MARSH & McLENNAN COMPANIES | Global Risk Center | WCD WomenCorporateDirectors
A Foundation Inspiring Visionary Boards Worldwide

CYBER RISK MANAGEMENT

Response and Recovery

GLOBAL GOVERNANCE INSIGHTS ON EMERGING RISKS

MARSH GUY CARPENTER MERCER OLIVER WYMAN

A NOTE FROM **WOMENCORPORATE DIRECTORS**

One of the most critical emerging risks weighing on directors' minds is the area of cybersecurity. Today, every single industry is digital, which means that we're all vulnerable to breaches, data loss, and ransomware attacks. When the next cyberattack comes (and it's a "when," not an "if"), boards want to be reassured that their organization is sufficiently covered to mitigate damage. But many directors are unclear about what this really means, or what role insurance plays in the whole cyber risk management framework.

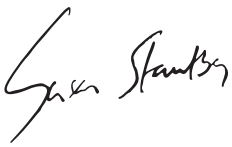
In this report, WomenCorporateDirectors (WCD) has teamed up with Marsh & McLennan Companies (MMC) Global Risk Center to provide an overview of what boards need to know about cyber risk and how cyber insurance fits into an organization's total risk management process. This paper arms directors with the right questions to ask management, advisors and potential insurers so that directors can go into discussions with the knowledge and background needed to address this growing risk.

At WCD, we are committed to bringing directors the most up-to-date insight around governance and strategy, enabling them to serve as highly effective corporate stewards. This valuable research from MMC is something every director should read and keep on-hand for cyber discussions ahead – especially as the risks continue to rise each day.

SUSAN C. KEATING

CEO, WCD

SUSAN STAUTBERG



Chair Emeritus and Co-founder, WCD

HOW TO USE THIS REPORT

Cyber insurance is a new and rapidly evolving field and many directors and management teams are uncertain how to assess its value. This report positions cyber insurance within a comprehensive cyber risk management framework, provides an overview of evolving coverage options, and identifies key questions for directors to explore with management to mitigate exposure and provide effective cyber risk management oversight.

READ ON TO LEARN MORE...

A HEIGHTENED FOCUS ON RESPONSE AND RECOVERY

Over a third of directors of US public companies now discuss cybersecurity at every board meeting. Cyber risks are being driven onto the agenda by high-profile data breaches[1], distributed denial of services (DDoS) attacks, and rising ransomware and cyber extortion attacks. The concern about cyber risks is justified. The annual economic cost of cyber-crime is estimated at US$1.5 trillion and only about 15% of that loss is currently covered by insurance.

MMC Global Risk Center conducted research and interviews with directors from WCD to understand the scope and depth of cyber risk management discussions in the boardroom. The risk of cyberattack is a constantly evolving threat and the interviews highlighted the rising focus on resilience and recovery in boardroom cyber discussions. Approaches to cyber risks are maturing as organizations recognize them as an enterprise business risk, not just an information technology (IT) problem.

However, board focus varies significantly across industries, geographies, organization size and regulatory context. For example, business executives ranked cyberattacks among the top five risks of doing business in the Asia Pacific region but Asian organizations take 1.7 times longer than the global median to discover a breach and spend on average 47% less on information security than North American firms.[2]

REGULATION ON THE RISE

Tightening regulatory requirements for cybersecurity and breach notification across the globe such as the EU GDPR, China's new Cyber Security Law, and Australia's Privacy Amendment, are also propelling cyber onto the board agenda. Most recently, in February 2018, the USA's Securities and Exchange Commission (SEC) provided interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.[3]

Regulations relating to transparency and notifications around cyber breaches drive greater discussion and awareness of cyber risks. Industries such as financial services, telecommunications and utilities, are subject to a large number of cyberattacks on a daily basis and have stringent regulatory requirements for cybersecurity.

Kris Manos, Director, KeyCorp, Columbia Forest Products, and Dexter Apache Holdings, observed, "The manufacturing sector is less advanced in addressing cyber threats; the NotPetya and WannaCry attacks flagged that sector's vulnerability and has led to a greater focus in the boardroom." For example, the

"The manufacturing sector is less advanced in addressing cyber threats; the NotPetya and WannaCry attacks flagged that sector's vulnerability and has led to a greater focus in the boardroom."

KRIS MANOS
Director, KeyCorp, Columbia Forest Products, and Dexter Apache Holdings

"The focus on cyber can vary across industries depending also on their perception of their own clients' concerns regarding privacy and data breaches."

CRISTINA FINOCCHI MAHNE, Director, Inwit, Italiaonline, Banco Desio, Natuzzi and Trevi Group

1 What Directors Think: Guided Optimism Amid a Shifting Political Landscape, Spencer Stuart, March 2017.

2 Cyber Risk in Asia Pacific: The Case for Greater Transparency, 2017 and Cyber Risk in Asia: Ramifications for Real Estate and Hospitality, 2017, both from Asia Pacific Risk Center, MMC.

