Tijdschrift voor Economie en Management
Vol. XLVII, 1, 2002

E-conomics of Trust

by K. DE BAERE

PriceWaterhouseCoopers,
Brussels

ABSTRACT

The Internet is like an engine driving commerce into a future rich with opportunity and challenge. Despite the potential, many organisations are reluctant to participate. Their executives feel they lack sufficient control in this new environment. Some want to take a more measured approach, with safeguards to protect them against hazards.

I. INTRODUCTION

As e-business evolves, many participants exhibit a fundamental lack of trust in this new approach of doing business. They worry about the confidentiality and authenticity of transactions conducted online, or they have concerns about controlling information once it is sent into cyberspace. They are aware that they can lose control when PCs and other systems operate outside of their direct supervision. These executives fear that the regulatory and legislative framework that protects them in their traditional business practices might be inadequate for e-business.

Whether activity stems from business-to-business (B2B) or business-to-consumer (B2C) transactions, participants have the same fears and often ask the same questions: How careful is the organisation with information? Do employees of the organisation respect information entrusted to them by customers, suppliers, or other stakeholders? Who has access to information? How reliable is the organisation's technology? Can it sustain growth? Are organisational processes and procedures synchronised with current technology? How vulnerable is the organisation to sabotage of information systems or theft of data? What are the costs to its financial position, market share, and reputation if its systems are open to assault? What should be done to protect the organisation? Does the organisation articulate its e-business policies and procedures to those with whom it does business? Does the organisation do what it says it will do?

These are hard questions that must be answered as Internet transactions multiply. Forrester Research expects B2B revenue to reach $1.3 trillion in 2003, up from $43 billion in 1998. In the same period, B2C revenue is expected to rise from $8 billion to $108 billion. Forrester predicts that organisations that have built trust in their online commercial endeavors will reap significant returns (Forrester Research, Cambridge, Massachusetts, Forrester.com (1999))

This document analyses trust and its different dimensions in this new environment and outlines ways to build trustworthiness in e-business.

II. WHAT IS TRUST?

Trust */noun - assured reliance on the charactei: ability, strength, or truth of someone or something.*

Trust *(believe)/verb - to have belief or conjìdence in the honesty, goodness, skill or safety of (a person, organisation or thing).*

Tmst is the glue that produces orderly, civilised society out of anarchy and disarray. In organisations, trust can bind people together to make them stronger and more effective. Trust increases the feeling of security, reduces inhibitions and lowers defences. Without trust, an organisation cannot hope to achieve excellence.

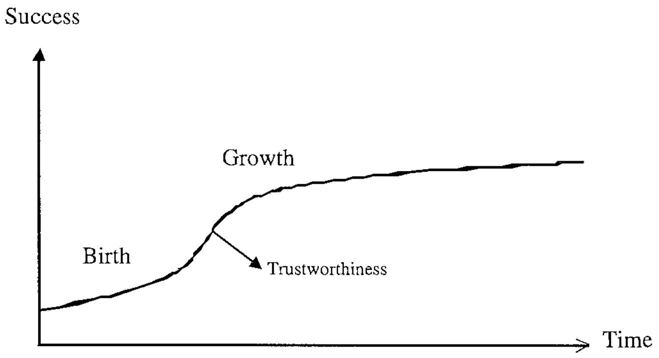
In e-business terms, trust has become largely synonymous with technology. But it is much more than this – e-business has not destroyed the foundation of trust on which all relationships are built. Indeed, tmst becomes even more important in a virtual world.

As delicate as trust can be in a commercial setting, it is nonetheless a formidable force. Once a trusting relationship has been developed, it becomes the cornerstone that supports the organisation in virtually every effort it undertakes. It is also the catalyst for increasing sales because it creates integrity, and customers trust organisations with integrity.

lhe traits that characterise trust must be examined early on. Many customers evaluate an organisation's history to anticipate how they will be treated in future transactions. An organisation must possess integrity and demonstrate that it is a safe choice, that it is competent, and that it deals fairly with its customers, suppliers, employees and partners. These traits indicate that an organisation is reliable, honest, and communicative in its dealings. Over time, these characteristics take on overtones of consistency, from which predictable behaviour is defined and there develops, in actual fact, faith in the organisation's ability to conduct its affairs with a high level of integrity.

