Economist Intelligence Unit

The Economist

The global supply chain
Challenges for small and midsize enterprises

An Economist Intelligence Unit briefing paper
sponsored by IdenTrust

Preface

The global supply chain: Challenges for small and midsize enterprises is an Economist Intelligence Unit briefing paper, sponsored by IdenTrust. The Economist Intelligence Unit bears sole responsibility for this report. The Economist Intelligence Unit's editorial team executed the survey, conducted the interviews and wrote the report. The findings and views expressed in this report do not necessarily reflect the views of the sponsor. Russ Banham was the author of the report and Rama Ramaswami was the editor.

Our research drew on two main initiatives. We conducted a global online survey in May and June 2006 of 127 executives from various industries. To supplement the results, we conducted in-depth interviews with executives from around the world familiar with how global supply chain issues play a role within their organisation. Our thanks are due to all survey respondents and interviewees for their time and insights.

September 2006

Executive summary

The term "identity crisis" may sound dated today, but never has it been more applicable to business. As cyber fraud increases, organisations are hard pressed to keep their data safe from all manner of phishers, hackers and identity thieves, as well as to verify that communications from suppliers and other business partners are legitimate. At the same time, cyber fear is unrealistic: participating in global business, and moving goods and services across international borders, requires being able to communicate freely online.

For many small and medium-sized enterprises (SMEs), the ability to trade globally may well hinge on the extent to which they can authenticate their own identities and those of their business partners. Cash-strapped SMEs desperately need financing to invest in the automation that will integrate them with suppliers and partners worldwide. In particular, manufacturers are heavily dependent on cash to fund their complex supply chains. Lenders, however, are rarely willing to deal with unknown borrowers who lack a credit history. Employing authentication tools would enable smaller companies' identities to be verified with greater certainty, thereby improving their chances of obtaining funds to invest in supply chain automation.

About our survey

In May and June 2006 the Economist Intelligence Unit queried 127 executives on their global supply chain operations. Approximately 31% replied from western and eastern Europe, 40% from the Americas and 29% from the Asia-Pacific region and other parts of the world. Respondents represented a wide range of industries and functions; 28% cited manufacturing as their primary industry. About 50% of the respondents were C-level executives or board members. At 72% of the total sample, companies with less than US$500m in annual revenue were the most heavily represented group.

This briefing paper, based on a survey conducted by the Economist Intelligence Unit for IdenTrust, supports the conclusion that wider implementation of counterparty authentication technology may allow SMEs easier access to credit and the use of unconventional financing strategies such as reverse factoring. With this accelerated cash flow, smaller companies will enjoy greater liquidity for supply chain technology investments. Highlights of our findings include:

- More SMEs than the overall sample (38% compared with 33%) say the single most important step to safeguard the global supply chain is for governments and the UN to designate counterparty authentication standards.
- Fewer manufacturers (26%) and fewer SMEs (28%) than the overall sample (33%) comply fully with identity verification and other commercial transaction rules.
- SMEs are more concerned about the lack of international electronic standards (43%) than the whole group of respondents (38%).
- Manufacturers are more concerned about guidelines for interoperability (29%) than the respondents overall (21%).
- A majority of survey respondents cite "trust that payment would be certain" as the main factor that would assist their companies to integrate their operations with the global supply chain. Availability of more favourable financing, based on purchaser rather than supplier credit, was the second most important factor.
- Most companies say the greatest risk in automating the global supply chain is the reluctance of their suppliers to go paperless.

Insecurity over security

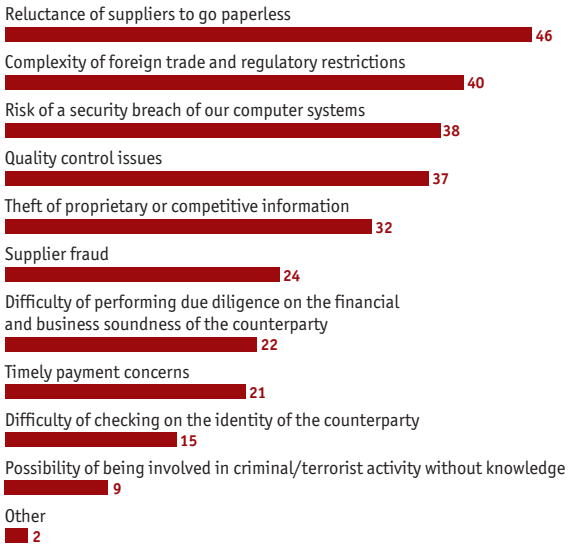
Cyberspace is fraught with peril. Security concerns are major impediments to SMEs investing in authentication and other supply chain technologies. There is widespread agreement among companies that their transactions and proprietary and competitive information, if sent over the Internet, are subject to theft by criminal organisations, competitors and even terrorists.

This is not an overwrought conclusion. Automated supply chain transactions, which involve a wider, unproven base of suppliers, increase the risk of fraud and the theft of proprietary data. In April the US Department of Justice released a report indicating that an estimated 3.6m households—roughly 3% of all households—had fallen victim to identity theft during a six-month period in 2004. One-quarter of these had their bank accounts used without their permission. The 2006 Corporate Security Survey conducted by Deloitte backs up these findings, noting that more than three-quarters (78%) of financial institutions reported a security breach from outside the organisation in the previous year, up from 26% in 2004.

In a supply chain context, authenticating the identity of counterparties is a dilemma. Identity fraud is of particular concern to corporations. Consumers often pay nothing or just a token sum of US$50 if they report unauthorised use of their credit cards, and even if subject to major scams rarely lose large sums of money to identity thieves. Companies, however, enjoy no limits on their liability if personal information is stolen. They stand to lose millions of dollars in punitive fines and damages, not to mention loss of customers and reputation. Fully 22% of Economist Intelligence Unit survey respondents, and 31% of the manufacturers in the group, are concerned about the difficulty of performing due diligence on the financial soundness of counterparties, particularly overseas suppliers (see chart 1). The security of data and dollars sent electronically is another worry. One-third of companies with less than US$500m in revenue cite "theft of proprietary or competitive information" as the greatest risk of automating the global supply chain, while 37% of these respondents and 46% of manufacturers express significant reservations over possible security breaches on the Internet. It is not surprising, therefore, that the majority of respondents (57% of SMEs and 61% of manufacturers) cite "trust that payment would be certain" as the main factor that would help their companies integrate their operations with the global supply chain (see chart 2).

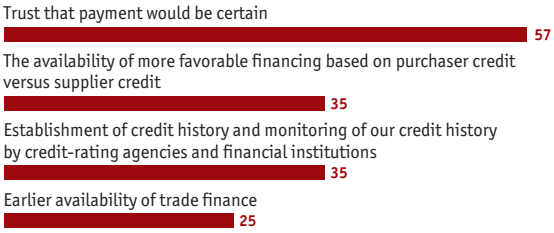
A survey by a Boston-based consulting firm, Aberdeen Group, offers further evidence of anxiety, noting that 35% of CFOs are taking a larger leadership

1. What do you consider to be the greatest risks of automating your company's global supply chain?
Select 3 options (% respondents)



Source: Economist Intelligence Unit survey, 2006

2. What would help your company to integrate its operations with the global supply chain?
Select all that apply (% respondents)



Source: Economist Intelligence Unit survey, 2006

3. Does your organisation currently review supply chain vulnerability in the following areas or does it plan to do so in the next three years?
Select 3 options (% respondents)

Source: Economist Intelligence Unit survey, 2006

role in managing global trade to reduce the risks inherent in their far-flung global supply networks. Among companies that are automated, the majority of respondents to our survey (63%) state that they are "reviewing their supply chains' vulnerability to fraud", while 48% say they are "reviewing their susceptibility to potential security breaches or terrorist attacks" (see chart 3).