3 See: GDPR Preparedness: An Indicator of Cyber Risk Management, Marsh, 2017; The Privacy Amendment (Notifiable Data Breaches) Bill 2016 was enacted in February 2017. Australian organizations now have to publicly disclose any data breaches, with penalties ranging from $360,000 for responsible individuals to $1.8 million for organizations. Also, China introduced a sequence of legislative reforms in recent years that seek to ensure stronger data protection, see more: MMC Cyber Handbook 2018. See: SEC Statement and Interpretive Guidance on Public Company Cyber Security Disclosures, February 2018.

virus forced a transportation company to shut down all of its communications with customers and also within the company. It took several weeks before business was back to normal, and the loss of business was estimated to have been as high as US$300 million. Overall, it is estimated that as a result of supply chain disruptions, consumer goods manufacturers, transport and logistics companies, pharmaceutical firms and utilities reportedly suffered, in aggregate, over US$1 billion in economic losses from the NotPetya attacks.[4] Also, as Cristina Finocchi Mahne, Director, Inwit, Italiaonline, Banco Desio, Natuzzi and Trevi Group, noted, "The focus on cyber can vary across industries depending also on their perception of their own clients' concerns regarding privacy and data breaches."

"Such events highlight vulnerability beyond your organization's control and are raising the focus on IT security throughout the supply chain."

SHIRLEY DANIEL
Director, American Savings Bank, and Pacific Asian Management Institute

LESSONS LEARNED: UPDATE RESPONSE PLANS AND EVALUATE THIRD-PARTY RISK

The high-profile cyberattacks in 2017, along with new and evolving ransomware onslaughts, were learning events for many organizations. Lessons included the need to establish relationships with organizations that can assist in the event of a cyberattack, such as law enforcement, regulatory agencies and recovery service providers including forensic accountants and crisis management firms.

Many boards need to increase their focus on their organization's cyber incident response plans. A recent global survey found that only 30% of companies have a cyber response plan and a survey by the National Association of Corporate Directors (NACD) suggests that only 60% of boards have reviewed their breach response plan over the past 12 months.[5] Kris Manos noted, "[If an attack occurs,] it's important to be able to quickly access a response plan. This also helps demonstrate that the organization was prepared to respond effectively."

Experienced directors emphasized the need for effective response plans alongside robust cyber risk mitigation programs to ensure resilience, as well as operational and reputation recovery. As Jan Babiak, Director, Walgreens Boots Alliance, Euromoney Institutional Investor, and Bank of Montreal, stressed, "The importance of the 'respond and recover' phase cannot be overstated, and this focus needs to rapidly improve."

Directors need to review how the organization will communicate and report breaches. Response plans should include preliminary drafts of communications to all stakeholders including customers, suppliers, regulators, employees, the board, shareholders, and even the general public. The plan should also consider legal requirements around timelines to report breaches so the organization is not hit with financial penalties that can add to an already expensive and reputationally damaging situation. Finally, the response plan also needs to consider that normal methods of communication (websites, email, etc.) may be casualties of the breach. A cyber response plan housed only on the corporate network may be of little use in a ransomware attack.

"There is a definite trend by boards to think more about preparedness, recovery and resilience because there is an assumption their organizations will be hacked. It is about how soon you can be back up and operating."

CATHERINE ALLEN
Director, Synovus Financial Corporation, El Paso Electric Company and Analytics Pros

Other lessons included the need to focus on cyber risks posed by third-party suppliers, vendors and other impacts throughout the supply chain. Shirley

4 Cyber: The Stakes Have Changed for the C-Suite, Marsh & McLennan Companies and FireEye, January 2018

5 National Association of Corporate Directors (NACD) Public Company Governance Survey, 2017-2018; Global Cyber Risk Perception Survey, Marsh and Microsoft, January 2018; See also, Practical Cyber Response: Being Fully Prepared for the Inevitable, Paul Mee and Chris Debrusk, Partners, Oliver Wyman, 2017

Daniel, Director, American Savings Bank, and Pacific Asian Management Institute, noted, "Such events highlight vulnerability beyond your organization's control and are raising the focus on IT security throughout the supply chain." Survey data suggests that about a third of organizations do not assess the cyber risk of vendors and suppliers.[6] This is a critical area of focus as third-party service providers (e.g., software providers, cloud services providers, etc.) are increasingly embedded in value chains.

FRUSTRATIONS WITH OVERSIGHT

Most directors expressed frustrations and challenges with cyber risk oversight even though the topic is frequently on meeting agendas. Part of the challenge is that director-level cyber experts are thin on the ground; most boards have only one individual serving as the "tech" or "cyber" person. A Spencer Stuart survey found that 41% of respondents said their board had at least one director with cyber expertise, with an additional 7% who are in the process of recruiting one.[7] Boards would benefit from the addition of experienced individuals who can identify the connections between cybersecurity and overall company strategy.

A crucial additional challenge is obtaining clarity on the organization's overall cyber risk management framework. (See Exhibit 1: Boards Need More Information on Cyber Investments.) Olga Botero, Director, Evertec, Inc., and Founding Partner, C&S Customers and Strategy, observed, "There are still many questions unanswered for boards, including: How good is our security program? How do we compare to peers? There is a big lack of benchmarking on practices." Anastassia Lauterbach, Director, Dun & Bradstreet, and member of Evolution Partners Advisory Board, summarized it well, "Boards need a set

"Much mission-critical data is housed by third-parties and it raises questions about how we can determine whether they are properly managing this information – or even our recourse if the information is mishandled across international borders."

SUZAN BAYAZIT
Co-Chair, Toplum Gönüllüleri Vakfı

6 Global Cyber Risk Perception Survey, Marsh and Microsoft, January 2018.
7 What Directors Think: Guided Optimism Amid a Shifting Political Landscape, Spencer Stuart, March 2017.

