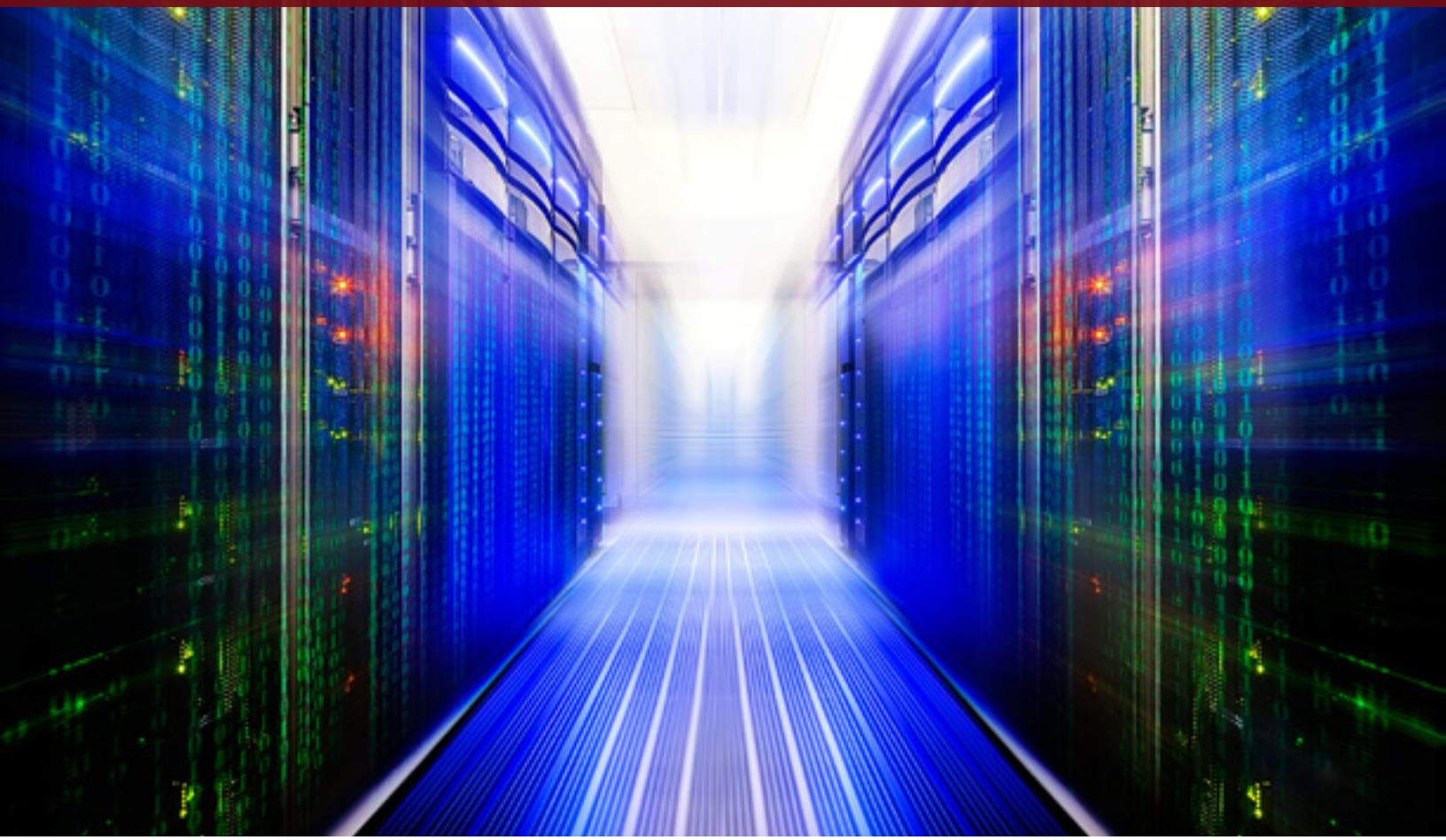


GUIDING PRINCIPLES FOR CYBER RISK GOVERNANCE:

Principles for Directors in Overseeing Cybersecurity

June 2018

The Directors and Chief Risk Officers Group
Leaders of the global risk governance community.

the DCRO
Directors and Chief Risk Officers Group

ABOUT THE DIRECTORS AND CHIEF RISK OFFICERS GROUP (THE DCRO)

The DCRO was formed in 2008 to focus on the top-level governance of risk in practice. Bringing together leading board members, chief risk officers, and other c-level officers whose jobs include a fiduciary responsibility for governance and risk management, the DCRO counts more than 2,000 members from large and mid-size for-profit and nonprofit organizations, coming from over 115 countries.

DCRO members participate in facilitated meetings, conference calls, benchmarking research, and governance councils that allow them to compare current practices with those adopted by fellow members, those being required by regulatory bodies, or those expected by investors.

Membership in the DCRO is strictly limited to active or recently active, board members, chief risk officers, or c-level executives with risk governance responsibilities.

For further information, or to provide comments on these guiding principles, please contact:

The Directors and Chief Risk Officers Group
e) info@dcro.org
w) www.dcro.org
t) +1-917-338-6631

the DCRO
Directors and Chief Risk Officers Group

Citations of this document should reference the originating work of the DCRO Cyber Risk Governance Council of the Directors and Chief Risk Officers Group (the DCRO).

