UK online for business

Securing trust
in electronic supply chains

Introduction 1

Trust in each element of the supply chain 2

Trust and security in action 3

Securing your future 4

Introduction: How issues of trust affect e-supply chains

Electronic supply chains are gaining ever wider acceptance by large organisations thanks to the economies of scale, speed and accuracy of transactions, greater efficiency, and reduced costs that they bring.

The other companies in these chains derive the same benefits of reduced costs, increased sales, and greater efficiency from electronic supply chains. But they can also be exposed to greater risks through participation in electronic chains they do not control.

One of the main inhibitors to the uptake of e-commerce in general, and the adoption of electronic supply chains in particular, has been concern about the security of online transactions. Once organisations can demonstrate to both customers and trading partners the security of their online operations, commercial prospects immediately improve.

It is important to remember that the fundamental goal of electronic supply chain network security is not to prevent the loss of sensitive data, but to maximise the economic return on such data, whilst always maintaining its integrity.

Trust in each element of the electronic supply chain

Trust in each element of the electronic supply chain

Every element of the electronic supply chain is affected by issues of trust and security.

- **Product Development.** Open communication is vital during product development, and sharing information and resources within the development team is in everyone's interest. Commercially sensitive information will need to be communicated in a secure online environment, through, for instance, secure e-mail services or virtual private networks.
- **Purchasing.** This time the goal is transactional confidence. Both parties must be confident in the ability of the other to deliver payment or goods, and to maintain the security of payment details provided - by credit or debit card, for instance. The use of digital signatures supported by certification authorities and encrypted transmissions (such as Secure Socket Layer or other end-to-end security products) can reassure customers that their details will be kept confidential.
- **Stock control/inventory.** By regulating who has access to your stock control system and who can update records you can make sure that you have an accurate picture of your stock holdings. This is particularly important when online customer/supplier interfaces are in use.
- **Order accuracy.** Greatly improved by e-mail, fraudulent ordering can be guarded against by the use of digital signatures and Certificate Authorities (CAs). CAs issue and manage security credentials to guarantee people are who they say they are.
- **Delivery.** Secure delivery information – where the information cannot be intercepted online – means that details of what you have purchased and where it will be delivered are secure. This protects against the possibility of high value items being targeted in transit by thieves.
- **Customer service.** Increased levels of trust and security in the electronic supply chain lead to better business relationships and greater levels of trading activity.

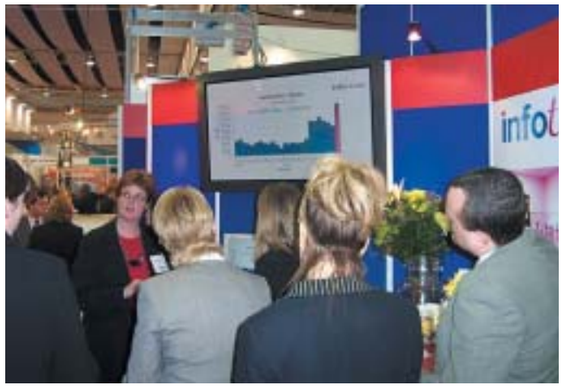
Trust and security in action

Infotel Solutions

Infotel Solutions is a hotel, conference and events reservation service based in Lincolnshire. It uses web and telephone technology to integrate its telephone call centre with its web site's online booking service for both its end customers and its hotel suppliers.

Mark Taylor is the company's information manager. "We have a number of security systems in place, including an extremely effective firewall that sits between our systems and the Internet, monitoring all traffic. Opening up your system to the Internet can leave you wide open, so a firewall is essential. It keeps all unauthorised intruders at bay, but allows customers in to browse our site."

Infotel also has all incoming and outgoing e-mails and attachments swept for viruses by its Internet Service Provider (ISP). "We get about twenty infected e-mails a day," explains Taylor. "The ISP keeps them in a quarantined area for me to look at – and also sends a courtesy message to the sender advising them that they have a problem." Inside the organisation staff have appropriate levels of access to corporate information through password identification, and transmit and store all transactional details in a securely encrypted fashion.



Wright publications

Based in West Yorkshire, Wright Publications specialises in technical publications and foreign language translations. Secure information is key to its business, and it decided to adopt British Standard 7799 back in 1998.

Customers have recognised the difference BS 7799 makes and have confirmed that it gives the company a distinct advantage against other suppliers, as it gives customers a greater sense of confidence in dealing with them. Adopting the standard also helped Wright Publications spot risks it had not considered before.

