Entrust® Securing Digital Identities & Information

Securing Your Digital Life

Information Security Governance (ISG)

An Essential Element of Corporate Governance

April 2004

The material provided in this document is for information purposes only. It is not intended to be advice. You shall be solely responsible for acting or abstaining from acting based upon the information in this document. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS DOCUMENT. THIS INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS, WARRANTIES, AND/OR CONDITIONS OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, TITLE AND FITNESS FOR A SPECIFIC PURPOSE.

Published April 2004

INFORMATION SECURITY GOVERNANCE

As a worldwide leader in identity and access management solutions, Entrust takes information security very seriously. Just as our customers depend on robust security solutions, so do we as a company. Given our leadership role and the increasing emphasis on cyber security, I directed Entrust's management team last year to undertake a sweeping review of the security of our internal operations. In doing so, we discovered that cyber security is best viewed, not solely as a technology challenge, but as a corporate governance issue. Moreover, like quality assurance, it requires continuous, incremental improvement over time. We also discovered that the framework necessary to systematically integrate information security into corporate governance is lacking.

Because it is imperative for the broader software industry to have an information security framework, I approached the Business Software Alliance (BSA) to see how the industry could best work together. At their recommendation, I co-chaired a task force of leading software companies that profiled a framework in its October 2003 report, Information Security Governance: Toward a Framework For Action.

As a result of the work with BSA, I was asked to co-chair a blue ribbon Corporate Governance task force at the National Cyber Security Summit hosted by the Department of Homeland Security and the National Cyber Security Partnership. The goal of this task force was to achieve consensus on an information security governance framework with broad application to business, educational institutions and non-profit organizations. This report, Information Security Governance: A Call to Action, was released in April 2004 and is summarized in the pages that follow.

As seen during the task force process, industry is rising to the cyber security challenge. We still have a lot of work before us, but increasingly we have a framework and process for how best to approach the problem and the toolset necessary for success.

By integrating information security into our corporate governance processes, we can allow for the deep integration with customers, suppliers, partners and other stakeholders that is so important to the extended enterprise, while protecting the critical infrastructure that is a cornerstone of our homeland security.

Please join us in embracing this vital corporate and civic responsibility.

Bill Conner

F. William Conner
Chairman, CEO and President

Entrust®
Securing Digital Identities
& Information

Table of Contents

1 Introduction

As a result of numerous business scandals, corporate governance has become an urgent issue. Defined, corporate governance is the set of policies and internal controls by which organizations are directed and managed. Information Security Governance (ISG) is a subset of corporate governance that relates to the security of information systems.

Information security is all too often perceived as a wholly technical issue. For companies, educational institutions, and non-profit organizations to make progress in securing their information assets, however, executives must make information security an integral part of core business operations. The best way to accomplish this goal is to highlight ISG as part of the internal controls and policies that constitute corporate governance. [1]

Until recently, organizations have struggled to find a consistent framework to guide their ISG efforts. The Corporate Governance Task Force of the National Cyber Security Partnership (NCSP) has recently issued an ISG Framework and recommendations to bridge this gap.

In December 2003 the Department of Homeland Security co-sponsored a National Cyber Security Summit to discuss ways to further implement the recommendations contained in February 2003's National Strategy to Secure Cyberspace. At this Summit, a blue-ribbon Corporate Governance Task Force co-chaired by Entrust Chairman and CEO Bill Conner was launched. In April 2004, this Task Force released its report, which included an Information Security Governance Framework, under the title, "Information Security Governance: A Call to Action."

