Insurance Governance Leadership Network

December 2021

IGLN

VIEWPOINTS

Responding to an intensifying cyber risk landscape

"Financial services is under attack more than many other sectors because we maintain a lot of critical data that can be very valuable."

– Director

Recent high-profile attacks on critical infrastructure and the explosive growth of ransomware attacks have revealed vulnerabilities to cyber risks, renewing a sense of urgency. In regulated or systemically vital sectors, the risk is even greater. One director said, *"Financial services is under attack more than many other sectors because we maintain a lot of critical data that can be very valuable."* Financial institutions not only face a rapid growth in cyber attacks, but also growing pressure from governments and regulators to enhance cybersecurity oversight, improve prevention and detection, and ensure resilience and recovery in the event of a damaging attack.

On November 4th (virtually) and 17th (in London), IGLN participants met to discuss how cybersecurity risks and responses have evolved and which risks are of particular concern to large insurers, including the potential of new approaches to cyber insurance. They also discussed incident response, advances in cyber risk management and oversight, and the possibility of expanding public/private partnerships. This *ViewPoints* draws on pre-meeting conversations with participants and the November discussions, and focuses on the following areas[1]:

- **Cyber risk is intensifying**
- **Insurers face mounting pressure to improve cyber risk management**
- **Cyber security oversight continues to evolve**

Cyber risk is intensifying

Cybersecurity incidents are inevitable; even companies with sophisticated strategies to prevent them will likely face a significant breach of some kind. Stories of high-profile cybersecurity incidents around the globe have surged over the past year as governments and businesses alike find themselves susceptible to damaging attacks. EY research published in early 2020 found that 59% of some 1,300 companies surveyed had experienced a major incident in the previous 12 months.[2] According to the World Economic Forum, executives in North America and Europe now see cyberattacks as representing the greatest perceived risk of doing business.[3] A recent joint

"We've seen an explosion in ransomware attacks. They are easy and cheap to deploy."

– Participant

Marsh and Microsoft survey of 1,500 business leaders revealed that cyber malfeasance now outranks economic uncertainty, regulation, and brand damage as the top business threat, and that even as companies' concerns about cyber risk grow, their confidence that they can manage it is decreasing.[4] In financial services, where real-time transactions and risk management are necessary, a participant noted, *"We are talking about halting operations, stopping things like dynamic hedging for billions of dollars. If you can't do it, it's an existential threat."*

The threat landscape is evolving

Management and boards of large insurers face a constant challenge to familiarize themselves with a broad scope of cyber threats, ranging from simple to highly complex. The attackers and their approaches vary widely and constantly evolve, exposing new vulnerabilities and emphasizing the need for agility in responding.

"With ransomware, it's getting down to protecting the daily operations of the business. It's a fundamental game changer."

– Executive

Participants identified key factors in the threat landscape:

- **The rising threat of ransomware.** Ransomware attacks have become a major risk for large corporations globally. One participant said, *"We've seen an explosion in ransomware attacks. They are easy and cheap to deploy, and operational changes caused by COVID-19 exposed vulnerabilities."* Between 2019 and 2020, ransomware attacks rose by 62% worldwide, and by 158% in North America alone.[5] The increase has continued in 2021, with attacks rising by 93% in the first half of the year.[6] Some industries have been disproportionately affected. For example, the banking industry experienced a 1,318% year-on-year increase in ransomware attacks in the first half of 2021.[7] The attacks are also proving more successful for hackers. A report from cybersecurity firm Palo Alto Networks found that the average ransom paid increased by 171% in 2020 versus the prior year, while the highest ransom paid and the highest ransom demands also doubled.[8] For many, the trend represents a shift in how businesses think about cyber risk. One executive said, *"Previously, cyber risk was more about the data that we own, the end-user's data, and how we protect it. But with ransomware, it's getting down to protecting the daily operations of the business. It's a fundamental game changer in the way cyber impacts this industry holistically."*
- **A growing focus on critical infrastructure and data intensive sectors.** Threats to critical infrastructure, such as the Colonial Pipeline hack in May, which resulted in gas shortages across the US East Coast, have been

"We are stuck in the position of just trying to maintain vigilant defense and trying to be ready to recover when it happens."