III. WHY DO WE NEED TRUST?

Trust is a critica1 element throughout the product's marketing life cycle. The following graph illustrates the dependence of success on tmst:



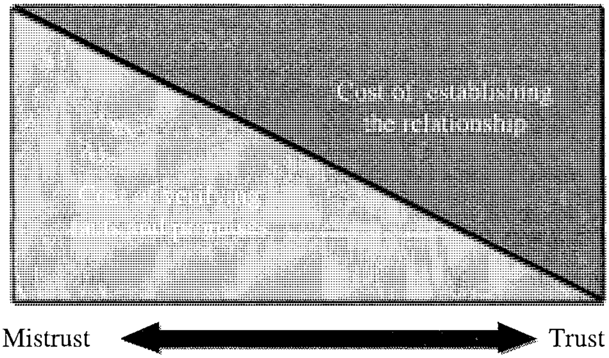
Trust is not a mandatory requirement in the initial stage of the product life cycle (birth). The need for trust increases remarkably through the product life cycle. In the growth phase, trust could be created with recommendations, community creation, personalisation, etc. If trust is not created within the growth phase success will not be guaranteed.

A. *Fundamental difference between trust and mistrust*

The importance of trust is dependent on the relationship in question. Put to the extreme, there are two options that companies can choose from while establishing their relationship with their partners - trust and mistrust.

Many companies prefer to work using the "mistrust" option. In this case, the cost of verifying facts and promises that are intrinsic to the relationship is very high. As a consequence, this option is mainly used for occasional transactions with multiple business partners.

Companies choosing for the "trusted" option are investing in the relationship with their partners. This reduces the further cost of data verification but involves an additional cost of establishing a relationship. This option is usually chosen by an organisation that deals with the same business partners and higher volumes of transactions. In this instance, service level agreements are often used to agree the underlying terms and conditions. The following graph illustrates the relationship between cost and the level of trust. In the mistrust option, the cost of verification is recurring time after time and covers each transaction individually. On the other side of the spectrum, the once-off cost of establishing a trusted relationship can be regarded as an investment yielding longer term cost benefits since verification costs are limited.



B. *Benefits of trust*

Trust enhances the cost/benefit ratio of a relationship between business partners. Usually, the once off cost of establishing a trusted relationship is lower than the recurring verification cost of operating in the mistrust environment. After an initial investment in establishing trust, there is no further cost to verify facts and promises made by a trusted partner, which helps businesses to reduce complexity and focus on the "who" and not on the "what". Also, trust stimulates collaboration, which, as a result, allows companies to focus more on innovation.

However, the impact is more far-reaching. By means of example, the following table analyses the more in depth characteristics of promiscuous (many different partners) versus true partnership arrangements in further detail:

	Promiscuous (mistrust)	*Partnership (trust)*
Supplier R&D?	Decreases	Increases
Supplier Capital Investment?	Decreases	Increases
Collaborative forecasting?	Irrelevant	Enabled
Problem escalation?	Haphazard	Direct to CEO
Service level monitoring?	Irrelevant	Fundamental
Lowest price?	For Goods	For total service
Shared risk?	No	Fundamental
Shared reward?	No	Yes

C. *Outsourcing of activities*

Outsourcing is nothing new. Traditional areas for outsourcing have included subassembly manufacturing, logistics/distribution, and employee benefits. Companies have also established reseller relationships to eliminate the cost of selling directly to the end-customers. However, lags in communication and a paucity of information have made outsourcing difficult to manage.

With the Internet and communication as a key enabler, outsourcing has become a way of business for many companies seeking to focus on their core competencies (leveraging outsourcers to achieve efficiencies in non-core parts of the value chain) or in search of additional capacity. These companies have improved performance in key areas while outsourcing functions as logistic/distribution and information systems. As a result, their operating and administrative costs have been significantly reduced.

Similarly, internal management processes – such as financial accounting, human resources, and maintenance and repair – can be outsourced. Some companies choose to outsource information technology processes, legal counsel, and elements of marketing and sales, if management regards these functions as non-core to customer management or to the strategic growth drivers of the organisation.

However, a decision to outsource is not easily made. To ensure that outsourced processes are up to standard, a company must develop a reliable network infrastructure and strong communication protocols. Often relationships with new business partners must be established to ensure co-operation among all the organisations involved. Each company must earn the trust of its new business partners and provide a strong strategy for creating value. An organisation's trusted business partners should all share in the value network's success and possess a sincere commitment to the win-win proposition. It is essential that business partners are provided with access to the formerly confidential internal information and must be trusted to act on behalf of the other party's best interest. Often, contracts between business partners will complete the setup and will formalise the nature of the partnership.