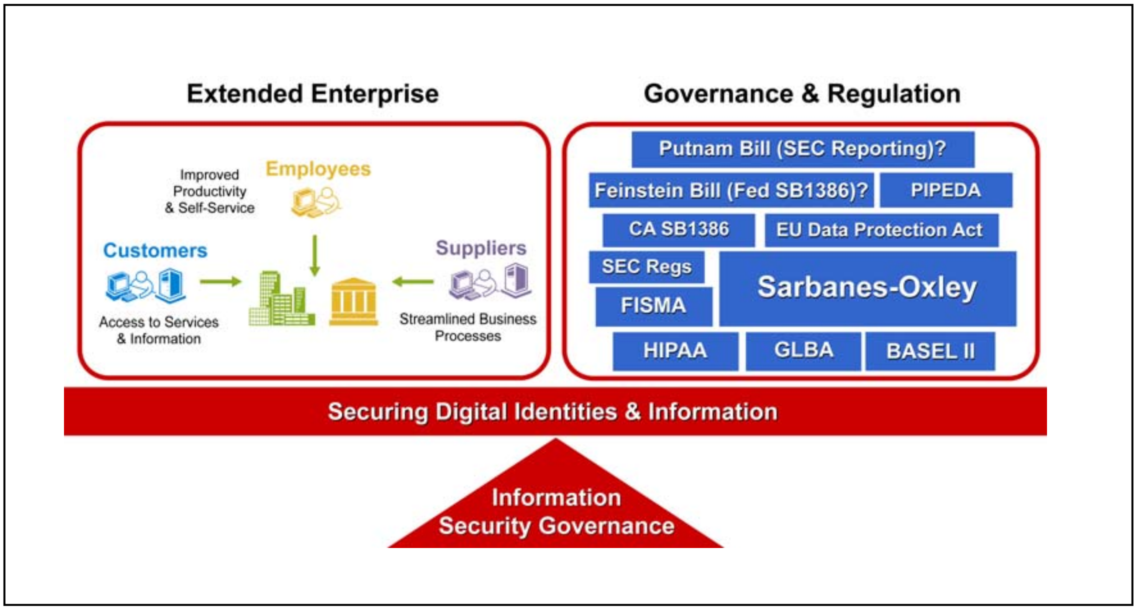
This white paper will review the recommended ISG Framework and outline how identity and access management solutions provide the foundation of an effective information security program, enabling the extended organization and improving business processes.

[1] "Information Security Governance: A Call to Action", National Cyber Security Partnership Governance Task Force, April 2004, p.1, www.cyberpartnership.org ("Task Force Report").

2 The New Reality

In order to grow and sustain competitive advantage, organizations are providing deeper access to information and services. This includes giving employees real-time access to the applications and information that increase their productivity, automating business processes and transactions with suppliers over the Web to drive speed and cost savings, and enabling customers to conduct transactions online to improve service, brand loyalty and revenues.

The new reality is that businesses and governments are in a constant balancing act, extending deeper access to their information assets and services while also complying with a myriad of global government regulations around information privacy and corporate governance. Moreover, in public corporations, this all has to be done while exceeding investor expectations for financial performance.


Extended Enterprise
Governance & Regulation
Improved Productivity & Self-Service
Employees
Customers
Suppliers
Access to Services & Information
Streamlined Business Processes
Putnam Bill (SEC Reporting)?
Feinstein Bill (Fed SB1386)?
PIPEDA
CA SB1386
EU Data Protection Act
SEC Regs
FISMA
Sarbanes-Oxley
HIPAA
GLBA
BASEL II
Securing Digital Identities & Information
Information Security Governance

Balancing these needs depends on secure information systems. The very openness and accessibility that stimulated the adoption and growth of private networks and the Internet also threaten the privacy of individuals, the confidentiality of business information, and the accountability and integrity of transactions. Key concerns include risk of theft, alteration, interception and dissemination of confidential data, as well as fraud, loss of reputation and economic loss. Threats to information security arise from external sources such as competitors and computer hackers, as well as internal sources, such as curious or disgruntled employees and contractors. All of which has made it very difficult for organizations to sufficiently protect digital information.

3 Cyber Security and Regulation

Over the past several years, cyber security has emerged as a pressing economic and national security concern. Unfortunately, progress has been slow. Billions have been spent on defensive or perimeter security, such as firewalls, intrusion detection software and virus scanning software, yet the frequency, volume and severity of security incidents continue to escalate.

In response to this threat, governments around the world have enacted legislation at the regional and federal levels. Consequently, organizations are faced with a maze of regulations with IT security elements, including:

- **US Sarbanes-Oxley Act**
- **US Health Insurance Portability and Accountability Act (HIPAA)**
- **US Gramm-Leach-Bliley Act (GLBA)**
- **US Federal Information Security Management Act (FISMA)**
- **Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)**
- **EU Directive on Data Protection (EU Data Directive)**
- **California Security Breach Information Act (SB1386)**

Carnegie Mellon's, CERT, noted that there were 137,529 security incident reports in 2003, a 68% increase over the 82,094 reported in 2002. And, according to the 2003 CSI/ FBI Computer Crime and Security Survey the theft of proprietary information caused the greatest financial loss amongst respondents at $70.1 million, with the average reported loss being approximately $2.7 million.

