INSIDE THE MINDS

Cybersecurity: Fixing Policy with New Principles and Organization

excerpted from

Recent Trends in National Security Law

Leading Lawyers on Balancing US National Security Concerns and the Rights of Citizens

James Arden Barnett Jr.

Rear Admiral, USN (Ret.), Partner and Co-Chair, Telecommunications Group

Venable LLP

ASPATORE

For customer service inquiries, please e-mail West.customer.service@thomson.com.

If you are interested in purchasing the book this chapter was originally included in, please visit www.west.thomson.com.

Introduction

A plethora of critical national security issues are plunging through the cracks in the political gridlock in our nation's capital, but one of the most substantial is cybersecurity. Enough hearings, press conferences, and cybersecurity conferences exist to fill every day in Washington, DC, but real accomplishments are few. Even those that seem within reach, by almost universal admission, will fall short of what is actually required to boost cyber security to an acceptable level. Indeed, the gridlock in Washington has changed the conversation from what *should* be done to what is *possible* to get done—unfortunately, even the possible-to-get-done actions are not getting done now.

Consequently, a lack of acceptable security persists for critical infrastructures, ranging from communications to energy to banking and financial institutions. Simply stated, cybersecurity protections for these and other critical infrastructure systems remain inadequate. The severity of the problem warrants that congressional leaders should overcome their political differences, but that will not happen until some other dynamics change. Luckily for the nation, those dynamics are not immutable. In this chapter, we will examine the policy stasis, the dynamics to move policy forward, and what should be done once the gridlock is broken.

Almost one hundred bills relating to cybersecurity have been introduced over the last five years, but no significant legislation has been enacted into law. In frustration over the failure by Congress to exercise its power, the Obama administration launched Executive Order 13636 in February 2013, instigating a yearlong process that culminated in the National Institute of Standards and Technology (NIST) Cyber Security Framework.[1] A key attribute of this initiative is that no action is required by Congress. The result is that much of the Framework is voluntary, and it will be difficult to monitor adoption and effectiveness. While other regulations imposing cyber security practices may ensue,[2] the Framework itself does not have the power of law and cannot be enforced.

---

[1] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Feb. 12, 2014, *available at* http://www.nist.gov/cyber framework/upload/cybersecurity-framework-021214-final.pdf.

[2] Presidential Policy Directive 21 (PPD 21) on Critical Infrastructure Security and Resilience, February 12, 2013, calls upon federal departments and agencies to review what regulatory authority may be used to enhance cybersecurity.

The Cybersecurity Framework may be summarized as the best practices, methods, and processes to improve cybersecurity in the industries that comprise the sixteen critical infrastructures, a roadmap to reaching a higher level of cybersecurity wherever a business entity starts. In the vacuum of decisive and effective legislation, the Framework is a competent and useful step forward, a superb example of a government-initiated, industry-led collaboration and benchmark. However, the strength of the Framework also subsumes its weakness.

To achieve broad acceptance for a voluntary program, and to ensure relevance, NIST assiduously sought and compiled input about best practices from the critical infrastructure industries through a yearlong process and numerous topical workshops. Since the entities that were most able to participate in the process were larger businesses and well-funded trade associations, much of the best practices and methodologies were previously implemented by those companies with the wherewithal to do so. These larger companies have the resources for cybersecurity personnel and programs, and they are not interested in a Framework that requires much more in the way expenditures for cybersecurity any more than they would ask for regulations to do the same. The medium and smaller companies may view the Framework as extremely useful guidance, but they may still lack the funding to implement the methodologies to the degree that the larger, better resourced companies are. Consequently, while the Framework is good, its effect may be muted or delayed, except where there are meaningful business-oriented incentives or actual enforceable regulations.

The Framework may influence a growing jurisprudence of cybersecurity as courts in various jurisdictions adjudicate lawsuits against entities claiming that a duty to keep data, network or the consumer protected against cyber attacks has been breached. In the absence of other standards, plaintiffs, and the courts, may examine the Framework as a source to develop a cyber standard of care. Such a standard of care will develop over years, even decades, and will certainly vary from state to state and in the different federal circuits.

