Economist Intelligence Unit

The Economist

Digital identity authentication in e-commerce

An Economist Intelligence Unit executive summary sponsored by IdenTrust

Preface

Digital identity authentication in e-commerce is an Economist Intelligence Unit report, sponsored by IdenTrust. The Economist Intelligence Unit bears sole responsibility for this report. The Economist Intelligence Unit's editorial team executed the survey and wrote the report. The findings and views expressed in this report do not necessarily reflect the views of the sponsor. Jackie Wiles was the author of the report and Rama Ramaswami was the editor. Richard Zoehrer was responsible for layout and design.

Our research drew on a global online survey in January 2007 of 246 senior executives. Our thanks are due to all survey respondents for their time and insights.

March 2007

Introduction

Driven by the inexorable forces of globalisation, leading companies of all sizes now complete business communications and transactions electronically, both across and within borders. Such digital exchanges can generate huge benefits for counterparties, but they also create a new breed of challenges and risks related to authenticating and certifying business partners and transactions.

Companies need to distinguish trusted counterparties in the ether of cyberspace—and they need to be recognised as trusted parties themselves. The imperative is both strategic and legal. In business terms, time wasted on authenticating transactions creates costs, delays receipts and undermines attempts to optimise the deployment of capital. In legal terms, companies risk recourse for failing to authenticate counterparties, and there is a risk that their corporate identity could be stolen and used fraudulently. Notably, some transactions, including certain government dealings, even demand anonymity and privacy at the very same time that documents and counterparties must be authenticated.

This survey of 246 senior executives, conducted by the Economist Intelligence Unit on behalf of IdenTrust, sheds light on the digital authentication approaches that businesses are using today, and explores how they would like to better secure and facilitate their electronic dealings.

About our survey

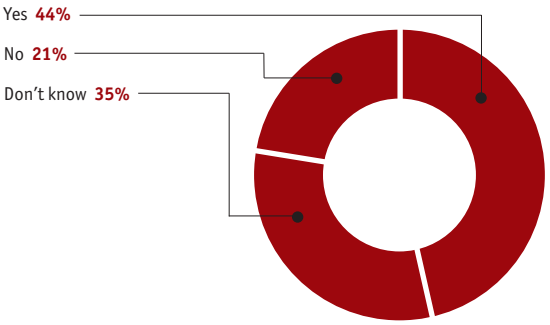
In January 2007 the Economist Intelligence Unit queried 246 executives on their digital identity authentication practices. Approximately 24% replied from western and eastern Europe, 38% from the Americas and 38% from the Asia-Pacific region and other parts of the world. Respondents represented a wide range of industries and functions. About 50% of the respondents were C-level executives or board members. Companies with less than US$500m in annual revenues represented 47% of the group; those with revenues of between US$500m and US$5bn, 31%; and those with revenues of more than US$5bn, 22%.

Identity authentication critical to business growth

The key survey findings are discussed below. In most cases, the responses by peer group (industry, region, company size) do not vary greatly from the aggregate results. However, we have highlighted some noteworthy divergences.

Most companies now see identity authentication strategy as critical, and many see identity authentication as a driver of business growth. About 45% of respondents say more effective identity authentication would enable their business to grow more rapidly over the next three years (see chart 4). Indeed, 67%

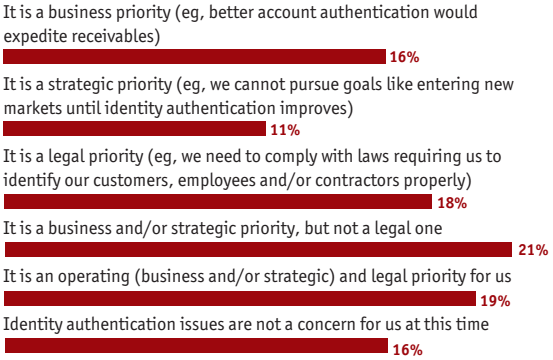
4. If identity authentication were more effective, would that enable your business to grow more rapidly over the next three years?



say it is currently a priority for their organisation to address issues of identity authentication because better identity authentication can deliver business benefits (eg, expediting receipts) as well as strategic benefits (eg, facilitating entry into new markets). Another 18% say it is a priority primarily for legal reasons—for example, compliance with laws demanding that they properly identify customers, employees and/or contractors (see chart 1).

- Nearly one-third of financial services companies, more than average, say they need to tackle identity authentication primarily for legal reasons.
- Fully 91% of IT and technology companies (far more than average) say it is a priority to address identity authentication, and 80% say that this is for business/strategy reasons.
- Fifty-five percent of the respondents from Asia (more than average) believe that more effective identity authentication would enable their business to grow more rapidly.