The Sarbanes-Oxley Act of 2002 is of particular interest because it mandates stronger internal controls and institutes personal liability for executives of companies that are publicly traded in the United States.

Despite all of these regulations, little progress has been made in improving cyber security. Since the majority of the critical infrastructure is owned by private enterprises in some countries, the security of corporate systems and information is of critical importance to national security. As a result of this and escalating consumer privacy concerns, frustrated legislators are contemplating additional regulation to force organizations to assess, remediate and audit the security of their IT systems.

More regulation, however, is unlikely to improve the situation. Nor is relying solely on organizations' CIOs and IT departments to fix the problem.

If we are to systematically strengthen information security, organizations must elevate the issue to a corporate governance priority. Specifically, CEOs and Boards of Directors must integrate information security into their overall governance program at all levels of the organization.

To accomplish this, organizations need a framework. The NCSP ISG framework provides this guidance to assist organizations with incorporating ISG into their corporate governance practices.

4 National Cyber Security Partnership (NCSP) Governance Task Force

The National Strategy to Secure Cyberspace was launched amidst much fanfare in February 2003, however, progress related to its recommendations has been slow. The U.S. Department of Homeland Security has become increasingly proactive in the cyber security area, and in December 2003 co-hosted a National Cyber Security Summit in Santa Clara, California. The immediate outcome of the Summit was the formation of the National Cyber Security Partnership and five NCSP task forces.

The Corporate Governance Task Force was formed to create a private sector framework for organizations to improve ISG on a voluntary basis. The Task Force, co-chaired by Entrust CEO Bill Conner and RSA Security CEO Art Coviello, was comprised of forty-five members from industry, educational and not-for-profit organizations.

The Task Force leveraged work from the Business Software Alliance[2] and TechNet[3]. The resulting Task Force report, “Information Security Governance: A Call to Action”, was released in April 2004 and is available online at www.cyberpartnership.org. The report outlines an ISG Framework that enables organizations to assess and remediate information security issues and comply with various privacy regulations. Acceptance and broad participation will ultimately result in improved national cyber security.

4.1 Summary of the Task Force Report

Cyber security is not only a technical issue, but also a governance challenge that involves risk management, reporting and accountability. The Task Force developed a framework, recommendations and tools that provide a strong foundation for organizations seeking to improve their ISG. Adoption of a framework represents an essential first step in the process of securing information systems, complying with regulations, increasing business process efficiency and strengthening homeland security[4].

The Task Force calls on organizations to make ISG a corporate board-level priority, leveraging these tools to launch internal ISG programs. The key focus is to begin the process, with the subsequent goal of systematic improvement of performance over time.

The Task Force report outlines an ISG Framework similar to a quality model of continuous improvement that:

- Showcases public-private collaboration for ISG (industry-led with support of government)

- Recognizes ISG as a core business/governance issue at the CEO and Board level (personal and corporate accountability)

[2] “Information Security Governance: Toward a Framework for Action”, Business Software Alliance, October 2003, www.bsa.org/usa/policy/index.cfm
[3] www.technet.org
[4] “Information Security Governance: A Call to Action”, National Cyber Security Partnership Governance Task Force, April 2004, Task Force Report p.4.

- Is not industry or country specific, but rather has broad business applicability (versus specific legislation: HIPAA, GLBA, EU Data Directive, etc.)

- Is based on industry standards (ISO 17799) and can be readily implemented through self-assessment (like the quality model, it is a continuous process of self-improvement)

- Promotes a balance between investment and business risk decisions (start with the critical risk areas then progress to others)

- Can facilitate compliance with governance regulations like Sarbanes-Oxley (sound internal controls need authentication, authorization and audit)

4.1.1 Recommendations for Government and Industry Action

The Task Force report[5] also lists a number of recommendations for government and industry action:

1) Organizations should adopt the ISG Framework described in the report to embed cyber security into their corporate governance process.