Other examples exist of good initiatives that will not come close to addressing the cyber security problem. Much of the cybersecurity policy conversation over the last few years has been about information sharing in three modes: business to business, business to government, and government

to business. The first mode raises antitrust and anti-competitive concerns. The second, business to government, alarms the private sector over how its customers and the public may perceive this sharing and what liabilities may arise. Finally, the third mode of government to business information sharing raises the anxiety of all who are concerned with privacy about what information is being shared and to whom does that information belong.

However, the efficacy of information sharing has militated discussion of how to enhance all three modes. Information sharing and analysis centers (ISACs) have proven effective in some of the critical infrastructure sectors. Numerous information sharing bills have been introduced in Congress, partly as a result of reports from various parts of the US intelligence community having information on current and possible attacks on specific businesses, but being unable to share that information due to legal restrictions. Privacy remains a major concern, and effective safeguards must be included in legislation, but a consensus has developed that information sharing is an effective tool that should be expanded and facilitated.

Yet no real information sharing legislation has been enacted into law. Again, in some frustration with the lack of congressional action, the administration, acting through the Department of Justice and the Federal Trade Commission (FTC) announced in April 2014 a policy that would give comfort from antitrust and anti-competition enforcement to businesses who legitimately share cyber threat and attack profile information.[3]

Information sharing is an important capability in cybersecurity, but even if it were fully implemented, the problem would not be solved. Information sharing legislation is currently a mausoleum and monument to actions that should and can be taken, but are not. Unfortunately, these untaken actions dominate the discussion and take up all of the oxygen for what actions must be taken for effective cyber security. Why?

Breaking Old Mental Models

When revolutionary discoveries and new challenges appear, humans attempt to understand them in the context of previous experience, applying

[3] Department of Justice and Federal Trade Commission, *Antitrust Policy Statement on Sharing of Cybersecurity Information*, Apr. 10, 2014, http://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf.

the principles and mental models that seem to best fit the disruptive information. Consider the mind-bending discovery of Anthonie van Leeuwenhoek as he peered into a microscope in the 1670s and found another world full of microbes. No one believed him at first, and even as the public began to believe in microbes, it took almost 200 years before medical science associated microbes with disease.

Cyber space is such a discovery, and even as the world has transformed itself and interconnected its parts, much of the insecurity of cyber space comes from the application of old mental models, organizations, principles and law to an unprecedented, unconventional domain.

Likewise, improvements in navigational techniques and instruments in the fifteenth century led to a significant increase in exploration at sea and oceanic commerce. In many ways, the promise of this exploration and commerce was as revolutionary and disruptive to those times as the Internet is today.

Right on the heels of the expansion of commerce at sea came a rash of piracy, independent and state-sponsored. Piracy continued to be a menace until three actions were taken. First, nations had to more fully develop the capability to fight piracy at sea. Second, nations had to adopt laws and a system of jurisprudence to deal with the perpetrators. Third, nations had to adopt international conventions and laws for dealing with piracy. This process took almost 200 years to develop, but now piracy makes the news because it is rare and is generally in places where the rule of law is weak.

Similarly, cyber space is much like a new, vast ocean of bits and pieces of our thoughts, our crafts, our commerce, our wealth, and even our identity, and its scope is still evolving. Understanding that cyber space demands a new mental model and a skeptical review of applicable principles can accelerate the development of an effective regimen, hopefully before the passage of centuries. Currently, the interplay of principles and a fundamental misunderstanding of the new and uncomfortable role of government impede real progress.

Conventional wisdom states that the Internet should be free and unfettered, open to innovation, a concept that is not disputed here. However, when this

concept is applied to insist that the government has little or no role to play, it is destructive of the government finding its proper role.[4] The advent of Edward Snowden and his Wikileaks revelations about government programs also has militated many to mistrust any role for the government in protecting cyber space, and those leaks have launched an important debate about privacy in cyber space and the role of intelligence agencies in gathering information domestically. These considerations should imbue the debate with richness, but should not be allowed to stop the definition of the proper role of government.

Principles for Addressing Cyber Security Policy

Allowing for a re-examination of how cyber space is viewed and the principles for dealing with it, the first two principles echo from currently held beliefs. The others reflect values that embrace a new mental model for cyber space, one that challenges rote responses to current roles.

1. *Cyber space should remain a place for innovation and free expression.* This is an enduring value, and any actions implemented must take this into account. Cybersecurity must be recognized as essential to innovation and expression in the same way that the rule of law was essential to bring the Wild West to fruition in the nineteenth century. Innovation and free expression must be the goals and the prime directives for cybersecurity, but they should no longer be used to thwart other principles and tools.