– Director

particularly eye opening for business leaders. One director said, *"Colonial Pipeline shook everyone up, particularly when it comes to critical infrastructure. Well, guess what? The financial sector is often part of critical infrastructure, and [it carries] some of the greatest risk."*

- **The difficulties in defending against bad actors.** Many cyber attacks are carried out with tacit or direct support from nation-states operating outside the bounds of international rules and norms, making it difficult for private companies to prevent or respond to threats. As one director said, *"It's very hard to actually do anything about the nation-state threat actors as a corporation. We are stuck in the position of just trying to maintain vigilant defense and trying to be ready to recover when it happens."*

Insurers are increasingly a target

Participants observed that insurers are facing an increase in cyber attacks. An EY expert said, *"Insurance has always been interesting when it comes to cybersecurity. Insurers have so much data that's critical to their business and that bad actors want. It's kind of the perfect spot for threat actors to land on, and insurers are becoming more and more of a target as a result."* Indeed, though large banks are often considered the top target for cyber attacks within the financial sector, there are reasons for insurers to be concerned:

"Insurers have started to lag behind the banks in cybersecurity."

– Participant

- **Recent attacks against prominent insurers have proven successful.** According to participants, cybersecurity has rapidly moved up on insurance board agendas following successful and very public hacks of well-respected firms within the industry. In May, CNA Financial, one of the largest insurers in the United States, paid hackers $40 million in ransom after an attack locked the company out of its own network for two weeks.[9] The same month, AXA was the victim of a ransomware attack, affecting operations in Thailand, Malaysia, Hong Kong, and the Philippines.[10] Other insurers have been successfully targeted as well.
- **Some insurers may be less prepared than other financial institutions.** According to *Forbes,* "An analysis in 2015 found that financial organizations were targeted four times more frequently than other industries. Only four years later, financial firms experienced as many as 300 times more cyber attacks than other companies."[11] Though the sector is often considered among the most sophisticated regarding cybersecurity and risk management, insurers may not be as advanced in this area as major banks. A participant said, *"Insurers have started to lag behind the banks in cybersecurity. Banks used to get the most attacks, but insurers*

are getting more and more attention because they may be viewed as a bit of an easier target."

"If we cannot protect our own business, our own data, that for me is the biggest fear."

– Director

- **The sector relies on maintaining the integrity of sensitive data.** To maintain the trust of their customers, business partners, and regulators, insurers must safeguard the integrity of the data they collect. Yet, experts have noted that the nature of that data makes it even more attractive to hackers for use as leverage for extortion attempts.[12] According to *The Wall Street Journal,* "Previously, ransomware attackers focused on encrypting the victims' data, making it inaccessible and potentially disrupting business operations until a ransom is paid. Over the past year, new ransomware hackers looked for leverage in the form of information that would potentially harm a company if made public."[13] Senior leaders recognize the challenge. As one director said, *"In insurance, we're in the protection business. So, if we cannot protect our own business, our own data, that for me is the biggest fear."*
- **Digital transformation efforts may create new vulnerabilities.** An executive said, *"A lot of the sector has been going through major digital transformations, and those large-scale transitions can make firms vulnerable in unexpected ways."* As many insurers continue to invest in upgrading legacy systems, deploying emerging technologies at scale, and pursuing partnership opportunities, it is critical to be vigilant regarding new sources of cyber risk.

Under stress, cyber insurance may need to evolve

"Large-scale transitions can make firms vulnerable in unexpected ways."

– Executive

Cyber risk has presented revenue-generating opportunities for insurance carriers willing to offer coverage to businesses. In 2020, two cyber insurance programs exceeded $1bn for the first time.[14] In the United States, half of all companies that purchase insurance now include cyber insurance in their coverage.[15] As the cyber threat environment has intensified, cyber insurance losses have mounted, however. According to one report, insured cyber losses rose to $1.8bn in 2019, a 50% increase from the previous year.[16] The exponential increase in ransomware attacks, and resulting losses, are driving insurers to increase premiums. According to *The Financial Times,* premiums increased 27% from April to mid-May over last year's levels.[17] A participant described, *"You have two carriers that dominate the market, limits are coming down, premiums are going up, and exclusions are going up."*

The stress in the cyber insurance market is fueling conversations about the future of the business. Some participants questioned whether cyber risk is

"The cyber insurance market is broken. Policies were being handed out like candy."