Risk management throughout a value network requires controls that meet the mutually agreed agreements of dependent partners. To develop business relationships to this level of mutual control, suppliers and/or customers in the value-chain must be electronically linked through real-time information-sharing networks. By means of example, Cisco has connected its manufacturers, assemblers, distributors and logistics partners through Manufacturing Connection Online, a supply chain portal that provides Cisco and its partners access to real-time manufacturing information including forecast data, inventory, and purchase orders.

D. *What's different in the new economy?*

The following different dimensions of trust are present in the new economy:

Social trust

Francis Fukuyama in his book "Trust" (1995) divides societies in two groups. First, the "low-trust" societies as Italy, France, Korea and Taiwan, and secondly, the "high-trust" societies as the US, Germany and Japan. Fukuyama develops a theory of trust based on the cultural habits affecting the amount of family exclusiveness. This family exclusiveness affects how open the family structure is and the amount of interaction among the members of the society. Fukuyama proclaims that the amount of trust developed in a relationship is the key that allows a society to develop the large economic corporations and businesses that are essential in the world market. He believes the future is the network organisation and this will give a natural advantage to those societies that have a high degree of social trust.

Social trust is more difficult to implement in an e-business context as the Internet offers less verifiable information about market participants. People transacting over the Internet do not know whom they are dealing with. Also, they often lack information about the financial stability of the partner; this creates a need to develop trust as it is not present from the beginning. One of the common ways to create confidence is to build virtual communities as people tend to more easily trust people with similar interests and problems. Some companies use negative (blacklists) and positive reporting systems to help people to interact in a trusted manner. However, due to the fact that identities can be changed and the reporting scores can be modified, these systems are not necessarily very reliable.

Legal trust

E-business offers a completely different way to conduct business. However, new business practises are routinely scrutinised by governments and regulatory bodies, organisations can therefore expect continued official review, especially when issues of trust surface. Companies operating in global markets are often slow in embracing the reality of legal issues and government oversight, ignoring compliance of the process. Without an understanding of country-by-country regulations and the laws in multiple jurisdictions, they fall into expensive, time-consuming, and embarrassing traps. They become subject to fines, judgements, and legal fees, all of which diminishes trust.

Business methods that are effective and acceptable in one jurisdiction might not work well or even be permitted in other markets Organisations should accept variations in practice across national boundaries, despite the best efforts of international rule-making bodies.

In the online world, a business's ability to succeed derives not merely from defending established positions, but from securing itself and its assets in the first place and then using legal strategies to transform the business to gain competitive advantage and trust amongst the customers.

There are several key components to establish trust and achieve success in the e-business market place. They evolve interdependently, requiring the organisation to:

- address questions of business transformation;
- protect name, reputation and assets;
- assure that transactions are enforceable;
- manage liability risk;
- form alliances;
- effect website control; and
- focus on compliance and privacy policies.

E-business initiatives by definition create a free flow of information and activity – valuable assets, which must be protected as they are lost in the cyberspace. Whilst cyber incidents are often trans-border, the legal environment for business differs from one country to another and foreign laws are often onerous, confusing and interpreted in a manner to which we are unaccustomed.

For example, many countries now have specific laws protecting information privacy (data protection laws) that cover customer and employee information. Data protection laws require disclosure and/or customer consent for the lawful collection of personal information and restrict the purposes for which it can be used. Cross-border data flows have become problematic, especially since the EU directive on data protection came into force in 1998. This and other data protection laws restrict the ability of the e-business enterprise to transfer data to countries that do not provide similar privacy protection, and/or face criminal and civil sanctions for doing so.

At the same time, changes in the legal environment can serve as a catalyst to change the way the business operates. For example, new laws regulating electronic signatures and certification of identity such as the EU directive on electronic signatures, will permit businesses that currently undertake paper transactions (because of legal requirements for signatures) to sell their products instead by electronic means. In addition, an organisation that understands these electronic signature laws is presented with a new business opportunity.

Brand trust

A company's brand plays a significant role in the degree of trust it achieves. It is even more important in the e-business world than in the physical world. On the Internet, if a company does not have strong brand recognition, it will be lost among all of the start-ups - and increasingly – the incumbents.