In addition to these pressures, many governments are introducing regulations compelling companies to enhance identity management processes. The Data Accountability and Trust Act, for example, requires companies that store confidential personal information to notify customers of any security breach. The Sarbanes-Oxley Act, the Patriot Act, Markets in Financial Industry Directive (MiFID) and the Single Euro Payments Area in Europe, among many other global regulations, similarly compel companies to invest in authentication technology and related identity management procedures.

"There are many drivers compelling companies to invest in authentication technology, including concerns over fraud and money laundering and, especially, the need to trace goods, products and materials from cradle to grave," comments Al Bissmeyer, director of marketing and memberships at RosettaNet, a company that develops universal standards for the global supply chain based in Lawrenceville, New Jersey. Mr Bissmeyer says that the company has launched two successful pilots of its RosettaNet Automated Enablement (RAE) standard, which is expected to reduce SMEs' cost of interfacing with partners and will soon be released as a standard.

Maria Lewis Kussmaul, founding partner at a Boston-based investment bank, America's Growth Capital, nicely sums up the need to create more robust authentication practices and tools. "Corporate networks are more porous than ever as enterprises are enabling employees, customers, partners and suppliers to connect to the enterprise network. The need to provide critical applications, services and data stores to this extended enterprise has exponentially increased the security risk of network infiltration and information theft. Hence, there is a need for an authentication solution that can establish trust by proving the identity of the user."

Establishing creditworthiness

Proving its identity is crucial when an SME is trying to obtain credit to borrow funds to invest in supply chain automation. Many small companies are denied ready access to financing because they often lack the reliable credit history that lenders require. More than one-third of our respondents, and nearly 40% of the manufacturers in the sample, believe that establishing a credit history and having it monitored by credit-rating agencies and financial institutions would help them connect their operations with the global supply chain. One fail-safe way to establish credibility with vendors is identity authentication, but it requires a level of automation that few SMEs can afford. A sizeable 29% of the smaller companies in our survey cite "financing constraints" as their greatest obstacle to setting up a fully automated supply chain. Manufacturers are especially bothered by lack of funds: they are more likely than small companies (36% compared with 33%) to want financing based on purchaser credit rather than supplier credit, to have trouble paying on time (23% compared with 16%), and to favour earlier availability of trade finance (33% compared with 25%).

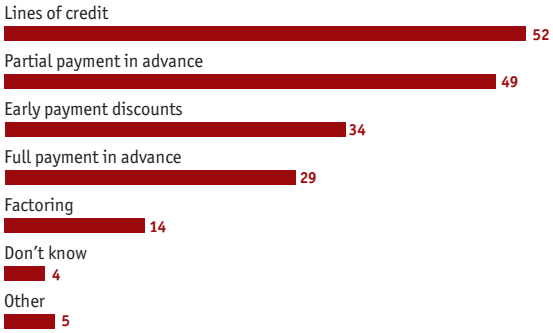
"Often the limited resources of SMEs are ignored when offering market solutions for straight-through processing," notes Tom Buschman, chairman and CEO of The Transaction Workflow Innovation Standards Team (TWIST), a not-for-profit alliance of corporate treasurers, banks, system suppliers, electronic trading platforms and other groups that want to connect the financial supply chain to the physical supply chain by creating user-driven, non-proprietary standards. "Structured and standardised supply chain processes will help SMEs to obtain lower costs of credit via reverse factoring," explains Mr Buschman. "This will be a valuable incentive for them to invest in automated solutions with their trading partners. Authentication technology will be an important component of this automation as well as the credit provision. One of the problems for financiers of SMEs is fraud risk, due to the fact that they can't verify the authenticity of the trade documents to be financed. Thus, if they are able to be authenticated, they can automate their supply chains based on market standards used by their clients and obtain lower costs of credit."

For a global supply chain to work efficiently, an SME must have access to two broad categories of trade finance: preshipment financing to make or buy the material and labour necessary to fulfil the purchase order; or post-shipment financing to have cash flow while waiting for payments from buyers. In either case, the lender is unlikely to advance funds without ascertaining the identity—and thereby the creditworthiness—of the buyer. Often, several tiers of suppliers are required to create the finished product that the buyer has ordered. In order for a buyer to secure financing, all of these suppliers need to be authenticated, both for the lender to establish the creditworthiness of the entire supply chain and for the buyer to verify the identities of all the suppliers involved.

Although most small businesses rely on lines of credit as their most common financing mechanism, they also avail themselves of the following trade financing techniques:

Factoring is often a quick source of working capital for SMEs. A factor is an organisation that purchases a firm's unpaid invoices at a discount and collects on the invoices. Factors typically provide 70% of the face value of the invoices within 3-5 working days, and

4. Which of the following payment methods does your company use?
Select all that apply (% respondents)



Source: Economist Intelligence Unit survey, 2006

the remainder after final payment, after charging a service fee of 4% to 5%. In the Economist Intelligence Unit's survey, manufacturers are especially in favour of factoring, with 29% using it, compared with 14% of the overall sample (see chart 4).

Forfaiting is another common financing mechanism, whereby a bank purchases an exporter's sales invoices or promissory notes, which usually carry the guarantee of the importer's bank.

Purchase order financing. Most domestic buyers agree to pay sellers in 30-60 days. Overseas buyers, however, may ask for letter-of-credit terms, which leave the seller without any cash coming in during the manufacturing or transit period. A lender who offers purchase order financing solves this problem by buying product inventory, using the inventory and confirmed purchase orders as collateral.

Large multinational banks are the most experienced in trade finance, but they are often reluctant to finance SMEs because of risk and credit issues—and here is where authentication comes in. "Authentication solutions that include identity verification and Internet technology allow businesses of all sizes to participate in automated global supply networks," states Lorenzo Martinelli, executive vice-president of E2open, a supply chain software company based in Redwood City, California. "This will make processes more efficient, reduce excess inventories and give easier access to financial liquidity instruments for all participants in the end-to-end supply chain."

John Sculley, former CEO of Apple Computer and president and CEO of Pepsi, and currently chairman of the board of IdenTrust, agrees: "When you're dealing with the financial supply chain, this seven-trillion dollar market, what you need to authenticate is not site access but the parties involved with the transaction. An SME supplier in China with a buyer in the Czech Republic doesn't need its treasurer to have every transaction vector back, as long as the signatories to the transaction are authenticated."

The A to Z of authentication

There are many different types of authentication solutions, from traditional login, user ID and password methodologies to more robust multi-factor authentication involving the deployment of additional identity management technologies, such as biometrics, USB tokens and digital signatures. The Radicati Group, a technology research firm based in Palo Alto, California, estimates that the market for identity management software currently amounts to more than US$1.2bn in worldwide revenue, and will exceed US$8.5bn by 2008.

According to a 2005 report on online ID theft prepared by Radix Labs, an independent research organisation, for the US Department of Homeland Security, the most popular method of preventing identity theft is two-factor authentication. This technique, notes the report, requires "proof of two out of the following three criteria to permit a transaction to occur: what you are (eg, biometric data such as fingerprints, retinal scans, etc); what you have (eg, a smart card or dongle); and what you know (eg, an account name and password)."