– Participant

insurable at all, noting that it may be an area where governments need to provide a backstop. One participant asserted, *"The cyber insurance market is broken. Policies were being handed out like candy. Now, everyone is backing away."* Others disagreed, with one saying, *"To say that cyber risk cannot be insured is ridiculous … Otherwise, you're saying you give up on the future. This is a huge market for this sector, and a government program cannot backstop something this big."* A director said, *"That's what this sector does, it enables people to do business. I believe the opportunity exists … there is a major opportunity to get some products in there that both help businesses and also work for us."*

To capitalize on the opportunity, new approaches may be necessary. An executive said, *"You do have to do it a bit differently versus other insurance. Yes, it's fraught with challenges. Yes, it's difficult. But as an insurer you must believe it's a problem that can and must be solved."* The executive explained, *"All these corporations have just gone through a pandemic, are under extreme pressure to digitally transform, and amidst that they are supposed to protect against a risk that no one is actually really protected against. For an insurer, it's hard to imagine a market that's more interesting than cyber insurance."*

"For an insurer, it's hard to imagine a market that's more interesting than cyber insurance."

– Executive

To underwrite the risk, insurers may need to look for ways to establish a better understanding of a corporation's current exposure and risk management strategy. An EY expert said, *"Insurers are increasingly balancing the value of being able to provide coverage while also finding better ways to determine that this company is taking the appropriate measures."* Insurers are conducting more client risk assessments, offering guidance on expectations, and identifying areas for improvement as part of the underwriting process. Participants expect these practices will expand, and in fact, the insurance sector could serve as an important catalyst for improving cyber risk management standards. An executive observed, *"It's becoming about asking the right questions of the business and making this work for both sides. I truly feel this industry has a chance to push the organizations it is covering to improve their cyber risk posture."* Another participant said, *"Security assessments are becoming standard practice, and there are quite a few third-party organizations that will do those as well."*

New approaches are not without their own set of risks. For instance, if enhanced cyber assessments become common, firms will need to find ways to attract and retain the right talent to perform the assessments. A participant said, *"I agree that this is the best approach, but the challenge is, are there*

enough people out there that can be hired by an insurer and credibly do the assessment of the company? I'm not sure there are."

Some new approaches are emerging, for example using software to monitor, in real time, a company's vulnerabilities and improve data gathering. According to one participant, *"This is a huge market, but we need a new approach. Data sharing could vastly improve the underwriting process. Cyber is dynamic; the risk assessment changes almost real time. We need an approach that is more like a partnership where we are helping companies improve security, where we pay out for pre-emptive measures to improve security."*

"This is a huge market, but we need a new approach."

– Participant

Insurers face mounting pressure to improve cyber risk management

Following the Colonial Pipeline hack and other high-profile incidents, governments, regulators, and investors are focused on private sector cyber risk more than ever before.

Governments are prioritizing cybersecurity

In August, several insurance company leaders participated in meetings with US President Joe Biden, who stated, "The federal government can't meet this challenge alone. You (executives) have the power, the capacity, and the responsibility, I believe, to raise the bar on cybersecurity."[18] Many participants expect that new government policies are likely to play a major role in shaping the way forward. A director said, *"My biggest focus right now is how can we lead on policy and guide the sector and the private space more broadly towards a better environment and better practices? I think we need to be really careful that we do not let policy get formed without the reality of enterprise needs being fully considered."* Some would like to see the public sector adopt a more aggressive posture towards bad actors, as reported by one participant, *"In the Washington Post on November 3, there was a report that a ransom gang was shut down by US Cyber Command and a foreign government; that's an accurate report. So, there is a lot more active work by security services."*

"We need to be really careful that we do not let policy get formed without the reality of enterprise needs being fully considered."

– Director

Regulators are increasing scrutiny of insurers

Cyber risk is rapidly becoming a top area of concern for regulators in the insurance sector. In October, the Bank of England expanded an initiative to test the resilience of the UK financial sector's cyber defenses to include insurers and their cyber attack scenarios.[19] Separately, the Bank of England

has given financial services companies until March 2022 to deliver detailed plans on how they would handle a cyber attack.[20]

Concerns about cyber risk have grown as operational resilience—the ability of an organization to prevent, respond to, recover, and learn from operational disruptions without harm to customers and the wider market—has become a primary focus of regulators. A participant said, *"A lot of this focus on cyber ties back to the focus on resilience … Regulators everywhere have been driving the operational resilience agenda. A great way to understand resilience is to define what your critical business services are and what key bits of those processes are actually critical to you, and what third parties are mapped to that. From a cyber resilience perspective, that's a great place to start … you can understand by looking at it quickly."*

"I do not think boards go deep enough when it comes to third-party relationships."