2) Organizations should signal their commitment to information security governance by stating on their Web site that they intend to use the tools developed by the Corporate Governance Task Force to assess their performance and report the results to their board of directors.

3) All organizations represented on the Corporate Governance Task Force should signal their commitment to information security governance by voluntarily posting a statement on their Web site. In addition, TechNet, the Business Software Alliance, the Information Technology Association of America, the Chamber of Commerce and other leading trade associations and membership organizations should encourage their members to embrace information security governance and post statements on their Web sites. Furthermore, all Summit participants should embrace information security governance and post statements on their Web sites, and if applicable, encourage their members to do so as well.

4) The Department of Homeland Security should endorse the information security governance framework and core set of principles outlined in this report, and encourage the private sector to make cyber security part of its corporate governance efforts.

5) *The Committee of Sponsoring Organizations of the Treadway Commission (COSO) should revise the Internal Controls-Integrated Framework so that it explicitly addresses information security governance.*

[5] Task Force Report, p.1-4.

4.1.2 ISG Tools Included in Report

The report also includes:

- The ISG Framework Document
- An ISG Functions and Responsibilities Guide and Matrix
    - Detailed responsibilities for each functional group for large, medium and small enterprises and public agencies
- Organization and Process for Implementation Model
    - Based on work from Carnegie Mellon University's Software Engineering Institute
- An ISG Assessment Tool
    - Includes evaluations of Business Dependency, Risk Management, People and Process
- An Education and Non-Profit Implementation Plan

5 The ISG Framework

The Task Force report states that the purpose of the document is:

“to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources; to provide effective management and oversight of the related information security risks; to provide for development and maintenance of minimum controls required to protect an organization’s information and information systems, and; to provide a mechanism for oversight of the information security program.”[6]

The major elements of the ISG Framework include:

- **Organizational Responsibilities and Authority:** A description of the ISG responsibilities and functions of each member of an organization, including the Board of Directors/Trustees, Senior Executive, Executive Team Members, Senior Managers and all employees. Each has a significant role to play in ISG.

- **Information Security Program Components:** A description of the essential components of an information security program, with detailed guidance specified in the security practices of ISO/IEC 17799. This includes assessment, policies and procedures, training, testing, remediation of risks, detection and response to incidents and business continuity planning.

- **Reporting and Independent Evaluation Recommendations:** A description of the contents, frequency and audience for reporting to satisfy governance oversight requirements. Each independent organizational unit should assess, remediate, and report on its information security program. Additionally and where appropriate, each year an independent information security program evaluation should be completed in accordance with generally accepted auditing standards and the results reported to the Board of Directors/Trustees

5.1 Benefits of Implementing the ISG Framework

The benefits derived by organizations that implement the ISG framework go beyond facilitating compliance with applicable legislative, regulatory and contractual requirements. ISG and its associated information security program also result in tangible business benefits, including:

- **Improved internal processes and controls:** Authentication, authorization and auditability of the people, devices and applications on the network improves efficiency and effectiveness of business processes.

- **Potential for lower audit and insurance costs:** Better governance and the ability to demonstrate an auditable, complete ISG program can result in lower insurance costs and decreased audit costs.

[6] Task Force Report, p.12.

- **Market differentiation through a continuous improvement process:** Industry first resisted quality-improvement processes as added cost, but soon evolved to embrace it as a method for improving productivity and customer loyalty. Ultimately, quality became a market differentiator. Over time, an ISG program may also provide results that help determine a market leader.
- **Self-governance as a better alternative than regulation:** Implementation of an industry-led solution based on open standards and best practices will help mitigate the requirement for new governmental regulation. Should new legislation emerge, organizations that have invested in an ISG program are likely to benefit.

Corporate Governance Task Force
Stated Core Set of Principles for ISG

- CEOs should have an annual information security evaluation conducted, review the evaluation results with staff, and report on performance to the board of directors.
- Organizations should conduct periodic risk assessments of information assets as part of a risk management program.
- Organizations should implement policies and procedures based on risk assessments to secure information assets.
- Organizations should establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability.
- Organizations should develop plans and initiate actions to provide adequate information security for networks, facilities, systems and information.
- Organizations should treat information security as an integral part of the system lifecycle.
- Organizations should provide information security awareness, training and education to personnel.
- Organizations should conduct periodic testing and evaluation of the effectiveness of information security policies and procedures.
- Organizations should create and execute a plan for remedial action to address any information security deficiencies.
- Organizations should develop and implement incident response procedures.
- Organizations should establish plans, procedures and tests to provide continuity of operations.
- Organizations should use security best practices guidance, such as ISO 17799, to measure information security performance.