1. Is it currently a business, strategic or legal priority for your organisation to address issues of identity authentication?
Select the one statement that is closest to your circumstances.
(% respondents)



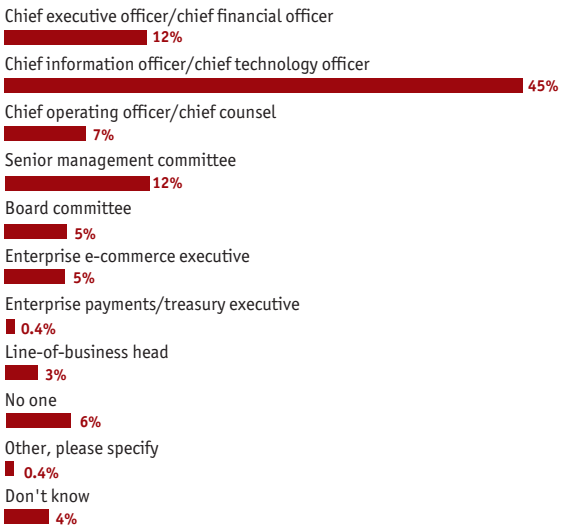
Source: Economist Intelligence Unit survey

Senior management usually steers identity management strategy. Identity management is squarely on the radar at the most senior levels in today's corporations. Governance of identity authentication strategies is usually a brief for the executive management team: 76% of respondents say a senior executive or executive-management team is chiefly responsible. Most often, however (45%), the chief information or technology officer (CIO or CTO) gets charged with the task (see chart 3, p. 6).

Global business will become ever more complex in the next three years, with more suppliers, more customers, and more digital payments. Many companies (56%) expect to be using more suppliers in the next three years, and 20% expect the number to be up by more than 20%. At the same time, 75% expect to be dealing with more customers, and 39% expect the customer population to increase by more than 20%. Companies also expect electronic payments to rise significantly from today's levels. For example, 31% of companies expect more than 75% of all receivables to be arriving electronically in three years, and 38% expect to be settling more than 75% of payables electronically (see charts 5,7,9, and 10 on p. 7).

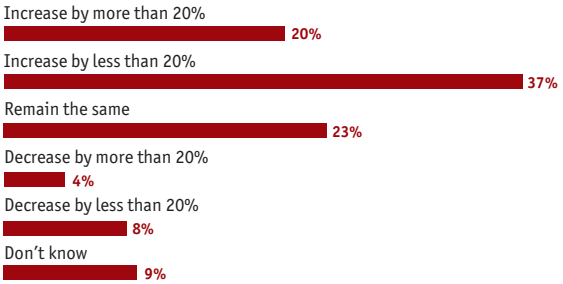
E-commerce risks are not solely about monetary loss. Of all respondents, 57% say the potential monetary loss from fraudulent transactions is one of the major e-commerce security threats facing their company today, but even more (59%) say they fear the unauthorised use of proprietary or competi-

3. Who is chiefly responsible in your company for shaping the identity authentication strategy?
(% respondents)



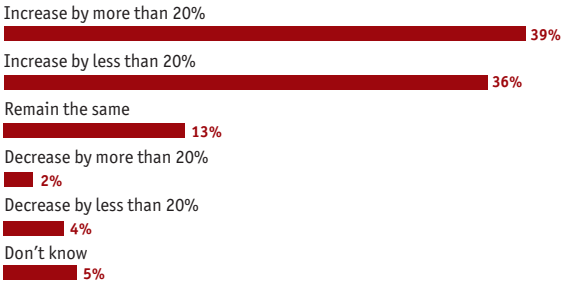
Source: Economist Intelligence Unit survey

5. What increase or decrease do you expect in the next three years in the number of suppliers your company uses??
(% respondents)



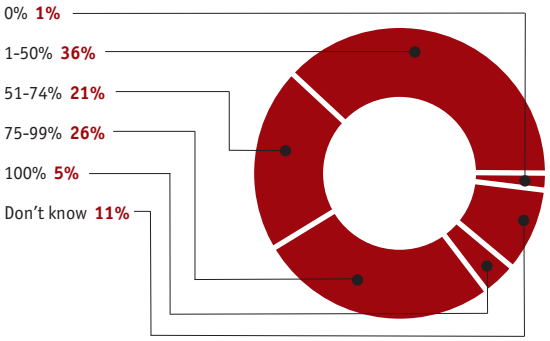
Source: Economist Intelligence Unit survey