One-time passcodes (OTPs) are the most common second-factor authentication device, but they are all too easy to hijack. Other forms of second-factor authentication, such as smart cards, USB dongles (devices attached to a computer without which the software will not run) and biometric systems, are more sophisticated—albeit more expensive—and can perform cryptographic processing that hackers cannot intercept.

Of the various methods of second-factor authentication, **biometric systems** are sparking the greatest commercial interest. A well-designed biometric authentication program, notes the Radix Labs report, uses a challenge-response protocol that prevents responses from being reused. According to the International Biometric Industry Association, the biometrics market will increase from US$165m a year in 2000 to US$2.5bn by the end of the decade. Fingerprint biometrics remains the market's mainstay, representing 55-75% of the total commercial biometrics market. Fingerprint scanners and sensors are being built into keyboards to authenticate users, as well as into mobile phones, personal digital assistants (PDAs) and laptops to enable e-commerce.

Facial recognition is another common biometric tool. A person's face is photographed and scanned into software that measures dozens of features, such as the distance from the bottom of the nose to the top of the upper lip, the angle of the head and the overall facial shape. These measurements are then encoded, digitalised and stored in a database for comparison purposes. A single visage can be compared against millions of other faces in seconds. Similar technology is at play in voice recognition.

Other biometric authentication technologies also warrant mention, such as iris scanning. Patterns in the iris (the coloured portion of the eye) are even more complex, and therefore verifiable of a person's identity, than fingerprints: the false-rejection rate for iris recognition systems is zero, compared with 3% for fingerprint recognition systems. More advanced biometric tools include measuring the speed at which a person types on a computer, as well as the pressure of the keystrokes.

The benefit of biometrics is the certainty they provide. The drawbacks are their affront to civil liberties—the Big Brother argument—and cost. "While biometrics offer the ultimate in convenience and portability," notes Ms Kussmaul of America's Growth Capital, "biometric readers are expensive."

Case study: Creating virtual links

Digital certificates guarantee that electronic agreements made to ship goods and pay for them are as rock-solid as paper-based legal documents. Arrow Electronics, a provider of products and services to industrial users of computers and electronic components, based in Melville, NY, has established a public key infrastructure with its key customers worldwide. It employs digital certificates to assure its customers that a purchase order is both legitimate and legally binding. "We use a digital certificate and the RosettaNet standard to identify ourselves to our customers, and our customers use it to identify themselves to us," explains Pam Webber, Arrow's senior manager of supply chain technology. "With large customers, you can't get through their firewalls unless they can identify you."

In the automated global supply chain, where purchase orders, invoices and remittances are sent electronically, digital certificates offer a way to effect transactions without fear of illegal interception or misrepresentations that lead to repudiation. Sending an e-mail or using file transfer protocol—the language used for transferring a file from one computer to another across the Web—does not allow for the sharing of a legal commitment at the transactional level. By using a digital certificate that is built into the RosettaNet standard, all parties to a transaction can be certain that the transactions are legitimate.

"If I send a company a message and they opened it, I know they received it," says Ms Webber. "This way, if something goes wrong on your side and you come back to sue us, arguing, for instance, that you didn't agree that we would ship you a product, we have verification that you received our electronic document notifying you of the shipment. This level of security on a purchase order and shipment is no different than how banks are transacting. If a purchase order goes awry or someone intercepts it, we know there was no way this could have happened because you have identified me, and I know that because verification was pinged back to my server that you received it."

In addition, Ms Webber says, "from a legal perspective, this is a legal document even though it was sent electronically."

Ms Webber adds that other forms of identity management technology, such as biometrics or tokens, would not provide the level of authentication that Arrow requires. "Tokens would not work for what we are trying to do, nor would other identity management concepts because a token is at the desktop and we need authentication behind the firewalls." The cost of digital certificates is "not prohibitive, but bear in mind we're a large shop". A new RosettaNet standard for SMEs leveraging digital certificates should bring down this cost.

Arrow offers its small customers an alternative way to transact electronically. For example, it helps EPM Global Services Inc., an electronic manufacturing services provider based in Toronto, to offer EPM's own customers short lead times, high on-time delivery rates and flexibility to respond to changes in demand. Automation is key to this effort. "Arrow understands what our requirements are via electronic data sharing," says Cyril Fernandes, EPM's senior vice-president of marketing and corporate development. "We send them an electronic file called MRP Share instead of a single purchase order. The file is based on our strategic customers' demands. In effect, Arrow understands our demand and then stocks their 'store' based on the information. We take possession of supply at the point when we are ready to put product on the floor. It literally goes from Arrow's shelves into our production at the point of use."

According to Lianne Bastiem, CFO of EPM, the company has received quantifiable benefits from automation. "Our inventory utilisation, in terms of our inventory turns, increased from six to ten for Arrow-supplied parts, while our on-time delivery performance to customers increased from 80% to 85%. Additionally, we posted significant reductions in purchase order reschedules, since we do not pull on-site inventory until needed."

Digital signatures and certificates are both an alternative and additional authentication solution. Digital certificates are electronic documents that involve the exchange of mathematical algorithms with unique identifiers, providing mutual authentication of two parties involved in a transaction. These certificates are issued by a certificate authority, which can be any trusted third-party organisation that is willing to vouch for the identities of those certified.

A digital certificate typically includes information such as the following:

- the holder's name and other unique identifiers such as an e-mail address and the URL of the Web server using the digital certificate;
- the subject's public key, or cryptographic algorithm that is available publicly;
- the name of the certificate authority that issued the digital certificate;
- a serial number; and
- the validity period of the digital certificate, defined by start and end dates.

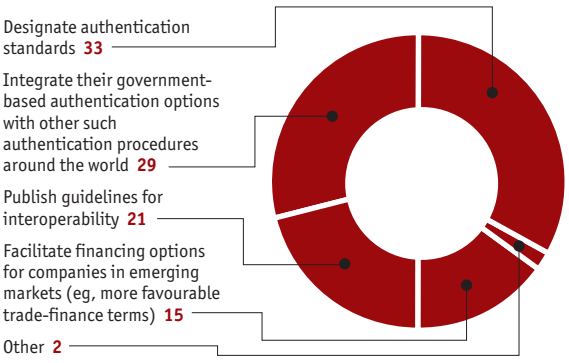
"Digital certificates assure with absolute certainty that an electronic transaction or communication must only have come from a particular party," Ms Kussmaul explains. "It does this through a system called PKI, or public key infrastructure. There is a public key and a private key pair for every participant in the system. If a company wants to send another company a message, it looks up the other company's public key and signs it with its private key. If there is a match, the document can be opened. Underneath the exchange of keys are mathematical algorithms."

Ms Kussmaul adds: "Enterprise PKI using digital certificates offers a powerful solution for authentication, encryption, digital signing, access control and non-repudiation. Nothing is stronger than PKI, which provides comprehensive, robust protection against phishing, eavesdropping and back-end systems vulnerability."

Making digital connections

It would seem that digital certificates would be an ideal way for SMEs to establish their identities and streamline supply chain processes. So far, however, the use of digital certificates in a supply chain context is not widespread, although they are common in government transactions and in certain industrial sectors. For example, Canada and the European Union have embraced digital certificates as the means of conducting business with the public. The pharmaceutical industry also uses digital certificates to ensure the delivery of drugs to the appropriate party. In the United States, the federal government's D-Trade system for the Department of State requires a digital certificate for electronic submission of forms from exporters. "In the military, digital certificates are in the background of the computer chip cards carried by servicemen and -women," explains David Birch, director of Consult Hyperion, a technology security consulting firm based in Guildford, the UK. "The cards interface with BlackBerries so that soldiers and officers can read their e-mail. The Department of Defense has issued the cards because of the security they provide. In the background are digital certificates providing authentication of parties."

