

white paper

## The Power of The Trusted Enterprise Model

Security Leadership Institute

visibility

“A good reputation attracts customers, investors and talented employees leading to higher profits and stock prices...companies that nurture their reputation enjoy a halo effect that makes people trust them and gives them the benefit of the doubt during rocky periods.”

Ronald Alsop :The 18 Immutable Laws of Corporate Reputation

## Executive Summary

In an expanding global market space, many organizations feel competitively stressed in seeking to comply with growing regulatory requirements while also looking to succeed in a dynamic global marketplace. Many challenges and threats to organizations' products, services and business strategies are beyond their control and while addressing these threats is important, the activity is, by its very nature, reactive, costly and often counterproductive.

The Security Leadership Institute (SLI) believes there is an alternative approach.

To better understand how their approach would affect organizations today, the Security Leadership Institute sought to better understand the challenges CEOs face in protecting their organizations, employees and assets. As a result, the SLI conducted a series of high-level interviews with CEOs and public sector agency chiefs in the United States and Canada. The discussions ranged from how leaders view today's market place, what they consider to be the challenges of the global market, how they respond to concerns about ethical business practices and what their commitments are to employees and their safety. Also explored was what it means to operate businesses in a more demanding regulatory environment and the need for increased information security and privacy, including asset protection and intellectual property. The discussions considered why a gap exists between what CEOs and Boards think about security and privacy and what their leadership teams think. Our conversations explored the increased importance of intangible corporate assets such as reputation and customer trust has on shareholder value as well.

Throughout the research we asked these business leaders to define, consider, assess, weigh and prioritize the risks associated with running their businesses. Issues explored in depth included: what does "security" mean? What are the connections between "securing their business" and "managing risk?" How important is being viewed as "secure" to their brand and reputation?

What we learned is that successful CEOs are focused on delivering value to the market place, maintaining the respect of their peers and competitors and protecting their business environment while sustaining or enhancing share value.

Through our understanding of these challenges and how CEOs are responding to them, the concept of "the Trusted Enterprise" emerged.

## The Trusted Enterprise Model

Many of the CEOs we spoke to thought the word security meant either physical protection of employees or cyber protection of data networks and other technologies. While CEOs acknowledged these are important issues for their organizations, they see them as part of the domain of senior executive subordinates who reported to their leadership team. However, when the conversation shifted to operational risk management, CEOs readily began to address the full spectrum of business protection issues they personally owned.

And, not surprisingly, in the successful enterprise, the CEO sees the issues as all linked. For them, operational risk management addresses such issues as: business continuity, integrated business processes, development of human capital, privacy, corporate ethics, intellectual property protection, and compliance. They weigh operational risks in light of their organization's strategy and the external market environment, both domestic and international.

---

*A Canadian technology company working to comply with US Department of Justice security requirements discovered the unintended benefits of speed and operational excellence. As they sought to meet the security and network availability requirements, they developed new processes and applications that reduced their computer restore and repair time from a day to a matter of minutes. They are now exploring packaging these applications to create a new set of products and services to offer their customers.*

---

As one CEO reflected, "Security is not about circling the wagons. Security is about making sure we get across the mountain safely."

What became clear is that organizations are seeking ways to demonstrate their commitment to continuously earning customer, shareholder and employee trust. This SLI Trusted Insight begins to amalgamate and benchmark the Best Practices across a variety of organizations and industries to create The Trusted Enterprise Model.

The Trusted Enterprise Model encourages organizations to evaluate business decisions against the fundamental tenet of “does this further the trusted status of the organization.” The Trusted Enterprise Model acknowledges that corporate governance and compliance, in and of themselves, have little impact on an organization’s reputation and trusted status. It is the communication, operationalization and continuous monitoring of the business strategy, policies and practices related to governance and compliance that impacts customer, shareholder and employee trust.

The Trusted Enterprise Model is personified by organizations that embrace a set of corporate values and behaviors that guide and direct their business practices and decisions. They tend to be highly ethical organizations, which treat their customers, employees, partners and shareholders with extraordinary respect. The CEOs and Boards are deeply engaged in proactively understanding the organization’s operational risk profile and mitigation policies/practices. They are organizations that operate with consistency. They are focused on ultimately delivering highest value to their customer.