Exhibit 1: Boards Need More Information on Cyber Investments

45%

of risk and technology executives said they send information on

YET ONLY...

18%

of directors said they receive such information

Source: Global Cyber Risk Perception Survey, Marsh & Microsoft, 2018

of KPIs for cybersecurity highlighting their company's unique business model, legacy IT, supplier and partner relationships, and geographical scope."

Nearly a quarter of boards are dissatisfied with the quality of management-provided information related to cybersecurity because of insufficient transparency, inability to benchmark and difficulty of interpretation.

EFFECTIVE OVERSIGHT IS BUILT ON A COMPREHENSIVE CYBER RISK MANAGEMENT FRAMEWORK

Organizations are maturing from a "harden the shell" approach to a protocol based on understanding and protecting core assets and optimizing resources. This includes the application of risk disciplines to assess and manage risk, including quantification and analytics.[8] (See Exhibit 2: Focus Areas of a Comprehensive Cyber Risk Management Framework.) Quantification shifts the conversation from a technical discussion about threat vectors and system vulnerabilities to one focused on maximizing the return on an organization's cyber spending and lowering its total cost of risk.

Directors also emphasized the need to embed the process in an overall cyber risk management framework and culture. "The culture must emphasize openness and learning from mistakes. Culture and cyber risk oversight go hand in hand," said Anastassia Lauterbach. Employees should be encouraged to flag and highlight potential cyber incidents, such as phishing attacks, as every employee plays a vital role in cyber risk management. Jan Babiak noted,

8 See also, "Deploying A Cyber Risk Strategy: Five key moves beyond regulatory compliance," Paul Mee and James Morgan, Oliver Wyman, 2017.

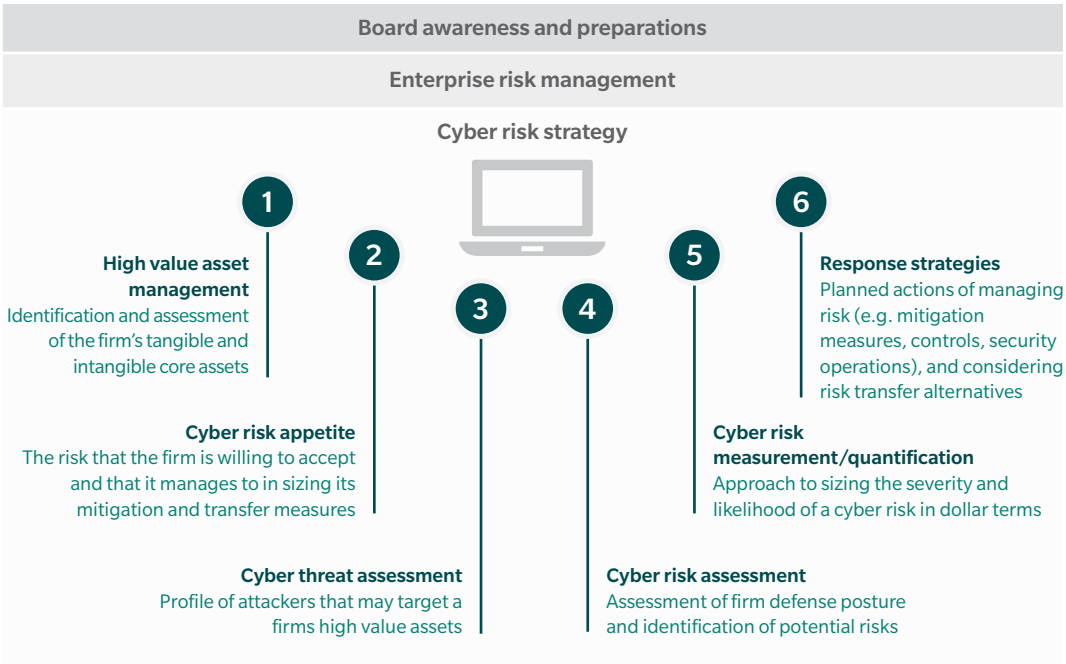
"Establishing IT-related accountability within the enterprise is important."

WENDY WEBB
Director, ABM Industries

"Boards need a set of KPIs for cybersecurity highlighting their company's unique business model, legacy IT, supplier and partner relationships, and geographical scope."

ANASTASSIA LAUTERBACH, Director, Dun & Bradstreet, and member of Evolution Partners Advisory Board

Exhibit 2: Focus Areas of a Comprehensive Cyber Risk Management Process



Source: Marsh & McLennan Companies

"If every person in the organization doesn't view themselves as a human firewall, you have a soft underbelly." Mary Beth Vitale, Director, GEHA and CoBiz Financial, Inc., also noted, "Much of cyber risk mitigation is related to good housekeeping such as timely patching of servers and ongoing employee training and alertness."

Boards also need to be alert. "Our board undertakes the same cybersecurity training as employees," noted Wendy Webb, Director, ABM Industries. Other boards are putting cyber updates and visits to security centers on board "offsite" agendas.

"Boards should be presented with a detailed overview of their risk profiles to ensure cyber risk mitigation and insurance coverage is in line with risk appetite."