5. What is the single most important step that individual governments and the UN could do to safeguard the global supply chain and ensure that more companies are integrated into it?
(% respondents)



Source: Economist Intelligence Unit survey, 2006

In Mr Birch's view, using digital certificates in a supply chain context has merit if the technology remains in the background, as it does in automated teller machines (ATMs). "People don't want to know what a public key infrastructure is or that they're exchanging these private and public keys," he explains. "What's great about digital certificates is that you can tell users that there are these little fairies in the background taking care of authentication. You can give them a chip card that replaces a magnetic stripe on a card with an actual computer chip, a computer in their pockets. They wave it at a reader at their desk, as does someone else at the other end, and a secure transaction is conducted."

Mr Birch adds that digital certificates cost less than other technologies. "Digital certificates and chip cards were thought to be too expensive, but as the Department of Defense has proved, once standards are in place this actually is among the least expensive means of providing authentication."

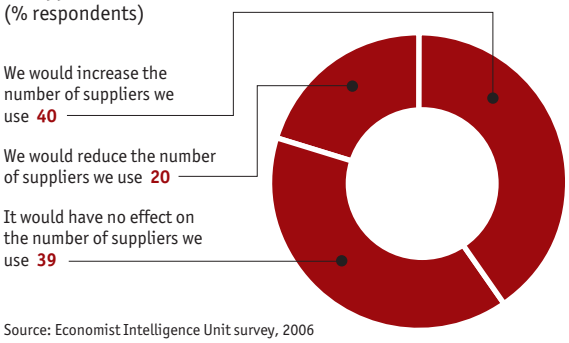
This is good news for SMEs, for whom authentication is critical to attract more customers. Indeed, 33% of our survey respondents believe that designating authentication standards is the most important step that governments and the UN can take to integrate more companies into the global supply chain (see chart 5). An even higher percentage of smaller companies, 38%, adopt this view. Nearly one-third of our respondents accord top priority to integration of government-based authentication standards with similar global procedures. Guidelines for interoperability are another important issue, especially among manufacturers, of whom 29% cite

this as the most crucial step for governments and the UN to take to streamline the supply chain.

The importance of authentication extends to suppliers as well. Our survey indicates that 34% of the manufacturers polled, as well as 40% of SMEs and survey respondents overall, would increase the number of their suppliers if their companies could authenticate the financial stability of their vendors (see chart 6). And given governments' ever-tightening cargo security rules, merchandise needs to be authenticated as well.

"There is no question that the use of digital certificates and other authentication technologies will proliferate, given that there are more and more drivers out there requiring adherence to authentication protocols, particularly in an international context, in terms of tracing the authenticity of goods coming and going," declares Mr Bissmeyer of RosettaNet. His firm, he says, is in the process of signing up trading partners with high-tech companies to require digital certificates for trading documents electronically. Adds Mr Bissmeyer, "Companies want to trace documentation all the way back in the supply chain, from supplier to supplier to manufacturer to the retail shelf, akin to tracing a purchase of sand through to that sand becoming a semiconductor chip in a laptop computer sold in a store. Digital certificates provide the ability to validate the actual movement of goods to determine, for example, if the goods are what they were purported to be. In the pharmaceutical industry, for instance, there is a need to validate that specific drugs sold in a drugstore were indeed produced by Pfizer or Merck and didn't come from somewhere else. Obviously, there is a big economic component to this, cutting out a big grey market."

6. What effect would it have on your procurement practices, if your company were able to authenticate the financial stability of suppliers?
(% respondents)



Source: Economist Intelligence Unit survey, 2006

Case study: Certainty pays

In addition to authenticating counterparty identities for financial transactions and contract non-repudiation, digital certificates provide a way to verify a trading partner's health, safety and environmental record.

Quadrem, an Amsterdam-based global electronic marketplace launched in 2000 by 19 of the largest mining and metals companies around the world, employs digital certificates on its trading platform to provide a secure channel for supply chain data exchange. "When an order flows out of a buyer's system into a supplier's order entry system, the digital certificates manage the orders, authenticating each party's identity for security purposes," explains Brandon Spear, Quadrem's senior vice-president. "But another really interesting use of the technology is in validating that information represented by a trading partner is accurate and not contrived."

Mr Spear believes that as more companies reach out to suppliers in foreign countries, digital certificates will provide a means of vetting the suppliers' performance criteria. "In machine-to-machine transactions, where there is no human interface, trust becomes critical," he says. "A buyer will want to ensure that information presented by a supplier in countries like South Africa, Brazil or Chile is accurate before they choose to do business with that supplier. For example, the buyer might want to know if the supplier has a reliable health and safety record, or a clear policy with respect to environmental issues."

The objective is to validate the accuracy of information presented by suppliers and ensure that this data has not been tampered with. "Organisations like Dun & Bradstreet already collect a lot of this information, but presenting it in a format so the buyer can be absolutely certain that it hasn't been tampered with has been a challenge," Mr Spear admits. "By encapsulating the data in a digital certificate, the information is validated."

In Mr Spear's view, digital certificates provide a service in this area similar to their use in ensuring the validity and non-repudiation of purchase orders, shipment notices and invoices. "In both cases, the certificates obviate concerns over fraudulent data," he says. Quadrem is embarking on the use of digital certificates in this context this year.

The missing link

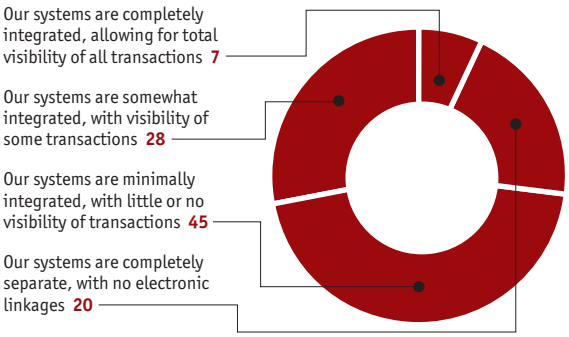
This is all very well, but what about funds to invest in the necessary technology? Typically, single-factor authentication software resides within supply chain management or procurement applications—which few small companies can afford—and even inexpensive solutions require an automated infrastructure. In addition, few of the leading suppliers of supply chain execution systems include sophisticated authentication software. "Most providers of supply chain execution software follow fairly rudimentary encryption protocol," says Ian Hobkirk, director of the supply chain consulting group at Beacon Systems, a logistics and systems consultancy based in Tewksbury, Massachusetts. "The only transactions that are really encrypted are credit card or other financial transactions, and these use 128-bit SSL (Secure Sockets Layer) encryption. For data that is sent over a wireless network, basic WEP encryption is still the standard most companies follow." WEP, or wired equivalent privacy, a protocol that encrypts data over radio waves, does not offer total security. Even with encryption, the parties to the transaction are still unable to authenticate the identity of the originator or receiver.