2. *Privacy must be protected in cyber space.* Those who see the need for more government activity in cyber space must ensure that privacy, as defined by this generation, is afforded effective safeguards and oversight. These safeguards and the oversight will be seen as an impediment to law enforcement, to intelligence and to governmental actions in general, just as similar safeguards and oversight have been in other domains and settings.

3. *Security in cyber space and the protection of the Internet is the responsibility of the private sector.* The cybersecurity fight is the province of business and

[4] The government playing no role or being an instrument which stifles innovation belies the fact that the government initiated the Internet (through its inception in Arpanet) and has facilitated governance to allow innovation.

industry, which owns or operates 80 percent or more of cyber space. The government simply cannot do it effectively. This is the first critical realization as to what the role of the government should be.

4. *The primary function of the government should be to support and aid the private sector in providing cybersecurity.* This is the corollary to the private sector owning the cybersecurity responsibility, and it is the most difficult part of breaking old mental models. Government can send in the cavalry when the border is attacked. The National Guard can be mobilized to assist with natural disasters. Armies can be raised and deployed to defend the nation. But the government cannot take the lead in protecting the Internet and will do harm if it attempts to be the primary actor. It must reinforce the private sector. This is not to say that there may be incidents that rise to the level of national security and the government's role would be primary as it is when the nation is attacked in more conventional ways. In addition, reinforcement of the private sector does not mean that the private sector will be the arbiter of what support and assistance it receives, as will be discussed.

5. *Where the market will not provide adequate cybersecurity, the government should provide incentives and regulations to raise the bar.* The last decade has made it abundantly clear that the market will not provide acceptable, adequate levels of cybersecurity, and that being the case, one role that government can play is creating a cybersecurity market through legislation, regulation, incentives, or some combination thereof. Certainly, regulation is not the sort of "support" that the private sector would seek, even if it would be good for many of the industry sectors overall. Creating a security market has to include business-oriented incentives as well as requirements. The government has many examples in health, agriculture, and other areas.

An example of the government creating a market is the national emergency number system. Dialing 911 started in 1968, and Americans have come to take it for granted that help in an emergency is a phone call away. However, the market did not provide the 911 system, and it would not exist without government regulation. The telecommunications industry has embraced the

911 system, and an industry has grown up to support the capability, providing jobs and continued innovation. Importantly, government incentives are part of this system. On a state-by-state basis, telecommunication companies may be reimbursed for their participation in the 911 system from the small, government-imposed fee on telephone bills. No one likes the fees, but no one complains about having a 911 system that would not otherwise exist. This example may be analogous of what should happen to create a cyber security market.

Principles are essential foundations for effective policy, but they remain the stuff of whiteboards and conference room tables unless they are embedded in organizations and implemented.

Organizing for Cybersecurity

If government has a role in cybersecurity, and it is to support the private sector, is the government organized to accomplish the goal? A close examination of the best organization for cyber security is nearly impossible when the discussion is locked in a dispute as to the role of government.

Organizing (or re-organizing) around a problem or challenge is very typically American. In the 1920s, a major problem with organized crime arose during Prohibition. The federal government addressed that problem by creating the Federal Bureau of Investigation (FBI). Likewise, when Sinclair Lewis' book, *The Jungle*, flayed the raw facts about meat packing, the Food and Drug Administration (FDA) was created in 1906. The Department of Defense (DoD) was created after World War II, along with the joint chiefs of staff, to ensure the cooperation among the branches of the Armed Services. And more recently, after the attacks on September 11, 2001, the Department of Homeland Security (DHS) was created to coordinate the government's response to disaster and terrorist threats. DHS has now been assigned the responsibility for handling domestic cyber security policy, but that role was not part of the calculus for its creation.

In fact, no major institution of government has been created or re-organized to address domestic cybersecurity. The Department of Defense created a new command, US Cyber Command or CYBERCOM, in 2008, but like the re-tooling at the National Security Agency and other intelligence

agencies, the purpose of the cyber efforts is directed at the enemies and potential foreign adversaries of the United States. Despite horrendous disruptions and losses in the billions of dollars from cyber crime and attacks, the United States cannot point to an agency of government that has been created to address these challenges.