– Participant

Third-party risk is also under the microscope. Last year, the European Union proposed rules that would allow authorities to force financial institutions to sever relationships with cloud providers and other IT service providers if those providers failed to rectify cybersecurity flaws identified in government inspections.[21] A participant commented, *"I do not think boards go deep enough when it comes to third-party relationships. It's not just about using or not using a provider, it's about what you are using it for, and we really want to understand those decisions."*

Investors expect better information on cyber strategy

"The frustrating part for investors and the company is if you ask for too much… you might also get more successful attacks."

– Investor

Investors are also seeking improved information and forward-looking insight into how insurers are managing cyber risk. Yet, investors and companies both face challenges in this area, as more expansive public communication of cyber defenses could put the company at risk. An investor explained, *"The frustrating part for investors and the company is if you ask for too much and get what you wish for, you might also get more successful attacks. The other option is just holding people accountable at the back end, which might be all I can do."* For now, investors are largely reliant on very limited information: *"What is the current industry standard? It's depressingly simple, really. It's looking at past incidents and in the worst-case scenario, you sell the stock after the incident,"* according to one investor.

Investors are pressing firms to take a number of steps to provide increased clarity on cyber activity without adding risk. Participants discussed several potential approaches:

- **Offer greater detail on the board's oversight structure and expertise.** An investor said, *"An important aspect is just looking at the governance*

"Every board I know has a compensation consultant, but many do not have a cyber consultant. Why?"

– Investor

processes that you have in place. Who on the board oversees it? What committee? This is something most financial institutions have in place but could do a better job of detailing." Another participant observed, *"Five years ago, it wasn't clear any board committee had oversight of this risk. Firms should identify who will oversee this risk and explain how those people feel about their own knowledge. Do they need more training, and do they have time to do it? Is that a skills gap that you need to fill and maybe fill quietly?"*

- **Disclose financial metrics and preparedness plans.** Investors want to understand how boards and management are prioritizing cybersecurity and adjusting strategy to respond to the evolving threat environment. Budgeting decisions can be one way to reflect such prioritization. A participant said, *"Share your security spend as part of your IT budget."* A thoughtfully considered breach response plan can be another helpful data point to investors: *"What is your impact tolerance, have you thought this through and defined it? Do you have a thorough incident response plan?"*

- **Engage and disclose third-party support.** In certain areas, such as compensation, boards have been very transparent that they rely on third parties to provide insight to inform decision making. Some investors would like to see boards take a similar approach to cyber. One said, *"Every board I know has a compensation consultant, but many do not have a cyber consultant. Why? We do not expect every director to be a security expert, but we know the board hires experts for various things, like compensation, so do they have the ability to hire someone and have them come in and talk about the quality of the plan?"* Boards can also disclose how they are working with external parties to test their current defenses.

"There is no magic bullet, but there is huge value in simple metrics to ballpark things."

– Investor

- **Share common cyber maturity scorecard results.** Investors are keen to compare strategies among firms. Communicating cyber maturity scorecard results could provide investors with an opportunity to differentiate between top performers and laggards. Not everyone is convinced that this is the right approach. A director said, *"They come up with some arbitrary number that's not really insightful or helpful."* An investor acknowledged, *"They are not massively effective, but we find them helpful for benchmarking. We are just really interested in who is doing a better job in a given industry and who is not doing as well. There is no magic bullet, but there is huge value in simple metrics to ballpark things."*

Even with better information on cyber risk management, in the event of a cyber event, investors are increasingly looking to hold firms and their boards

accountable. One participant stated, *"Engagement is the carrot, proxy voting is the stick."* An investor said, *"Does a breach warrant a vote against? It depends on the nature of how this happens. Everyone here is getting attacked, so what was the nature of it, was it something simple that seems to us could have been prevented? Then we look at other boards those folks sit on and go talk to them as well and do our due diligence and make sure the same thing won't happen there."*

Cybersecurity oversight continues to evolve

"Every organization seems to be grappling with ransomware policies."

– Participant

The financial sector is generally thought to be among the most engaged and mature with respect to board-level governance of cyber threats. Though large insurers have invested a tremendous amount of time, attention, and capital in cybersecurity, few leaders are confident that they have mastered oversight and governance of the risk, particularly at the board level. A director said, *"How do we keep current as non-executive directors today? Everything is moving so fast, and we all have information overload. How do we keep current and also constantly refresh what we know? Because it gets stale quickly."*

Improving ransomware preparedness

Participants stressed that ransomware preparedness has become perhaps the most urgent aspect of cyber oversight. *"Every organization seems to be grappling with ransomware policies, whether to pay or not pay, how to protect data and have backups, establishing a plan of communication. There is a whole host of issues that boards need to consider, and they need to do that today rather than waiting for an attack,"* said one participant.

