WHITE PAPER

Understanding Information Intensity and Cybersecurity for Strategic Success

Cybersecurity, Corporate Strategy, and the Value Proposition

By Samuel Sanders Visner, Senior Vice President and General Manager, Cybersecurity, ICF International

Overview

While many regard cybersecurity as a compliance mandate, the "information intensity" of many enterprises argues for cybersecurity to be treated as intrinsic to the value proposition and an element of corporate strategy.

Discussions relating to cybersecurity, including those at the Board and C-Suite levels, continue to be dominated by questions of risk and compliance. Senior decision-makers seek to understand the cybersecurity risks to enterprise operations, public safety, privacy information, intellectual property, and economic viability. Boards seek to know if corporate executives understand and are addressing the myriad controls, requirements, and standards pertinent to the cybersecurity of each industry. Government department and agency executives hold tight to analogous concerns relating to the Federal Information Security Management Act, Homeland Security Presidential Directive 12, and other requirements. In all of these cases, cybersecurity is treated as a cost to be borne where necessary and minimized if possible. Seen as a mandate, cybersecurity is all-too-frequently regarded as yet one more problem to be addressed with constrained resources.

This approach to cybersecurity recalls Detroit's approach to safety in the 1960s and 1970s, when safety requirements were regarded as compliance mandates and resisted as competition to eight-track tape players and other options.[1] Today's enterprises that regard cybersecurity in a similar fashion fail to appreciate it strategically and as an element of value to the enterprise's many stakeholders.

Such a situation need not be the case.

What is Information Intensity?

In the general economy, information—and by extension, the security of that information—is recognized as a vital aspect of corporate strategy and (more importantly) of an enterprise's overarching value proposition. The concept of "information intensity" reflects the recognized value of information; it's a concept that has existed for decades, but which gained currency in the 1980s and has experienced rising importance through the present day.

There are two types of information intensity, both of which are vital to today's enterprise: *product information intensity and value chain information intensity.* [2]

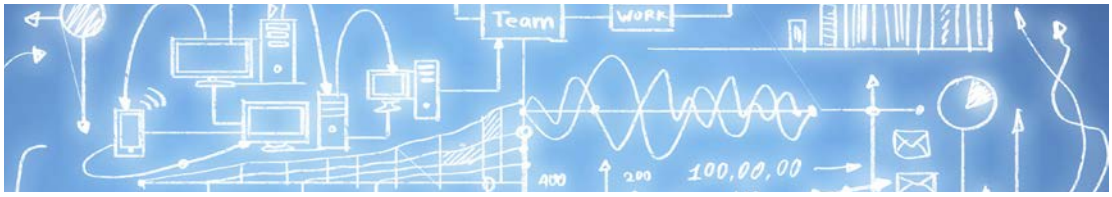
Product information intensity measures the extent to which a product is information-based, which is increasingly the case in today's global economy in general, and in the

About the Public Sector

The President's 2006 Comprehensive National Cybersecurity initiative described cybersecurity as an element of national strategy. It characterized the cybersecurity of government, military, critical infrastructure, defense industrial base, and other domains as an important component of the national interest, enhancing national security, strengthening economic competitiveness, and helping to secure our nation's role in global affairs. The Strategy spoke not of cybersecurity compliance, but of cybersecurity as a vital national imperative. The current Administration shares this view, and its policy declarations have reflected consistency with the 2006 perspective.

1 This approach endured even as competitors, such as Volvo, appropriated safety as an element of the automobile's value proposition. Volvo's strategic approach to safety presaged today's imperative that cybersecurity be considered an element of corporate strategy.

2 Department of Information Technology & Operations Management, Florida Atlantic University and Jim Quan, Department of Information Technology & Operations Management, Florida Atlantic University



United States and other advanced economies in particular. Any business that provides information-for-value (e.g. financial reporting and transactions, media, social networking, etc.) delivers one or more products that comprise principally (or solely) information. For such enterprises, the security of the information they employ and provide affects materially the value of the product they convey to their customers. Their value proposition can exist and thrive only to the extent that cybersecurity and information assurance (relating to provenance, processing, and delivery) are present.

Value chain information intensity describes the extent to which information contributes to the production and delivery of non-information products. Global supply chains related to the manufacturing of aircraft, for example, rely on a complex web of information, ranging from specifications and test data, to pricing and delivery schedules and every element of this information is vital to the production of an aircraft. In fact, many of the processes used in manufacturing are information-technology controlled, enhancing the level of information intensity on which these products and their value chains rely. Cybersecurity failure in these value chains can result in faulty parts, dangerous industrial operations, loss of intellectual property, and non-delivery of the product as promised.

Why Does Information Intensity Matter?

The importance of the concept of information intensity is not new. Compelling work by Michael E. Porter and Victor A. Miller[3] in 1985 described the value of information in both information-as-product and in value chains. The authors describe the concept of Manufacturing Information and Distribution Systems (MIDS), noting that "an information intensive MIDS will generally bring value to a company if it adds high value to the product."[4] In today's world, such systems are of vital importance.

