



## THE ECONOMICS OF DEVELOPING A SECURE ORGANIZATION

In March 2006, the I3P held a workshop where chief information security officers (CISOs) from Fortune 500 firms—including 3M, Align Technology, Bank of America, Bose, BP, Cisco Systems, Colgate, Dell, Dow Chemical, Eastman Chemical, Eaton, Hewlett-Packard, IBM, Lowe's, Medtronic, Staples, Time Warner Cable, and the U.S. Army—debated the challenges of organizing for security. Executives discussed how to embed security into the organization, touching on issues of organizational structure and culture, measurement, and investment. The following are the main findings from the workshop:

### Executives ranked tools to measure the benefits of cyber security as the number one security imperative.

- Security metrics must be more tightly linked to the business and communicated in simple terms.
- Security executives need tools that can measure the benefits of a secure networking infrastructure, such as whether security initiatives save the company money or add business value.
- Composite metrics combine a variety of elements tailored to the needs of differing units, and can help determine an acceptable level of risk across organizations.
- Increased benchmarking within an industry and between sectors can help an organization compare itself to its peers and evaluate the relative effectiveness of its security program.
- Standards and certifications provide only a basic level of security.

### Globalization and outsourcing have increased the challenges of securing the extended enterprise.

- Today's companies are global. The rapid pace of business, constantly changing threats, geographic distribution of infrastructure, and the need to comply with the laws of multiple jurisdictions can quickly stretch security resources thin.
- The flow of information within and between firms is increasing, with more sensitive information migrating to devices at the edge of the network. To protect intellectual property in this environment, security should focus on behavior rather than technology.
- As more businesses enter into strategic partnerships and outsource vital functions, they must ensure that business partners do not create new holes in their security programs.

### Customers and business partners are demanding stronger security.

- In some sectors customers ask more questions about security and business continuity than about pricing and availability.

- The public is becoming wary of e-commerce as the media report more high-profile data breaches. This makes the need to protect a company's reputation a major security driver.
- Customers are asking potential partners to verify that they adhere to industry security standards and best practices. Contracts now often include security clauses mandating minimum standards, but enforcement remains problematic.

### Building a culture of security requires a sustained effort.

- Companies must inculcate information security into the DNA of their organizations.
- Executives and senior management must set the tone for the rest of the enterprise and commit the resources necessary to make security work.
- There is a strong need to find and develop security talent that can understand the business and communicate the business case for security.
- Executives must realize that high-level decisions, such as mergers and joint ventures, often have security implications.
- Security is strongest when employees take personal responsibility for protecting information. Creating rewards for good security and imposing costs for bad security can help personalize the issue for employees.

### Security must become proactive and aligned with strategic objectives.

- Information security investments must move from reactive add-ons to proactive initiatives that are aligned with a company's strategic goals.
- The organizational structure of businesses must remain flexible enough to respond to changes in a company's operational environment, business goals, the external risk environment, and new regulations.

The Institute for Information Infrastructure Protection is a national research Consortium composed of more than two dozen research entities, including academic institutions, federally funded labs and non-profit organizations. In collaboration with government and industry, the I3P is able to bring Consortium member experts together to identify and help mitigate threats aimed at the U.S. information infrastructure that we depend on to sustain our way of life. In effect, the I3P functions as a virtual national lab with the ability to organize and reconfigure research teams with the skill sets required to study the vulnerabilities within the information infrastructure.