dentons.com

DENTONS

A cybersecurity guide for directors

By R. William "Bill" Ide III and Amanda Leech, Dentons Governance Center

A cybersecurity guide for directors

By R. William "Bill" Ide III and Amanda Leech, Dentons Governance Center[1]

With the ever-present reality of cybersecurity breaches, there has been a tendency in board governance literature to treat cybersecurity risks differently than other risks facing the organization. In practice, however, boards have long been tasked with protecting their companies from significant risks. While cybersecurity may appear to many board members to be a daunting new risk, the long-established "tried and true" board governance approach to risk oversight described herein works well and should be applied to cybersecurity risk.

Board duties generally fall within six categories: (i) governance, (ii) strategy, (iii) risk, (iv) talent, (v) compliance and (vi) culture. With respect to cybersecurity, the board's duties in each of these categories play a critical role in effective oversight of a company's cybersecurity program.

Every director should have a general understanding of cybersecurity risk and what it means for directors' oversight responsibilities. While the basic business-judgment obligations of directors are the same for this emerging area of risk, cybersecurity itself is a dynamic and complex subject. The purpose of this guide is to provide a "plain English" review that helps directors and senior managers carry out their cybersecurity oversight duties, including cyber strategy development and governance. Effective oversight in this area can mean the difference between "learning the hard way" and incurring significant damages, or successfully mitigating the damages that frequently accompany a significant breach.

While this guide is specific to boards of directors, the fiduciary principles of oversight apply to senior management as well. Senior management also delegates and oversees, but at a more granular level than boards. In the end, senior managers should also follow the principles of this guide to establish proper oversight, ensure that sufficient processes and controls are in place and assure their boards that cyber risks are identified and managed well.

Cybersecurity oversight: The role of the board

For company management and boards of directors, a record number of recent incursions—such as those at Target and Sony—demonstrate that cybersecurity risk is as significant as other critical strategic, operational, financial and compliance risks under boards' purviews.

Since the passage of the Sarbanes–Oxley Act of 2002, the Delaware courts have repeatedly broadened proactive duties of oversight for independent directors in areas of material impact on shareholder value such as risk, compliance and executive compensation. Just as boards are charged with overseeing a company's financial systems and controls, they also have a duty to oversee a company's management of cybersecurity, including oversight of appropriate risk mitigation strategies, systems, processes and controls.

Without effective oversight and accountability, an organization's cybersecurity governance systems, policies and procedures can be rendered meaningless, leaving the enterprise vulnerable to attack. In today's world of continually reported material data breaches, boards cannot claim lack of awareness as a defense against allegations of oversight failures. Regulators and shareholders are increasingly demanding more evidence of director attentiveness to cyber risk. As the Target breach demonstrated, breaches can result in calls for director removal. Even if directors are re-elected, the board and the company will likely face numerous shareholder derivative and class action lawsuits.

Cybersecurity governance

The first question for the board is: Who owns management of the cybersecurity risk at the board level and management level? Typically, boards delegate cybersecurity oversight to the audit committee—or to the risk committee if one is part of the board's governance structure—for a more concentrated review, with periodic reports to the full board. Others approach cybersecurity as a matter to be overseen by the full board. Company size, industry and existing board risk management structures will dictate the best approach. For the foreseeable future, cybersecurity will require considerable attention by boards working with management, internal audit, enterprise risk management (ERM) and cybersecurity experts as the threats continue to evolve and the total enterprise seeks to adjust. Processes, systems and controls must remain fluid for the foreseeable future.

At the management level, the CEO is ultimately accountable to the board for management of cybersecurity risk. Often, a CEO looks to business information technology (IT) or, in larger organizations, a chief information security officer (CISO) to interface with the board and hold accountability for cybersecurity risk management. This approach builds from a technology knowledge platform, but the major challenge is governance of the total enterprise requiring established management skills of communications, project management, behavioral science and command presence.

Technical solutions are one piece of managing the risk, but as the following chart shows, every function in the enterprise has a role to play. For success, each business unit must own and embrace cybersecurity as a priority. Tension between a decentralized business model and cybersecurity's desire for centralization requires high-level management attention to resolve conflicts. Decentralization favors local decision-making by each unit; on the other hand, cybersecurity must by its nature be centralized, and at times must seek to override those local decisions. Accordingly, IT or the CISO should report to a senior management member who can oversee the enterprise's cybersecurity program decision-making, and to whom the board can look as accountable for cybersecurity.