OLGA BOTERO
Director, Evertec, Inc., Founding Partner, C&S Customers and Strategy

THE ROLE OF CYBER INSURANCE

Although the perception of many directors is that cyber insurance provides for limited coverage, the insurance is increasingly viewed as an important component of a cyber risk management framework and can support response and recovery plans. Echoing this sentiment, Geeta Mathur, Director, Motherson Sumi Ltd, IIFL Holdings Ltd, and Tata Communication Transformation Services Ltd., commented, "There is a lack of information and discussion on risk transfer options at the board level. The perception is that it doesn't cover much particularly relating to business interruption on account of cyber threats." Cristina Finocchi Mahne also noted, "Currently, management teams may not have a positive awareness of cyber insurance, but we expect this to rapidly evolve over the short-term."

Insurance does not release the board or management from the development and execution of a robust risk management plan but it can provide a financial safeguard against costs associated with a cyber event. Cyber insurance coverage should be considered in the context of an overall cyber risk management process and cyber risk appetite.

With a robust analysis, the organization can quantify the price of cyber risk, develop effective risk mitigation, transfer and risk financing strategy, and decide if – and how much – cyber insurance to purchase. This allows the board to have a robust conversation on the relationship between risk, reward and the cost of mitigation and can also prompt an evaluation of potential consequences by using statistical modeling to assess different damage scenarios.

"Insurance firms are constantly developing their offering to respond to changing cyber threats. The process of reassessing coverage can help the organization understand their exposure and push the organization to really consider mitigation and response plans."

ANNALISA GIGANTE
Director, Foundations for Learning and Jagex

CYBER INSURANCE ADOPTION IS INCREASING

The role of insurance in enhancing cyber resilience is increasingly being recognized by policymakers around the world, and the Organisation of Economic Co-operation and Development (OECD) is recommending actions to stimulate cyber insurance adoption.[9]

Globally, it is expected the level of future demand for cyber insurance will depend on the frequency of high-profile cyber incidents as well as the evolving legislative and regulatory environment for privacy protections in many countries. In India, for example, there was a 50% increase in companies buying cybersecurity coverage 2016 to 2017.[10]

9 UK Cybersecurity: The Role of Insurance in Managing and Mitigating the Risk, Marsh LLC, 2015, and Enhancing the Role of Insurance in Cyber Risk Management, OEDC, 2017.

10 Demand for cyber insurance cover jumps 50%, Economic Times, January 4, 2017.

Research suggests that only 40% of US boards have reviewed their organization's cyber insurance coverage in the past 12 months.

LIMITING FINANCIAL LOSSES

In the event of a debilitating attack, cyber insurance and associated services can limit an organization's financial damage from direct and indirect costs and help accelerate its recovery. (See Exhibit 3: Direct and Indirect Costs Associated with a Cyber Attack.) For example, as a result of the NotPetya attack, one global company reported a decline in operating margins and income, with losses in excess of US$500 million in the last fiscal year. The company noted the costs were driven by investments in enhanced systems in order to prevent future attacks; cost of incentives offered to customers to restore confidence and maintain business relationships; additional costs due to claims for service failures; costs associated with data breach or data loss due to third-parties; and "other consequences of which we are not currently aware but may subsequently discover."

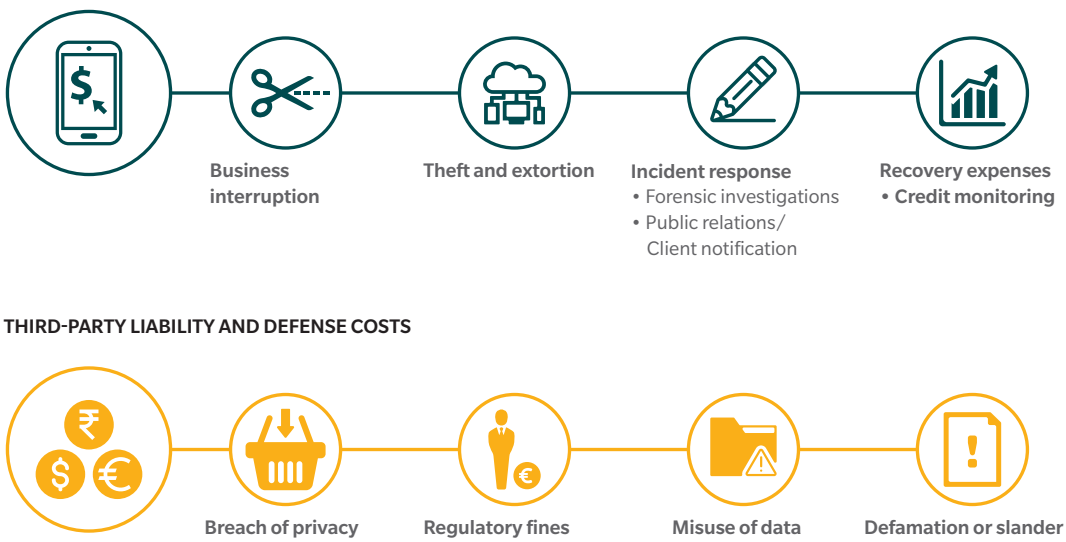
Indeed, the very process of assessing and purchasing cyber insurance can bolster cyber resilience by creating important incentives that drive behavioral change, including:

- Raising awareness inside the organization on the importance of information security.
- Fostering a broader dialogue among the cyber risk stakeholders within an organization.
- Generating an organization-wide approach to ongoing cyber risk management by all aspects of the organization.
- Assessing the strength of cyber defenses, particularly amid a rapidly changing cyber environment.

