MAXXSURE
CYBER RISK MANAGEMENT

CRISIL
An S&P Global Company

A Cyber Risk Guide for Corporate Leaders

What You Should Know About Cyber Risk Management and Cyber Insurance

By Chris Burrow and Shawn Wiora

Since early 2020, cyberattacks have targeted American corporations at an unprecedented rate. According to the FBI, Cybercrime reports have increased 400% since the onset of the coronavirus. These incidents include ransomware, phishing and malware attacks and web, network and insider threats.

And as Russian missiles rained down on Ukraine beginning in March, 2022, the global cyber threat reached an entirely new level – that as an instrument of warfare. As stated in the New York Times, “destructive malware has flooded hundreds of Ukranian websites and computers since Putin announced his invasion. It would be a mistake to assume such attacks will remain limited to Ukraine targets.”

Cybercrime is projected to hit $6 Trillion by the end of 2021 according to a recent report by Cybersecurity Ventures[1]. It is estimated that global ransomware attacks alone will reach $120 billion in 2021, 57 times the amount in 2015. “Ransomware and cyberattacks are victimizing businesses large and small across America and are a direct threat to our economy,” U.S. Treasury Secretary Janet L. Yellen said in a statement in September.

The Colonial Pipeline ransomware attack in May 2021 was a wakeup call around the globe. It was the largest such breach of an oil infrastructure operator in U.S. history. As the largest supplier of gasoline and jet fuel serving the Southeastern U.S., the breach forced the shutdown of the entire pipeline system. The operator paid $4.4 million in ransom demands. The FBI identified the Russian criminal hacking group “DarkSide” as being behind the attack.

As stated in a report by the consulting firm McKinsey, “debilitating attacks on high-profile institutions are proliferating globally, and enterprise-wide cyber efforts are needed now with great urgency. It is widely understood that there is no time to waste: business leaders everywhere, at institutions of all sizes and in all industries, are earnestly searching for the optimal means to improve cyber resilience[2].”

Fortunately, there are solutions to managing your organization’s exposure to these critical cyber risks. It is important to understand that cyber risks are different from more traditional risks (such as economic or market risks), which risk managers have long experience modeling. As pointed out in a recent study by PwC, “these risks come from strategic adversaries who are constantly switching up their technology and methods to seek out weak spots in yours[3].” It can be particularly challenging to develop a reliable risk assessment model to address this constantly evolving set of social, behavioral, economic and technical factors.

> ***Our “Cyber Risk Guide for Corporate Leaders” offers top executives some basic solutions for managing cyber risk including specific steps you can take now to protect your operations. This includes strategies for identifying, quantifying and managing cyber risk - and transferring cyber risk using cyber risk insurance.***

How to Protect Your Operations

In this guide, we offer some basic approaches and best practices in cyber risk management and provide specific steps you can take to protect your operations. As a first line of defense, we provide guidelines to achieve cyber resilience. This includes proven strategies for identifying, quantifying, and managing cyber risk with the use of enterprise risk management (ERM) practices.

As a second line of defense, we focus on transferring risk through the use of cyber risk insurance and provide An Executive Guide to Cyber Risk Insurance (see page 5).

Your First Line of Defense

Building Cyber Resilience

Based on a recent survey by McKinsey and Company regarding the general understanding of cyber risk among corporate leaders, some get it and some don't[4]. The survey showed that many entities rely on a patchwork of solutions from a range of sources to manage cyber risk. Leaders at those organizations are unable to measure the return on their cybersecurity investments. They lack the necessary information about cyber risk levels, the effectiveness of countermeasures, and the status of protection for key assets. And many don't have a cohesive risk management plan in place.

On the other hand, those organizations which have maintained successful cyber risk practices first define the scope of their risk exposure and quantify their level of risk. This allows them to establish their cyber risk management objectives. They begin by taking stock of how cyber risk information is gathered and how they decide on counter measures. These organizations have assumed a risk-based approach which focuses on the most important assets and the biggest, most probable threats.

Decision makers can then allocate investments accordingly. "Resilience is thereby improved without an increased cybersecurity budget. In many cases, a state-of-the-art cyber risk management information system (MIS) allows reductions in operating expenditures as well," according to the report[4].