Cybersecurity strategy and risk oversight

Too often, IT presents boards with cybersecurity reports that are technical but lack an enterprise-wide strategic overlay. For effective oversight, boards should hold senior management accountable to ensure that a clear and concise cybersecurity strategy, understandable in nontechnical terms, is in place, along with systems and controls to monitor its implementation. This requires regular dialogue between the board and management, and the sharing of accurate and useful information, including metrics to track performance and provide accountability. Most importantly, a concise, high-level, "plain English" cybersecurity strategic plan must be agreed to by the board and senior management.

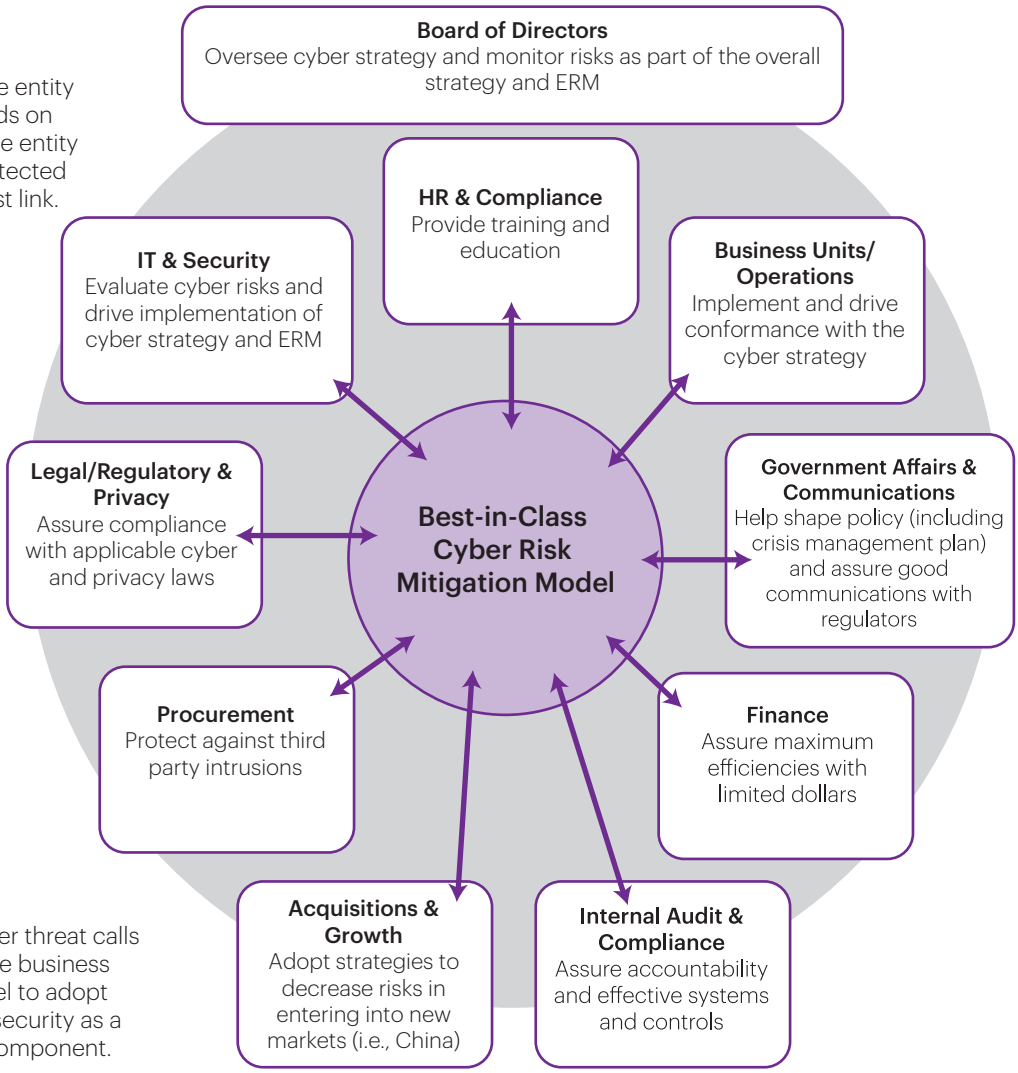
Risk-based strategy

Instead of a castle-and-moat, "keep the bad guys out" prevention-based approach, cybersecurity strategy has evolved to a risk-based approach. Because a perimeter defense cannot provide complete protection, the risk-based approach focuses instead on prioritizing and protecting identified "crown jewels" (for example, third-party information, intellectual property and critical process control networks). Risk-based defense includes detecting and responding before the additional protections around the "crown jewels" can be compromised, while also stopping intruders before they inflict other forms of disruptive and reputational damages, as in the Sony breach.