"Your cyber insurance carrier can be of tremendous help with the process for responding to a breach, such as identifying the right experts to help assess your exposure and the remediation necessary. These processes can be longer and costlier than anticipated, and many boards may not have a sense of the expertise required."

MARY BETH VITALE
Director, GEHA and CoBiz Financial, Inc.

Exhibit 3: Direct and Indirect Costs Associated with a Cyberattack



Source: Marsh & McLennan Companies

OPTIONS FOR CYBER COVERAGE

Insurers are responding to evolving cyber threats and costs by providing expanded coverage options for business interruption, extortion, and costs associated with response and recovery. (See Appendix: Guide to Cyber Coverage Options.)

Cyber insurance can be obtained on a standalone basis or through cyber-specific endorsements to traditional policies. As an additional benefit, standalone cyber insurance products include access to service providers that can assist policyholders in responding to cyber incidents and preparing response plans. For example, training, forensic experts to assess the extent of the intrusion, legal expertise on necessary notification and disclosure, public relations support and response plan protocols. Small organizations especially benefit from the expert assistance.

COMMON INSURANCE OVERLAPS

Cyber insurance is intended to cover the gaps in traditional insurance coverage, as well as covering new digital risks. As organizations assess their cyber insurance coverage options, it is important to understand how cyber incidents may be covered in existing policies. This is a challenge for many organizations as there can be overlaps or "silent coverage" for cyber incidents in existing policies. For example:

- Property
- Casualty
- Crime
- Errors & Omissions (E&O) or Professional Indemnity
- Kidnap and Ransom

However, insurers are increasingly excluding cyber coverage under existing policies, which places a growing focus on the need and value of standalone policies. To help identify gaps and overlaps, management teams can work with insurance brokers to conduct a comprehensive gap analysis across all insurance lines and develop a dashboard of existing coverage.

In evaluating a cyber insurance purchase decision, organizations can also use broad industry benchmarks, such as comparisons of insurance coverage by peer firms or cyber coverage per dollar of revenue. "Management needs to research and provide analysis that ensures the organizations they serve buy insurance from a holistic perspective. That means a wide range of risks are covered, not just cyber," noted Catherine Allen, Director, Synovus Financial Corporation, El Paso Electric Company and Analytics Pros.

Nevertheless, when determining insurance coverage, organizations should undertake a detailed analysis of their digital assets, their exposures and overall cyber risk appetite to tailor coverage to their needs. Each organization is unique; even in the same industry differences exist – in the amount of data captured by companies, in the way they use, process or store data is different, and with the vendors/suppliers they rely on.

"High-profile attacks are pushing more formal cyber risk discussions into the main board agenda, but risk mitigation is being discussed around technology related interventions and business continuity planning, but not insurance."

GEETA MATHUR
Director, Motherson Sumi Ltd, IIFL Holdings Ltd, and Tata Communication Transformation Services Ltd

CONCLUSION: RISING PRESSURES

As cyber risks continue to grow and their potential impact on the economy increases, organizations will face rising pressures to implement a robust and comprehensive cyber risk management framework. Cyber insurance is increasingly viewed as a critical element to help manage the costs and impacts of a cyberattack on an organization. As the product continues to evolve, directors should question management on their approach to cyber insurance and adoption of this risk transfer mechanism. Spend the time and attention to develop a comprehensive framework for response and recovery and be prepared to mitigate cyber risks by investing in appropriate levels of insurance coverage.

"If every person in the organization doesn't view themselves as a human firewall, you have a soft underbelly."

JAN BABIAK
Walgreens Boots Alliance, Euromoney Institutional Investor, and Bank of Montreal

| PROTECTING DIRECTORS AND OFFICERS |

PROTECTING DIRECTORS AND OFFICERS: WHAT YOUR D&O INSURANCE SHOULD COVER

It is critical to ensure the organization's Directors and Officers (D&O) Liability insurance—in addition to cyber coverage—will respond under a regulatory investigation and/or litigation alleging traditional claims for breach of fiduciary duties relating to a cyber event. A D&O policy should provide cover in the following areas:

INVESTIGATION COSTS
Regulatory investigations arising out of a cyber incident, and at full policy limits.

INSURED INDIVIDUALS
All persons who are involved in significant cyber-related decisions and implementation on behalf of the company.

INVESTIGATION OF CYBER CIRCUMSTANCES
Costs incurred investigating any circumstance resulting from a cyber event where litigation is anticipated.

ALLOCATION
Clear demarcation between the entity and the individual with loss attributable to the directors allocated appropriately.

SHAREHOLDER ACTIONS
Shareholder actions against the company which arise as a result of a cyber-related incident (for example, following a stock-drop).