So, the United States has applied the institutions it already had. The Department of Justice and the FBI have developed expertise in detecting, analyzing, and prosecuting cyber crime. The Department of Treasury and the Secret Service play important roles in cyber attacks in the financial sector. NIST has developed an expertise in the standards and operation of the Internet. In fact, many federal departments and agencies have responsibilities for cyber security in their respective areas of expertise.

DHS has been designated as the entity responsible for domestic cyber security, but it does not have regulatory powers and for the most part, it is not a law enforcement agency with regard to cyber security. The newest of federal departments, DHS is still actively striving to forge an effective organization from the twenty-two agencies and entities, with their divergent cultures and missions, that were amalgamated after 9/11. The debate over which agencies should come under DHS was fierce, and while the department does an admirable job for an impossible mission set, DHS still struggles with agility and responsiveness, two attributes essential to cyber security.

DHS is steadily building expertise (at the pace of government hiring) and capability, but the department is still, in many ways, first among equals. Other agencies engage in competitive cooperation. One such competitive partner is the National Telecommunications and Information Administration (NTIA), which was created by President Nixon under the Department of Commerce to handle wireless radio and telecommunications issues. Approximately 200 people work for this agency, tiny by federal standards. NTIA is responsible for managing all federal government-related telecommunications issues and spectrum as well as cyber space-related issues. For instance, the NTIA has worked with the Internet Corporation for Assigned Names and Numbers (ICANN). It represents the United States at meetings of international organizations that deal with cyber space and communications. In addition, the NTIA was recently given a new

responsibility—management of a $7 billion public safety broadband network program called First Responders Network Authority (FirstNet).[5]

A close analysis of the federal effort on cybersecurity reveals dedicated professionals, many with remarkable expertise, who are laboring under (and in spite of) old organizational architectures and legal structures. The coordination of these efforts is often at the interagency level in a committee-like process. Policy issues and disputes can and are resolved within the executive office of the president, but the process involves a clash between the two gangs in the Eisenhower Executive Office Building, the National Security Staff and the National Economic Council that may not optimize a coherent cyber policy. Indeed, the flexing of the two staffs over cyber security and Internet policy mirrors the larger problem: will economic policy hold sway over cyber space or will national security priorities have the upper hand? The answer, of course, is that both economic and security goals must be weighed and met in cyber policy, but the process has not been designed to do so. The position of cybersecurity coordinator has been useful in pushing forward important initiatives (such as the Cybersecurity Framework and trusted identities in cyber space), but the position has not been accorded the power and influence to coordinate and make coherent policy throughout the executive branch.

As with a new mental model for cyber space, so too is a new organization required. Such a requirement does not have to trigger concerns for expansion of government. Rather, a proposal for re-organizing the government to address cybersecurity can be seen as consolidation of disparate and loosely organized efforts. The federal government still needs to grow its cyber expertise across the government, but the reorganization alone does not necessarily imply growth and may indeed yield some efficiencies.

One concept would be to create a US Department of Cyber Space and Communications at the cabinet level by extracting the DHS Cyber Security and Communications (CS&C) Directorate and combining it with NTIA, which would be excised from the Department of Commerce. NTIA has been chronically undermanned and resourced since its inception, given its responsibilities. By way of comparison, the Federal

[5] Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96, 126 Stat. 156 (Feb. 22, 2012).

Communications Commission (FCC) is more than seventy-five years old; it has developed significant expertise in all forms of communication; and it is staffed by about 1,800 people. While the NTIA is staffed by approximately 200 dedicated professionals who are doing a good job, they simply do not have the depth or breadth of experience to handle many key cyber space issues. Their expertise and effect would be magnified and empowered in the new department.

Other parts of government should be reviewed for combination into the new Department of Cyber Security and Communications. Many other nations have an executive communications department or ministry of communications as well as a federal communications regulator such as the FCC. The new department could be remade with a new culture just as new organizations like the FBI created new ethos for law enforcement. New authorities could streamline the government's ability to support the private sector and fulfill the other principles set forth above.