"By the time a ransomware attack comes to you, what do you need to know and how long will you have?"

– Participant

Developing a robust ransomware response plan

As one participant remarked, *"Regulators are now talking about a 100% probability that ransomware will happen to you, it's not 'if', it is 'when'."* The explosive growth of ransomware attacks has shown the vulnerabilities of businesses everywhere, and many are now shifting their focus from prevention to response. This shift is becoming a preferred approach by key stakeholders, as well. Boards and management should collaborate in developing a detailed response plan that outlines various factors such as escalation policies, roles and responsibilities, communications with customers, clients, and law enforcement, and many other factors, participants noted. One said, *"By the time a ransomware attack comes to you, what do you need to know and how long will you have? When is the board notified? When do you communicate to the media and customers? Do you have*

backups for your data? Having that clear plan is Step Number One, then things start to fall into place."

Participants stressed that the plan itself should be carefully stored and protected to prevent hackers from accessing it. A director said, *"We learned in some of the most recent attacks, the attacker was able to get into the policy and see what the actual coverage was, and they were increasing the ransom to very specific levels because it was discoverable."* A participant added, *"It should be held very tightly, because you don't want them to understand your pain points and when you'll be willing to pay ransom. It probably should not be stored within the organization."*

"I think there is very little downside in structured communications with the FBI or law enforcement."

– Participant

Thinking through communications strategies

Communications should be an area of particular focus when developing incident response. An executive said, *"The communications piece is actually the least practiced and understood but can actually do the most damage."* Another participant agreed, adding, *"Understanding the facts, knowing who to report to, whether you have to tell your customers, all of that is important and it has to happen very quickly. The worst situations are the ones where you have to put communications out even though you do not have anything solid to communicate yet."*

Often, it is also important for firms to notify relevant law enforcement about ransomware attacks. According to the US Cybersecurity and Infrastructure Security Agency (CISA), "Every ransomware incident should be reported to the US government. Victims of ransomware incidents can report their incident to the FBI, CISA, or the US Secret Service."[22] Yet, some firms may be hesitant to involve outside parties before they have a full view of the situation. Experts stress that notifying law enforcement can be a critical step for a variety of reasons, but some note that this can be handled in a considered fashion. One participant said, *"I think there is very little downside in structured communications with the FBI or law enforcement with whom your organization has an existing relationship and understanding of how that relationship works."*

Weighing the pros and cons of paying the ransom

Though ransomware attacks may be inevitable, paying the ransom may not be. A participant said, *"Response is successful if the organization is able to immediately contain the threat, have minimal interruption, address any data issues quickly and in ways that minimize risk, and not pay the ransom."* When an incident occurs, firms may be tempted to make the payment, particularly if

"As a principle, it is better not to pay, but if you're not going to, you better have a solid Plan B in place."

– Participant

it has resulted in a major business interruption. Leaders should have a clear view of whether this will resolve the challenge the company is facing. An executive said, *"There is a lack of understanding of what paying gets you. It may take you just as long to get up and running after you get the encryption key as it would have to not pay at all. So, it's about understanding that paying is not the magic bullet and making sure we're thinking through ways to avoid making that payment."* Another participant said, *"Even if you pay, how sure are you that you'll even get the actual data back? Will the data have integrity? And once you pay, how do you know they won't come back? So, as a principle, it is better not to pay, but if you're not going to, you better have a solid Plan B in place."*

In practice, many companies will conclude that the best option is to pay. An executive said, *"The reality is that most companies will end up needing to pay. After the Colonial Pipeline outcome, the US regulators in particular are changing their approach and realizing this maybe is not worth the argument over $5 or $10 million."* Paying does carry its own risks: it sets the precedent of willingness to pay and creates reputational challenges. A participant said, *"I do think 90% will pay, but the challenges for the board [are] realizing that you may go bust now by not paying, but you may also just go bust later because many of those that have paid find they haven't fixed the vulnerability. So, if you're a supplier, business partners start leaving the business anyway and you'll go bust in six months."* Companies also need to be cognizant of unintentionally violating international laws or sanctions through payouts.

Focusing on data recovery and resilience

"You have to assume something will happen, so how quickly can you recover and minimize the damage?"