6 Entrust: A Trusted Advisor for the ISG Process

As a cyber security leader, Entrust began its internal ISG program in January 2003. Beginning with the BSA task force on ISG that issued an October 2003 report laying the groundwork for the NCSP task force work, Entrust has worked with industry associations to develop a methodology for self-assessment, remediation and reporting that could be generally applied to organizations of all types and sizes.

As the ISG Framework has evolved, Entrust has modified the internal program, field-testing concepts and guidance. Several lessons key to successful deployment have emerged, including:

- **Use simple, subjective risk assessments**
  - Focus on improving security posture, not performing complex risk analyses
  - Express risks in a language meaningful to business managers
  - Use universal red-yellow-green rankings, where red reflects a threat to mission capability

- **Focus where the business need is greatest**
  - View ISG as a continual improvement process (similar to quality)
  - Perform a series of small assessments on segments of the business
  - Start with identification and assessment of key information systems and resources

- **Understand the bulk of the work is policy and process**
  - Transparent reporting to senior management is a critical element of governance
  - Concentrate on policy and processes first -- two thirds of ISO 17799 guidance deals with this. Technology should leverage guiding policy to make process effective and efficient.

For over a decade Entrust has been a leader and innovator in the information security market with more than 1,250 customers who have turned to us to act as trusted advisors regarding their information security needs. Recognizing the lack of a generally accepted ISG process, Entrust has worked extensively with the US Federal government and industry associations within and outside the NCSP project to develop effective ISG programs. By evolving an internal program in concert with that initiative, Entrust is uniquely qualified to help organizations establish solid ISG programs. Entrust is now offering a three-day **ISG Quick Start** package.

The overall objective of the Quick Start engagement is to educate customer primes on the value of ISG, content of the ISG Framework, the self-assessment process, and how it supports corporate governance, and to raise awareness of the information security risk profile to the CEO and board level. At the end of the session, participants will receive a jointly developed preliminary “report card” and a prioritized list of actions to execute against.

7 Remediating Information Security Risks: Identity and Access Management

Recognition of the need to establish a strong ISG program, maintain centralized control and audit the enforcement of corporate policy, is the first step to realizing the productivity benefits of technologies used to extend the enterprise. The next step is to identify and adopt the technologies that will best strengthen internal controls and move the organization towards regulatory compliance.

Traditional approaches to security such as firewalls, intrusion detection and virus scanning software are very important but have not stemmed the rising tide of security incidents and losses resulting from breaches. They deal with protection at the perimeter of the organization and do not deliver the security required to protect the identities and information used in an extended enterprise environment. They also provide little value in addressing data privacy and internal controls required by government regulations.

The technology solution to address these issues is found in Identity and Access Management software that enables organizations to securely extend access to stakeholders while protecting critical information assets. Identity and Access Management enables the organization to:

- **Understand who they are dealing with** in the online world by managing identities and access rights for large numbers of users both inside and outside the organization
- **Protect privacy and confidentiality** of online transactions and communications to mitigate risks of unauthorized access or theft of personal information (identity theft) and sensitive business information (business plans, partner agreements, customer lists, financial records, and much more)
- **Provide centralized visibility, control and audit** of who has access to what, and how and when they are using it, so that security policy is enforced

Identity & Access Management

- connecting identities to information
- providing for integrity of information
- controlling access to sensitive information
- protecting the content of information
- centralizing policy management
- auditing the enforcement of policy
- improving corporate governance through a strong information security governance framework