TABLE OF CONTENTS

Governance Council Co-Chairs 2

Introduction 3

Principles for Directors in Overseeing Cybersecurity

I. Cybersecurity as an Element of Enterprise Risk 4

II. Cybersecurity as a Strategic and Managerial Issue 6

III. Broad Concepts of Cybersecurity 8

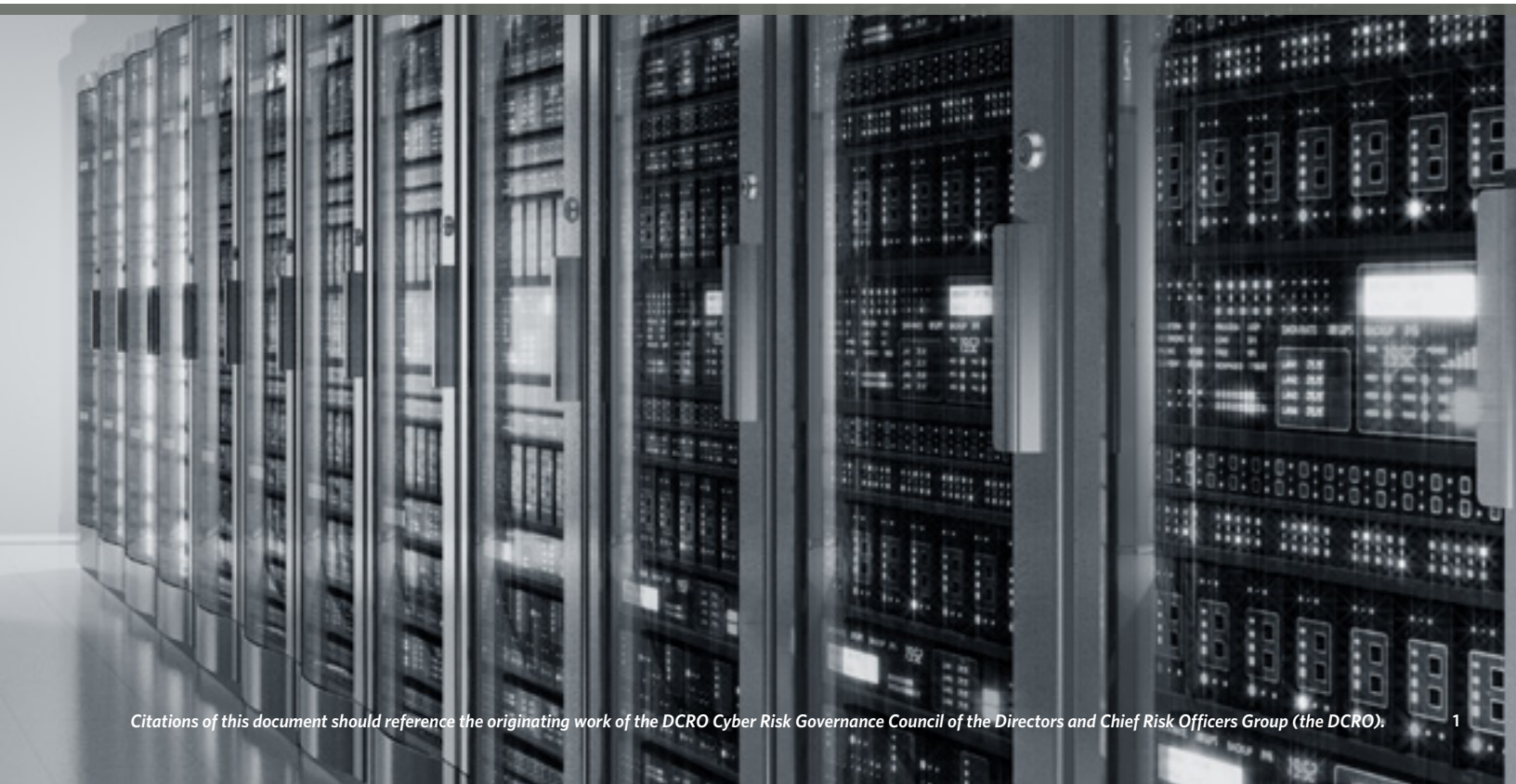
IV. Understanding Exposure to Third-party Vendors 10

V. Developing a Corporate Culture that Values Cybersecurity. 12

Conclusion. 14

Guiding Principles for Cyber Risk Governance 15

DCRO Cyber Risk Governance Council Members 16



DCRO CYBER RISK GOVERNANCE COUNCIL CO-CHAIRS

We offer special thanks to the co-chairs of the DCRO Cyber Risk Governance Council for their leadership on this initiative.

Roel C. Campos is a partner at the law firm of Hughes Hubbard & Reed in Washington, DC and is Chair of the Securities Enforcement practice. Mr. Campos' practice consists of advising senior management and boards in their most sensitive and complex issues. His practice often involves conducting internal investigations and defending matters involving financial regulators, such as the SEC, DOJ, CFTC, and FINRA. He also advises boards on items such as cybersecurity, governance, cryptocurrency and proposed rulemakings by financial regulators.

Beginning in 2002, Mr. Campos was appointed twice by President George W. Bush and confirmed by the U.S. Senate as a Commissioner of the SEC, serving until 2007.

Prior to being appointed to the SEC, Mr. Campos raised venture capital with partners, was a senior executive and operated a radio broadcasting company.

After attending Harvard Law School, he worked in Los Angeles for major law firms. Mr. Campos also served in the U.S. Attorney's Office in Los Angeles. He prosecuted major narcotics cartels and, in a celebrated trial, he convicted several kingpin cartel members for the kidnapping and murder of a DEA agent.

David X Martin is an expert in cybersecurity, having co-chaired a public/private initiative with the FBI and major corporations on intelligence sharing and best practices, consulted with the Central Bank of Israel on cybersecurity audits of Financial Institutions, chaired an information security committee for a public corporation, worked as a senior advisor on cybersecurity for Oliver Wyman, and published numerous articles on innovative approaches to managing cybersecurity. He is the co-managing director of cybXsecure, a cybersecurity consulting and development company.

Mr. Martin is an acknowledged expert on risk management and valuation issues and has extensive experience with investment strategies and operations, quantitative research, exchanges, and supervising trading desks. He was the founding Chairman of the Investment Company Institute's Risk Committee and Co-Chair of the Buy Side Risk Committee. He is a veteran financial executive whose 40-year career includes senior positions at PricewaterhouseCoopers (PWC), Citibank, and AllianceBernstein, where he served both as Chief Risk Officer and a Director of Sanford Bernstein LLC.

Mr. Martin is also an Adjunct Professor at NYU's and Fordham's Graduate Schools of Business, author of *Risk and the Smart Investor*, published by McGraw Hill in the fall of 2010, and author of *The Nature of Risk*, published by Amazon in 2012. He has also published numerous white papers on cybersecurity, compliance and risk, enterprise risk management, and corporate governance.

Mr. Martin serves as a member of the Sanctions Subcommittee of the US Department of State's Advisory Committee on International Economy Policy and as a Special Counselor to the Center for Financial Stability on cybersecurity and emerging risks.

Citations of this document should reference the originating work of the DCRO Cyber Risk Governance Council of the Directors and Chief Risk Officers Group (the DCRO).