Companies who build strong brand loyalty via trust establish focus on attributes other than price. A strong brand results in fewer competitive entrants, marked product differentiation, less price sensitivity, and increased customer loyalty. Companies with strong brand loyalty attract high value prospects while retaining high value customers and create opportunities to cross-sell additional products and services to them.

In the sales cycle, one can notice the difference between pure plays (new entrants) versus traditional existing businesses (incumbents). Pure plays will have to create trust in the second stage of the sales cycle, while the traditional businesses can often overleap this due to the trust already deeply rooted in their brand.

Hi!
You need!
Hurry!
Buy!

Even if a company can combine the three main components that communicate trustworthiness on the web site – a well-known brand, strong navigation and strong fulfillment – it can't ensure that its site will be perceived trustworthy if its brand isn't considered trustworthy. Finally, consumers usually put more trust in brands that are geographically closer to them.

Technology trust

A fundamental requirement to e-business success is the requirement that an organisation's technological infrastructure supports its e-business. If the basic technology is not reliable or resilient, and it cannot sustain the processes, it is, by definition, untrustworthy. Advanced technologies are making enterprises more competitive, but without proper safeguards, these organisations can make themselves vulnerable to greater risk. Companies need to balance the introduction of new technologies and approaches with risk management.

An organisation can lose customers because of conspicuous problems like web site failures caused by unreliable hardware or software. An organisation also loses trust if its Internet site becomes overloaded as a result of an unforeseen excessive demand for access that degrades the system, reduces performance, or causes a complete loss of service. An organisation certainly loses revenue during the crisis, but it can lose revenue forever if customers decide to move on to more trusted providers.

People present as many opportunities and as much risk as does technology. The importance of user training can not be underestimated. Often, systems are thrust on employees without appropriate learning opportunities, which dooms a system to a lifetime of inefficiency and limited productivity before it even gets started. Training is probably the single most important factor regarding a rollout of any new system.

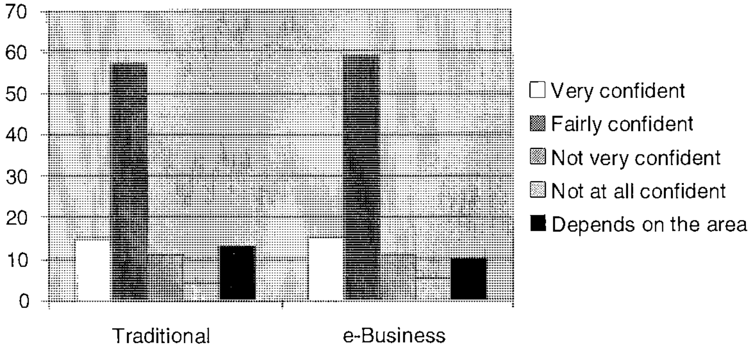
Data quality

As e-business becomes increasingly pervasive, data quality in on-line commercial relationships becomes critically important. These relationships can only flourish where all parties have complete confidence and trust in the data being transferred between them. An organisation whose data cannot be trusted will find its commercial opportunities increasingly limited, with suppliers, customers and trading partners increasingly inclined to look elsewhere for companies whose data they can trust.

In 2001, PriceWaterhouseCoopers conducted a Global Data Management survey and asked 600 leading companies across the US, Australia and UK about their experience in data management. The survey found that three-quarters of respondents reported significant problems as a result of defective data. And the same proportion said they had realised clear commercial benefits from effective data management. Almost 60% has cut their processing costs and well over 40% had managed a boost sales through better analysis of customer data. E-business companies saw the main benefits in greater sales, while traditional companies mainly experienced lower reconciliation costs.

In many areas of on-line business activity, nothing less than total confidence in data is sufficient. However, the PwC survey showed that only 15% of respondents professed themselves 'very confident' about the quality of other organisations' data, suggesting vast chasm of unease among respondents over the accuracy and integrity of the mass of data now passing between organisations. Since absolute – and shared – confidence is vital, greater discussion at senior management level in every company would be a logical step towards establishing trust.

Data management is critical to the future of businesses of all types. Only through an agreed, documented and rigorously implemented data strategy indivisible from the rest of company's strategic drivers, with committed leadership from board level and clear lines of responsibility, will a company put itself in a position to create value in the future.