While perimeter defenses remain essential for deterring less sophisticated attacks, effective cyber strategies now allocate security resources around a company's information and processes, with additional layers of protection around the most valuable assets. Tomorrow, new technologies and techniques may require further shifts in strategies. Boards should regularly seek independent third-party reviews on strategic best practices for companies with a similar industry, size and risk profile.

Cybersecurity Governance Components

Success of the entity now depends on cyber – and the entity is only as protected as its weakest link.



The cyber threat calls for the business model to adopt cybersecurity as a key component.

These critical components all need to collaborate and be a part of the cybersecurity strategy.

Risk prioritization

This key part of strategy begins with the identification and prioritization of cyber risks. Cybersecurity resources are finite, so the strategy should focus on the most material cyber risks, considering the likelihood of harm if risks were realized. To facilitate this prioritization, many companies maintain a risk register of material cyber risks—a central repository for all risks identified by the company, including data, locations, access points, security devices and other related information. The risk prioritization process should precede the budget and resource allocation process to ensure alignment between resources and risks.

Ranking risks and determining which to accept, mitigate or transfer is a substantial undertaking. Its effectiveness depends on the quality of information and knowledge of individuals who make the recommendations. Board members must be assured that every function in the company has been solicited to contribute to the strategy's development. In particular, those with responsibility for law, privacy, physical security and crisis management response will need to offer integral input. Many industries will have specific regulatory concerns that must be woven into the strategy. As part of the risk prioritization process, senior management should provide detailed recommendations about the plan to the board, including identification of risks to be accepted, mitigated or transferred (through cyber insurance).

Strategy best practices and standards

Cyber risk has escalated so rapidly, and so publicly, that entities everywhere are scrambling to regain ground and keep up with the evolving cyber threat. Governments, regulators, industries, companies and thought leaders alike are looking for the right approach—or approaches—to address this complex and dynamic issue. So it's no surprise that cybersecurity strategy best practices, standards and public policies are still very fluid and multiplying rapidly.[1]

Today, it is unclear today what standards will become widely viewed as best practices, and whether those standards will vary by industry and/or company size. Boards and management should agree on the best approach for their company. For purposes of demonstration, let's assume that the standards defined below are the right approach in the present discussion.

In February 2014, in response to Executive Order 13636, the National Institute of Standards and Technology (NIST) released its Framework for Improving Critical Infrastructure Cybersecurity, a set of industry standards and best practices for cybersecurity risk management.[2] The NIST Cybersecurity Framework was developed as a voluntary framework to reduce cyber risks to critical infrastructure, and incorporates globally accepted technical standards, guidelines and practices, including ISO 27001, ISA 62443 and COBIT 5, among others. The framework includes five functions that together can comprise the foundation of a cybersecurity risk strategy for any enterprise:

- Identify: Develop organizational understanding of the overall cyber risk context, including asset management (systems, data, hardware, devices, communication flows), business environment (prioritization of risks, objectives and activities) and governance (every part of the enterprise must know its role and be accountable). In other words, what are the cyber activities that could be harmed and in what ways?

- Protect: Deploy safeguards to prevent intrusions, including access control, awareness and training, data security, information protection processes, maintenance and protective technology.

- Detect: Enable timely discovery of a cybersecurity breach to limit the harm from intrusions through surveillance, detection of anomalies and events; continuous security monitoring; and detection processes.

- Respond: Implement plans and activities to contain any damage resulting from a cybersecurity breach through comprehensive crisis management incident response planning and implementation of tabletop exercises.

- Recover: Develop plans and activities to resume normal operations following a cybersecurity event, including post-event mitigation and lessons learned.