However, another type of gridlock will prevent this organization from occurring or even reaching a meaningful discussion. The Internet and cyber space are caught between the homeland security committees in the House and Senate and the commerce committees in the House and Senate. This is not a partisan dispute, but an internecine power struggle for oversight of these topics. No member, Republican or Democrat, on a homeland security committee is likely to yield jurisdiction over cyber security to a commerce and communications committee, and vice versa. The current organization, or lack of it, will remain a hostage to this struggle.

One possible method to break through the committee jurisdiction deadlock is a select committee. The Senate Select Committee on Intelligence, and its counterpart in the House, have had notable bipartisan successes in the past, drawing on the special mission of these select committees. A select committee for the Senate and the House, drawn perhaps from the members of both homeland security and commerce and communications committees could provide the congressional basis for a useful reorganization of federal efforts in cyber policy.

In the absence of the Herculean effort it would take in Congress and to legislate a new federal department, an interim step would be to separate DHS's CS&C Directorate into its own agency, allowing it new authorities

the resources for expertise and programs and the ability to take action and make policy decisions with more agility and some autonomy. Without a new cabinet secretary, a stronger position in the White House would be needed to set and make coherent federal policy across all departments and agencies.

The Unaddressed Cybersecurity Problems

Without a new mental model and vision, a re-examination of our principles and goals in cyber space, and the organization to act on those principles to accomplish the goals, US progress on cybersecurity is likely to be incremental, costly, and frustrating to those who work on it. Ultimately, the US economy, national security, and American citizens will suffer for it. A brief examination of what is not being discussed and is not getting done may illuminate what the loss is from the political gridlock and the failure to organize.

Former cybersecurity advisor to presidents George W. Bush and Obama, Melissa Hathaway and her co-author, John Savage, have written a white paper about the eight duties of Internet service providers (ISPs).[6] These duties, briefly stated and paraphrased, are:

1. To provide reliability.
2. To provide authenticated routing.
3. To provide authoritative naming information.
4. To provide anonymous security incident information to the public.
5. To educate customers about threats.
6. To notify customers about possible malware infections.
7. To warn other ISPs of dangers and to assist in emergencies.
8. To assist affirmatively in thwarting criminal activity.

The problem is that these duties are not formalized. No telecommunications carrier or ISP is actually responsible or obligated to perform any of these duties, unless it does so voluntarily. Each carrier and ISP address cybersecurity for its customers and the public partially and each in its own way, but Hathaway and Savage would not have written this paper

[6] Melissa E. Hathaway & John E. Savage, *Stewardship of Cyberspace - Duties for Internet Service Providers,* Mar. 2012, http://belfercenter.ksg.harvard.edu/files/cyberdialogue2012_hathaway-savage.pdf.

if these duties were being universally observed and incorporated into business practices. This list of duties can be viewed as a list of what is not being done and is not likely to be done without the proper and restricted role of government.

The second duty to provide authentic and authoritative routing information is illustrative. In essence, this is the duty to prevent intentional or inadvertent Internet route hijacking. The Internet is more than 40,000 autonomous systems connected to one another by a protocol system that is based in large part on trust. Large and small ISPs route traffic to one another based on a self-declaration of the identity of the separate network. No central registry exists against which the authenticity of routing can be checked. As a result, sophisticated malicious entities can declare that traffic intended for ISP A from ISP B be routed to or through the route hijacker.

An example of this occurred in April of 2010 when a significant percentage of American Internet traffic was suddenly hijacked and routed through China for about eighteen minutes. That traffic was exposed to tremendous insecurity and no one has an estimate on the extent of the loss. Since that time, only minor steps have been taken to start addressing Internet route hijacking.[7]

In fact, no solution is on the horizon. Standards need to be developed, and even if one ISP spent the money to institute secure routing, it would not really be effective until all the other ISPs had the same system and protocols. Unless the government provides the requirement and the business-oriented incentives, Internet route hijacking will remain a vulnerability for a decade or longer. This problem is locked in the old paradigms of the carriers and ISP resisting all regulation and the Congress not wanting to provide financial incentives to the private sector for improving cybersecurity, whether those incentives are tax credits or limitations of liability.

In addition to Internet route hijacking, website spoofing is another problem the solution for which could be accelerated if the government could play its proper role. Website spoofing is the creation of a website as a hoax to lure

[7] The FCC has developed a voluntary program which is still not complete. Many others are working on programs, but no solutions are likely in the next few years.

readers into divulging personal or financial information. Domain Name Security Extensions (DNSSEC) could provide considerable safeguards against spoofing, but implementation has been slow. Again, the government could offer incentives to ISPs and light touch regulations to accelerate implementation. In their absence, full implementation of DNSSEC is not likely in the near term.