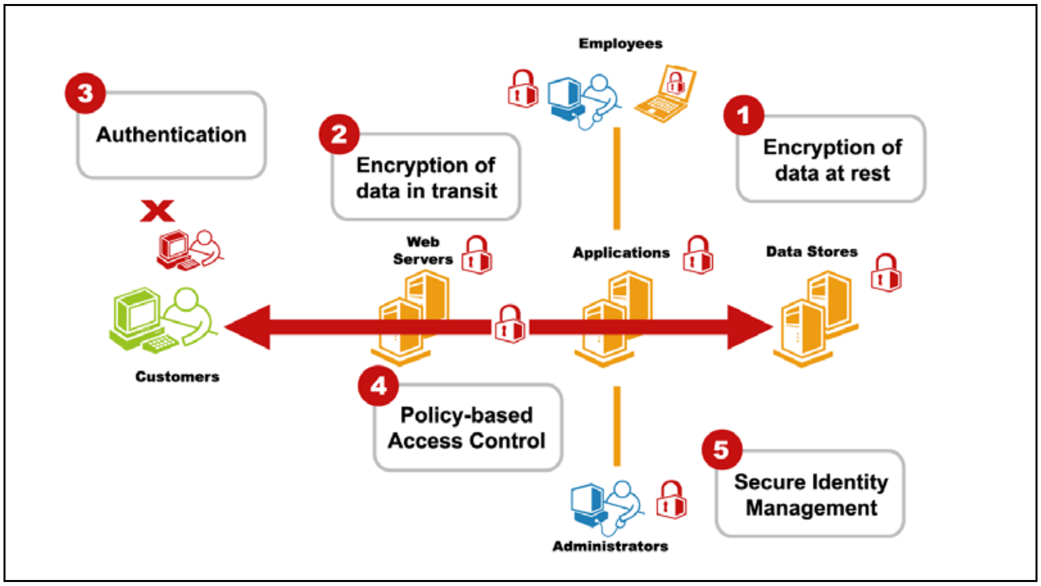
In addition to enabling the extended enterprise, Identity and Access Management solutions are essential for compliance with legislation that mandates the protection of sensitive information, and for establishing the internal controls that are fundamental to an ISG program. To illustrate this point, see the following two examples:

Identity and Access Management for Sarbanes-Oxley Compliance
The Sarbanes-Oxley Act of 2002 has literally rewritten the rules of corporate governance, auditing and reporting. It requires that organization not only have strong internal controls, but also have processes in place to review and attest to those controls. Since so much of the financial reporting process is electronic, enterprises must be confident that their systems provide the same **Accountability**, **Privacy** and **Audit** capabilities that are standard practice in the paper-based world. The security provided by Identity and Access Management solutions makes it possible for executives to have confidence in their electronic systems and information.

Accountability is a fundamental element of internal control. This means that only those who are authorized are able to access information or conduct transactions, and that they can be held accountable for their actions throughout the online business process. Identity and Access Management solutions support accountability by centrally managing the identities of all users in the organization, strongly authenticating users when required, and authorizing access rights for transaction they are allowed to carry out. Organizations verify transactions through digital signatures that validate authenticity and integrity, comparable to the function of a paper-based signature.

Information must remain private and confidential. In the electronic world, strong authentication and policy-based access control ensure that only authorized people are granted access to information. Encryption is necessary to protect the information from theft and/or manipulation by unauthorized individuals.

Finally, an organization must establish an auditable record of transactions, including approvals. Identity and Access Management solutions provide audit capabilities through digital signatures and a centrally managed security system that enables administrators to view and log user activity as they access various business applications.


Employees
3 Authentication
2 Encryption of data in transit
1 Encryption of data at rest
Web Servers
Applications
Data Stores
Customers
4 Policy-based Access Control
5 Secure Identity Management
Administrators

Identity and Access Management for HIPAA Compliance

As shown in the diagram above, an organization can use Identity and Access Management solutions to facilitate meeting some of its obligations under HIPAA's Privacy and Security Rules. The organization employs encryption technology to protect electronic personal health information both while it is at rest in servers and databases **(1)** and in transit through e-mail or over the Internet **(2)**. The organization authenticates users to prevent unauthorized access **(3)**, and deploys policy-based access controls to restrict access as appropriate **(4)**. The organization also utilizes an Identity and Access Management solution to better control the provisioning and revoking of user identities, and to perform a regular audit of their access rights to sensitive systems **(5)**.

8 About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world-leader in securing digital identities and information. Over 1,400 enterprises and government agencies in more than 50 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges such as identity theft and e-mail security into business opportunities.