INTRODUCTION

The purpose of this document is to provide boards of directors a set of Guiding Principles to enable the implementation of an effective cybersecurity program. A director should understand the full range of cyber risks facing his or her company and encourage management to develop appropriate strategies tailored to the company's operating environment, risk profile, and long-term goals.

The specific needs of any effective cyber program include careful planning, smart delegation, and a system for monitoring compliance – all of which directors should oversee. It's no longer a question of *whether* a company will be attacked but more a question of *when* this will happen – and how the organization is going to prevent it. Smart network surveillance, early warning indicators, multiple layers of defense, and lessons from past events are all critical components of true cyber resilience. When things go wrong, whether in a major or minor way, the ability to quickly identify and respond to a problem will determine the company's ultimate recovery.

Cybersecurity cannot be guaranteed, but a timely and appropriate reaction can.

Longer term, the board should understand and consider the strategic business implications of cybersecurity, foster the right company culture surrounding security, and encourage the integration of cyber risk management practices into other governance and approval processes. In essence, the board should consider cybersecurity as a managerial issue, not just as a technical one.

I. DIRECTORS SHOULD VIEW CYBERSECURITY AS AN IMPORTANT ELEMENT OF ENTERPRISE RISK THAT THEY MUST OVERSEE.

A. Identify the organization's essential assets ("crown jewels") that may be vulnerable to cyber attack.

B. Identify which cyber risks to avoid, which to accept, and which to mitigate.

C. Develop specific plans associated with each approach.

There are no offensive strategies in cybersecurity – only defensive ones. In addition, one cannot protect everything. It is therefore critical for board members to first determine which assets are most valuable, and second, to put in place the most effective strategy or strategies to protect these assets. Once the board ascertains the value of what needs to be protected, it can prioritize and allocate resources to avoid and mitigate cybersecurity threats. At that point, it can decide whether its cybersecurity budget is appropriate.

Defining an organization's risk capacity is a complex challenge because it requires all the personnel to be confident of the following items:

- Knowing their inventory of information assets is both complete and up-to-date;
- Being certain that the process used to prioritize the value of these assets is accurate and appropriate;
- Understanding the effectiveness of the key actions that have been taken to protect the most important assets, e.g., the crown jewels;
- Having a comprehensive command of the terms and conditions of other risk-mitigating items, such as insurance, with the corresponding knowledge of where insurance and other risk mitigation efforts will not be effective; and
- Possessing a deep understanding of the scale and robustness of the organization's business response and continuity plans that will be triggered in the event of a cyber incident.

Citations of this document should reference the originating work of the DCRO Cyber Risk Governance Council of the Directors and Chief Risk Officers Group (the DCRO).

The five elements listed above represent a sample of the component elements in the "risk capacity" calculation that board directors and senior management need to perform on an ongoing basis. The first three are critically important to directors to ensure they know what programs, investments and resources management has dedicated to protecting the most valuable holdings, because the theft, unauthorized access, or damage to these assets could represent an existential risk.

The last two also factor into the capacity calculation as inputs because the costs and benefits of mitigation actions, such as third-party cyber insurance and remote back-up facilities are also important. These traditional risk management activities play an important role in how the organization assesses its capacity to endure or "weather" a pre-defined type of business continuity event.

The business continuity framework can help gain insight into the priority of the assets to be recovered after a cyber-breach has occurred. Of course, any "pre-defined" event estimate will likely not match what happens in reality, but an organization can use frequent simulated attacks in order to identify and assess whether other "less critical" assets are appropriately evaluated from a risk mitigation perspective.

To meet this duty of care, directors must be able to demonstrate that they have discharged their oversight function of cybersecurity in a reasonable common sense manner. To that end, directors should receive regular assessments and assurances from both the CEO and the CISO that the work being performed by the entire organization (i.e., not just the technology function) is highly focused on protecting the crown jewels and other high priority assets. These work initiatives should involve functional segmentation, robust identity access management, and higher levels of employee training, along with the leading-edge security practices at the network and end-point levels.

Also, acknowledging mistakes and learning from them leads to better decision making. Cybersecurity post mortems should be encouraged in briefings about the company's security model and vulnerabilities. There is no substitute for the proper deliberation and engagement of cybersecurity issues.

Of course, when developing new products and services, a company needs to strike the right balance between innovation and risk. In most cases, the more that security is increased, the less user-friendly and convenient the product becomes. Processes that should be reviewed for a cyber filter include strategic planning, M&A, product development, and capital allocation and budgeting. Even HR processes should have a cyber-filter to understand recruiting, leadership development, and cyber resource retention strategies.

II. DIRECTORS SHOULD VIEW CYBERSECURITY AS A STRATEGIC AND MANAGERIAL ISSUE AND SHOULD THEREFORE HOLD MANAGEMENT ACCOUNTABLE FOR RECOMMENDING AND IMPLEMENTING THE OVERALL CYBER RISK MANAGEMENT STRATEGY AND POLICIES.

A. Management should be accountable for reporting their actions and cyber breaches.

B. Where appropriate, the board should require key executives to attest that certain important aspects of the cybersecurity plan have been executed.

C. Promoting employee awareness and training is crucial.

D. Third-party testing of cyber vulnerabilities can provide a high degree of deterrence.

E. Boards should maintain an external team of professionals that are available for training and in crisis situation.

Directors must understand security through a broader lens than simply information technology (IT), since the potential harm to a company can be devastating. Cybersecurity risk demands C-level accountability and board oversight to drive the agenda and manage empowered employees with the right skill sets.

Discussions about cyber risk management with the accountable corporate officer should be given regular and adequate time on board and board committee meeting agendas.

The accountable officer's leadership skills – communication and crisis management – should be considered equally, as they are often more important than technical skills. Clearly, in the day-to-day management of technology, or in a crisis, it is far better to have a skillful leader rather than a subject-matter expert.

The board should also create a self-assessment framework in terms (and language) that they fully understand to ensure that best industry practices are being implemented and real progress is being made. A strong focus on outcomes should replace pure activity-based reporting.

Directors need to promote a robust state of cybersecurity and resilience by encouraging appropriate interaction between all levels of management and subordinates.

Citations of this document should reference the originating work of the DCRO Cyber Risk Governance Council of the Directors and Chief Risk Officers Group (the DCRO).