Through BS 7799, the company learnt to apply electronic solutions in controlling electronic information, and to integrate different administrative and management procedures into a single system for complete visibility. The proof of its effectiveness? When Wright Publications suffered a serious break-in, its security provisions meant that all its information remained safe and it was back in business in just a few hours.

Securing your future

Data is frequently an organisation's most significant asset, and deciding how to manage and control your data is one of the most significant business decisions any company has to make. It is also the one commodity traded by every company in your supply chain. British Standard 7799 is the standard on information security management. Following its provisions will ensure you comply with legal requirements, can help achieve the level of trust that will allow you and your supply chain partners to trade securely together.

The use of BS 7799 allows you to develop a practical Information Security Management System (ISMS), that involves three simple steps:

- Set the goals and direction of information security in your organisation through a management framework for information and an agreed security policy. Work with your customers and suppliers to ensure your solution works for all concerned.
- Assess the risks you face - small and medium sized businesses may be unlikely to be the target of professional hackers, but data loss could cost your business a lot. Think also about the potential risks to your customers and suppliers – this could affect you too. Balance your security spending against the risks you and your face.
- Once you've agreed a policy and identified risks it's time to choose and implement the security measures you will take to keep risk down to an acceptable level. You also need to consider the 'trust' implications involved in any security measures. Will regular customers and suppliers be happy to remember user names and passwords?

Communicating the reasons behind your security measures and the benefits they'll bring will ensure the transition to a more secure trading environment goes smoothly. Always involve your key supply chain partners in these discussions. It will enable you to identify potential problems and work on solutions to them earlier.

Practical ways in which you can begin preparing for this process include:

1 Determine the value of the data you hold

- SEC 1 (low security classification) – non-critical data that all your employees can access – and probably some of your customers and suppliers too, through a password protected web site. This could include inventory information, for instance.
- SEC 2 (medium security classification) – business critical data that should be kept confidential within the company, with access allowed on a limited basis through passwords and similar measures – this might include mailing lists, financial information, and so on. You might want to make this available to selected customers and suppliers.
- SEC 3 (high security classification) – essentially private information access to which should be strictly controlled. It may also be necessary to hold this information in encrypted format – as in the case of credit card details, for instance.

2 Identify threats

These come in two basic forms - malicious threats, and accidental threats. Malicious threats might include hackers, disgruntled employees, and so on. Accidental threats might include system failures or internet-born viruses. Take into account the threats to your supply chain partners. If they're sharing electronic information with you, breaches to their security could affect you too.

3 Identify weaknesses

In the light of the risks you have considered, where is your system vulnerable? Are there regular backups? Is access carefully and appropriately regulated? How secure are your suppliers' systems? How easily can your customers get in and out of your systems? To reap the benefits of working collaboratively you need trust, you also need to be aware of any vulnerabilities in the links between you and the rest of your supply chain.

4 Establish countermeasures

These range from external backups through firewalls and virus protection programs to strong token passwords, and might also include software to monitor internet and extranet traffic. However secure your counter-measures are, if key suppliers and customers are vulnerable then there is a good chance that any security breach to their systems will affect you too.

5 Managing risk

Once security measures are in place that's not the end of the story. Security is an ongoing issue, and each new business development or new customer or supplier acquisition brings new security implications in its wake. To be effective any security policy must include regular reviews of the situation. Involve key supply chain partners in any reviews. To be truly effective any security measures must work for the whole supply chain.

Further help and advice

For more information on securing trust in electronic supply chains, and a wealth of other information, visit our web site at www.ukonlineforbusiness.gov.uk/supply

www.dti.gov.uk/cii/datasecurity/index.shtml The DTI web site with extensive links and lots of downloadable information on security.

To find out details of your local *UK online for business* adviser:

- Call the *UK online for business* Infoline on 0845 715 2000
- Visit our web site at www.ukonlineforbusiness.gov.uk

The Supplying Electronically CD-ROM will give you information about working in supply chains.

If you are a smaller business, read *E-security – a guide for small businesses* available from *UK online for business*.

These can be obtained from the Infoline or the web site.

Other useful sites

www.rsasecurity.com commercial provider of electronic security services.

www.trustuk.org.uk online hallmarking organisation.

http://www.open.gov.uk/dpr/dprhome.htm Data Protection Commission web site – provides information on your legal requirements when storing data.

http://www.bsi.org.uk/disc provides detailed information on British Standard BS7799.

Published by the Department of Trade and Industry.