The Trusted Enterprise Model requires that organizations self-scrutinize. It demands a high degree of visibility through and across the organization. There are greater accountabilities and stricter enforcement of policies. The Trusted Enterprise Model views regulatory compliance not as an impediment but as an opportunity to improve business processes and outcomes. Within organizations aggressively building their ‘Trust Status’, the management teams are linked and act with consistency. The work environment fosters internalizations of accountability while embracing conformance with business policies. Teams proactively and holistically address risk, balancing potential reward against appropriate mitigation. All recognize that improved processes are critical for increased agility and productivity, not a restricting requirement.

The Trusted Enterprise Model is a formidable force that creates win/win/win equation for customers, shareholders and employees. Organizations that embrace this approach

are proactively pursuing improved and protected work environments. They regularly evaluate operational risks and seek ways of integrating risk mitigation into business processes. They do not simply invest in point fixes to increase security. Their resultant decision-making is not slowed, but is actually more nimble and competitive because their employees have a framework by which to evaluate their decisions and grasp their roles in achieving corporate success.

The Trusted Enterprise Model allows organizations to maximize their investments, increase their competitive advantage and balance their risk reward ratio delivering totality of value to the shareholder.

---

*The CEO and Founder of a leading online home mortgage and auto loan lender in the nation realized that the success of his company is predicated on earning customer trust in how sensitive personal information is collected, used and kept secure. Despite economic pressures after the crash of major dot.com companies, the CEO stayed the course of placing privacy and data security as a top issue for his company.*

*Today, his company is considered one of the few success stories in the Internet marketplace, competing head-on with rivals such as major mortgage lenders and retail banks. The CEO is viewed as a leader in the privacy and data security community – proving that good privacy is good business*

---

This model also enables organizations to better manage their risk. They:

- Lead the curve on appropriate regulatory compliance requirements.
- Experience fewer information security breaches.
- Improve employee safety.
- Implement better control of inventory & assets.
- Practice ethical information management both internally and with business partners.
- Earn customer trust and confidence in the ways their information is retained, used and shared.

## Principles of the Trusted Enterprise Model

Organizations pursuing the Trusted Enterprises Model have several common operating principles. We view the following four operating principles as foundational aspects or “trust pillars” for any organization striving to lead in the marketplace.

- Management, at all levels, proactively evaluates, measures and manages operational risk.
- Organizations relentlessly pursue **corporate transparency**, within the firm and across all of its processes and practices.
- CEOs and Boards **continuously engage** in understanding and mitigating the organization's entire risk profile and assessing its impact on the business' strategic objectives.
- Organizations develop **risk savvy cultures** with clear accountabilities and enforcement practices.

Embodiment of these principles in the culture and day-to-day operations provide Trusted Enterprises the ability to proactively assess and manage their revenue, reputation and risk consequences, and benefits of their decisions and strategies.

## The Trusted Enterprise Model for Success

The Trusted Enterprise Model relies on the committed engagement of its CEO and Board, the integrity of its day-to-day leadership and the commitment of its employees to both set and deliver the vision and values of the enterprise. Business processes and procedures are more open, generating a sense of trust among employees and delivering a greater degree of flexibility to users. The linkages and accountabilities between business units and/or functional groups are clear. Partners and suppliers are willing to integrate into their systems because of the perceived benefit of collaboration and protection from exploitation.

To achieve this, the Trusted Enterprises Model continually monitors several critical organizational vital signs. These

vital signs combine to create the Trusted Enterprise Model Index. The CEO and Board are encouraged to look not only at the current health of each area, but also proactively scan each for possible weaknesses in the future. This enables them to anticipate and mitigate potential risks as well as take full advantage of opportunities. While within each organization the rank of each component may vary, the list remains consistent across a variety of institutions and industries.