Our research indicates that despite the clear benefits of supply chain automation, many SMEs have not made the necessary investments to automate their transactions with customers and suppliers. Indeed, 46% of overall respondents in our survey cite suppliers' reluctance to "go paperless" as the chief impediment to an automated supply chain, with 51% of manufacturers pointing to this problem (see chart 1, p. 3). While 62% of overall respondents cite the "high cost of paperless supply chain software, training and support" as a major obstacle to automation, 69% of manufacturers hold this opinion (see chart 7). Electronic linkage is

7. What do you consider to be the greatest impediments to the implementation of a fully automated global supply chain for your company?
Select 3 options (% respondents)

Source: Economist Intelligence Unit survey, 2006

8. Which of the following statements best describes the level of integration between your organisation's procurement system and that of its suppliers?
(% respondents)



Source: Economist Intelligence Unit survey, 2006

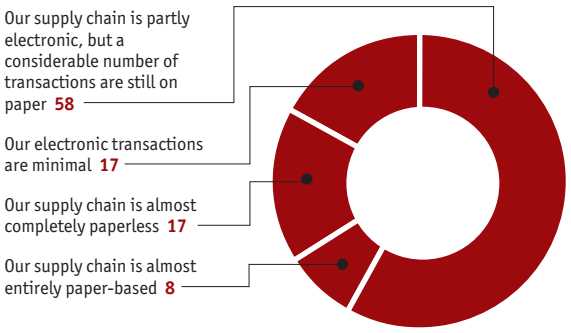
remarkably low: 45% of the respondents, and 51% of manufacturers, report that their systems are "minimally integrated" with their suppliers'; 26% of manufacturers say their systems are "completely separate". And compared with 17% of the respondents overall, 31% of manufacturers say their electronic supply chain transactions are "minimal" (see charts 8 and 9).

High cost is a common refrain. In Aberdeen Group's survey, for instance, 75% of respondents say they are discouraged from automating by the high cost of technology and related resources. "The top challenges are to get the IT resources and money to electronically connect with partners and maintain those connections," says Aberdeen analyst Beth Enslow. Often, trade-offs between costs and benefits are involved. Digital certificates, for example, require a PKI infrastructure that can be difficult and expensive to implement, points out Ms Kussmaul of America's Growth Capital, but "they have a very low incremental cost and can be deployed easily and inexpensively when leveraging already established PKIs." Tokens require only a moderate back-end infrastructure but carry a high per-unit cost; biometric readers offer great convenience but are expensive to install.

Economist Intelligence Unit survey respondents point to "cost and labour efficiencies via order management automation" as the primary benefits of automating the global supply chain, with 62% of total respondents offering this opinion, and 64% of companies under US$500m a year in revenue citing it. Other benefits cited by both large companies and small companies include immediate notification of problems and exceptions, integration with other supply chains, improved tracking of supplier performance and contract compliance, and greater speed to market (see chart 10).

Several executives interviewed for our survey emphasise the advantages of automation. For Bill Ferko, vice-president and CFO of Genlyte Group, a manufacturer of lighting fixtures based in Louisville, Kentucky that posted US$1.2bn in 2005 revenue, supply chain automation has brought the benefits of aggregating the company's spending and increasing its visibility into the costs of materials, components and commodities across vendors. "We have been able to identify substantial opportunities for cost reductions, where we can negotiate purchase agreements with

9. To what extent is your organisation's end-to-end supply chain paperless ie, managed electronically?
(% respondents)



Source: Economist Intelligence Unit survey, 2006

10. What do you consider to be the greatest advantages of automating your company's global supply chain?
Select 3 options (% respondents)

Source: Economist Intelligence Unit survey, 2006

suppliers who want to partner with us at a more efficient level," says Mr Ferko. "We have also improved our advance planning, and are more able to give a promise to our customers of product availability."

Colin Campbell, vice-president of purchasing and inventory management at Newark InOne, a distributor of electronic components and test equipment to the aerospace and defence industries, says that making the move to automated transactions has reduced order processing errors and assisted the company's sales efforts. "We would receive an order from a customer and then issue and fax a purchase order to a vendor that was not automated with us," he explains. "We'd make visible to our sales force all the information available on the purchase order, so they knew when the product was coming in to secure the order with the customer. We'd then learn too late that the vendor either didn't receive the fax or lost it. It was an embarrassing situation when the vendor says it never received the fax, and even worse for us from an investment management standpoint."

SMEs will soon have no choice but to make these sorts of embarrassments disappear quickly, warns Dwight Klappich, vice-president at Gartner, a technology research firm. "Large enterprises are tired of inaccuracies and slowdowns because their SME suppliers have little or no technology," he says. "A lot of SMEs have their heads in the sand if they think they can continue to do things the way they have. SMEs used to compete on flexibility and cost, but now that big companies are automating their supply chains, becoming more flexible and lowering their costs, small companies will need to follow suit or be left in the dust."

Reversing gears

On the bright side, once SMEs get over the authentication hurdle, they have access to innovative financing methods for supply chain automation. Several organisations seek to create reverse-factoring opportunities for small enterprises, enabling them to accelerate cash flow to provide liquidity for investments in supply chain technology. "SMEs' credit situation makes it difficult for them to borrow funds from a bank to invest in automation, and many are forced to fund their liquidity in accordance with their purchasers' accounts-payable cycle," explains Mr Sculley of IdenTrust. "When Basel II came in, it started to shut down the oxygen for SMEs since it was skewed to getting capital to more creditworthy larger companies. The only way small companies could get working capital was to sell their receivables at an extremely high cost to them, anywhere from 25% to 40% per annum, a huge discount. Plus they had to pay

Setting up standards of trade

For SMEs and their suppliers, the high cost of technology is exacerbated by the lack of a widely accepted international electronic information standards governing the financial supply chain. "For small suppliers, there are just too many options—EDI, XML, Internet applications, RosettaNet, and a host of different methodologies and mechanisms for connectivity between organisations," says James Wetekemp, vice-president of product management at Verticalnet Inc., a supply chain management solutions provider based in Malvern, Pennsylvania. "It can cost upwards of US$40,000 to plug into an EDI system. Buyers have a hard time forcing this on the supplier. The solution is a standard mechanism for communications protocols, rather than many standards."

Several organisations have made some headway towards creating such standards. RosettaNet, based in Lawrenceville, New Jersey, develops universal standards for the global supply chain, and implements and certifies adoption of these standards, ensuring that one set of governance rules applies worldwide. The Transaction Workflow Innovation Standards Team (TWIST), a not-for-profit group, has created standards for more efficient transactions with financing partners. "There are no comprehensive and internally consistent open standards now, which is why automating the supply chain is so costly," responds Tom Buschman, TWIST's chairman and CEO.

Mr Buschman explains that most operational treasury activities, such as foreign-exchange execution, payment processing, supply chain financing and credit management, are traditionally delivered via bespoke solutions from individual banks. "Corporate treasurers are forced to wait for their relationship banks to offer the services they need to execute core activities more efficiently ... in a supply chain context. With the trend towards treasury centralisation, they have inherited a myriad of different proprietary solutions to work with and support. Yet, many corporat[ion]s are stubbornly insistent on multi-bank delivery of core treasury services, and there is a growing dialogue between the major banks to facilitate this."

TWIST has developed non-proprietary XML payment standards that are harmonised with the bank-owned SWIFT network. In addition, it has created a set of working capital management standards, with the goal of providing automatic reconciliation services, electronic invoicing and supply chain financing to companies. Mr Buschman sums up: "XML makes it much easier for unambiguous communication and rapid connectivity to multiple parties, and using these standards over the Web is a far less costly option than EDI, which most small companies cannot afford."

accountants and lawyers along the way."

Traditional factoring is no help to companies engaged in crossborder transactions because it is done on a country-by-country basis, he adds, noting that there is "no payment scheme for crossborder transactions".