In order to become a cyber resilient organization, it is imperative that risk management practices are implemented across the entire operation and institutionalized and reviewed regularly by the entire organizational leadership.

Such an approach involves:

- **Replacing** fear, uncertainty and doubt with **Awareness**
- **Identifying** the unique cyber risks for your organization's budget
- **Quantifying** those risks within the context of your organization
- **Managing** those risks by providing your leadership with the appropriate tools to mitigate them

By adopting this approach, organizations can:

- Confidently prioritize their cyber risk remediation measures;
- Make educated decisions on risk acceptance levels;
- Use concrete data to help determine appropriate levels of cyber risk insurance coverage that aligns with budget and risk tolerance.

Principals of Enterprise Risk Management (ERM)

As advised by the National Institute of Standards and Technology, NIST, and as part of their governance responsibilities, executive leaders should establish clear and actionable risk management guidelines based on enterprise mission and sound business objectives[5]. Leaders at every level of an organization should establish specific parameters regarding risk appetite and risk tolerance. These values represent an enterprise strategy to ensure that various risks are managed to an acceptable level.

In the context of such a strategy, It is important to determine internal leaders, suppliers and other stakeholders' expectations regarding risk communications. It is also important to use readily understandable and agreed upon terms such as strategic objectives, organizational priorities, decision-making processes, and risk reporting methodologies. These should include regular risk management committee meetings and discussions.

As advised by NIST, an effective ERM program defines and communicates enterprise risk appetite so that meaningful risk tolerance statements can be created, used and monitored. Risk appetite also serves as a guidepost and reflects strategic risk direction from leadership. As the risk landscape evolves due to technological and environmental changes, organizational leaders should continually review and adjust their risk strategies.

Cyber Risk vs. Cybersecurity

Corporate leaders should understand some basic principles of risk management as well as the difference between cybersecurity and cyber risk. ***Cybersecurity*** *r*efers to the practice of protecting systems, networks, and programs from digital attack. ***Cyber risk*** refers to the exposure of potential business losses including operational, financial, regulatory, and reputational risk across an entire organization.

Cyber Risk Management is the practice of valuing assets in business terms (cost, revenue, etc.) and determining priorities and alternatives to optimize prevention of a cyber event AND resiliency from a cyber event.

Cyber risk management provides a methodology that allows leaders to work together to evaluate the range of cyber risks across the operation, prioritize the level of such risks, and apply risk mitigation and/or transfer risk through the use of cyber insurance.

Cyber Risk Management: Step by Step

All organizations should develop a strategy for addressing cyber risk including the following:

Step 1. Identify Your Cyber Risk Exposure

Identifying your organization's cyber risk exposure is the essential first step in order to make informed decisions about addressing that risk. Cybersecurity risk identification is comprised of four inputs:

1. Identification of the organization's mission supporting assets and their valuation
2. Determination of potential threats that might jeopardize the confidentiality, integrity, and availability of those assets and potential information and technology opportunities that might benefit the organization
3. Consideration of the vulnerabilities of those assets
4. Evaluation of the potential consequences of the loss or compromise of those assets

Organizations will likely require the assistance of a professional cyber risk management firm in order to adequately identify all their cyber risk exposure. A professional cyber risk consultant can help quantify an organization's cyber exposure. This includes estimating potential financial costs to respond to a breach, systems replacement, business interruption costs, potential fines and potential penalties and reputational damage. These risk practitioners may perform risk identification as both a top-down and bottom-up exercise.

Once an organization has considered critical or "mission-essential" functions, it may also consider various types of issues that could jeopardize those functions as an input to risk scenario development, a top-down approach. Cyber risk assessors may also consider how those threats might affect various assets, conducting a bottom-up assessment. This bidirectional approach helps support holistic and comprehensive risk identification.

It is critical to gain senior stakeholders' guidance regarding the determination of which assets are critical or sensitive - not just limited to an IT insider. The relative importance of each enterprise asset will be a necessary input for considering the impact portion of the risk analysis.

