



accenture

High performance. Delivered.

Security and Privacy Compliance

More than 10 years ago, in one of the first high profile computer-security breaches in Canada, "Coaxial Karma" broke into a university system—after 72,000 unsuccessful login attempts. It is no news that would-be intruders since then, everywhere, have become more efficient, sophisticated and determined.

Some security observers estimate that an average of 450 new worms, viruses and Trojan horses are created and released into cyberspace each month. And the intrusions grow more pernicious—the estimated global business loss from just two of last year's more famous events, the SoBig and Blaster attacks, was \$35 billion.¹

In reaction, governments and their responsible ministries or regulatory agencies continue to issue a steady stream of market, industry, and situation-specific regulations. Affected organizations—both private and public—struggle to keep up, often in piecemeal fashion and sometimes with unintended downside effects. The fast-changing nature of information technology itself only exacerbates these pressures. Legal systems by their nature are historically conservative and even reactive; the pace of technology innovation could hardly be more dynamic.

How some enterprises master the security challenge

There are some companies that have learned to "get it right." As part of its High Performance Business initiative, Accenture has formally committed to understanding what drives the minority of publicly held companies that have demonstrated the consistent ability to create value for shareholders. Using widely accepted financial metrics, a rigorous methodology, and continuous industry-specific research, we have developed and are now validating a number of hypotheses on the distinguishing characteristics of these enterprises.

In the meantime, as it pertains to security, our experience points to certain factors that differentiate leaders. The most important one is strategy, that is, the grounding of security initiatives in a solid business case.

Shared compliance models, tailored details

While the nuances of their security models are organization-specific, our experience indicates that leading enterprises share generally similar approaches. First, they have a deep understanding of both the relevant security and privacy regulations in their industries, and of the business needs of their customers and partners, as well as a commitment to develop clear policies, standards and strategies around these requirements. Second, they understand that effective policies depend on robust controls (technical and non-technical) and security architecture, and they design and implement controls and architecture accordingly. Third, they support the viability of their compliance programs with an effective governance model, which establishes clear decision-making, monitoring, audit and enforcement mechanisms, fully cognizant of cultural realities within the organization. Lastly, they calculate for the inherently dynamic nature of security and privacy compliance, and cultivate senior executive and even board-level commitment, with clear plans for change leadership.

Technical and business compliance: Two different disciplines

As enterprises virtualize both geographically and functionally, the points of external and internal vulnerability in their information technology infrastructures only disperse and multiply, creating a two-front challenge. Externally, the enterprise must both manage and anticipate new information security and privacy rules on multiple regional, industry and functional fronts. Internally, it must inculcate a culture of security-mindedness, while continuously absorbing the organizational impact of generations of new security technology.

While technical solutions are by no means simple, Accenture's experience indicates that the most problematic privacy compliance challenge (and by extension, security challenge) is organizational and strategic. Simply put, an airtight regulatory-response mechanism, coupled with multiple technology solutions, will eventually fall short without an equally strong security-strategy vision. This kind of vision, tied to the specific objectives, culture and operations realities of the enterprise, is what differentiates security leaders from laggards.

Our approach responds by first steering clients to questions of comprehensive strategy. The most effective solutions, we have found, help clients emphasize the building of trust with their customers and business partners, rather than simply focusing on point compliance solutions. High-performance clients have shown us that information security and privacy practices are integral to credibility, viability and growth. To achieve these goals, executive sponsorship and support is

Sidebar: The Development of a Discipline

Until a few years ago, "security" as a function was often defined in terms of protecting investments in hard physical assets, and "security technology" was defined on the level of card access, cameras and security guards. Since then, some enterprises (again, both public and private) have built dedicated information security organizations, hired chief information security officers, chief security officers, and developed policies and procedures, all aimed at the protection of critical internal assets and resources. Even more recently, organizations have begun to realize that protecting external assets, such as customers and business partners, is just as important as protecting internal assets. This has led to the hiring of chief privacy officers and the development of privacy programs to augment existing security programs.