As an initial matter, the company should develop a detailed plan highlighting the gaps between current practices and best practices in each of the above functions, along with concrete steps for remediation. High priority should be given to implementing a robust incident response plan to minimize damages from breaches. In addition to any required remediation, the board should monitor the development of the complete cybersecurity strategy, beginning with risk prioritization, as well as the program's effectiveness. There are two major activities to monitor: (i) the build-out and installation of the strategic plan and (ii) the effectiveness of the plan. The utilization of dashboards to monitor the installation and effectiveness of the strategic plans is essential for meaningful board oversight of cybersecurity strategy.

Dashboards

With respect to cybersecurity, effective dashboards should be carefully tailored to meet the needs of the company and its board. As a result, creating a dashboard requires input from both management and the board. The general trend is a bifurcated approach, in which maturity and overall effectiveness are monitored by separate dashboards. Below are descriptions of both, as well as sample dashboards that can be modified to the particular dynamics of industries and size.

Maturity dashboards

The maturity dashboard presents metrics that depict the maturity of the company's cybersecurity program. At its most basic, this dashboard can simply be an assessment of the company's cybersecurity strategy with respect to the five NIST designed functions, detailed above. NIST recommends that, with respect to each function, a company determine the maturity of its program using the following terms: (i) partial, (ii) risk-informed, (iii) risk informed and repeatable or (iv) adaptive. For companies that have previously identified weaknesses and remediation efforts in its cybersecurity program, the maturity dashboard should also include metrics that allow the board to monitor the progress of the identified improvement efforts.

Sample maturity dashboard

- NIST assessment

Function	Target	Actual	Change
Identity			
Protect			
Detect			
Respond			
Recover			

**Actual state can be color coded. for example, red can be used if the target state has not been achieved; green can be used if the target state has been acheived.*

- Implementation of projects

Project	Projected Timeframe	On Track	Notes
1.			
2.			
3.			
4.			

**Additional rows should be added to table as needed.*
† The "on-track" column shuold include "yes" or "no." Again, the boxes can be color-coded for ease of review

- Summary of implementation challenges

Project	Item Number:
Summary of Challenges	
Proposed New Timeline:	# of Previous Extensions:

Effectiveness dashboards

In contrast to the maturity dashboard, the effectiveness dashboard provides metrics that allow the board to ascertain how effective the program is. It generally focus on threat assessment, threat detection, remediation metrics and recovery metrics. Some boards also request certain protection-related metrics when the program is maturing; however, as protection efforts become consistent, these metrics have limited usefulness. The effectiveness dashboard is most useful when it provides numerical metrics rather than high-level conclusory determinations based on underlying numbers not provided to the board.

Sample end-of-quarter effectiveness dashboard

- 1. Number of severe incidents: _____
- 2. Description of severe incident

Type of Incident		**Status: Resolved or Ongoing**
Description		
How Discovered:		
Time to Discovery:	**Time to Resolve:**	**Estimated Cost:**

** Table should be reproduced for each severe incident in the applicable time period. External incidents that suggest new forms of risk should also be reported with description of mitigation activities.*

- 3. Detection metrics

  Physical access controls – number of incidents: _____
  Environmental controls – number of incidents: _____

Item	Detected/Received	Resolved	Notes
Unauthorized User Accounts			
Unauthorized Devices			
Credential Theft			
Incidents Involving PPI			
Alerts from Security Service Provider			

4. Training metrics

Metric	End of Q1	End of Q2	End of Q3	End of Q4
Percent of New Hires Competing training w/in 30 days				
Percentage of Employees Current on Annual Awareness Training				

**Metrics should be included for cuirrent and at least two previous quarters to show trends.*

While it is management's responsibility to develop and implement the cybersecurity strategy, and boards should not micromanage, boards have an obligation to retain the prerogative to fully understand a company's risk exposures. In the event that a board finds itself in need of additional information about a particular issue, it can engage in a deep dive. Similarly, if a board observes a large number of stakeholders providing input on the same cybersecurity concern—or if management faces delays in implementing a particular aspect of the strategy—the board can use a deep dive to assure proper management of the identified risk area. While boards should generally stay focused on the macro and defer to management on the micro, as noted above, there are times when they should be more deeply involved in the tactics and implementation of strategy (for instance, in the event of a material cyber incident). On these occasions, especially, good communication and leadership are critical for maintaining trust between management and the board.