CASE STUDY:

SolarWinds Breach Traced to Russia

When hackers targeted SolarWinds by deploying malicious code into its Orion IT monitoring and management software, they hit the mother lode. Orion has been used by over 100,000 corporations and governmental agencies around the globe. The hackers were able to spy on companies including Microsoft, Cisco, Intel and Deloitte as well as U.S. government agencies including the State Department, the Department of Homeland Security and the Treasury Department.

The hackers used a method known as a supply chain attack to insert malicious code into the Orion system. A supply chain attack works by targeting a third party with access to an organization's systems rather than trying to hack the networks directly.

More than 18,000 SolarWinds customers installed the malicious updates placed into the software, with the malware spreading undetected. This allowed the hackers to access SolarWinds customer information technology systems. Federal investigators believe a Russian espionage operation – most likely Russia's Foreign Intelligence Service - was behind the attack.

Increasingly, many of the IT assets on which an organization depends are not within the organization's direct control. These external technical assets may include, but are not limited to, cloud-based software or platform services, telecommunications circuits, and video monitoring.

A core concept of ERM is prioritizing attention and resources on those assets that have the greatest impact on an enterprise's ability to achieve its mission.

Step 2. Quantify Your Cyber Risk for Financial Leadership

Year over year, many organizations allocate increasing amounts of budget, time, resources and technologies into cybersecurity. Yet it's difficult to determine the necessary cybersecurity investments without first quantifying cyber risk, complete with a translation into estimated financial costs. It's essential to be able to calculate the return on investment (ROI) for security budgets.

Variables impacting the magnitude of potential financial costs include data breach loss, cost per record loss, service disruption, IP loss, and reputational damage. Quantifying an organization's cyber risk is key to making informed decisions about addressing - and reducing - that risk and developing a strategy to manage that risk on an on-going basis. This is essential to share with the entire leadership team including the CFO, legal counsel and all others.

Without a concrete quantification of cyber risk in financial terms, leadership will struggle to allocate funding that properly safeguards their assets. An organization should adopt a solution that provides clarity of their cyber risk exposure and the financial impacts so better management decisions can be made.

Business metrics such as key performance indicators (KPIs) help steer leaders to make the best cyber risk management decisions for their organizations, thereby demonstrating due diligence and minimizing their potential financial loss.

Step 3. Monitor Insider Threats

An insider threat originates inside a target organization and could be orchestrated by a current or former employee or even a company officer. Studies have shown that as much as 47% of cyber breaches involve internal actors or due to HR deficiencies.

Any insider who has access to an organization's critical data, IT, IP, or has network access and/or control is a potential threat. They can be malicious insiders, such as disgruntled employees, or simply employees who inadvertently expose company assets without malicious intent.

Common signs of malicious insider activity that should be monitored include:

- *Downloading or accessing an unusual amount of critical internal files*
- *Extensive and frequent searches of critical data*
- *Copying sensitive files*
- *Emailing sensitive data to others*

Step 4. Evaluate and Track Third Party Risk

Third parties include external actors, such as people in a company's supply chain who are participating in providing goods and/or services. They include subcontractors, suppliers and vendors. These parties can expose an organization's confidential data such as intellectual property, financial data and customer records if proper measures are not in place. Every organization should monitor and track the cyber risk management policies of their third-party vendors just as they would their own company.

Step 5. Engage the Entire Management Team

Good governance and a holistic approach to managing cyber risk are critical, affirming that leaders are committed to performing a comprehensive appraisal and adoption of a unifying platform for their operations. It is important that organizations develop a risk model that is specific to that organization and then develop a risk mitigation, risk education and risk management plan.

Corporate leaders should work as a team and demand a holistic and objective examination of both their internal and external threat environments so that they can properly quantify their organization's cyber risk. The resulting business metrics and supplemental insights will steer leaders to make the best cyber risk management decisions for their organizations, thereby demonstrating due diligence and minimizing their potential financial loss.

In today's high-risk environment, addressing cyber risk at the leadership level is of utmost importance. The leadership team must recognize cyber risk as a business problem, not just an IT problem. Cyber attacks jeopardize business assets and, by extension, the financial livelihood of the entire enterprise.

Step 6. Engage in Ongoing Cyber Risk Management

Organizational leaders should work to assure that cyber risk quantification is performed on a continuous basis to gauge progress toward program goals. Cyber risk management must be treated as an ongoing process because cyber risk is constant, ever-present and continuously evolving. Conducting regular audits, making cyber a strategic priority, and performing cyber risk assessments are some of the most important steps organizations can take to prepare for cyberattacks.