Professional accreditation programs such as Certified Information Systems Security Professional (CISSP) have aided the process. In just six years, for example, nearly 20,000 IT professionals have earned CISSP credentials, and the SysAdmin, Audit, Network, Security (SANS) Institute since 1989 has provided training to more than 160,000 professionals. Our experience points to continuous raising of corporate standards, which of course vary by region, industry, function—and of course, enterprise.

One result is that privacy and information security compliance has advanced rapidly, as technical disciplines. A quick scan of research published by think tanks such as the SANS Institute shows an impressive body of knowledge and experience at the application or systems level, for example, with archives of research papers on specialized subjects such as "YASSP Tool for Hardening Solaris" or "Bastille-Linux Script to Secure Linux and HP-UX." The British Standards Institute has developed a robust and meticulous information security standard in its BS 7799 certification program. And leading IT providers, particularly database companies such as Oracle and SyBase, have formed platform-specific information collaboration and support networks.

The other result is that function- and industry-specific solutions have proliferated. Leading companies interested in absorbing lessons learned outside their industry or core competency have many more options to evaluate. Some of these companies, looking for accelerated solutions and results, have turned to external partners to help them navigate.

Sidebar: Regulatory Enforcement and Jurisdiction

An entirely new generation of jurisdiction questions has made compliance enforcement more complex, brought on by the circumstances of instantly and distantly transmitted (and relayed) cyber data. For enterprises that aspire to industry or functional leadership, this set of moving goalposts has only increased a willingness to leverage the experience and perspective of external subject experts. Accenture, for example, is often called upon to assist organizations that operate on a transnational basis, helping them establish protocols that address multiple regulatory approaches.

The question of “who regulates” is a common one we have seen transnational enterprises attempt to address. In the United States, legal jurisdiction has historically been determined by the physical residency of parties, a determinant which loses clarity in cyberspace. Canada, by contrast, has chosen to centralize all authority for computer-related security issues within a single federal office, the Information Technology Security Branch (of the Royal Canadian Mounted Police). The European Union (EU), having awakened to the commercial and competitive implications of allowing the United States to set legal and regulatory precedents, is just now considering establishment of a European Network and Information Security Network, an admittedly ambitious endeavor considering the complexity of EU national-integration issues.

paramount. Awareness and the willingness to act must percolate up from the technical ranks to include the C-suite and even the board of directors. The result: an approach that embraces both improved cost effectiveness and improved performance, measurable by clearly defined and meticulously collected metrics.

A legacy of overlapping regulation

The confusion of the regulatory environment is real. Organizations are often whipsawed between overlapping, over-focused and uncoordinated regulations, laid down along geographic, industry, and situation-specific lines. In 1996, for example, the United Nations passed a model legal template for electronic commerce, and there have been increasing calls for international cooperation and coordination of privacy and information security regulations from some governments. Further confusing the issue of compliance is the existence of a multitude of non-mandatory security standards. Created by industry groups and various standards bodies, security standards have long been used by organizations where adequate

From our perspective, some of these questions are a matter of an evolving body of cyberspace law. Others are more structural in nature. The political question of central regulatory authority, or lack of it, in a major structural driver of sometimes unclear jurisdiction. Although the United States passed its first identity theft legislation in 1988, its federalist legal structure and traditional wariness of concentrated authority has produced a middle road between centralized and decentralized jurisdictional approaches. Since 9/11, momentum has been moving in the direction of increased cooperation and coordination on the national level.

Section 103 of the USA Patriot Act (“Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism” Act), for example, allocated more than \$600 million for the FBI’s Technology Support Center. Section 105 of the same act similarly increased resources for and commitment to the agency’s information crime task force. The National Strategy to Secure Cyberspace report, issued in February 2003, however, shows that the United States still holds back from a formal commitment to a centralized, national cyberspace defense model.

regulation has not existed. Now, with the proliferation of legislation, in addition to existing standards, the compliance challenge has increased significantly, especially for companies with transnational or offshore-outsourcing operations. An organization operating in the United Kingdom, for example, would fall under both the UK Data Protection Act and the European Union Directive on Privacy and Electronic Communications. Geographic regulations also operate at the provincial or state-level function: Although California’s Security Breach Notification Act (SB 1386) is the most well known piece of American state legislation, 45 other US states also have information privacy laws on their books.