7. How do you expect your customer population to change in the next three years?
(% respondents)

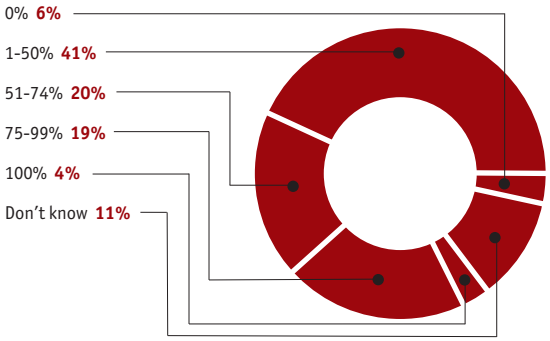


Source: Economist Intelligence Unit survey

9. Approximately what percentage of your company's receivables do you expect to arrive electronically in three years?



10. Approximately what percentage of your company's payables is currently settled electronically?



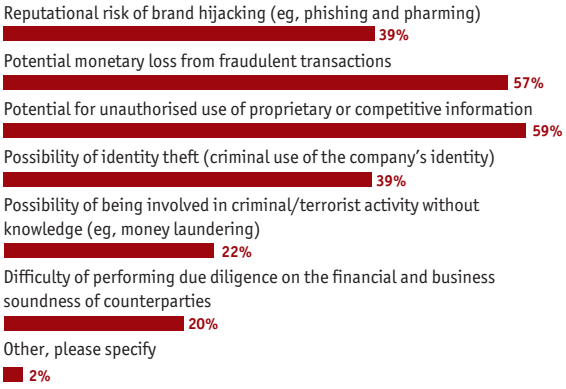
tive information, and a substantial number (39%) are concerned about the reputational risk of brand hijacking, as occurs in "phishing" and "pharming" attacks[1] (see chart 2).

- IT and technology companies are the most concerned about the reputational risk of brand hijacking, with 51% saying malicious attacks are a major e-commerce concern.

Many companies use Internet-based digital certificates for transactions and communications, including government interactions. Nearly one-half of all respondents already use Internet-based digital certificates for e-commerce transactions or communications. The certificates are also used for a variety of interactions with local or national government agencies. For example, 48% of companies use digital certificates in filing their corporate taxes electronically, and 44% use them to file sales taxes (eg, value-added tax). Major reasons that non-users give for shunning the certificates include government restrictions on usage and the failure of certificates to interact with corporate systems (see chart 12 and charts 14 and 16 on p. 8).

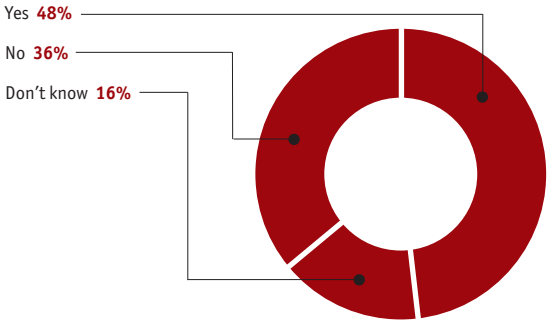
[1] "Phishing" is the act of sending an e-mail to a user pretending to be a legitimate enterprise in order to scam the user into surrendering private information. "Pharming" seeks to obtain personal information through domain spoofing, or directing users to a fake Web site.

2. What are the greatest e-commerce security threats your company faces today?
Select up to three responses.
(% respondents)



Source: Economist Intelligence Unit survey

12. Does your company currently employ Internet-based digital certificates for e-commerce (communications or transactions)?



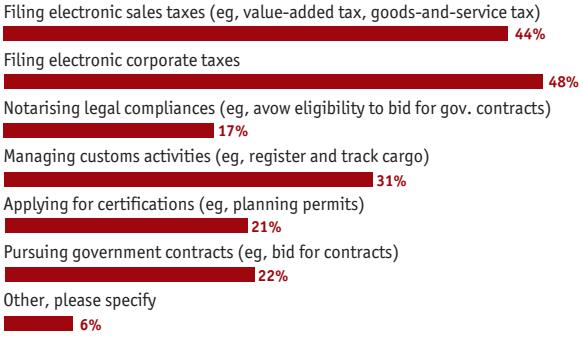
- More than half of non-users have annual revenues of $1 billion or less.
- Among the few companies with more than $10 billion in annual revenues that do not use digital certificates, 31% say the single biggest reason is that they want one globally accepted certificate, while 25% cite government restrictions on certificate usage.

Overall, users seem happy with the security that certificates provide, but satisfaction varies by segment. Private providers and banks are most often (among 65% of respondents) the certifying authority for Internet-based digital certificates used by companies

today, and 49% of users say they are satisfied with the security these certificates provide (see chart 12).