Tom Cox, president of Cox Business Consulting, based in Portland, Oregon, believes that reverse factoring offers huge benefits to small businesses. "Clearly one of the key challenges to SMEs wanting to break into the electronic supply chain is cash flow. It's killed more businesses than every other cost combined. If a company could get 97 cents on the dollar for a product that arrived at the buyer's shop today, it is a worthwhile discounted pre-payment. It will do much to accelerate the cash-to-cash cycle and help a lot of companies invest in the technology to go paperless and thrive."

E2open is also a reverse-factoring champion. "Currently, suppliers must fund their liquidity in accordance with the purchaser's accounts-payable cycle," says Mr Martinelli. "By leveraging the high credit rating of a purchaser, you can provide a meaningfully lower cost of funds that enables the supplier to accelerate its cash flow, providing cost-effective liquidity for further growth. Buyers also benefit by increasing their cash position through the extension of payment terms, and reducing accounts-payables processing costs through staff reduction and costly paper check payments. At the same time, the buyer improves suppliers' stability by assisting them to obtain cost-effective liquidity without burdening its own balance sheet."

Conclusion

Economist Intelligence Unit survey respondents and interviewees indicate that investment in authentication software can put SMEs within reach of financing to invest in an automated supply chain. Much progress has already been realised, and numerous private and public sector organisations are guiding more robust implementation of automated solutions. Yet SMEs continue to resist automation because of the perceived high cost and maintenance of the technology involved.

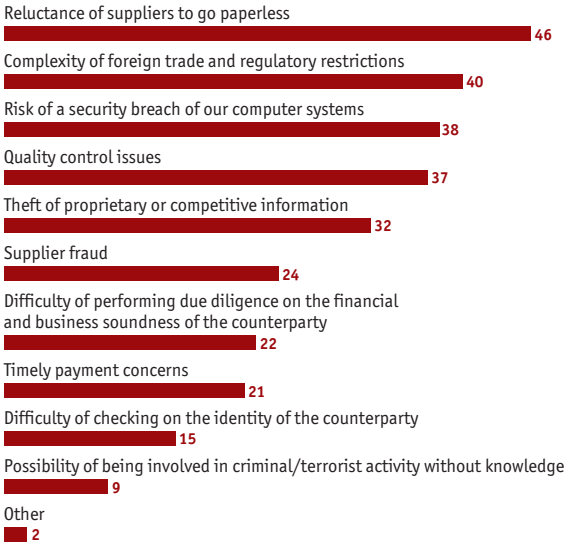
These problems can be solved, however. Offering particular hope are the various identity authentication technologies, notably digital certificates, which are rapidly moving from largely financial environments to supply chain operations, and which offer the promise of swift creditworthiness and access to financing. A particularly intriguing financing method is reverse factoring, which seeks to provide SMEs with more routine cash flow to invest in supply chain technology and growth.

Appendix: Survey results

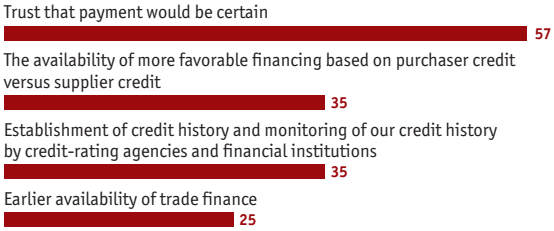
In May and June 2006, the Economist Intelligence Unit conducted an online survey of 127 executives from Europe, the Americas and the Asia-Pacific region. Our sincere thanks go to all who took part in the survey.

Please note that not all answers add up to 100%, because of rounding or because respondents were able to provide multiple answers to some questions.

1. What do you consider to be the greatest risks of automating your company's global supply chain?
Select 3 options (% respondents)

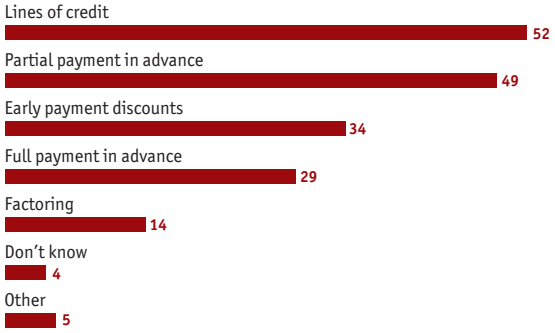


2. What would help your company to integrate its operations with the global supply chain?
Select all that apply (% respondents)

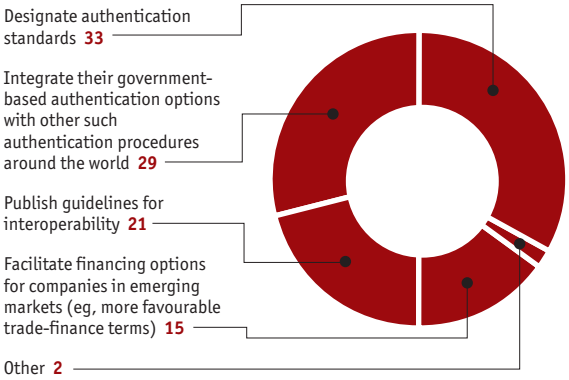


3. Does your organisation currently review supply chain vulnerability in the following areas or does it plan to do so in the next three years?
Select 3 options (% respondents)

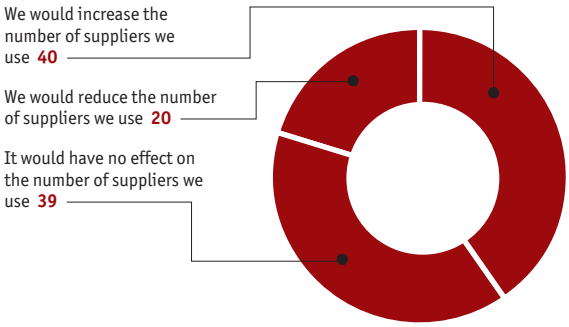
4. Which of the following payment methods does your company use?
Select all that apply (% respondents)



5. What is the single most important step that individual governments and the UN could do to safeguard the global supply chain and ensure that more companies are integrated into it?
(% respondents)

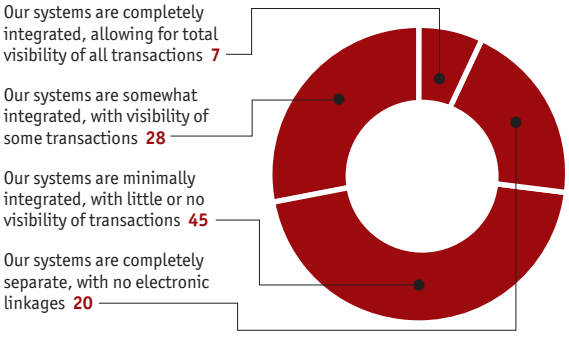


6. What effect would it have on your procurement practices, if your company were able to authenticate the financial stability of suppliers?
(% respondents)

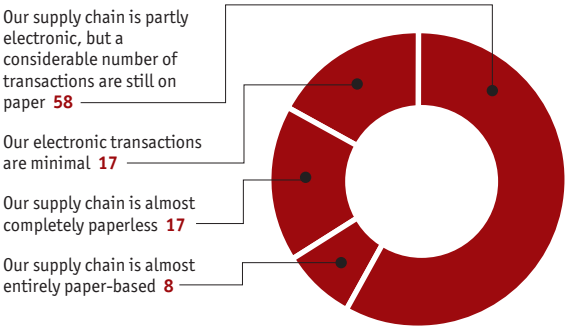


7. What do you consider to be the greatest impediments to the implementation of a fully automated global supply chain for your company?
Select 3 options (% respondents)