Step 7. Transferring Risk with Cyber Insurance

Cyber insurance can be an effective way to transfer risk to a third party. Roughly 60% of for-profit and non-profit organizations currently carry cyber insurance while 100% are potentially at risk for a cyber breach. Of those organizations that do maintain such policies as many as 80% are underinsured for the potential cyber risk they face. The available coverage, limits, and premiums for cyber insurance are changing constantly. Due to the complexity of cyber risk insurance, in the following section we provide a detailed overview of cyber insurance entitled ***"An Executive Guide to Cyber Insurance."***

State of the Cyber Insurance Industry

Cyber insurance can be an effective way to transfer risk to a third party. Roughly 60% of organizations currently carry cyber insurance while 100% are potentially at risk for a cyber breach. Of those organizations that do maintain such policies as many as 80% are underinsured for the potential cyber risk they face.

However, the cyber insurance marketplace is complex and can be confusing. The cyber insurance industry is still in its infancy and is therefore evolving rapidly in terms of its availability, pricing, limits and exclusions.

At the same time, the cyber insurance marketplace is highly volatile. According to Tom Johansmeyer in the Harvard Business Review, "while more attacks could stimulate demand, they also create a supply problem, making insurers warier of providing coverage and reinsurers less interested in backing cyber liabilities. On top of that, the lack of historical loss data adds another layer of unpredictability for all involved[6]."

Cyber insurance is getting more costly by the month, limits are being reduced and exclusions are being expanded. It's possible that cyber insurance could become prohibitively expensive for many companies or the option for cyber insurance could be lost altogether. That would be the loss of an important risk transfer vehicle for organizations with significant technology exposure.

According to a recent report by Gallagher, "carriers have been under pressure due to the increasing frequency and severity of cyber claims and a rapidly expanding regulatory environment at the state, federal and international levels." As a result, there will likely be a reduction of capacity in the market, which will likely continue to drive up pricing. Some industries are already seeing significantly higher premiums and a "pulling back" from high-risk industries all together[7].

So what are the options? Organizations may have to plan without the possibility of being able to acquire the adequate level of cyber insurance to cover their full cyber risk exposure. That could include "stacking" several policies of cyber insurance to get to a higher level of coverage as well as adding self-insurance strategies (such as reserving capital for future cyberattacks).

Cyber Policies Cover Two Types of Risk

Cyber policies generally tend to fall within two types: policies that provide First Party coverage and policies that provide Third Party coverage.

> ***"While more attacks could stimulate demand, they also create a supply problem, making insurers warier of providing cover and reinsurers less interested in backing cyber liabilities. On top of that, the lack of historical loss data adds another layer of unpredictability for all involved."***
>
> Tom Johansmeyer
> Harvard Business Review

First Party Coverage

First Party coverage policies typically cover costs associated with the immediate response to a cyber event and are designed to mitigate a breach or attack.

First Party coverage may include:

- The cost of investigating and quantifying the cost of a breach, including forensic costs
- The cost of the overall network security system and associated services including hardware and software in case these were totally disabled and must be replaced
- Legal expenses
- Business interruption losses as a result of a cyber event
- Crisis management fees and costs to retain a communication and public relations firm, including notification costs associated with informing affected parties
- Coverage related to cyber extortion such as ransomware
- Losses in third party systems
- Costs of replacing lost or stolen equipment including laptops and mobile devices
- The costs of credit monitoring and crisis management

Third Party Coverage

Third party coverage policies are intended to cover costs that are associated with a cyber event but may be less immediate and include costs that are often subsequent to the actual breach such as:

- costs of privacy liability lawsuits
- negligence lawsuits
- copyright lawsuits
- costs associated with penalties and fines levied by regulatory authorities
- legal fees associated with fighting and responding to such cases

Types of Cyber Coverage

A cyber policy can include coverage for a wide range of risk types and risk components. The following types of coverage may be included in a comprehensive cyber policy or it may be necessary to add additional “endorsements” to a basic policy.