IV. BUILDING E-BUSINESS TRUST

Time is essential for building trust and confidence, and the Internet is still in the puberty with corresponding lack of self-confidence and lack of direction. However, organisations can take measures to communicate trustworthiness. E-business trust can be built with these components:

A. *History*

Trust is understood by most consumers to be a dynamic process. It deepens or retreats based on experience. The trusting process begins when an individual perceives indications that suggest a firm might be worthy of trust. These indications can include behaviours such as manner, professionalism and sensitivity. These forms are designed to represent trustworthiness, they become straightened over time and are eventually transformed into "character traits", such as dependability, reliability and honesty.

As it becomes clear that "character" underlies the indications, one will be willing to participate in more informal transactions. When only forms are known, one will only engage in formal, written contracts with a firm. However, as one begins to rely on a sense that a "trustworthy character" underlies the firm behaviour, one will require progressively less new information.

Experience over time in a commercial relationship is vitally important in making transactions smoother, simpler and more likely to become habitual. With each transactional experience successfully completed, a pattern emerges. Over time, experience replicates itself and ultimately a sense of trustworthiness develops based on all that has come before. Each successful venture bodes well for a continuation of the process, even if it diverges into other areas.

B. *Governance*

Establishing an effective governance structure is one of the cornerstones in building a trustworthy e-business. The ability of the founders and management to adapt and align their corporate culture to the e-business environment as well as their reputation are important critical success factors. Furthermore, financial stability plays an important role in building trust. Incumbents with balance sheets that have been available for public scrutiny are generally more trusted than pure plays without proven financial records.

Effective governance will maintain the alignment of an organisation's business goals with its operations. Clearly defined managerial guidelines for governing processes can help to achieve a set of e-business strategic objectives and build trust in an e-business environment. Due to the heavy reliance on business partners in most e-business activities, organisations should include their partners in governance discussions, as open communication is the best way to prevent misinterpretation.

C. *Brand*

An organisation's brand is an important asset for communicating trust, especially in a B2C environment. A brand-name product is one that a consumer prefers to other products in the same category for reasons other than price. If consumers can be persuaded to remain loyal to brands, the organisation's e-business activities are likely to extend its brand position.

Trust is complex and this compounds the problems facing dot.com market entrants – companies are most likely to trust companies that have physical presence. Often, companies can assume leadership through association. A description of the affiliation with other well-known, trusted organisations – e.g. portals and aggregators and solution providers - affirms the commitment to excellence.

Reputation, trust and brand are crucial to organisation's ability to compete. As with trust,- the reputation is something that successful businesses build up over time.

D. *User experience*

An easy to find and understandable web site is fundamental to an organisation's successful e-business. Navigation, presentation, the functionality of underlying technologies, and scalability together can provide a rewarding experience.

- *Navigation* – the design of the navigation system must be clear and consistent. The site should have prompts, guides, and instructions to aid usage and searches. Terminology for navigation and content should be easy to understand.

- *Presentation* – The web site should use graphics that convey its content and purpose. The web site should be professionally designed, and its format should conform to that of other trusted sites.
- *Technology* – The site should be fundamentally sound, operate reliably, and function easily. It also should provide links to related web pages.
- *Scalability* – An organisation must be able to keep pace with its growth. As its products and services become desirable, an organisation can lose its momentum if it does not have scalability, the capacity to provide a high level of customer service regardless of the continued growth of the business. An organisation must compare projected volumes against the abilities of its processes and technologies to manage both day-to-day peaks in transaction volumes and long-term growth.

E. *Process effectiveness and integrity*

One of the essential requirements in building competence trust is to have a transparency across the processes. Track records should be kept in an accurate way. Status overviews need to be up to date and complete. Regular and reliable backup procedures are crucial, as incomplete or inaccurate data affects the entire e-business.

Process integrity is under scrutiny as companies look closely at the way they manage businesses. E-business can not be treated only as a front-end or only an IT-driven solution. It is the result of a corporate wide commitment to a new ways of doing business. It is important to take into account the input and support from all areas.

Accountability in the e-business combines policies of trust with responsibility. Delegate processes to operational levels with clearly established business rules, assists companies in assigning ownership and clarifying responsibilities.

F. *Technology*

The message, that a physical presence is essential for establishing trust, is not valid in a virtual online world. Trust has to be redefined – after all, no-one can build a physical presence on the Internet. The basis of physical trust can be transferred into the online world by using certificates, web-seals and risk management processes to secure and control the processes.