8. Which of the following statements best describes the level of integration between your organisation's procurement system and that of its suppliers?
(% respondents)

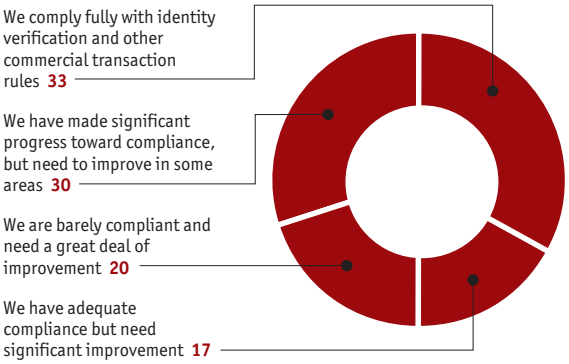


9. To what extent is your organisation's end-to-end supply chain paperless ie, managed electronically?
(% respondents)

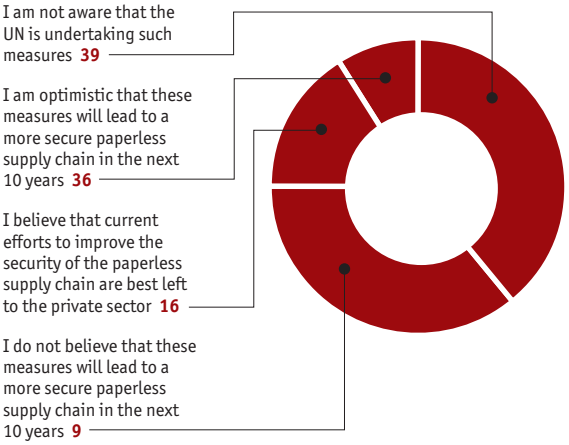


10. What do you consider to be the greatest advantages of automating your company's global supply chain?
Select 3 options (% respondents)

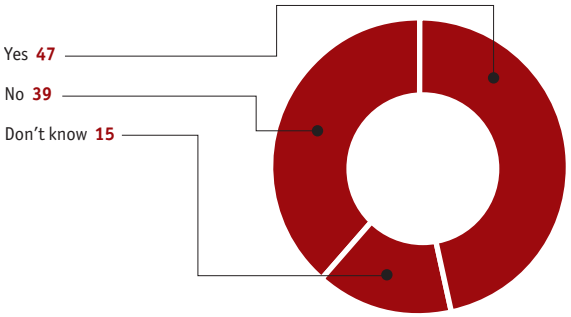
11. Which of the following statements best describes your organisation's level of compliance with regulations governing the global supply chain such as account authentication rules?
(% respondents)



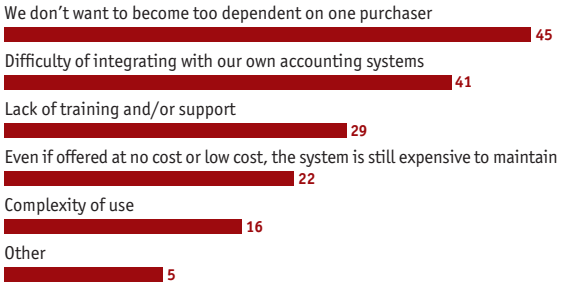
12. What is your opinion of efforts by the United Nations to standardise trade documents and to encourage governments to digitise the commercial forms completed by companies?
(% respondents)



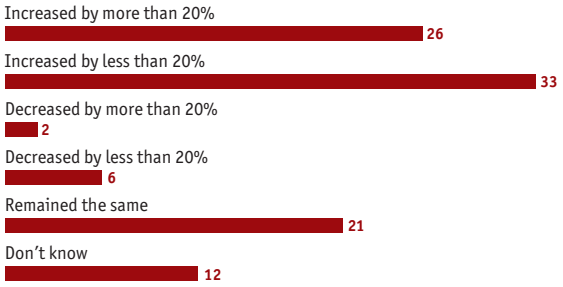
13. Does your company use any automated procurement systems offered by your purchasers?
(% respondents)



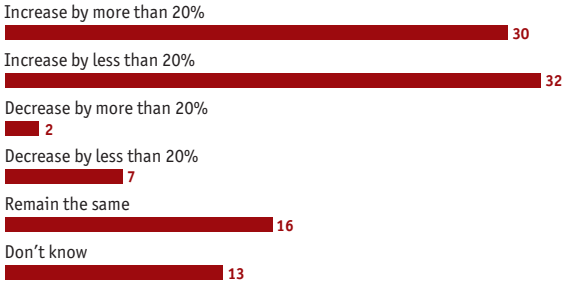
14. If not, why not?
Select all that apply (% respondents)



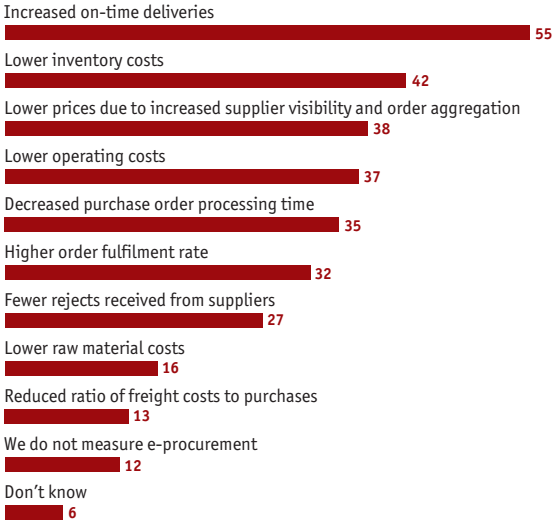
15. How has the number of your organisation's global suppliers changed in the past three years?
(% respondents)



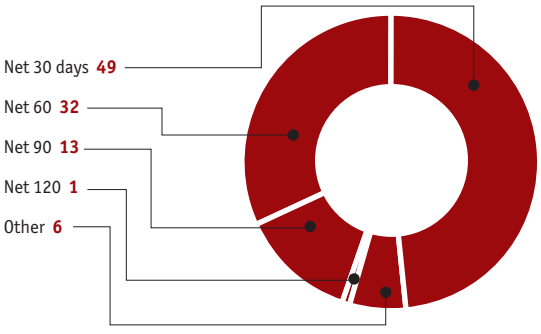
16. How is the number of your organisation's global suppliers likely to change in the next three years?
(% respondents)



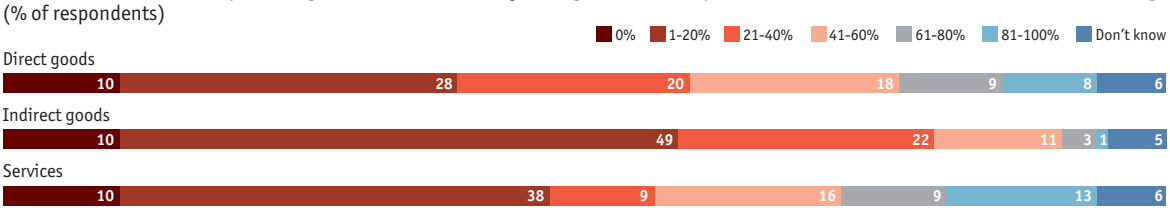
17. Which of the following measures does your organisation use to evaluate the success of its e-procurement efforts?
Select all that apply (% respondents)