– EY expert

Accepting the inevitability of attacks, companies' have shifted their focus to protecting the most critical assets, while response strategy has shifted towards protecting critical data and ensuring key business processes remain functioning or are stabilized as quickly as possible. As one EY expert said, *"You have to assume something will happen, so how quickly can you recover and minimize the damage? Frequently, that comes down to data and data access. It is about how prepared you are to manage post breach. Do you have the right backups and recovery procedures in place?"* Being well positioned to recover and return to normal business operations can protect companies from making the difficult decision to pay bad actors. A director said, *"What I find creates the highest risk and most desire to pay is the business interruption … It's really about getting up and running and being prepared."*

Implementing "Zero trust" models

"Zero trust is the right concept to move towards, but to get there you have to start small."

– Participant

To better prevent breaches and safeguard data as their work perimeters continue to expand, many businesses are moving to "zero trust" models. These models attempt to remove the concept of trust from an organization's network architecture, requiring continuous and thorough authentication processes for data access. While some insurers have already implemented aspects of zero trust into their operations, the process can be daunting. An EY expert said, *"For organizations maintaining a lot of legacy systems, which covers a lot of the major financial institutions, they are operating very old technology and to build zero trust into that is conceptually a great idea, but the reality of implementation becomes very hard and expensive, practically speaking."* A gradual transition will require collaborative decision making, as different parts of the business will likely need to weigh tradeoffs. A participant said, *"Zero trust is the right concept to move towards, but to get there you have to start small. Where and how you apply it is where the business has to make critical decisions. The cost of putting this in across the environment is astronomical. It's about the criticality of what is being accessed, balancing user experience with the roadblocks you are putting in place. That's where the business and technology sides of the company need to sit down and decide where to apply it."* An executive added, *"All the large institutions want to do it, but it's probably a five-year journey."*

"Post-cyber incident, regulators are essentially requiring organizations to adopt zero trust."

– Participant

Zero trust presents yet another somewhat technical topic for boards as they exercise their oversight responsibilities. A director stated, *"It's not a hot topic at the board level yet, but it's a part of the conversation and one of the many tools that the CISO has at their disposal which they should share with the board along with adequate metrics, testing, stuff like that."* And it may become a hot topic shortly. Zero trust is gaining traction within the regulatory community. A participant said, *"From a regulator's perspective, zero trust is very attractive. We have seen, post-cyber incident, regulators are essentially requiring organizations to adopt zero trust and there is an emerging debate about what that actually means, because it is a principle."*

Grappling with oversight challenges

Even experienced board members at organizations with sophisticated cybersecurity measures in place note that remaining knowledgeable on the topic requires constant efforts and assessing effectiveness is difficult.

Participants discussed several areas where oversight of cybersecurity is evolving.

"The starting point is figuring out what our exposures are today, but that's not a trivial task."

– Participant

- **Understanding exposures and tolerances.** Participants noted that tracking progress remains particularly difficult because companies often lack a clear view of their current circumstances. One director said, *"What's missing, at least to me, is I don't think the board really understands what risk they're actually exposed to in a granular way. We hear a lot about the efforts to mitigate the risks, but what risks are we implicitly accepting given the structures we currently have? That's an obvious question, but a very valuable answer, and very important to the board: What risk are we accepting today? And if we don't agree with it, what can we do about it?"* Another said, *"The starting point is figuring out what our exposures are today, but that's not a trivial task."*

- **Accounting for third-party risk.** One director said, *"The ecosystem in financial services is so intertwined, we are so connected to third parties and to each other as institutions. Sitting on the board you have to think of where to draw the line when it comes to oversight. Do you go to your third parties? Do you go to your fourth? Fifth? What do you do to draw the line and bring your arms around the risk and vulnerabilities?"* At a minimum, boards should have a clear understanding of where the institution is relying on third parties for critical business processes, as a participant said: *"If you are using it for payments, it's not a huge deal if that goes down temporarily. But if your third party is critical for day-to-day operations, that's a more complicated situation."*

- **Improving board knowledge.** A participant said, *"Firms need to be thinking about educating the board and C-suite on this. Boards hear a lot of buzzwords and see the headlines, but they need to understand how the risk comes alive."* Board members often participate in outside programs to enhance their own cybersecurity expertise, invite experts to speak to their boards, and sometimes hire advisors to the board. A director said, *"We very strongly encourage board directors to get the necessary credentials by the [National Association of Corporate Directors] or organizations like that. Directors need to be smart on this topic and they need to do it now."* Many firms in the financial sector have also added cyber experts to the board to help oversee the risk. An EY analysis of cybersecurity-related disclosures by Fortune 100 companies found that 54% included cybersecurity as an area of expertise sought on the board or cited in a director biography, compared with 40% in 2018.[43] However, identifying cyber experts who will also make good directors and are willing to join the board of a financial institution is not always viable.