The growth of e-business has been staggering; it has caused the beginning of a major structural shift in how businesses actually conduct themselves. Fundamental to that shift is infrastructure. Companies are seeking ways to move from their closed proprietary environments, designed to manage back-end business processes, to open, Internet-connected, environments focused on front-end business processes. In trusted electronic communications and transactions, reliability and security must evolve further to enable this to occur.

1. Reliability

When an organisation's processes and procedures combine well with the underlying technology, its performance increases dramatically. It is essential that the organisation's strategy, technology, and processes are integrated to achieve optimal results. If not, operations become chaotic as the business processes that span e.g. the organisation's supply chain change. When a company fails to link its front – and back-end systems or evolve its operations to meet growth in demand in an orderly manner, it loses credibility. This is especially important today as e-business enables companies to perform all over the world, working continuously in real time with no "time out" during which problems can be fixed manually.

Virtually every participant in e-business knows that systems need constant attention if an operation is to run smoothly and inspire confidence. Even the most sophisticated e-business enterprises can fall victim to unexpectedly heavy demands on their logistics. The business processes must have built-in resilience through such items as comprehensive well-tested disaster contingency and recovery plans and technology components (for example, fault-tolerant hardware and uninterruptible power supplies) that provide resilience.

2. Security

While the security of business information is important to the success of any operation, in the world of e-business it is crucial. Some fundamental fears stem from uncertainty that is endemic to the Internet. There remains great confusion about e-business, largely due to a lack of understanding and precedent of business conducted this way. Electronic transmission and storage of e-mail, proprietary information, contracts, money, and even products themselves can be fraught with danger if systems are not secure from the outset.

Information can leak out very quickly, sometimes untraceably. When it is gone it is lost forever or, worse, it becomes a co-opted asset of the competition. Alternatively, competitors can come into possession of proprietary information as strategic alliances are formed. Although security is fundamental to success, it is often considered an afterthought in the e-business enterprise. Companies looking to maximise business opportunities often look first to applications, considering infrastructure issues at another time.

Whether activity stems from business-to-consumer or the much larger realm of business-to-business relationships, trust stems from the belief that the technology is sound, that systems have integrity, that transactions are legal, that the time, place and the confirmation of transactions can be proved, that confidentiality is guaranteed.

There are several elements of e-business security:

Risk management: The formal analyses to identify threats, vulnerabilities, risks and security cost-benefits.

Physical security: Those barriers made up of locks, personnel badges, and badge and biometric access control devices.

Personnel security: Those processes and controls in place to ensure that only people of integrity, without criminal record or drug problems, are employed.

Administrative security: Those processes and controls such as e-business security policies, procedures and awareness, and training programs.

Communications security: The protection of information transmissions, e.g. encryption.

Operations: Those processes and controls related to normal, day-to-day operations on ramps to the Internet, system configuration, and system maintenance.

Digital certificates are a key enabler to evolve to a more open security environment, as they offer an integrated solution, making security nearly invisible. Enterprises can leverage the unique capabilities of digital certificates for both internal identification and authentication requirements and for creating secure and reliable communications networks between trading partners.

A digital certificate is an electronic record that ensures confidentiality, establishes the identity of the certificate bearer, and validates a digital signature to other parties. Essentially, a digital certificate is an electronic passports provided through Public Key Infrastructure ("PKI"). A digital certificate is a file that contains the name of an entity (a person, server, or other device), the public key of that entity, name and identification number, and the credentials of the company that issued the certificate.

Together with other functions (including directories, validation authorities, certificate revocation lists, and key escrow services) digital certificates and Certificate Authorities (CAs) constitute a PKI. Digital certificates provide the functionality for the encryption, decryption, and authentication that form the basis for secure communication and secure commerce.

Certificate technology is available from a variety of suppliers. Some enterprises have chosen to build internal CA infrastructures to provide the functions of certificate issuance, maintenance of certificate revocation lists, and validation of certificates. Because expertise in this technology is extremely scarce, some organisations outsource the process and others join industry-led groups.

G. *Policy and disclosure*

Fundamental to creating trust is an organisation's willingness to disclose its business practices, protect its information, and ensure transactional integrity to its customers. Those businesses that are not willing to undertake such activities risk the perception that they are disinclined to conduct themselves in accordance with prescribed standards. They may underestimate the vulnerability of business to public pressure and the public relations nightmare that can result.