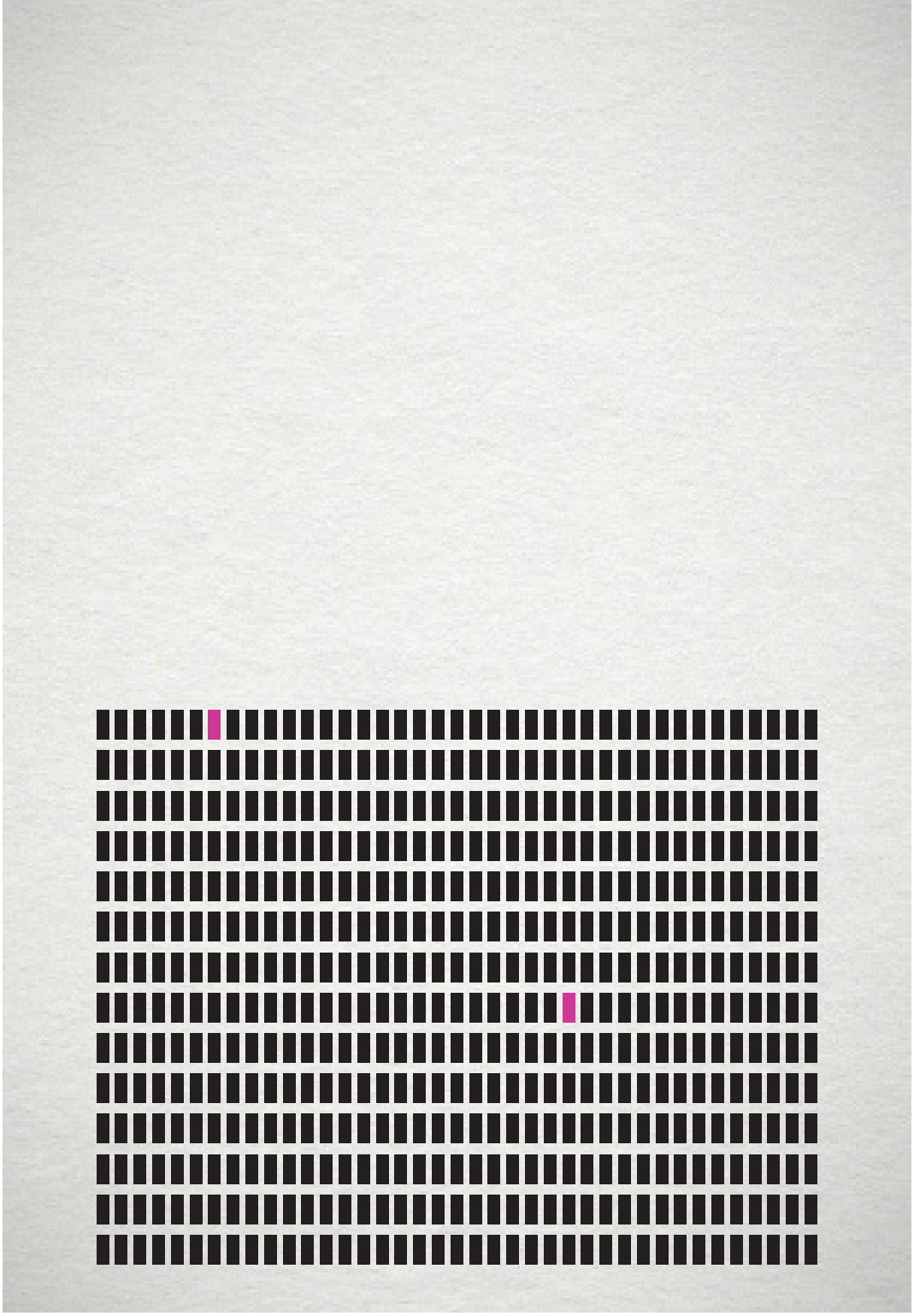
REPUTATIONAL DAMAGE COSTS FOR DIRECTORS
Costs of mitigating any reputational injury resulting from a cyber incident.

On a broader level, it is critical to ensure the organization has sufficient D&O limits of liability. Directors should also consider if there are cyber exclusions on the policy which may invalidate cover, such as is there an applicable professional services exclusion or is there an invasion of privacy exclusion?[1]

1 See, Evolving Directors & Officers Liability Environment: Emerging Issues & Considerations, Marsh and NACD, 2017

TEN QUESTIONS
TO ASK MANAGEMENT ABOUT YOUR ORGANIZATION'S CYBER READINESS

- ☐ 1 What cyber risk management framework does the organization use to assess and benchmark our approach and risk profile (e.g., NIST)?
- ☐ 2 Given management's assessment of our cyber risks and mitigating procedures, where are our most significant residual vulnerabilities?
- ☐ 3 Where do we rank in cyber preparedness compared to relevant peers and how frequently does management perform cyber scenario testing/war games? How do we benchmark our performance?
- ☐ 4 Which leaders across the organization have accountabilities for cyber risks within IT, functions, business and operational areas, etc.? How do we ensure we have enough resources dedicated to each?
- ☐ 5 How are our business continuity/resiliency plans adapting in response to dynamically evolving cyber threats? For example, what company policy and protections are in place regarding ransomware threats and related payments? Do these plans consider local laws?
- ☐ 6 Have we quantified and assessed the potential financial impact of an interruption caused by a cyber event?
- ☐ 7 Do we have a dedicated cyber insurance policy, or are we relying on add-on products or blended coverages? What exposures does our cyber insurance coverage address and what risks have we elected not to insure?
- ☐ 8 What are the limits of liability of cyber insurance that we have available, and how can we determine if they are sufficient?
- ☐ 9 How often will the board be updated on the status of cyber risk management and cyber insurance coverage, and what will be the format of that report?
- ☐ 10 How have we compared our cyber insurance program to our fundamental risk profile, as well as to similarly-situated peers in our industry, or those with similar risk/threat profiles?