It is well documented that approximately two-thirds of successful unauthorized cyber-attacks are directly attributable to the actions (or inactions) made by employees. Therefore, improving awareness of employees to cyber risk exposures represents a meaningful opportunity to enhance an organization's overall cyber resilience. Any measurable improvement to employee awareness through initiatives such as gamification and continuous training that is operational in nature would be highly accretive to an entity's capacity to protect and respond to a cyber-incident.

From a board director's perspective, it is important to receive in-depth analysis and evaluations of real and simulated incident response events that describe in detail the interactions between the various functional teams beyond the three described above. Such evaluations (perhaps performed by an independent third party) would provide insight into the organization's overall cyber resilience which is, at best, a continuously evolving objective.

An important part of cyber resilience entails establishing relationships with external experts and firms to support a more decisive response to a data breach. The post-breach environment is not the optimal time to be searching for required expertise or negotiating contractual terms, so having a team of external resources "at the ready" can speed recovery and resumption of operations. These external experts can include forensics, legal, communication, and systems remediation, among others. The approach to law enforcement (FBI and others) should also be considered in advance of an incident.

III. DIRECTORS SHOULD BE GUIDED BY TWO BROAD CONCEPTS OF CYBERSECURITY:

A. Ensure that cybersecurity is managed within three lines of defense, and

B. Ensure that cybersecurity is managed based on constantly reacting to gathering intelligence and promoting adaptation to the changing risk environment.

A. Three Lines of Defense

Cybersecurity requires an approach that goes beyond being the sole concern of the information security group. A preferred approach is a three-lines-of-defense model. The first line of defense, "risk identification and assessment," is the responsibility of the business units and information security teams. Therefore, they have the direct accountability for owning, understanding and managing cyber risks and making the directors aware of their risk assessments.

The second line of defense, "risk management," is the responsibility of the company risk management team to provide functional oversight from a strategic business perspective regarding the potential impact of threats, the determination of priorities, and the allocation of resources. The risk management team should also provide constructive, strategic business challenges to the first line's approach to cyber risk, ensuring that the right policies and procedures are in place, and that cybersecurity is effectively integrated into operational and enterprise risk. Again, periodic reports of the effectiveness of risk management should be provided to the board.

The third line of defense, "risk monitoring," is the responsibility of internal auditing to provide assurance to the board and senior management of the effectiveness of cyber risk governance for the enterprise.

These three lines of defense should be guided by an active, engaged board of directors that approves and oversees the firm's approach to cybersecurity, approving strategic decisions and priorities, while providing a credible and effective counterbalance to management.

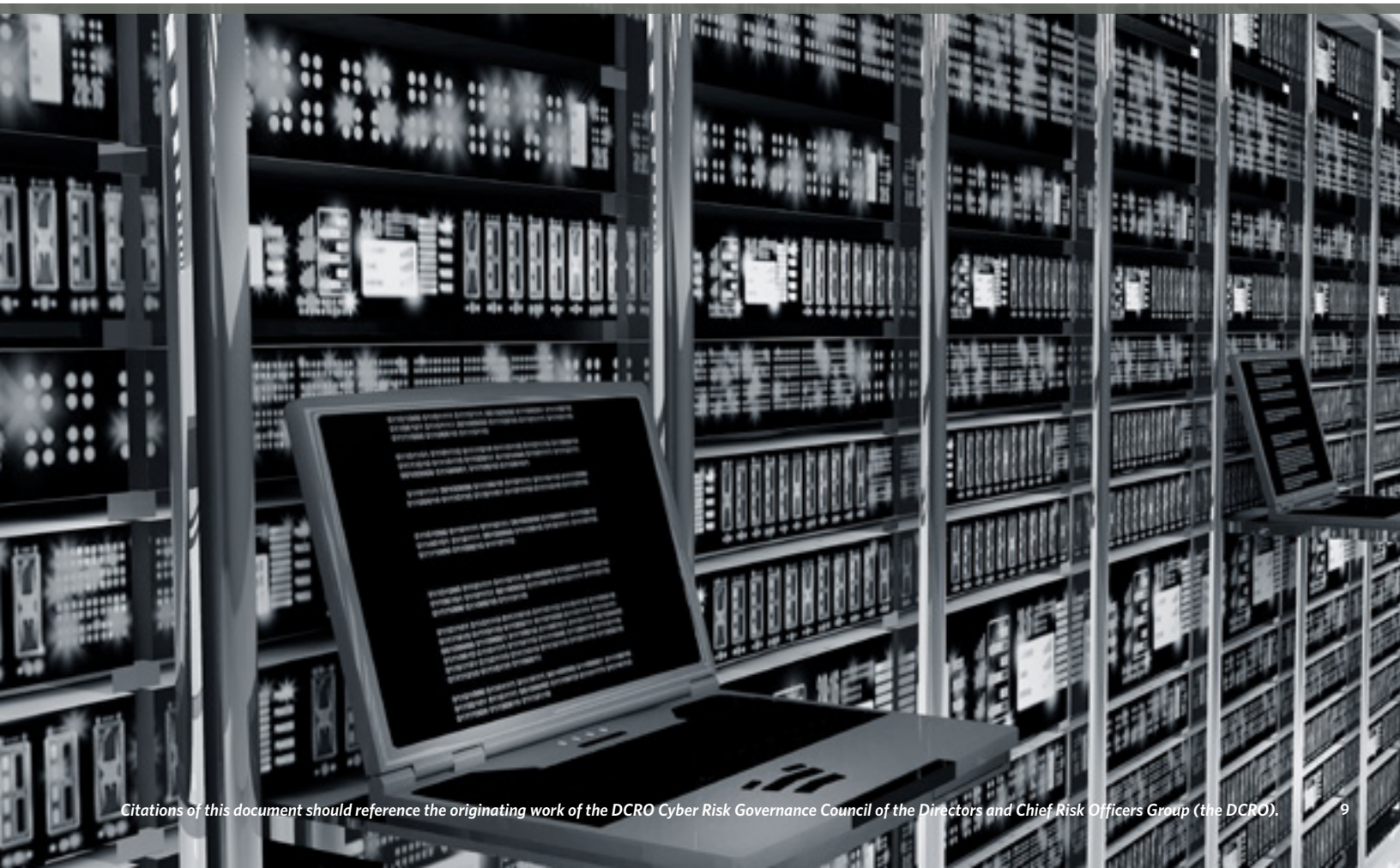
Citations of this document should reference the originating work of the DCRO Cyber Risk Governance Council of the Directors and Chief Risk Officers Group (the DCRO).