"Boards hear a lot of buzzwords and see the headlines, but they need to understand how the risk comes alive."

– Participant

- **Adjusting board structure.** While board responsibility for oversight of cyber risk varies by institution, participants consistently said their boards have added new committees or changed board structure to address cybersecurity more effectively. One director said, *"This topic now receives one-third of the risk committee's agenda time, and we've split it out of the audit committee. We got it out of audit on all my boards because it's way too big of a topic."* As board structure changes, it is important to document who bears responsibility for cyber. A participant observed, *"We are starting to see a demand by regulators to revise charters to ensure cyber is specifically accounted for at the committee level."*

"The most beneficial conversations are still about basic housekeeping."

– Participant

- **Probing management.** Boards often struggle with best practices regarding asking the right questions of management. Participants said directors should not overcomplicate matters, noting that simple questions can provide a fairly thorough view. One said, *"The vast majority of the vulnerabilities still come back to basic housekeeping matters, not sophisticated vulnerabilities being exposed. Simple questions can go a long way. Things like 'Are we running the latest software? What patches? Where are we seeing issues?' All of those are straightforward."* Another said, *"The most beneficial conversations are still about basic housekeeping. Emails, controls, backups, continue pushing on all that housekeeping stuff."*

"We are seeing CISOs moved up one or two levels from an organizational perspective."

– EY Expert

- **Rethinking management roles.** Some also suggested management structures may be due for some reconsideration, particularly the Chief Information Security Officer (CISO). Finding qualified, effective CISOs can be challenging today given the complex nature of the role. An EY expert said, *"They need to speak the language of the business, be able to consider broader strategy, understand regulations, have the breadth of technical expertise, understand the systems infrastructure, and be able to add value to the business. Where do you find that person? I'd love to know; it is very hard to find."* Once the right person is in place, boards are becoming increasingly thoughtful about how to best-position the role internally given its often strategically critical and vast responsibilities. The EY expert said, *"We are seeing CISOs moved up one or two levels from an organizational perspective. I have seen the role being split into two, where one focuses on the transformational agenda while the other is more business driven. It depends on your organization, what your aspirations are as a firm. There is no single best approach, but boards should think about that role more strategically and position it the best way possible."*

Another participant said, *"I know one major firm that recently elevated the CISO role, and [the CISO] became someone with real voice at the C-suite level, that helped … quite a bit."*

****

Cyber risks have changed and multiplied at a relentless pace in 2021. While the threat is well recognized, the need to continually adapt responses requires constant diligence from management and boards. Leaders of larger insurers continue to respond to events and the risks and opportunities they create. As one director said, *"I don't think any of us consider ourselves protected today. I think there is a real sense we are putting in the effort, but you just need to stay ahead of the ones next to you and not be the weak link in the system. That's increasingly today's thinking."*

Appendix

The following individuals participated in these discussions:

Participants

- Jeremy Anderson, Risk Committee Chair, Prudential
- Marty Becker, Non-Executive Director, Axis Capital Holdings
- Paul Bishop, Non-Executive Director, Just Group
- Jan Carendi, Non-Executive Director, Lombard International Assurance
- Eileen Collins, Non-Executive Director, USAA
- Bill Connelly, Chair of the Supervisory Board and Nomination and Governance Committee, Aegon
- Julie Dickson, Non-Executive Director, Manulife
- Ryan Dodd, Founder and Chief Executive Officer, Intangic
- Cheryl Francis, Non-Executive Director, AON
- Drew Hambly, Executive Director, Global Stewardship, Morgan Stanley Investment Management
- Sheila Hooda, Risk Committee Chair, Mutual of Omaha; Chair Nominating and Governance Committee, Enact Holdings
- Leslie Ireland, Member, Chubb Cyber Advisory Board
- Jonathan Kewley, Partner, Co-head, Tech Group, Clifford Chance
- Sara Lewis, Former Audit Committee Chair, Sun Life Financial
- Lyndon Nelson, Former Deputy CEO, Executive Director, Supervisory Risk Specialists and Regulatory Operations, Prudential Regulation Authority, Bank of England
- Andrew Nye, Head of Cyber Assessment, Prudential Regulation Authority, Bank of England
- Debora Plunkett, Non-Executive Director, Nationwide
- John Reizenstein, Audit and Risk Committee Chair, Beazley
- Caspar Siegert, Global Sustainable Investing Research and Data Analyst, Sustainable Investment, JPMorgan Asset Management
- Kory Sorenson, Audit Committee Chair, SCOR; Remuneration Committee Chair, Phoenix Group Holdings
- Phyllis Sumner, Chief Privacy Officer, Data, Privacy and Security Practice Leader, King & Spalding
- Jim Sutcliffe, Risk Committee Chair, Liberty Holdings; Chair, Bought by Many