APPENDIX

GUIDE TO CYBER COVERAGE OPTIONS

COMMON TYPES OF CYBER INCIDENTS	IMPACT ON ORGANIZATION	COVERAGE AND ASSISTANCE available via cyber insurance	POTENTIAL COVERAGE AND ASSISTANCE available via other policies
Data Confidentiality Breach – Third-party e.g., unauthorized access to or breach of third-party personally identifiable information, or third-party corporate information	• Incident response costs (e.g., notification costs, call center costs, credit monitoring costs, public relations costs) • Reputational damage • Consumer class actions • Regulatory investigations and defense costs • Legal defense and indemnity costs • Fines and penalties • Payments under corporate indemnity agreements • Shareholder lawsuits and derivative claims	• Privacy and data breach liability • Crisis management • Incident response expenses • Regulatory investigations • Payment Card Industry Data Security Standards (PCI-DSS) fines and penalties	• Directors' and Officers' Liability • Professional Liability / Errors & Omissions Liability
Data Confidentiality Breach – Own Data e.g., theft of trade secrets, unauthorized access to or breach of employee data, or insertion of malicious code or computer virus to information systems	• Intellectual property theft • Shareholder lawsuits and derivative claims • Incident response costs (e.g., notification costs, call center costs, credit monitoring costs, public relations costs) • Employee lawsuits	• Network business interruption • Crisis management • Digital asset damage and restoration • Regulatory investigations • Privacy and data breach liability • Network Security Liability • PCI-DSS fines and penalties	• Directors' and Officers' Liability • Employment Practices Liability • Intellectual Property Coverage
Operational Technology Malfunction e.g., remote access to and manipulation of control system or insertion of malicious code or computer virus	• Business interruptions costs (e.g., loss of profit or increased costs of working during the period of downtime and any additional specified period) • Physical asset damage • Bodily injury and death • Fines and penalties • Shareholder lawsuits and derivative claims	• Network business interruption • Crisis management • Digital asset damage and restoration • Regulatory investigations • Network Security Liability	• Property Coverage • General Liability • Workers' Compensation Coverage • Directors' and Officers' Liability
Network Outage e.g., denial of service attack on a server leading to the unavailability of a company website	• Incident response costs (e.g., IT forensic costs) • Business interruption costs (e.g., loss of profit or increased costs of working during downtime and any additional specified period) • Reputational damage • Shareholder lawsuits and derivative claims	• Network business interruption • Crisis management • Digital asset damage and restoration • Network Security Liability • Regulatory investigations	• Directors' and Officers' Liability • Technology Errors & Omissions Liability

Source: Marsh & McLennan Companies; Enhancing the Role of Insurance in Cyber Risk Management, OECD, 2017

COMMON TYPES OF CYBER INCIDENTS	**IMPACT ON ORGANIZATION**	**COVERAGE AND ASSISTANCE** available via cyber insurance	**POTENTIAL COVERAGE AND ASSISTANCE** available via other policies
Inadvertent Disruption of Third-party System e.g., transmission of malware to a third-party system	• Legal costs • Reputational damage • Regulatory investigation and defense costs • Payments under customer service level agreements • Indemnity obligations • Shareholder lawsuits and derivative claims	• Network Security Liability • Crisis management • Regulatory investigations	• Directors' and Officers' Liability • Technology Errors & Omissions Liability
Disruption at External Service Provider e.g., disruption to software application provided by a cloud service	• Business interruptions costs (e.g., loss of profit or increased costs of working during downtime and any additional specified period) • Service level agreement payments to downstream customers • Consumer class action • Legal defense costs and indemnity • Regulatory investigations • Fines and penalties • PCI-DSS fines and penalties • Reputational damage • Shareholder lawsuits and derivative claims	• Privacy liability • Network business interruption • Contingent business interruption • Crisis management • Digital asset damage and restoration • Regulatory investigations • PCI-DSS fines and penalties • Crisis management	• Technology Errors & Omissions • Directors' and Officers' Liability
Deletion or Corruption of Data e.g., malware that leads to deletion of or inability to access data on connected computers	• Incident response costs (e.g., IT forensic costs) • Costs to recreate lost data • Regulatory and legal investigation and defense costs • Costs to replace damaged hardware • Shareholder and derivative lawsuits	• Network business interruption • Network Security Liability • Crisis management • Digital asset damage and restoration • Regulatory investigations	• Technology Errors & Omissions Liability • Directors' and Officers' Liability • Property
Encryption of Data e.g., ransomware that impedes access to data until a ransom is paid	• Incident response costs (e.g., IT forensic costs) • Cyber ransom and extortion costs • Reputational damage • Legal defense and indemnity • Shareholder lawsuits and derivative actions	• Cyber extortion • Network business interruption • Crisis management • Digital asset damage and restoration • Regulatory investigations • Privacy Liability • Network Security Liability	• Kidnap and Ransom Insurance • Directors' and Officers' Liability
Cyber Fraud/Theft e.g., illegitimate financial transfer is made as a result of network intrusion or social engineering	• Loss of monies or funds • Legal costs • Shareholder lawsuits	• Privacy Liability (for personally identifiable information that was transferred, i.e., social security numbers) • Regulatory investigation • Crisis management	• Crime Insurance

Source: Marsh & McLennan Companies; Enhancing the Role of Insurance in Cyber Risk Management, OECD, 2017

ACKNOWLEDGEMENTS

This paper is the first in a series on "Global Governance Insights on Emerging Risks." It is presented as a partnership between WCD and MMC Global Risk Center and is intended to provide insights, advice and guidance for members of WCD. We thank the following WCD members for sharing their insights in developing this paper.