B. Intelligence Driven Approach

The traditional approach to security relies on prevention strategies. It treats incident responses using an exception-based approach. In contrast, an intelligence-driven mindset is based on the assumption that the company has already been compromised and therefore the need exists to continuously evolve to stay ahead of the curve in terms of intelligence and incidents.

An adaptive security architecture allows decision making for security related issues that is based on the following: accurate threat modeling, a quantifiable asset valuation, and 'what if' scenarios that consider the deterrence factors of a security measure or process, as well as their cost. The right intelligence driven approach is based on prior experiences, current threat intelligence, understanding of breaches that have impacted other companies, trends, valuation of assets, and analysis of the safeguards to guard these assets constantly, including when controls fail.

Directors should also encourage the review of new technologies for access management, artificial intelligence, and distributive data that could potentially enhance the companies' cyber defenses.



IV. DIRECTORS SHOULD UNDERSTAND THE COMPANY'S EXPOSURE TO THIRD-PARTY VENDORS.

Third parties can be impactful to an operating environment, since boards and companies are not usually as attuned to cybersecurity risks from third parties as they are for their own businesses, even though third parties can create the same adverse, long-term effects.

Organizations that are laser-focused on delivering their missions through core competencies leverage the strengths of other providers and partners as a critical and viable business strategy. Companies manage hundreds, if not thousands, of vendor, third-party provider, and other types of outsourcing arrangements. These external parties are a primary source of incremental risk by creating new entry points into a company's technology environment. The sharing of data and communication is no longer fully in control of the internal operations of the organization, adding complexity and potential volatility to the operating environment.

Legal and other practical considerations can (and should) be employed to partition and mitigate the risk; however, the risk, no matter where it originates, will revert to the company in times of crisis or stress. Customers (corporate and individual) simply look to the company with which they are doing business for explanations and relief.

Many organizations are playing "catch-up" when it comes to vendor management. The ability to create a full inventory of vendor relationships is clearly "table stakes" in an overall program. The basics for a third-party program should include the following:

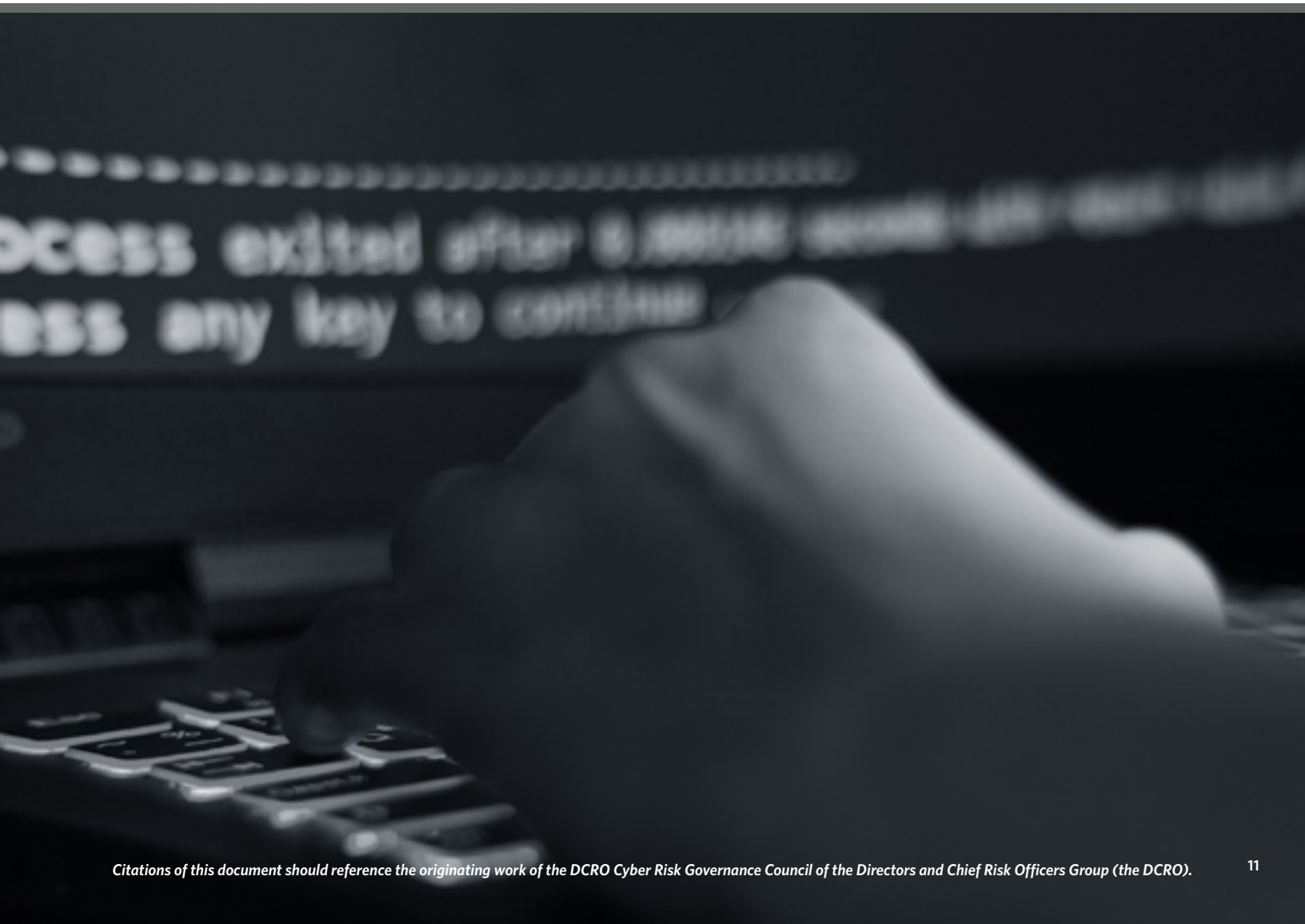
- Complete and comprehensive inventory of all third-party contracts
- Third-party exposures prioritized based on risk (including cyber) to the organization
- Clear assessment tools in place for the onboarding of any new relationships
- Ongoing, risk-adjusted monitoring processes in place to assess adherence to contract terms
- Third-party assessment of vendor practices through Service Organizational Control (SOC) reporting
- Joint disaster recovery testing with primary service providers

Citations of this document should reference the originating work of the DCRO Cyber Risk Governance Council of the Directors and Chief Risk Officers Group (the DCRO).