Talent

A major responsibility of a board is to ensure the company has the right talent to accomplish its goals. Selection, evaluation and compensation of the CEO is the major task. However, it is also important that the board ensures the right skills and experiences are brought to bear in managing something as vital to the organization as cybersecurity.

Following the departure of Target's CEO, much was made of the fact that the company did not have a CISO or a chief security officer (CSO).[4] A key area of board oversight is ensuring that the company's organizational structure is aligned behind its strategy, and that management has the skills and experience to execute the strategy.

Historically, the business IT function has primarily been a technology provider, charged with delivering top quality data, Internet connectivity, hardware, software and other technologies to business units. Many companies also allowed business units to use third-party technologies. Following decades in which entities have become totally dependent on IT for their flow of information, the cyber threat has now developed into something far more dangerous than previously anticipated. Nevertheless, many companies that relied on the IT function for cyber risk management continued to do so without considering that the threat has grown exponentially beyond just a question of technology.

As cyber threats have continued to escalate, it is increasingly unrealistic to expect that IT alone is able to provide adequate protection against cyber risks. These should be managed through the lens of the entire enterprise. History demonstrates that "viewing data breaches as a 'technical issue' is a recipe for failure."[5] While IT will likely always have a major role in cyber risk mitigation, there are significant differences in the skills and goals of the IT function and the information security function.

More and more enterprises are appointing a CISO to lead cybersecurity. While the CISO must honor and reinforce the business support mission of IT, his/her highest responsibility is prioritizing security measures to mitigate cyber risk. Further, the CISO must have a national security outlook, including awareness of "tail risks" and "black swans." It will be rare that a CISO will have the business operations, project management, communications and C-suite skills to eliminate the need of a senior management member overseeing the CISO for the CEO and the board.

Distinguishing responsibility between the delivery of IT and information security is an important governance step. Assuring cyber risk management throughout the full enterprise, beyond IT, raises other governance dynamics. The cyber threat involves information in the hands of suppliers and other third parties beyond the purview of IT, in which procurement and legal experts must be involved. Dealing with significant insider risks and pressures to compromise are also beyond the scope of IT. Further, limiting oversight to IT can restrict the budget, influence and authority required to manage cyber risk effectively, which places the whole company at greater risk.

The risk-reward considerations for cybersecurity management are so significant that senior management must be in charge of the process. In addition, "deferring responsibility to IT inhibits critical analysis and communication about security issues, and hampers the implementation of effective security strategies."[6] In the end, senior management must lead cyber risk decisions so the appropriate cybersecurity strategy can be effectively implemented and monitored throughout the enterprise, with effective oversight by the board.

In addition to the management skills and experiences needed to address cyber risk, an advocate is needed

to assure such skills and experience at the board level. As noted previously, cybersecurity is primarily a governance challenge beyond IT. A CEO whose company manages cybersecurity well would bring to valuable insights and experiences. The right IT technologist could be a positive contribution to a board, but for most companies that would not be necessary.

Compliance

In general, boards rely on the general counsel, internal audits and ERM, among other functions, to provide independent risk assessments and to confirm risk management processes are in place. For the foreseeable future, cyber risks are potentially more consequential than other enterprise-significant risks. It is important that the general counsel, internal audits and ERM give cybersecurity a high priority. Boards should undertake regular, proactive discussions with these functions to ensure their leaders recognize that cyber risk is dynamic and requires continuous external screening for new forms of threat mitigation. For example, internal audits can no longer focus solely on perimeter defense controls, without consideration of risk-based controls. Likewise, ERM should monitor and screen externally new forms of cyber risks, with the awareness that some cyber risks are more qualitative and difficult to measure.

Increasingly, cybersecurity is becoming more of a legal and regulatory area where the general counsel's lead on assuring disclosures, full understanding of legal risks and adequate crisis management plans will be critical.

For independent verification as to the status of the company's cybersecurity program, the board should strongly consider authorization of an ethical hacking program. Ethical hacking is designed to uncover vulnerabilities, and is conducted internally or by an external contractor. Few companies receive pristine reports from ethical hacking. While the greatest value from ethical hacking can be achieved by leveraging findings across the enterprise to remediate immediate security vulnerabilities, the activity also has important awareness-raising implications for internal audits, ERM and the board. Finally, internal auditors and the general counsel should periodically commission a third-party cybersecurity strategy and governance review to assure that the company is keeping pace with best practices and that the picture presented to the board is verified as accurate.

