**18 August 2004**
# Financial Times
## FT SUMMER SCHOOL

The safety of secrets in extended enterprises: Globalisation and the internet have exposed companies' information systems to new security threats, writes M. Eric Johnson.

By ERIC JOHNSON

The traditional method of integrating a business by situating employees in the same building has been unshackled by information technology. The rise of cheap computing, networked via the internet, has changed the way work is organised to such an extent that executives and policy makers are struggling to understand the opportunities and consequences. One consequence is the battle to keep business information private and secure; companies spend billons trying to address risks unimagined 10 years ago.

Only a few years ago, Hewlett-Packard located product designers, marketers and manufacturing workers in the same set of buildings. Products in research and development could be carried down a flight of stairs to an assembly line for prototyping and testing. Marketers played volleyball over the lunch hour with design engineers - often exchanging ideas on customer needs or competitive threats.

Today, many of those same people work in an extended enterprise comprising different companies spread over the globe and communicating via the web. Through a web browser, a designer can implement an engineering change for a factory half a world away; a procurement specialist can change a supplier order; a supply chain manager can monitor factory production; or a customer engineer can co-ordinate a delivery. Every one of those interactions could be potentially observed or disrupted by youthful hackers seeking a thrill, or other more malicious individuals pursuing competitive gain.

These changes are not limited to technology companies. The internet has dramatically improved companies' ability to shift work to its most efficient location. For example, Wal-Mart has moved many traditional retail functions to its suppliers, which it requires to use electronic communications for co-ordinating routine purchasing and supply chain planning. Carmakers such as General Motors have pushed product design functions back to their suppliers and now exchange design information over the web.

As they rush towards outsourcing and other ways of reducing costs, large companies encounter new risks ranging from supply disruptions and delays to theft of shared intellectual property and disappointed customers. They have stitched together applications for disparate departments, such as manufacturing, distribution, accounting and human resources. Virtual teams with members from different companies are now communicating via a wide range of personal devices including laptops, personal digital assistants and mobile phones - often creating new points of vulnerability.

Many older manufacturing control applications were developed to run in isolation, with little thought for security. Integrating them with other systems can leave security gaps. Similarly, when two companies link their networks to speed the flow of information, their network security arrangements may be different, creating a virtual swing door between them through which

anything can move. The level of risk of an integrated network is often determined by the least secure company in it.

Simply tracking and managing the flow of work around the globe can be challenging. Once outsourced, work and its associated information quickly flow to the supplier's supplier and beyond. The enterprise can include thousands of companies.

Raytheon Aircraft, a subsidiary of the defence contractor, learnt the implications of this last summer when it signed an outsourcing agreement with International Business Machines to implement its enterprise software project. When IBM indicated that it planned to use subcontractors based in India to keep costs low, executives at Raytheon quickly realised they had a problem. Since the work involved sensitive data on aircraft design, the company would not be complying with US regulations if the contract were to go ahead as planned. To save the deal, IBM agreed to keep the work at home until it could develop a secure management system.

Deleting virus-infected e-mails from the inbox has become routine - part of the ritual of starting another working day. Yet it is all too easy to see these small security lapses as nothing more than a nuisance of working in the internet age. In fact, small failures often lead to much more devastating outcomes.

Those hoping technology will solve our security problems will be disappointed as even companies that are in the business of selling technology solutions are quick to admit. At a summit held in May at Tuck Business School, chief information officers from diverse industries agreed that information security was a management problem, addressed by a combination of culture, education and effective risk measurement.

During the 1980s, when many European and US manufacturers faced a growing quality gap with Japan, companies found that breakthroughs in quality could not be delivered by the quality control department - they had to be part of the organisation's culture. Similarly, security is everyone's responsibility. Business managers cannot be passive, waiting for protection from the information security police. Information chiefs must articulate the risks and executives must balance them.

Brad Boston, Cisco chief information officer, described how his part of the company moved from acting as a traffic policeman - simply saying yes or no to managers' requests - to helping them make good decisions. "Our job is to identify the risk, the threat of that risk actually occurring, and tell them what the options are to (remedy) them. Then a business decision is made about which risks are acceptable and which are not."

This responsibility resides at every level in the organisation up to and including the board. One CIO complained that when he presents updates to his board on new IT applications, their eyes light up. When he talks about security, they glaze over. Having board members who understand the risks and can help other members see those risks is vital for effective IT governance.

How should the organisation be educated about IT security risks? First, it should be targeted and relevant to specific functions. Too many security managers have simply broadcast fear, crying wolf to generate awareness. This approach gains attention at first, but has little long-term effect. For CIOs, gaining and maintaining the confidence of other executives requires them to articulate the risks and opportunities in a business context - not simply forecast doom.

Scott Day, global information protection manager at Cargill, describes how the agricultural group split up its training. "We've identified what the roles are and the business unit leaders that are in those roles. What does the business manager need to know? How it affects his decision rights. We've taken that on because we think that's something that will help internalise it into the culture. When everybody knows what they are responsible for and how they are going to be held accountable, they can go and get what they need and make sure they are up to speed on it."

Second, achieving security across the extended enterprise requires careful scrutiny of both suppliers and customers; in other words, continuous evaluation of the security risk they pose. They should be warned of the risks and nudged towards better security practices. For instance, many financial companies require customers to use the most recent versions of web browsers to protect both themselves and their clients.

Sometimes protecting the extended enterprise means choosing not to work with companies where risks outweigh benefits. Jim MacDonald, CIO of management and research at Fidelity, says information security issues have affected his company's partnering practices.

"Working with small technology companies' terrific innovative systems is an issue for us. We tend to like those companies because they can help us get a competitive advantage," he says. "(But) when we go in and do security assessments, (we find) it usually hasn't been an area of focus for the company and may be somewhat lacking. We've been slower to create partnerships with those types of companies - we see the technology and it's terrific, but they just don't have enough (security) emphasis."

Qualifying suppliers according to their IT security risk is as important as measuring their financial risk or quality. As Mark Hillman, a supply chain executive at General Motors, says: "If you do a lot of outsourcing, you need to go poke at everybody." "Poking" means assessing the risk and then monitoring it like any other a supplier may generate. It means ensuring that suppliers' access to your systems does not compromise your network or that their security is sufficient to protect the intellectual property you share. In the new world of the extended enterprise, security can never be taken for granted.

*M. Eric Johnson is director of the Center for Digital Strategies at the Tuck School of Business*.