The activities should result in actionable and timely summarized board reporting; leveraging a technology-enabled vendor management solution is also a best practice. An emerging trend is a fourth-party assessment to understand what activities have been further outsourced causing change to the risk profile for cybersecurity.

For cybersecurity risk, "risk-adjusted" is no longer purely a dollar filter, e.g., based on the financial size of the contract. With the proliferation of inexpensive applications and other narrow, but highly effective, tools to fully capture the risk profile of the relationship, other filters must also be used to understand the impact to the organization.

A strong third-party vendor management program does more than strengthen cybersecurity risk management – it can support spending decisions, contracting strategies, service levels, and other critical operational activities to support the attainment of core business objectives.



V. DIRECTORS SHOULD COMMIT TO DEVELOPING A CORPORATE CULTURE THAT PLACES A HIGH VALUE ON CYBERSECURITY.

A. With management, directors should define appropriate behavior for cybersecurity and then demonstrate clearly the importance the organization places upon strict adherence.

Risk culture is the glue that binds all aspects of risk-taking and risk management together through shared organizational values, beliefs, and attitudes. Through awareness and deliberate planning, risk culture can be proactively influenced to enhance an organization's risk and business management environments. Cybersecurity is no exception; establishing a strong cybersecurity culture is an essential component of any program, given that the vast majority of cyber risk can be initially traced to people and related behaviors, not technology.

However, most employees aren't interested in their personal digital security – much less their company's. Therefore, changing a company's culture to strengthen security is especially difficult – requiring a paradigm shift in order to keep pace with the evolving threats. Historically, anything to do with IT security was kept away from users by IT teams. Little wonder that users show no or little interest in the company's security.

But in reality, users should be the front line of data security. They create and handle the information – therefore they are best-placed to understand its value. Directors should request their management to develop interactive training and accountability programs that engage with users. Using modern game based training and thereafter monitoring how users and employees apply their training helps transform a company's culture into one where cybersecurity is everyone's concern.

Without a strong risk culture, even the best cybersecurity management framework would be vulnerable to weaknesses and failures. Given the continuously changing and quickly evolving cyber environment, embedding a strong cyber risk culture provides employees with principles and values to guide activities when policies are yet to be drafted or updated. Specific guidance may not always be available, relevant, or remembered. Indicators of a strong cybersecurity culture include:

- Clear and concise cybersecurity policy framework reflective of risks faced by the organization and the evolving operating environment;
- Board and leadership agendas prominently include cybersecurity;

Citations of this document should reference the originating work of the DCRO Cyber Risk Governance Council of the Directors and Chief Risk Officers Group (the DCRO).

- Cyber risk is not managed in a silo – discussions on cyber are woven into all management processes, such as new product approvals, merger due diligence, and third-party outsourcing arrangements;
- Continuous learning environment, including relevant and memorable training and tools to support strong cyber hygiene ranging from password protocols to anti-phishing campaigns to "bring your own device" policies;
- The existence of a safe environment for employees to bring forward risks or issues, employees need to know they are supported if they identify an unmitigated risk or emerging threat.

Another hallmark of a strong cybersecurity culture is that no one in the organization is exempt, including the board. Boards should demonstrate their knowledge of strong cybersecurity practices by participating in company cybersecurity training, avoiding personal e-mail for company business, and safeguarding (physically and electronically) confidential information.

B. Directors need to understand the legal and regulatory implications of cyber risks as they relate to their company's specific circumstances including their fiduciary duties and the overarching legal terrain.

High-profile incidents affecting Deloitte, Equifax, Facebook, and many others over the past year or so, remind us how quickly the risk of breaches and response to those events can impact a company's reputation. A breach of sensitive customer and company data and systems brings enormous scrutiny from shareholders and regulators and poses a significant risk to a firm's operations as well as to its stock price. Furthermore, under securities laws, directors are gatekeepers who have responsibilities to shareholders in preventing wrongdoing.

Of course, Directors have fiduciary duties of care, loyalty, and good faith to ensure to protect corporate assets, including customer information, as well as the firm's reputation and shareholder value. This includes ensuring the existence of an effective Cybersecurity Program that satisfies legal requirements and maintains multi-layered security measures that protect sensitive information from unauthorized modification, destruction, or disclosure – whether accidental or intentional.

To meet their responsibilities, directors should schedule regular briefings from their General Counsel and/or outside lawyers to brief the directors on cybersecurity and privacy implications for federal, local, and state laws.

CONCLUSION

Public scrutiny after cyber-attacks and the regulators have made cybersecurity a board issue and key responsibility. In crisis, the only thing people remember when it comes to judgement calls is the outcome. A good outcome is usually the result of a well-considered, disciplined process that demonstrates collective wisdom and commitment to corrective results.

Board meetings are an opportune time for corporate directors to reassess how they exercise their governance responsibilities with regard to the management of cybersecurity risk. In today's global cyber minefield, it is essential that boards of directors not just monitor performance, but incentivize excellence in this area.

Citations of this document should reference the originating work of the DCRO Cyber Risk Governance Council of the Directors and Chief Risk Officers Group (the DCRO).

APPENDIX

The DCRO Guiding Principles for Cyber Risk Governance

Principle 1: Directors should view cybersecurity as an important element of enterprise risk that they must oversee: identifying the company's essential assets that may be vulnerable to cyber attack, which cyber risks to avoid, accepts, or mitigate, and to develop specific plans associated with each approach.

Principle 2: Directors should view cybersecurity as a strategic and managerial issue and should therefore hold management accountable for recommending and implementing the overall cyber risk management strategy and polices.

Principle 3: Directors should be guided by two broad concepts of cybersecurity: ensuring that it is managed within "three lines of defense" and based on reacting and adapting to gathering intelligence and the changing risk environment.

Principle 4: Directors should understand the company's exposure to third-party vendors.

Principle 5: Directors should commit to developing the corporate culture that places a high value on cybersecurity.