Some e-businesses bungle the ordering process, deliver the wrong (or inferior) products, double-bill, or provide no methods for recourse or contact when problems arise.

Organisations that do deliver on their promises and do have strong track records in cyberspace will move forward into new areas. They can proceed, confident of drawing interest, because they have developed a measure of trust over the years that will stand them in good stead as they continue to innovate online.

The organisation must determine exactly how it will conduct its business with all stakeholders and hold to that policy to ensure reputational integrity and avoid corruption of history. Organisations should be judicious in the statements they make and the guarantees they express on their web sites or links to other sites. Once a corporate statement or promise has been made, it must be upheld. The organisation must sell the price it has been posted; deliver within the term it has described; give timely notification of delay or cancellation; and provide recourse when problems arise. Special attention should be given to security and data protection. Complaints should be handled in a timely and correct manner.

Organisations should take heed, because governments and international regulatory bodies are already working to define several legal issues, to understand their practical impact, and to determine whether and where regulation of e-business is necessary. Accordingly, companies must anticipate the threat of government-imposed regulation if industry fails to establish its own rules.

H. *Endorsement (seals of approval)*

Trust can be assured through the inclusion of third-party oversight that reinforces credibility of the institution. The use of icons and text that symbolise the reliability of the operations as a whole (Webtrust, BBB Online) or, more specifically, merchant service security (MasterCard, VISA, Amex), is a good shortcut to assuring that customers concerns have been addressed early.

Trust seals are quality marks that signify that an organisation abides by a code of integrity. There are, however, many levels of approval. Does the seal cover privacy only? Does it require an audit of business practices and transaction integrity? Does it imply that an organisation will refrain from giving confidential information to others not involved in the transaction? Does it go on to say that it also will ensure that on one can reach into its systems to take the information?

There is also an important distinction between the verification processes underlying various seals of approval:

- Self-assessment – some seals are based on self-assessment; the organisation itself claims that it is adhering to best practises.

Although the organisation claims that it intends to hold itself to high standards, there is no third-party review for attestation. If there is a problem, one can expect the organisation to resolve it. If breaches that become known to the public occur frequently, the marketplace will be the arbiter, and the public may judge the organisation to be untrustworthy. A seal issued from a self-assessing entity indicates an intention to conduct itself admirably. It does not, however indicate how reliable the organisation is, and it does not describe the organisation's qualifications or abilities.

- Independent review – Companies wanting to ensure e-business trust with greater conviction and a broader scope than by self-assessment open their operations to scrutiny. The formal approval of an oversight authority, its seal visible on a web site, shows the intention and effort of the sealed company to conduct itself with integrity at all times through behaviour corroborated by independent audit.

There are several independent review seal programs available on the market, which leads to some confusion among the users. EU lead initiatives as eConfidence, and industry lead initiatives as Global Business Dialogue, are co-ordinating the seal programs on the global level.

Some of the widely recognised independent review seal programs are:

- *WebTrust Program*, an international e-commerce trust program developed and managed jointly by the AICPA and the CICA. WebTrust provides report on the control environment for one or more of the following principles, covering security, privacy, availability, confidentiality, non-repudiation, business disclosures and transaction integrity, and customised disclosures.
- *AICPA SysTrust*™ attestation service, developed to create trust between business parties performing e-commerce, and focuses on systems reliability. It reports on the availability, security, integrity and maintainability of an organisation's system.
- *Customized OnLine Attestation (COLA),* developed by PwC, focuses specifically on risks that an organisation has identified as being important to them and their trading partners. The resulting attestation will be displayed on the organisation's web site for a predetermined period of time.

- *VeriSign* seal, created to provide an instant authentic site recognition among web surfers, focuses on security.
- BBBOnline, a wholly owned subsidiary of the Council of Better Business Bureaus (BBB). Its mission is to promote trust and confidence on the Internet through the BBBOnline Privacy and BBBOnline Reliability programs.
- *TRUSTe*, an independent organisation dedicated to build consumer trust and confidence over the Internet. TRUSTe seal is awarded to Web sites that adhere to established privacy principles.

Online Privacy
WebTrust
SECURITY
VeriSign
Secure Site
click to verify
PRIVACY
BBBOnLine
BBBOnLine
reviewed by
TRUSTe
site privacy statement