A final example (among many others that could be offered) of cyber security problems that are not being addressed or even discussed adequately is communications supply chain security. Often, cybersecurity is regarded in terms of bad guys breaking into a network from the outside, or perhaps, insiders breaching security. Supply chain security involves insecurities potentially being built into the network, either intentionally or through exploitable problems from counterfeit chips or parts.

Some members of Congress have focused inquiry on Chinese corporations that manufacture communications network equipment. The US connection with the rest of the world is mostly carried over undersea fiber optic cables that are manufactured in China. The fact remains that much of American communications equipment is not made within the United States. Many US corporations that manufacture globally have supply chain safeguards in place (especially those that contract with the Department of Defense), and yet most will admit there are still concerns. These examples are just a few of the cyber space problems that should be addressed and are receiving scant attention and even less in the way of resources.

Conclusion

Political gridlock, a commitment to inapplicable principles and outmoded mental constructs for cyber space are preventing the examination of serious cyber security challenges and meaningful solutions. Current efforts are worthwhile, but they will fall short of an effective system of cyber security. Ensuring that the Internet remains a domain for innovation and free expression does not mean that the government should not play a circumscribed role in reinforcing the private sector's efforts in providing an improved level of cybersecurity. That role may include light touch regulations to create a security market, but they must be accompanied by meaningful, business-oriented incentives.

Unless new mental models and principles are applied to the approach to the governmental role, the duties of the private sector for cybersecurity will remain less than what is needed. Adopting a new mental construct and affirming new principles and goals for the government's role must be followed by organizing the federal government to more fully address cyber security, just as the United States has done for other serious challenges throughout its history. Once this is done, and probably not until this is done, the other serious problems and threats to cybersecurity will remain largely unexamined and unsolved.

Key Takeaways

- Principles for addressing cyber security policy include the following:
    - Cyber space should remain a place for innovation and free expression.
    - Privacy must be protected in cyber space.
    - Security in cyber space and the protection of the Internet is the responsibility of the private sector.
    - The primary function of the government should be to support and aid the private sector in providing cybersecurity.
    - Where the market will not provide adequate cybersecurity, the government should provide incentives and regulations to raise the bar.
- The principles should be followed by the creation of a new organ of government with the expertise, resources and authority to support the private sector with incentives that are meaningful to the private sector and to create a security market.
- Several serious cyber security problems are not being adequately addressed in the absence of these principles and organization.

James Arden Barnett Jr., Rear Admiral USN (Ret.), is a partner and co-chair, Telecommunications Group, in the law firm of Venable LLP, working in the firm's cybersecurity practice. Admiral Barnett was previously the senior vice president for National Security Policy for the Potomac Institute for Policy Studies, a science and technology policy think tank in the Washington, DC area.

Admiral Barnett served as the chief of the Federal Communications Commission's Public Safety and Homeland Security Bureau from 2009 to 2012. He was responsible for overseeing FCC activities pertaining to cybersecurity policy, public safety, homeland security, emergency management, and disaster preparedness. Under his leadership, the FCC adopted three major voluntary initiatives: the U.S. Anti-bot Code of Conduct, acceleration of adoption of Domain Name System Security Extensions, and initial steps at defeating Internet route hijacking through improved Border Gateway Protocol.

ASPATORE

Aspatore Books, a Thomson Reuters business, exclusively publishes C-Level executives and partners from the world's most respected companies and law firms. Each publication provides professionals of all levels with proven business and legal intelligence from industry insiders—direct and unfiltered insight from those who know it best. Aspatore Books is committed to publishing an innovative line of business and legal titles that lay forth principles and offer insights that can have a direct financial impact on the reader's business objectives.

Each chapter in the *Inside the Minds* series offers thought leadership and expert analysis on an industry, profession, or topic, providing a future-oriented perspective and proven strategies for success. Each author has been selected based on their experience and C-Level standing within the business and legal communities. *Inside the Minds* was conceived to give a first-hand look into the leading minds of top business executives and lawyers worldwide, presenting an unprecedented collection of views on various industries and professions.

ASPATORE