committee Member, American International Group
- Ms Paola Sapienza, Investment Committee Member, Risk and Control Committee Member, Assicurazioni Generali
- Mr Giri Sivanesan, former UK Head of Cyber and Information Assurance, Lockheed Martin
- Mr Bob Stein, Nominating Committee Member, Remuneration Committee Member, Risk Committee Member, Aviva
- Mr Stan Talbi, Executive Vice President, Global Risk Management and Chief Risk Officer, MetLife

EY

- Mr Steve Bell, Partner, Financial Services Advisory
- Mr Shaun Crawford, Global Insurance Sector Leader
- Dr Andreas Freiling, EMEIA Insurance Leader, Financial Services
- Ms Carolyn Myers, Director, Financial Services
- Mr John Santosuosso, Global and Americas Insurance Assurance Practice Leader
- Mr George Tsantes, Principal, Financial Services

Tapestry Networks

- Mr Dennis Andrade, Principal
- Ms Leah Daly, Senior Associate
- Mr Jonathan Day, Senior Adviser
- Mr Peter Fisher, Partner

Appendix 2: Common cybercrime targets, actions, and actors and motivations

Targets	Customer data	Data often include personal identifiers such as national ID numbers, addresses, dates of birth, and financial information.
	Financial resources	Data includes personal or corporate accounts, including bank accounts, investments, and other funds. Cybercriminals may use information systems to commit fraud, directly steal money, or redirect payments.
	Intellectual property	Intellectual property includes information on systems, products, or company structures that can give an advantage to competitors or make financial crimes easier to commit.
	Property or systems	Physical assets may include buildings and related operating systems (i.e., heat, ventilation, energy, electricity, etc.), or hardware such as computers or servers. Virtual systems may include operating systems, software, or programs.
Actions[20]	Denial of service attacks	Some actors may attempt to destroy or limit access to information systems. Denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks are a common example of this type of cybercrime that can render a network resource unavailable for intended users.
	Insertion of malware	Criminals may insert malicious software into a system with the goal of changing its function. Malware comes in many forms, including viruses, worms, and Trojan horses, and is frequently used to capture passwords or payment information, download data, or disable controls.
	Hacking	Hacking encompasses any attempt to access or harm information assets. Hacking includes use of stolen credentials, accessing systems through back doors, and brute force attacks.
	Social engineering	Social engineering attacks involve manipulating users to gain access to systems. Common methods include phishing, bribery, and extortion.
	Misuse	Misuse comprises malicious or unauthorized use of company resources by employees or vendors. Examples include abuse of privileges, mishandling of data, and use of unsanctioned hardware or software.
	Physical attacks	Physical attacks are attacks on infrastructure and physical property (e.g., ATM skimming, tampering, and theft).
	Actions taken in error	Damage can be caused accidently (e.g., accidentally publishing or emailing data or documents).

[20] Threat action taxonomy based on Verizon RISK Team, *2013 Data Breach Investigations Report* (New York: Verizon, 2013).

Actors and motivations	Organized crime	Traditional organized crime syndicates are updating their arsenals, developing dedicated cybercrime groups around the globe. Russia and Eastern Europe are notable locations for this activity.
	State actors	Reasons for state-sponsored attacks include financial gain, intelligence gathering, warfare, or terrorism. China and the Middle East are believed to be the key sources of many state-sponsored attacks. Revelations about US National Security Administration spying indicate that the US government is also active in this arena.
	Employees and vendors	Insiders are typically motivated by desire for financial gain or retribution. Individuals may also be compromised accidently or make mistakes. Poorly vetted employees or vendors with access to critical systems pose a special threat.
	Activists	Activism is frequently motivated by political or religious beliefs; goals can include publicity, public policy change, and defamation.

Appendix 3: Cybersecurity questions for boards

- What are the information assets most critical to our company's business objectives, operations, revenue, and brand? What are the risk tolerances associated with them?
- Is our information security strategy aligned with our business strategy?
- What risks do business relationships introduce into the organization? What risks do we present to partners?
- Does our organization have a program to assess and implement improvements to stay ahead of the threat landscape? How do we reliably demonstrate improvement over time?
- How much time elapses between when adversaries penetrate our systems and when we identify them? Is the delta widening or narrowing?
- What is our incident response plan?
- Is the security operation appropriately organized, trained, staffed, equipped, and funded?
- How have board and management governance practices for cybersecurity risks changed over time? Has understanding of the risks influenced reporting structures and content, responsibility for risks, and board or management expertise?
- Are governance procedures sufficiently robust to respond to attacks and demonstrate good governance? How do we know?