Culture

Cyber risks should be managed through the lens of the entire enterprise. Every employee has a role to play, and a top-down culture of cybersecurity is essential for containing and managing this evolving risk. Studies show that employee lapses are the major enablers of cyber intrusions. A strong culture of inspiration and accountability is the best preventive measure for threats from misinformed, inattentive or malicious employees. Peter Drucker said, "Culture eats strategy for breakfast."[7] He might have added that it feeds on policies, systems and controls which are only as effective as the culture of the organization in which they exist. With regard to cybersecurity, the culture either supports and reinforces policies, systems and controls, or it overrides and undermines them. It is essential that all employees—without exception—understand that everyone has an equally important role and obligation to protect the enterprise from cyber intrusions. They must feel empowered to so act.

Cybersecurity, like all major risks, requires a culture of accountability, collaboration and continuous education and training, with all efforts geared toward supporting the strategy and mitigating cyber risks. Creating that culture drives individual awareness and acceptance of the strategy, shared commitment to its implementation and, ultimately, cyber risk mitigation. All of this starts with a "tone at the top" from the board and senior management. For values and behavior to permeate through the organization, the highest levels of the enterprise must lead by example. If a board member or C-suite member is cavalier about passwords or phishing, that will soon be known throughout an organization. Cybersecurity requires all at the top to live in glass houses.

About the authors:

R. William (Bill) Ide, III, a partner at Dentons, chairs the advisory board to the Conference Board's Governance Center and serves as the general counsel and secretary of the EastWest Institute. Bill formerly served as senior vice president and general counsel of Monsanto Company. He was counsel to the United States Olympic Committee and president of the American Bar Association, and he previously served as a member of the board of directors of Albemarle Corporation and Popeyes Louisiana Kitchen, Inc.

Amanda K. Leech is a senior managing associate at Dentons. She focuses her practice on general corporate counseling of both privately held and public companies, focusing on mergers, acquisitions, joint ventures and strategic alliances. Amanda also counsels boards of directors on implementing corporate governance and compliance programs, and assists boards of directors with special independent review and investigations.

Endnotes:

[1] Bill Ide and Amanda Leech are Members of the Dentons Governance Center and the Guide is based upon their working with and service on public company boards. Dentons Governance Center colleagues Joseph Blanco and Crystal Clark made substantial contributions to this Guide.

[2] The International Organization for Standardization's ISO 27001 has been an international information security management standard since 2005. In 2011, the SEC issued interpretive guidance on companies' disclosure obligations regarding cybersecurity risks and material breaches, and has prioritized information sharing about cybersecurity practices and incidents. In 2014, the FTC asserted itself as the Federal government's principal cybersecurity regulator with a series of rules requiring employers to take "reasonable" cybersecurity measures. And in January 2015, the Obama Administration proposed new cybersecurity legislation to address online fraud and data breaches. Similar activities are taking place at the state level and in the Congress. While this is far from an exhaustive summary, as long as the cyber threat continues, it is reasonable to assume that legislators and regulators will continue to respond with new policy proposals.

[3] http://www.nist.gov/cyberframework/

[4] Brian Krebs, The Target Breach, By the Numbers, Krebs on Security, May 6, 2014, http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

[5] Online Trust Alliance, 2014 Data Protection & Breach Readiness Guide 4 (2014).

[6] National Association of Corporate Directors, Cyber-Risk Oversight Handbook 7 (2014).

[7] Bill Aulet, Culture Eats Strategy For Breakfast, Techcrunch.com, April 12, 2014, http://techcrunch.com/2014/04/12/culture-eats-strategy-for-breakfast/

About Dentons

Dentons is a global law firm driven to provide a competitive edge in an increasingly complex and interconnected world. A top 20 firm on the Acritas 2014 Global Elite Brand Index, Dentons is committed to challenging the status quo in delivering consistent and uncompromising quality in new and inventive ways. Dentons' clients now benefit from 3,000 lawyers and professionals in more than 80 locations spanning 50-plus countries. With a legacy of legal experience that dates back to 1742 and builds on the strengths of our foundational firms—Salans, Fraser Milner Casgrain (FMC), SNR Denton and McKenna Long & Aldridge—the Firm serves the local, regional and global needs of private and public clients.

www.dentons.com.

DENTONS Know the way

dentons.com