Here’s a breakdown of coverages to consider:

1. **Network Security, Data Breach, Ransomware and Cyber Extortion** - This is coverage in the event of an overall network security failure. This could involve a data breach, cost of extortion, ransomware, and the cost of restoring systems and data to pre-breach levels. Expenses covered may include IT forensics, legal expenses, public relations and communication expenses, and negotiation expense and payment of a ransom.
2. **Privacy Liability** - This includes liability costs that result from a cyber incident or the violation of certain privacy regulations. Such costs can result from contractual liabilities or regulatory investigations from state, federal and even foreign regulatory agency fines. Be aware, contractual liabilities include any indemnifications an organization might have made with other parties to compensate them in the event of a cyber incident or data breach.
3. **Business Interruption** - Often referred to as Network Business Interruption coverage, this covers organizations whose network operations are halted due to a cyber event. This applies to self-owned networks as well as third party networks that operations are dependent on. This coverage can cover lost revenue and expenses incurred while an organization was affected and may apply to a security breach such as a ransomware attack or a system failure caused by human error.
4. **Reputational Damage Coverage** - Media coverage of a major breach may result in the decline in popularity or desire for a specific product or service. A major breach can also cause a loss in confidence in public officials and/or other personnel. However, the impact of such reputational damage can be difficult to prove. Reputational damage coverage is typically a part of network business interruption and can continue long after the initial damage occurred.
5. **Media Liability** - This provides coverage for intellectual property infringement resulting from the advertising of an organization’s services. It often applies only to online advertising, including social media posts, but it’s possible to expand this coverage to include printed advertising as well.

The Benefits of Cyber Insurance

- Companies often maintain large volumes of personal data on individuals including those owning property and paying taxes, those purchasing services, and those paying penalties and fines. *Cyber insurance can help cover costs for companies to comply with such laws after a cyber breach*.
- Like most organizations, most people today are likely dependent on technology to operate. If access to those systems is lost or interrupted, *cyber insurance can help reduce the financial impact on the operation.*
- Emergency back-up is often included in cyber policies. *Cyber policies typically include a team of experts who help take charge in the immediate aftermath of a breach.* These may include ransom negotiations, forensic specialists, communication specialists, and legal counsel.
- *Cyber insurance carriers typically provide associated services that include security recommendations, avoidance strategies, and discounted services that can be of value to an organization*. These are referred to as “pre-loss services.”

6. **Third Party Liability Coverage - This coverage can include oto Third Party liabilities arising in relation to product liability and defective operations, coverage for third party claims relating to failure to provide adequate technical service or technical products including legal costs and expenses relating to a cyber attack or IT failure. Such coverage can also include coverage for third party claims relating to failure to provide adequte professional services or products.**
7. Errors & Omissions (E & O) - if a cyber event prevents an organization from fulfilling contractual obligations and delivering services to customers, E & O coverage addresses allegations of negligence or breach of contract in such cases. Coverage can include legal defense costs or indemnification resulting from a lawsuit or dispute with customers.

Cyber Insurance Exclusion Review

Cyber insurance can be tricky and present unwanted surprises when the unfortunate time comes to fall back on it. Here are a few tips on what to look for in terms of common reasons for claims being declined - or reduced. It is important to understand the key concepts of sub-limits, exclusions, and failures to perform specific responsibilities as directed in the cyber policy.

A cyber risk consultant can help guide leaders through a proposed policy and carefully review the exclusions, limits and sub-limits. Just remember, an insurance broker may be highly professional with years of experience - but his or her goal is to sell a policy! Here are some key exclusions and clauses to understand and review in a cyber risk policy.

Failure to Maintain

Sometimes referred to as the "failure to follow" exclusion, this eliminates coverage for claims resulting from the insured's failure to maintain minimum or adequate security standards. This is a broad and sometimes vague exclusion that might read "failure to continuously implement the procedures and risk controls identified in the insured's application." In some cases, claims have been denied due to a lack of the use of basic controls such as employee

PCI Fines & Assessments

Coverage can be denied for payment card industry (PCI) or self-regulatory fines and contractual liability exclusions. Some policies contain exclusions for viruses or self-propagating code which could also result in the loss of PCI coverage. Insured parties should also carefully review their internal contractual obligations with third parties and suppliers and understand the requirements as spelled out in the policy.