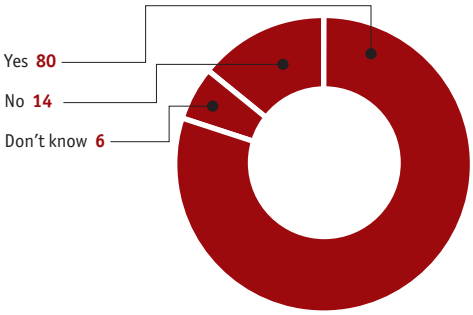
18. What are your company's payment terms?
(% respondents)



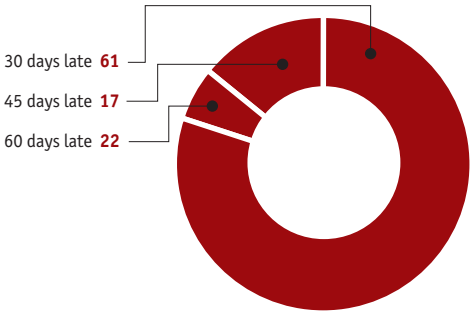
19. Please estimate what percentage of the total value of your organisation's e-procurement activities are focused on the following:
(% of respondents)



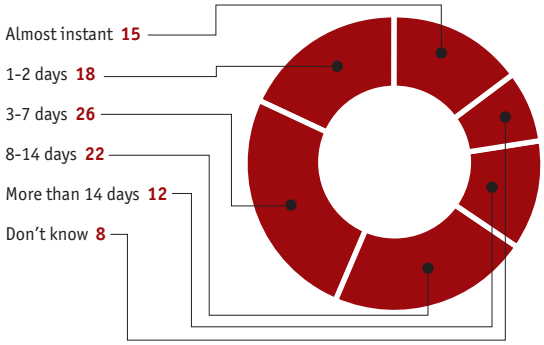
20. Does your company regularly pay on time?
(% respondents)



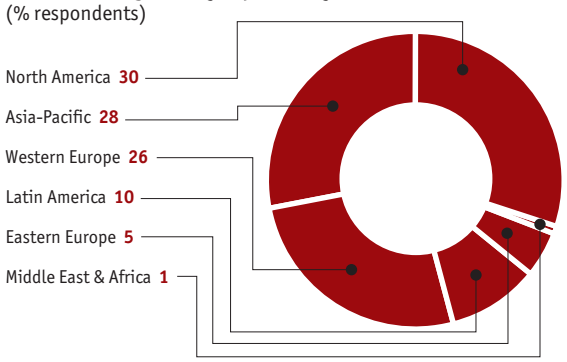
21. If not, what is your usual payment pattern?
(% respondents)



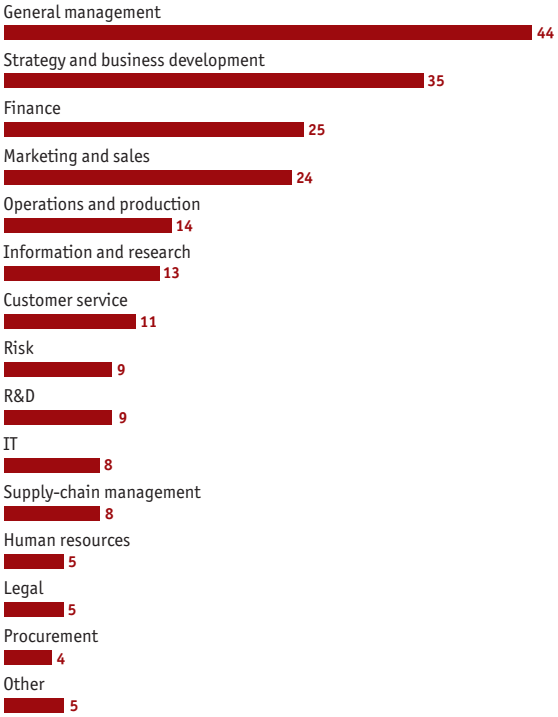
22. What is your company's average time for approval of payments to suppliers?
(% respondents)



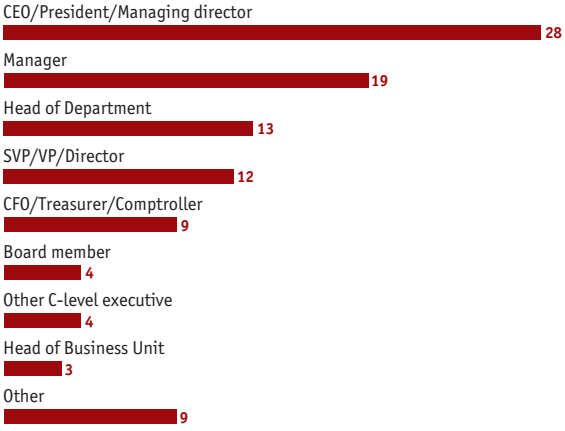
23. In which region are you personally based?
(% respondents)



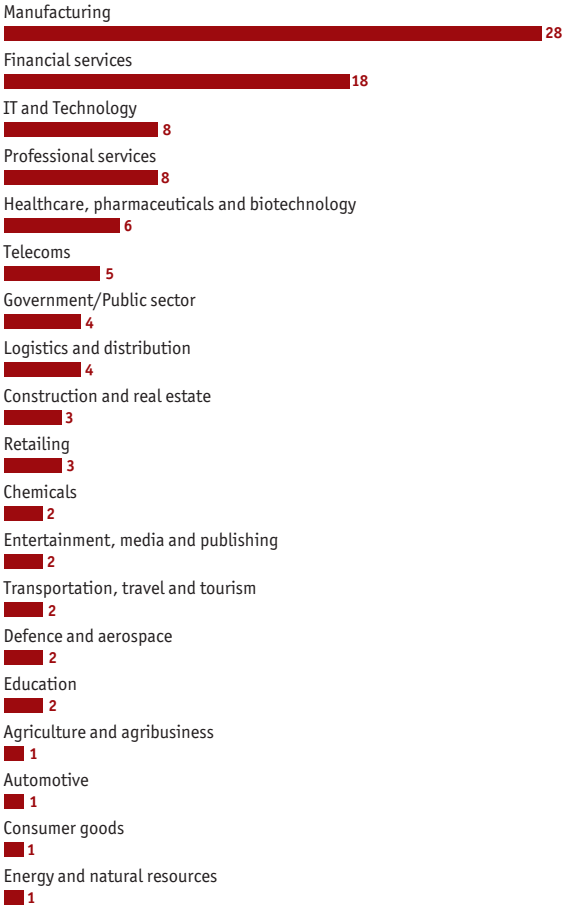
24. What are your main functional roles?
Please choose no more than three functions.
(% respondents)



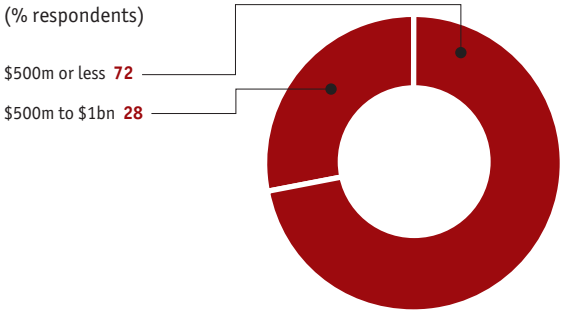
25. Which of the following best describes your title?
(% respondents)



26. What is your primary industry?
(% respondents)



27. What are your organisation's global annual revenues in US dollars?
(% respondents)



LONDON
26 Red Lion Square
London
WC1R 4HQ
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8476
E-mail: london@eiu.com

NEW YORK
111 West 57th Street
New York
NY 10019
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
E-mail: newyork@eiu.com

HONG KONG
6001, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com