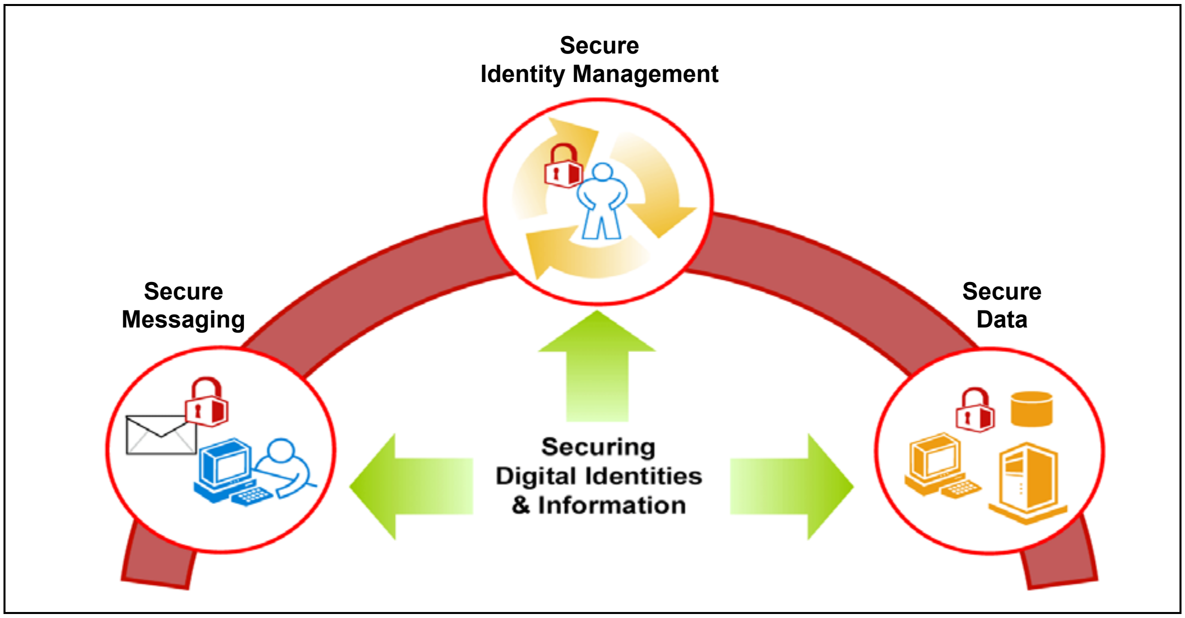
8.1 Entrust Customers

Over 1250 major government agencies, financial institutions, governments and Global 1500 enterprises in more than 50 countries have purchased and deployed the Entrust secure messaging, secure data and secure identity management software solutions that integrate into the broad range of applications organizations use today to leverage Internet and enterprise applications to improve productivity. More than 50 percent of the Fortune 100 are Entrust customers or partners. With an aggregate of over 100 patents and patents pending, Entrust takes the initiative in authoring and driving industry standards boards and technology forums.

Entrust has a long and distinguished list of customers who are market leaders in their respective industries. These companies, many with large scale deployments, are realizing value by using our solutions to extend their enterprises, protect their transactions and facilitate compliance with applicable laws and regulations.

Healthcare	**Government**
• Merck • Novartis International • GlaxoSmithKline • Kaiser Permanente • Blue Cross Blue Shield MI • Baptist Health Systems • UK National Health Service . . . and over 50 more	• US Dept. of Homeland Security • US Dept. of Energy • US Dept. of State • Govt. of Canada • HM Customs & Excise (UK) • Danish Government • Spanish Mint . . . . and over 300 more
Financial Services	**Large Enterprise**
• Citibank • Capital One • JP Morgan Chase • Prudential • Egg Bank • Lloyds TSB • Credit Suisse . . . and over 150 more	• Cox Communications • Delta Airlines • Hughes Network Systems • Lowe’s Home Centers • Vodafone • Verizon • 3 (formerly H3G) . . . and over 700 more

8.2 Entrust Solutions



Entrust Secure Identity Management Solution

Organizations today need to extend access to corporate resources to an ever-growing number of employees, partners, suppliers and customers. Effectively managing the increasing number of users is a significant challenge in itself, adding to this challenge is the complexity of delivering access to enterprise resources in multiple ways such as client-server, Web and Web Services applications.