DCRO CYBER RISK GOVERNANCE COUNCIL MEMBERS

Co-Chairs

Roel Campos (US) | Partner, Chair of SEC Enforcement Defense Practice. Hughes Hubbard & Reed LLP; Former Partner, Head of Securities Regulation and Enforcement, Locke Lord LLP; Former Commissioner, U.S. Securities and Exchange Commission

David X Martin (US) | Expert Witness, Founder and Managing Partner, David X Martin, LLC; Special Counselor, Center for Financial Stability; Advisory Committee Member on International Economic Policy: Sanctions Subcommittee, U.S. Department of State; Adjunct Professor, NYU Stern School of Business; Former Chief Risk Officer, Alliance Bernstein; Former Chairman and CEO, Knightsbridge Capital Management; Former Enterprise Risk Manager, Citi

Council Members

Florence Angles (Switzerland) | Chief Risk Officer, REYL & Cie Ltd; founder of a Risk Manager Association in Switzerland: GIROS ; member of Club de lecture et de Présélection du Prix Turgot (Paris, France)

Masood Aziz (US) | Chief Risk Officer, FINCA International; Former Head of Compliance and Risk Management, State Street / PIMCO; Former Principal Advisor & Senior Diplomat – White House, State Department, Pentagon, and Congressional Leadership

Kevin Brock (US) | Founder, NewStreet Global Solutions, LLC; co-Founder, CyberXplore, LLC; Senior Fellow for Cybersecurity Strategy, The Center for Financial Stability; Former Assistant Director of the Directorate of Intelligence, Federal Bureau of Investigations (FBI); Former Principal Deputy Director, National Counterterrorism Center (NCTC)

Hannah Derry (US) | Global Head of Technology Risk Management, BlackRock; Former Director, Technology Services Division, Pacific Exchange (now NYSE Euronext)

William Ding (US/China) | President and CEO, SolarWind Capital & Risk Advisors, Former Chief Risk Officer, Woodbine Capital Advisors, LP; Former Chief Risk Officer, D. B. Zwirn & Co, LP; Former Head of Risk Control, CDC IXIX Capital Markets North America; Former Co- Regional Director, PRMIA Boston and Former Steering Committee Member, PRMIA New YorkCarol Gray (Canada) – Board Member and Member of Board People and Remuneration Committee, IFM Investors Pty (Melbourne); Board Member, ISPT/IFM International Property Management; Board Member and Chair, Board Risk Committee, Amex Bank of Canada; Former President, Equifax Canada; Past Board Member and Chair Ontario Realty Corporation; Past Board Member and Chair, Board Risk Committee, Infrastructure Ontario

Ignacio Fuentes (US) | Research Scholar, Digital Governance and Risk Management in Global Strategy and Block Chain in Digital Currency Initiative, Massachusetts Institute of Technology; Former Risk Governance Director, Santander Holdings USA

Jacinthe Galpin (US) | Director of Enterprise Resilience, Lowe's Companies; Former Chief Risk and Audit Officer, Department of Justice, Victoria, Australia; Former Head of Risk Management, Telstra Business

Marc Groz (US) | Co-Founder, CyberXplore; Former Managing Director, SPM LLC; Former Chief Investment Officer, Topos; Regional Director (CT), Professional Risk Managers International Association

Philip Harrington Jr. (US) | Independent Director, Willow Street Group; Independent Director, ProLink Solutions; Former EVP, Risk, and CAO, CA Technologies; Senior Managing Director, Brock Capital Group

Chris Jones (UK) | Chief Risk Officer, LME Clear Limited; Former Chief Risk Officer, LCH.Clearnet

Nicole Killen (Australia) | Chief Governance and Risk Officer, Mine Wealth + Welbeing; Non-Executive Director, Recreo Financial Technologies; Former Head of Governance and Trustee Services, Zurich Financial Services (Australia); served as Interim CEO of Mine Wealth + Wellbeing

David R. Koenig (US) | Founding Principal, The Governance Fund; Founder, The Directors and Chief Risk Officers Group; Former Board Member and Chair, Professional Risk Managers' International Association; Former Board Member, Northfield Hospital & Clinics; Author, *Governance Reimagined: Organizational Design, Risk, and Value Creation*

Council member organizational affiliations are listed for identification purposes only and do not imply the formal endorsement by said organizations of these guidelines.

Lloyd Komori (Canada) | Board Member, Chair Audit, Risk and Investment Committee ETFO - ELHT, Board member, Former Chair, Governance and Nominating Committee, Toronto Central Local Health Integration Network; Former Senior Vice President, Risk Management, OMERS Administration Corporation; Former Board Member, OMERS Administration Corporation; Former Chief Risk Officer, Ontario Power Generation; Founding Faculty Instructor, The Directors College

Lynn Mattice (US) | Distinguished Fellow, Ponemon Institute; Senior Fellow, George Washington University Center for Cyber and Homeland Security; Managing Director, Mattice and Associates; Chairman Emeritis, National Intellectual Property Law Institute; Board Member, International Security Management Association; Former Chief Security Officer, Boston Scientific

Cyril Maybury (Ireland) | Non-executive Director and Chair of Audit Committee, Generali PanEurope Ltd; Non-Executive Director and Chair of Audit and Risk Committee, Concern Worldwide; Pension Trustee of a number of pension funds; Former Chair, Business Law Committee, Consultative Committee of Accountancy Bodies – Ireland; Former partner in EY Ireland with various roles leading Audit, Risk Management, Fraud Investigation and Litigation Support and Expert Witness Services.

Julie Garland McLellan (Australia) | Board Advisor; Non-Executive Director, Suburban Land Authority; Non-Executive Director, Fitness Australia; Board Member, Professional Speakers Australia; Former Non-Executive Director and Chair, Audit Committee, Bounty Mining; Former Chair, Board of Directors, Oldfields Holdings Ltd.