Industry sectors are affected by security regulation to widely varying degrees. As might be expected, the US financial services industry—with its history of tight regulation, heavy IT spending and pioneering efforts in electronic payment systems—illustrates one of the most elaborate compliance frameworks. In the United States, the Gramm-Leach-Bliley Act (1999) spells out additional identity-theft rules for financial services operators. The Financial Crimes Enforcement Network—which includes the Securities and Exchange

Case Study: Extending a Privacy Minded Culture

When a UK-based bank initiated its move into retail banking, the security of its information assets and privacy of client data were paramount concerns. As a longstanding provider of private banking services, the bank had developed an organizational culture of discretion. Now it wanted to safeguard that tradition through a critical expansion period.

The bank selected Accenture to develop a business-case-driven strategy and implementation plan for the new unit's security function. Bank executives understood that any solution would have to integrate with the enterprise-wide security needs of 35 million global customers, many of whom enjoyed multiple relationships with the bank, each with its

own access configuration. The new solution also would have to integrate with a privacy compliance structure geared to operation in more than 60 countries.

Client experience has shown that such integrated, strategy-intensive approaches produce far more return on security investment over time than smaller, iterative initiatives. In this case, a 250-person security organization was established from scratch, but only after Accenture conducted a comprehensive risk and organizational-impact assessment, followed by a full security strategic plan. The plan covered technical infrastructure, applications, policies and procedures, operations and governance.

Commission, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Federal Reserve Bank and the Federal Deposit Insurance Corporation—further coordinates the industry's regulatory apparatus. Contrast that to the information-intensive healthcare industry, in which the sole security and privacy regulation, the Health Insurance Portability and Accountability Act governs the gathering, confidentiality and transmission of all patient data.

Catching up, or not

What about organizations that have implemented only parts of a strategic security and privacy compliance model, or enterprises that seek to catch up with current-state regulatory demands? Accenture's experience shows that many may have to recognize that their existing compliance resources may be overmatched by a comprehensive, one-at-a-time change effort. Such organizations may eventually find that even when they have become compliant, they might not be secure. These enterprises may then be moved to find specialist partners adept at both designing and implementing compliance transformation. The focus of emphasis will of course vary by organizational need, but the general end-to-end approach will be consistent.

Given information security and privacy are most effective when they are least visible, the business case for increased compliance investment can be a difficult sell for organizations under IT-budget pressure. But information security analysts estimate that spending on security products reached \$64 billion last year, showing 11% growth, and is expected to surpass \$118 billion by 2007.² So the question is not whether

organizations will invest in IT security and effective privacy compliance. Given regulatory, marketplace, technology and competitive trends, the likelihood is that organizations will spend. The more pressing question, especially at the C-level, is whether they will spend wisely and effectively, driven by strategy and the business case, rather than by crises.

Notes

- 1 International Data Corporation - Featured in article: Blaster and SoBig change the landscape By Robert Jaques [03-09-2003] - *Security spending set to soar following unprecedented success of next-generation worms*
- 2 International Data Corporation Report Referenced in NetworkWorld Fusion Magazine on 10-13-03. Article title is "Security Spending Up" By Ellen Messemer. <http://napps.nwfusion.com/weblogs/security/003595.html>

About Accenture

Accenture is a global management consulting, technology services and outsourcing company. Committed to delivering innovation, Accenture collaborates with its clients to help them become high-performance businesses and governments. With deep industry and business process expertise, broad global resources and a proven track record, Accenture can mobilize the right people, skills and technologies to help clients improve their performance. With approximately 90,000 people in 48 countries, the company generated net revenues of US\$11.8 billion for the fiscal year ended Aug. 31, 2003. Its home page is www.accenture.com.