---

*A regional hospital is investing heavily in technology to increase the security of its facility and protect its patients, particularly infants. It recently implemented a wireless solution to tag infants. In addition, the hospital uses a wireless locator in their radiation oncology department.*

*These solutions worked so well, the hospital is now looking at implementing an enhanced solution that will allow real time communication with people throughout the organization. The collateral benefit, born of an initial security concern around infants is for patients' ability to communicate their care needs directly to their nurses as well as locate the nearest specialist in a patient emergency.*

---

## Trusted Enterprise Model Vital Signs

### Customer Centric Focus

- Are we focused on what's right for the customer?
- Does the leadership seek and internalize customer feedback?
- Are we “closing the loop” with customers?
- Do we evaluate our business decisions based on building customer and shareholder value?
- Is our view sufficiently external?

### Risk Savvy Culture

- Do our employees understand our core business values and mission well enough to make sound business decisions in support of them?
- Are our decision processes designed to encourage our employees to take justifiable business risks?

- Are we financially sound enough to survive a competitive attack in our most critical market?
- Are third party vendor and business partner controls sound and protected?
- Are managers honest and open in communicating the organization's areas of exposure upstream to senior executives?

### Organizational Vitality

- Are leadership and the workforce mutually active in pursuing new approaches to improving the enterprise and market positioning?
- Do leadership and the workforce see regulation and oversight as the pathway to better business practices and market advantage?
- Is there a governance process in place and is it a cross-functional activity (involving people from different business units)?
- Are leaders encouraged (given incentives) to ensure good governance practices?
- Do senior executives have accountability for mistakes made at lower levels?
- Are new laws and regulations evaluated to understand their impact on extant business practices?
- Do the CEO and Board obtain a compliance status report at each Board meeting?

### Protected Critical Infrastructure

- Is there a broad understanding of what is vital to sustain business operations and have active controls been put in place to protect them?
- Are the external links, to suppliers as well as customers, recognized as critical to success and protected appropriately?
- Are critical assets monitored on an ongoing basis?
- Are suspicious activities identified, investigated and stopped quickly?
- Are repeated patterns of negligence or complacency stopped?

### Organizational Agility

- Does the organization evaluate business opportunities in light of their impact on the organization's short and long-term fiscal health?
- Does the organization continuously evaluate its fiscal health with an eye on worst-case scenario planning?
- Does the organization maintain focus when considering new business opportunities?
- Is the organization fast enough to beat competitors at winning strategic relationships or acquisitions?
- Does the organization keep an open mind to new business deals and new ways to do business?
- Does the organization have technically savvy people to identify opportunities that involve the redeployment of technology?

CEOs committed to adopting the Trusted Enterprise Model achieve greater integration of their leadership team, deepen the loyalty of their workforce and engender more involvement from their Boards. Most important, they deliver stronger results to their shareholders and greater value to their customers.

## About the Authors

The Security Leadership Institute (SLI) is a forum of nationally recognized security experts from business and government that provide insight into emerging security issues and best practices to organizations worldwide. A goal of the SLI is to help both business and government leaders to see “beyond the horizon” and gain security insights that can become key factors in their long-range business strategy.

---

### ***SLI Members:***

*General Michael P.C. Carns*

USAF, retired; vice-president of Privasource, a software firm that specializes in securing large, sensitive databases.

*William P. Crowell*

Security consultant and former deputy director of the National Security Agency.

*James J. Flyzik*

Partner, Guerra, Kiviat, Flyzik and Associates, a consulting firm; former CIO, U.S., Department of Treasury.

*Norman D. Inkster*

Partner, Growlings Consulting; former commissioner of the Royal Canadian Mounted Police and former president of INTERPOL.

*Dr. Lawrence A. Ponemon*

Chairman and founder, Ponemon Institute, dedicated to advancing ethical information and privacy management practices.

*John C. Reece*

Consultant; former CIO of the U.S. Internal Revenue Service.

*Thomas L. Sheer*

Authority on corporate investigative strategy; former assistant director of the FBI New York office.

*Dr. Eugene H. Spafford*

Executive Director of the Center for Education and Research in Information Assurance and Security.

---

For more information, please visit our Website at:  
[www.unisys.com/public\\_sector](http://www.unisys.com/public_sector)

Specifications are subject to change without notice.

© 2005 Unisys Corporation.

All rights reserved.

Unisys is a registered trademark of Unisys Corporation. All other brands or products referenced herein are acknowledged to be trademarks or registered trademarks of their respective holders.