EY

- Abhishek Madhok, Principal, Cybersecurity
- Peter Manchester, EMEIA Insurance Leader and Global Insurance Consulting Leader
- Isabelle Santenac, Global Insurance Leader
- Kanika Seth, EMEIA Financial Services Consulting Cybersecurity Leader
- Steve Varley, Global Vice Chair, Sustainability

Tapestry Networks

- Dennis Andrade, Partner
- Brennan Kerrigan, Senior Associate
- Tucker Nielsen, Principal

About *ViewPoints*

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.

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.

Endnotes

[1] *ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby comments are not attributed to individuals, corporations, or institutions. Network participants' comments appear in italics.

[2] Dave Burg, Matt Hynes, Mike Maddison, Jeremy Pizzala, and Richard Watson, "How Does Security Evolve from Bolted on to Built-in?" EY, February 18, 2020.

[3] Phil Muncaster, "WEF: Cyber-Attacks Are Biggest Business Risk in Europe and US," *InfoSecurity Magazine*, October 2, 2019.

[4] Marsh Mircosoft, *2019 Global Cyber Risk Perception Survey* (Marsh, September 2019), 5–6.

[5] Lynsey Jeffery and Vignesh Ramachandran, "Why Ransomware Attacks Are on the Rise – And What Can Be Done To Stop Them," *PBS,* July 8, 2021.

[6] Sebastian Klovig Skelton, "Ransomware Attacks Increase Dramatically During 2021," *Computer Weekly,* August 3, 2021.

[7] Maria Henriquez, "Banking Industry Sees 1318% Increase in Ransomware Attacks in 2021," *Security Magazine,* September 20, 2021.

[8] "Highlights From the 2021 Unit 42 Ransomware Threat Report," Palo Alto Networks, March 17, 2021.

[9] Brittany Chang, "One of the Biggest US Insurance Companies Reportedly Paid Hackers $40 Million Ransom After a Cyberattack," *Business Insider,* May 22, 2021.

[10] Emma Woollacott, "AXA Ransomware Attack Comes Just Days After Insurer Pulled Coverage for Cyber-Attack Class in France," *The Daily Swig,* May 18, 2021.

[11] Roslyn Layton, "Hackers Are Targeting US Banks, And Hardware May Give Them An Open Door," *Forbes,* March 17, 2021.

[12] Tim Starks, "Top Insurer CNA Disconnects Systems After Cyberattack," *Cyber Scoop,* March 24, 2021.

[13] Catherine Stupp, "The Latest Cybersecurity Threat: Pay Us or We Release the Data," *The Wall Street Journal,* September 7, 2021.

[14] Tom Johansmeyer, "Cybersecurity Insurance Has a Big Problem," *Harvard Business Review,* January 11, 2021.

[15] Ian Smith, "Cyber Insurers Recoil as Ransomware Attacks 'skyrocket'," *Financial Times,* June 2, 2021.

[16] Tom Johansmeyer, "Cybersecurity Insurance Has a Big Problem," *Harvard Business Review,* January 11, 2021.

[17] Ian Smith, "Cyber Insurers Recoil as Ransomware Attacks 'skyrocket'," *Financial Times,* June 2, 2021.

[18] Andrea Shalal, "White House, Big Tech, Insurers Vow to 'Raise the Bar' on Cybersecurity," *Insurance Journal,* September 6, 2021.

[19] Laura Noonan, "Bank of England-backed Cyber Security War Game Opens to More Companies," *Financial Times,* October 5, 2021.

[20] Laura Noonan, "Bank of England-backed Cyber Security War Game Opens to More Companies," *Financial Times,* October 5, 2021.

[21] Catherine Stupp, "EU Seeks Authority to Cut Off Banks' Tech Suppliers if Found Wanting on Cybersecurity," *The Wall Street Journal,* October 6, 2020.

[22] https://www.cisa.gov/stopransomware/report-ransomware-0