Further adding to the challenge is the increasing number of Web Services applications and network devices required for the deployment and management of identities in an accountable and auditable manner. Enterprises and governments are also faced with intense pressure for increased accountability, driven by legislation as well as shareholder demands for more effective corporate governance. The dramatic rise in information and identity theft further underlines the need for a secure identity management solution. More effective internal controls, including the use of strong authentication, authorization and single sign-on (SSO), and centralized provisioning, can help organizations to comply with critical pieces of legislation such as Sarbanes-Oxley while at the same time realizing business benefits like cost reductions and increased levels of service.

The Entrust Secure Identity Management Solution consists of a suite of market-leading identity and access management products, which, in combination or deployed in modular stages, help organizations easily manage identities and access to information while decreasing costs. It can also improve the ability of organizations to enable legislative and corporate governance compliance. Supporting a broad range of client-server, Web and Web Services environments, the solution enables organizations to lower the costs associated with deploying and managing user, application and device identities while making it easier to securely access applications and information over the Internet. Through best-of-breed capabilities, the solution is easy to deploy and operate, includes secure administration, and cost-effectively scales to address large user populations.

Entrust Secure Data Solution

Applications such as enterprise resource planning, supply chain management, customer relationship management, workflow and e-forms have been migrated online to improve productivity and reduce paper costs and overheads. However, many organizations use only basic security solutions, such as a password, to secure these applications—a level of security that is inadequate for sensitive business information. Furthermore, enterprises are typically not securing the sensitive information in files and folders stored on desktops, laptops, enterprise servers or other electronic devices. This information is often left open to theft by insider and outside attackers. This lack of protection for sensitive information is resulting in identity theft attacks and the compromise of other types of sensitive information, including strategic business plans and customer information.

The Entrust Secure Data Solution consists of a comprehensive, highly scalable suite of data security products and services that help organizations mitigate the risk of data loss, corruption and disclosure so they can confidently capitalize on new technologies that enable greater stakeholder collaboration and, ultimately, business growth. It helps organizations secure sensitive and valuable information stored on computers, mobile devices, and corporate networks. The solution can also be a useful tool to help organizations meet their obligations under new legislative regulations that mandate stronger data security controls, without unduly burdening the people and processes that make use of this critical data.

Organizations can realize the promise of secure data through encryption that provides end-to-end data protection and privacy; through authentication, which strongly identifies the requesting users, device or application before releasing sensitive data; through policy-based access control, which manages individual user access rights to data and applications based on corporate policy; and through digital signatures which improves accountability for data transactions and protects the integrity of data involved in a transaction. Many organizations also provide data integrity through secure file transfer.

Entrust Secure Messaging Solution

E-mail has become the number one productivity tool for organizations, offering a low cost way to share information and accelerate decision-making. E-mail is fast and convenient, but not without inherent risks. In order to mitigate the risks of communicating valuable information, organizations need to secure sensitive e-mails. Unauthorized access to client records, sales forecasts, intellectual property or other valuable information can do significant damage to an organization's brand and competitive position. And with recent government regulations such as Sarbanes-Oxley, HIPAA, GLB and California SB 1386, the need to secure e-mail communications becomes an important element of regulatory compliance.

By transparently adding "end-to-end" security to e-mail applications such as Microsoft Outlook and Lotus Notes, the Entrust Secure Messaging Solution may help mitigate risk and comply with government regulations regarding sensitive e-mail communications.

The Entrust Secure Messaging Solution contains the following key attributes:

- Seamlessly adds security to popular e-mail software programs; turning them into more secure communications vehicles;
- Offers flexible, standards-based options for secure communication with employees, partners and customers;

- Transparently manages security on behalf of the user to make it easy to send and receive secure e-mail;
- Delivers enhanced security that provides encryption and digital signature technology;
- Allows users to identify senders and recipients of e-mail communications with greater confidence;
- Verifies the integrity of message content and protects the privacy and confidentiality; and
- Capitalizes on mobile communications by extending security to Blackberry wireless handhelds.

ADDITIONAL RESOURCES

National Cyber Security Partnership
www.cyberpartnership.org

Business Software Alliance
www.bsa.org

TechNet
www.technet.org

US Chamber of Commerce
www.uschamber.org

Information Technology Association of America
www.itaa.org

US Department of Homeland Security
www.dhs.gov