Frank Morisano (US/China) | Chief Risk Officer, Industrial and Commercial Bank of China (ICBC) Limited, US Region and New York Branch; Non-Executive Director, ProfessioNext Limited (HK); Board Member, Ma Lee Advisory Limited (HK); Former Chief Risk Officer, Capital G Bank; Former Chief Risk Officer, GMAC RFC; Former Board Member, Basis 100 Inc. (Canada)

Michael Nawrath (US) | Senior Director of Global Information Security, World Fuel Services; Former Chief Information Security Officer, Direct Edge Stock Exchanges; Former Global Head of Information Security, Risk and Compliance for Networks, Credit Suisse

Braden Perry (US) | Co-Founder, Kennyhertz Perry LLC; Board of Directors, Kansas City Securities Association; Former Senior Vice President and Chief Compliance Officer, Mariner Holdings, LLC; Former Senior Trial Attorney, U.S. Commodity Futures Trading Commission

Vasilios Siokis (UAE) | Chief Risk Officer, Emirates Investment Authority; Former Chief Risk Officer, Cheyne Capital Management (UK) LLP; Former Head of Risk Management, Trafalgar Asset Managers

Stephen Soble (US) | Chairman and CEO, Assured Enterprises, Inc.; Former Chairman and CEO, API Development Group; JD Harvard Law; Developer of TripleHelix™ Cyber Risk Assessment system

Eric Staffin (US) | Chief Information Security Officer, Ipreo; Former Chief Risk Officer, S&P Global Market Intelligence, and Member of the S&P Global Risk Policy Committee

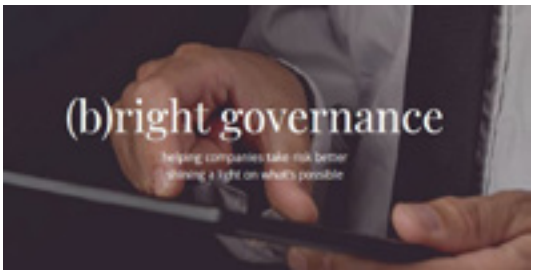
David Streliski (Canada) | Chief Risk Officer, Fiera Capital Corporation; Former Board Member, Professional Risk Managers' International Association (PRMIA); Co-Director, PRMIA Montreal

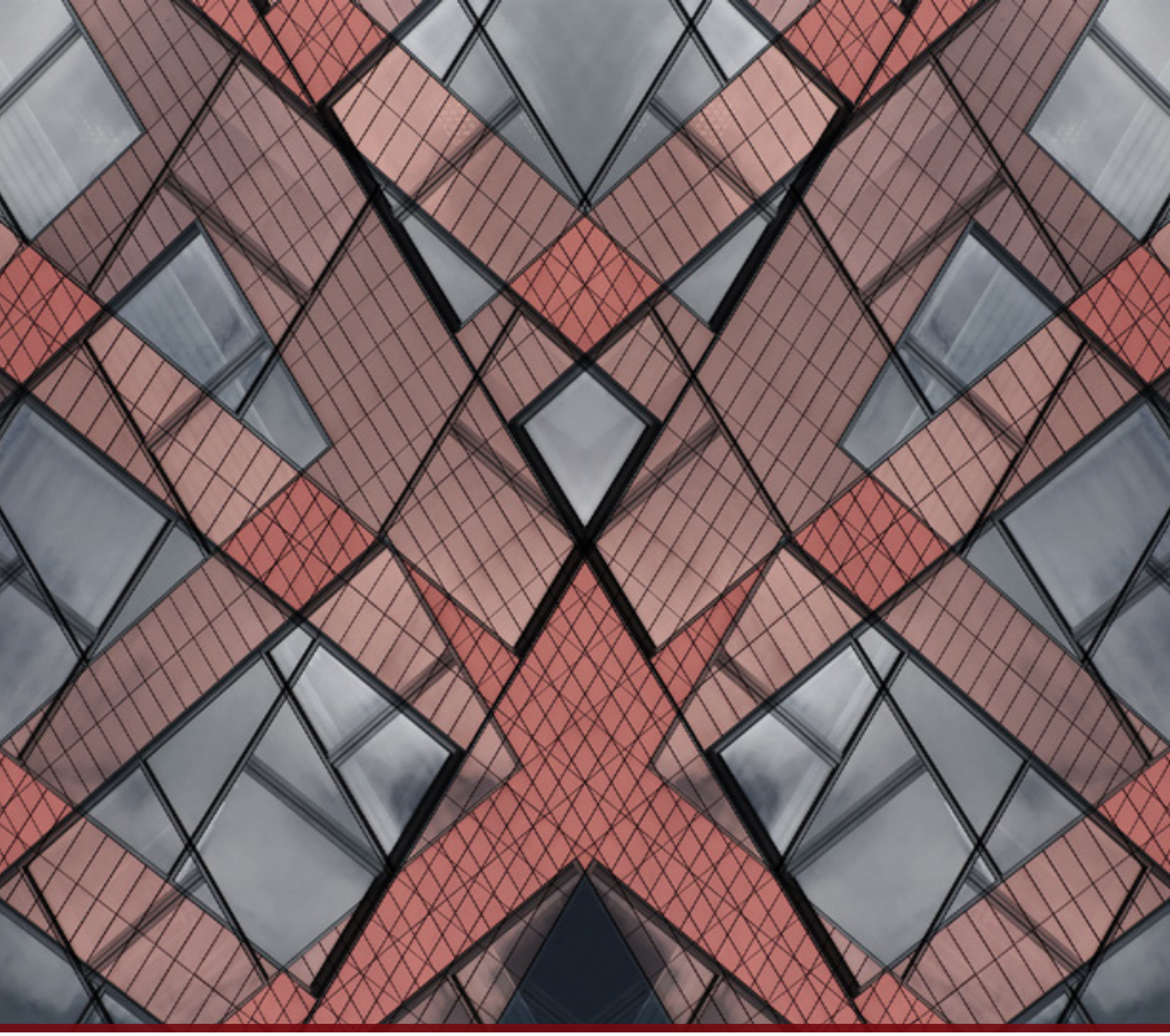
Mark Trembacki (US) | Managing Principal, Risk Management Levers, Inc.; Former SVP, Risk Integration and COO, Commercial Banking, BMO Financial Group; Adjunct Professor of Enterprise Risk Management, University of Illinois; Member, Chicago Steering Committee, PRMIA; Chair, Private Directors Association Cybersecurity Conference (2017)

Thank you to the sponsors of this document:

cybXsecure

Hughes Hubbard & Reed





The Directors and Chief Risk Officers Group

Leaders of the global risk governance community.

w) www.dcro.org
e) info@dcro.org
t) +1.917.338.6631

the DCRO
Directors and Chief Risk Officers Group

Citations of this document should reference the originating work of the DCRO Cyber Risk Governance Council of the Directors and Chief Risk Officers Group (the DCRO).