Cyber Extortion and Ransomware

While some ransomware payments may initially sound low, keep in mind that most of the costs and damages incurred as a result of a cyber breach typically are in the form of lost income, systems restoration and even longer-term reputation harm. An organization may pay a $100,000 ransom, for example, a significant portion of which might be covered within a policy. But $2,000,000 in damages incurred as a result of the breach may be largely excluded, depending on the language and limits spelled out in the policy.
Based on the above scenario, it is extremely important to closely evaluate the "extortion insuring clause" in a policy. This includes carefully reviewing all limits, sub-limits, deductibles and time deductibles spelled out in the policy.

An all-inclusive cyber policy should include "any business interruption due to cyberattack" as well as "information theft" and "any loss due to IT theft" and "identity theft."

Social Engineering Schemes/Fraudulent Transactions

Social engineering schemes are becoming more common and can take the form of phishing emails, by phone or using fake letterhead, or by altering bank account information. Many policies include clauses limiting coverage of such schemes.
For example, funds transferred by a person with authority using the insured's computer system (which might occur through a fake request from a supervisor). Or in some cases, losses have been incurred by clients but not by the insured. Or a fraudulent transfer of funds was carried out via phone as opposed to having occurred on an insured's computer.

It is important to protect against the risk of being denied coverage for such claims to make sure that a cyber policy includes an endorsement for social engineering as opposed to a computer fraud/forgery insuring clause alone. This may also be referred to as "social media liability" or "media liability coverage."

It is important to make sure that requested inclusions in a policy address any fraudulent transactions taking place online in the organization's bank account, e-wallet, credit or debit cards as well as financial loss incurred due to phishing and email spoofing.

Third Party Risks

As already stated, several of the major breaches occurring in 2021 have pointed to the rapidly growing threat from third parties. When purchasing a cyber risk policy, an organization should be wary of any exclusions related to third party coverage. Being aware of common exclusions is important but ensuring that specific inclusion language covering third parties is also critical. Two important inclusions regarding third party liability which should be considered are: “breach of data and privacy by a third-party leading to loss of personal information” and “any business interruption due to cyberattack, including those originating from third parties.”

Loss of Hardware and Software Systems

This is often an immediate and significant cost to organizations that have experienced a cyber breach. A policy should address this in clauses that cover areas such as “unrecoverable damage or loss of data belonging to your organization’ and “the expenses of replacing, repairing and updating your computer system.”

Additionally, requesting a “bricking coverage endorsement” is suggested. Since almost all cyber insurance claims contain some property damage exclusions, this endorsement covers damage to computers that can be caused by crypto-jacking and other such breaches and covers the costs to repair or replace computer systems that may be destroyed in the context of a cyberattack.

Another available endorsement is “System Failure Coverage” which covers lost income resulting from any unintentional or unplanned system failure. These often extend coverage to include lost income resulting from system failures that affect dependent third parties.

Exclusions Related to Reputational Damage

An endorsement for “reputational harm” or reputational loss” can cover losses incurred from lost income due to negative public relations following a cyber event. Such coverage is often severely sub-limited. Since a direct relationship can be hard prove, such as damage from a specific publication, endorsements that have no “direct” requirement to trigger coverage are preferred by the insured party.

Exclusions Related to Privacy Regulations

The relatively recent enactment of privacy regulations such as GDPR and CCPA now subject companies and their directors to more regulatory scrutiny and potential fines and penalties for privacy related violations. For this coverage, it may be necessary to obtain specific GDPR and CCPA endorsements that provide coverage for costs associated with violations of these laws.

In Conclusion: Prepare for the Future

Looking forward, new technologies will continue to influence cyber risk in 2022 and beyond. Expanded networks in the form of 5G will allow broader access for people and devices. More accessible broadband at higher speeds will lead to the development and use of everything from connected devices to virtual reality and artificial intelligence, according to guidelines provided by the World Economic Forum in 2020[9]. “With these network developments, more data will be created and collected than ever before, making policy attempts to protect this data more urgent,” the report stated.

To address this challenge and the elevated risk environment, corporate leaders should acquire new knowledge, approaches and technical tools to ensure responsible use of data to increase their cyber resilience.