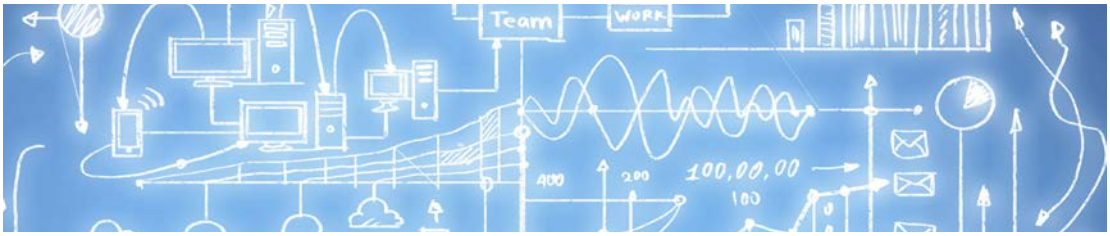
Whether an enterprise delivers information itself as a product, or products that rely on information to empower and mediate their value chains, it is clear that cybersecurity bears directly on information intensity, and on corporate strategy and the value proposition an enterprise delivers. Indeed, the cybersecurity of information intensive products is intrinsic to the value of those products and rises, therefore, to the level of a corporate strategic issue.

Recent research makes even more important the concept of information intensity, and makes more urgent the focus on cybersecurity. For example, this research provides powerful evidence that information intensive businesses that produce information-as-product should use information technology to disaggregate their production, just as value chain information intensive manufacturers are building global IT-enabled value and production chains.[5] Such disaggregation is an important component of corporate strategy, designed to take advantage of regional and local specialization and cost structures. At the same time, securing the IT infrastructures involved is essential for every aspect of development, production, integration, and delivery. Indeed, in all of these cases, the ability to provide effective cybersecurity is an essential enabling element of strategy, and can even be a competitive discriminator vis-a-vis competitors for which product quality (provenance, test data, etc.) and the integrity of information can be enhanced by cybersecurity.

3 See: Porter, Michael E., and Victor A. Millar. "How Information Gives You Competitive Advantage." Harvard Business Review 63, no. 4 (July–August 1985).

4 Ibid.

5 See: Is the World Flat or Spiky? Information Intensity, Skills, and Global Service Disaggregation by Sunil Mithas, Decision and Information Technologies, Robert H. Smith School of Business, University of Maryland, and Jonathan Whitaker, Management Department, Robins School of Business, University of Richmond, Richmond, http://terpconnect.umd.edu/~smithas/papers/mithaswhitaker2007isr.pdf



icfi.com

About ICF International

ICF International (NASDAQ:ICFI) provides professional services and technology solutions that deliver beneficial impact in areas critical to the world's future. ICF is fluent in the language of change, whether driven by markets, technology, or policy. Since 1969, we have combined a passion for our work with deep industry expertise to tackle our clients' most important challenges. We partner with clients around the globe—advising, executing, innovating—to help them define and achieve success. Our more than 5,000 employees serve government and commercial clients from more than 70 offices worldwide. ICF's website is www.icfi.com.

Four Initial Steps Toward Effective Cybersecurity

Given the rising importance of information and information intensity to a wide range of enterprises, Boards and C-Suite executives can and should do four things at least, and do them soon.

1. Senior decision makers should understand the strategic nature of information and cybersecurity, and approach the issue of cybersecurity from a whole-of-enterprise perspective that includes operations, IT, finance, communication, and other important enterprise-level functions. Such an approach is described in an ICF white paper, *Non-Containability: Whole-of-Enterprise Cybersecurity Planning and Recovery.* [6]
2. At a minimum, these same senior decision makers must understand the extent to which their business (or government mission) depends on information that must be kept secure. Lack of cybersecurity can lead to a binary outcome: a business can either deliver its value proposition or it cannot. Such an understanding goes beyond compliance, which may or may not result in cybersecurity adequate to delivering an enterprise's value proposition.
3. Decision makers should examine their current corporate strategy and value proposition, and evaluate the extent to which their strategy and value proposition depend on cybersecurity, and what level of cybersecurity is required to ensure that the strategy can be executed and the value proposition delivered.
4. The enterprise should ask itself if the corporate strategy can be enhanced–and the enterprise's competitive position strengthened–by more attention to cybersecurity, and if the quality and reputation of the value proposition delivered can be differentiated in an increasingly competitive market.

Information is employed intensively throughout the delivery of more products than ever, and is also in evidence increasingly in the public sector. Strategies that depend on information depend also on the cybersecurity applied to protecting that information. Cybersecurity is, therefore, a matter that goes beyond compliance and protection to the very core of an enterprise's strategy and value proposition. Approaches to addressing cybersecurity in this regard are emerging. Key decision makers should avail themselves of these approaches as they strive to succeed in an increasingly challenging world.

About the Author

Samuel Visner, is Senior Vice President and General Manager of Cybersecurity at ICF International. He also is an adjunct professor of cybersecurity at Georgetown University and the former chief of the Signals Intelligence Programs at the National Security Agency.

6 See: http://www.icfi.com/insights/white-papers/2015/noncontainability-cybersecurity-planning-recovery