CATHERINE ALLEN

Director, Synovus Financial Corporation, El Paso Electric Company and Analytics Pros,
UNITED STATES

JAN BABIAK

Director, Walgreens Boots Alliance, Euromoney Institutional Investor, and Bank of Montreal,
UNITED STATES

SUZAN BAYAZIT

Co-Chair,
Toplum Gönüllüleri Vakfı,
TURKEY

OLGA BOTERO

Director, Evertec, Inc., Founding Partner, C&S Customers and Strategy, Senior Advisor to the Boston Consulting Group,
COLOMBIA

SHIRLEY DANIEL

Director, American Savings Bank and Pacific Asian Management Institute,
UNITED STATES

ANNALISA GIGANTE

Director, Foundations for Learning, Jagex, AdvisorWorld 50, Co-Chair WCD Switzerland,
SWITZERLAND

SUSAN C. KEATING

CEO, WomenCorporateDirectors (WCD) Foundation,
UNITED STATES

ANASTASSIA LAUTERBACH

Director, Dun & Bradstreet, Venture Partner, Analytics Ventures, and Evolution Partners Advisory Board
GERMANY

CRISTINA FINOCCHI MAHNE

Director, Inwit, Italiaonline, Banco di Desio, Natuzzi and Trevi Group, Co-Chair, WCD Italy,
ITALY

KRIS MANOS

Director, KeyCorp, Columbia Forest Products, and Dexter Apache Holdings,
UNITED STATES

GEETA MATHUR

Director, Motherson Sumi Ltd, IIFL Holdings Ltd, and Tata Communication Transformation Services Ltd,
INDIA

SUSAN STAUTBERG

Chair Emeritus and Co-Founder, WomenCorporateDirectors (WCD) Foundation,
UNITED STATES

WENDY WEBB

Director,
ABM Industries,
UNITED STATES

MARY BETH VITALE

Director, GEHA and CoBiz Financial, Inc., Co-Chair, WCD Colorado,
UNITED STATES

MARSH & MCLENNAN COMPANIES' CONTRIBUTORS

Kelly Butler, Senior Vice President, National Cyber Leader, Financial and Professional Practice, Marsh Australia; Elisabeth D. Case, Managing Director, Cyber Advisory Leader, Marsh USA; Leslie Chacko, Director, Marsh & McLennan Companies' Global Risk Center; Queenie C.K. Chong, Senior Vice President, Financial and Professional Practice, Marsh USA; Bethany Greenwood, Managing Director, Financial and Professional Practice, Marsh USA; Paul Mee, Partner, Digital Practice, Oliver Wyman, USA; Lucy Nottingham; Director, Marsh & McLennan Companies' Global Risk Center; Siobhan O'Brien, Managing Director, UK Cyber Placement Leader, Financial and Professional Practice, Marsh UK; Nilay Ozden, Managing Director, Financial and Professional Practice Leader, Continental Europe, Marsh; Payal Patel, Vice President, Financial and Professional Practice, Marsh USA; Naureen Z. Rasul, Senior Vice President, Asia Specialty Practice, Marsh Hong Kong; Thomas Reagan, Managing Director, Cyber Practice Leader, Marsh USA; Jaclyn Yeo, Senior Associate, Marsh & McLennan Companies' Asia Pacific Risk Center.

WOMENCORPORATEDIRECTORS CONTRIBUTORS

Susan C. Keating, CEO; Susan Stautberg, Chair Emeritus and Co-Founder; Lisa Stella, Director of Development

TEMIN AND COMPANY CONTRIBUTORS

Davia Temin, President and CEO; Suzanne Oaks Brownstein, Managing Director; Trang Mar, Managing Director.

ABOUT WOMENCORPORATEDIRECTORS

WomenCorporateDirectors (WCD) is the world's largest membership organization and community of women corporate and private company board directors, with 80 chapters worldwide. A 501(c)(3) foundation, WCD is a trusted community of directors serving on more than 8,500 public and private boards around the world. WCD supports its thousands of global members in connecting with peers and advancing visionary corporate governance. Through events, publications, and tools addressing the latest news and trends in business and governance, WCD inspires and educates board leaders—and raises the bar for board service in public and large private companies globally. Over the past 15 years, WCD has been instrumental in training women for board service, providing board opportunities, and facilitating introductions to nominating committee chairs around the world. The result has been the placement of over 500 women on corporate boards, private boards and advisory boards.

ABOUT THE GLOBAL RISK CENTER

Marsh & McLennan Companies' Global Risk Center addresses the most critical challenges facing enterprise and societies around the world. The center draws on the resources of Marsh, Guy Carpenter, Mercer, and Oliver Wyman – and independent research partners worldwide – to provide the best consolidated thinking on these transcendent threats. We bring together leaders from industry, government, non-governmental organizations, and the academic sphere to explore new approaches to problems that require shared solutions across businesses and borders. Our Asia Pacific Risk Center in Singapore studies issues endemic to the region and applies an Asian lens to global risks. Our digital news services, BRINK and BRINK Asia, aggregate timely perspectives on risk and resilience by and for thought leaders worldwide.