SOURCES AND ADDITIONAL READING:

[1] *Cybercrime to Cost World $10.5 Trillion by 2025,* Cybersecurity Ventures, November 13, 2020

[2] *The Risk-Based Approach to Cybersecurity*, McKinsey & Company, October 9, 2019, by Jim Boehm, Nick Curcio, Peter Marath, Lucy Shenton, and Tobias Stahle

[3] *Cyber Risk Quantified. Cyber Risk Managed,* PwC, Global Digital Trust Insights 2021 Survey, by Joseph Nocera, T.R. Kane, Jason Stauffenecker, and Nick Blaesing.

[4] *Enhanced Cybersecurity Reporting: Opening Doors to Risk-Based Security,* McKinsey & Company, January 20, 2020, by Jim Boehm, James M. Kaplan, Peter Merrath, Thomas Poppensieken and Tobias Stahle.

[5] *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, October 2020, NISTIR 8286, an official website of the United States Government, by Kevin Stine, Stephen Quinn, Gregory Witte, and Robert Gardner

[6] *Cybersecurity Insurance Has a Big Problem*, Harvard Business Review, January 11, 2021, by Tom Johansmeyer

[7] The *2021 Cyber Insurance Market Continues to Harden,* Gallagher Market Conditions, February 2021, by John Farley, Managing Director, Cyber Practice

[8] *Cyber Insurers Hike Rates, Tweak Coverage as Loss Ratio Rises Again in 2020*, S&P Global Market Intelligence, June 1, 2021, by Calvin Trice and Kris Elaine Figuracion

[9] *Insurers Run from Ransomware Cover as Losses Mount,* Reuters Risk Management, November 19, 2021.

[10] *Why 2020 Is a Turning Point for Cybersecurity,* World Economic Forum, January 23, 2020, by Alois Zwinggi, Managing Director and Head, Centre for Cybersecurity, World Economic Forum

About the Authors

Chris Burrow is a Partner and Senior Strategic Advisor at Maxxsure Cyber Risk Management based in Addison, Texas. Chris has served in CEO, CFO, COO, and board positions in both for- profit and non-profit organizations for over 30 years. Those include organizations in the real estate services and advisory sectors as well as educational institutions and foundations. Chris enjoys cycling, golf, mountain climbing and business writing in his spare time.

chris.burrow@maxxsure.com
+1 214.244.5047

Shawn Wiora is a co-founder and CEO of Maxxsure. He is a keynote speaker and has appeared in national and international media discussing cyber risk management, cybersecurity and cyber insurance. These include the Wall Street Journal, CNNMoney and CIO.com. He is a cyber industry expert and moved the first healthcare company in the U.S. to be 100% in the cloud which received a designation as the most cyber-resilient healthcare company in the U.S. Shawn enjoys golf, staying fit, keeping abreast of the latest technology innovations in electric vehicles and virtual reality.

shawn.wiora@maxxsure.com
+1 214.649.0706

About Maxxsure

Maxxsure is a cyber risk quantification, management and advisory firm based in Addison, Texas. The firm's services and proprietary management platform enable clients to confidently identify, quantify and manage cyber risk.

The firm's customers include global industry leaders in commercial real estate services and investments, financial services, law, ratings, gaming, wealth management, telecommunications, and data management, to name a few. Customers range in size from $25 million to $25 billion in annual revenue.

Maxxsure was founded in 2016 with the mission of developing the best-in-class cyber risk quantification and management solution that takes a truly holistic survey of all internal and external influencing factors over the cyber risk posture of an organization.

With Maxxsure, organizations have continuous line of sight into their cyber risk, allowing them to access up-to-date data to make adaptations to their cyber risk management strategies as their needs and environments change. The company provides a platform for executive management, leveraging proprietary technology that:

- *Identifies, measures, and scores an organization's cyber risks*
- *Uncovers hidden risks in a business model, including vendors/supply chain*
- *Illustrates how prepared/resilient an organization is against a cyber event*
- *Estimates potential financial loss of future events*

MAXXSURE

www.maxxsure.com

CORPORATE OFFICE:
4570 Westgrove Drive Suite 235
Addison, Texas 75001 USA