- Financial services providers are most satisfied (64% are either satisfied or very satisfied) with the security digital certificates provide, and hardly any say they are actually dissatisfied. Slightly more than average (48% vs. 41% overall) use certificates endorsed by a private provider.
- Manufacturing companies are even more likely to use a private-provider certificate (57%), but fewer are satisfied (35%).
- In Asia, more companies use digital certificates backed by public authorities (free services) and governments than is the case in other regions, but private providers and banks still account for about half of the certificates used by those in the region.
- Overall, satisfaction levels are about equal whether certificates are issued by a bank or a private provider, but more users of private certificates are highly satisfied (17% vs. 8% of bank-certificate users).

14. For which of the following interactions with local or national government agencies does your company currently employ Internet-based digital certificates? Select all that apply.
(% respondents)



Source: Economist Intelligence Unit survey

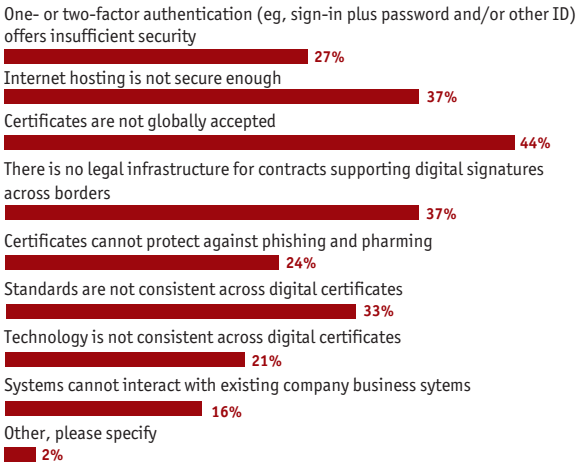
16. If you do not use Internet-based digital certificates, what is the single biggest reason?
(% respondents)

Source: Economist Intelligence Unit survey

Criticism of Internet-based digital certificates is rife, even among users, especially as certificates are not widely fungible. Both users and non-users cite a variety of problems with existing certificates, many related to the inability of certificates to function beyond certain boundaries. The biggest disadvantage, say 44% of respondents, is that the certificates are not globally accepted; 37% say Internet hosting is not secure enough (see chart 17).

- The complaints about bank-issued certificates are most often that Internet hosting is not secure enough (46%), there is no legal infrastructure for contracts supporting digital signatures across borders (44%), and certificates are not globally accepted (41%).

17. What do you see as the biggest disadvantages with existing Internet-based digital certificates (whether you currently use them or not)? Select up to three responses.
(% respondents)



Source: Economist Intelligence Unit survey

- The complaints about certificates backed by a private provider are similar: They are not globally accepted (42%), there is no legal infrastructure for contracts supporting digital signatures across borders (42%), and Internet hosting is not secure enough (33%).

The ideal identity trust infrastructure would feature global, multi-party acceptance, thus enabling global interoperability and reducing fraud risk. When asked to define the characteristics and benefits of a best-practice identity trust infrastructure, companies most often say digital signatures and credentials should be legally binding around the world (43%), should be able to guarantee multi-party, multi-bank transactions across borders (40%), and should provide a seamless experience for the user (30%). The business benefits, respondents most often say, would be less risk of fraudulent activities (57%), the creation of a single identity with global interoperability (46%), and consistent identity management across the enterprise (36%).

Strategic implications

The survey results reveal several business realities that companies need to understand, and imperatives they must act on, as they formulate and execute their identity authentication strategy. These include the following:

- **A sound identity authentication strategy is essential to support global business growth.** As the global network of suppliers, customers and payments becomes ever more complex, companies must be able to verify who they are dealing with—and be able to grant or deny them appropriate access to information and assets. It is therefore a strategic imperative for companies to design and execute a digital-authentication strategy. Those that discount authentication as an IT strategy, or wait for authentication standards and norms to reach best practice, will be at a competitive disadvantage.

- **Companies need identity authentication mechanisms that protect them properly against malicious use, not just monetary loss.** Companies are rightly concerned about the gamut of risks associated with identity authentication, from phishing and pharming to monetary fraud. Identity authentication strategy must look beyond the potential monetary loss from payments transactions and make sure the company's reputation, data, and other intellectual property and assets are also protected.

- **Firms must not underestimate the reputational risks of improper authentication management.** Hackers that manage to fraudulently portray themselves as a company can defame that company and steal usernames, passwords, credit card information and other personal information about its customers. While the intent of these thieves may actually be just to defraud the company's customers, irreparable harm will have been done to the reputation of the company itself, whether the hackers are successful in their end-game or not. Companies must therefore be proactive in protecting themselves against such breaches of corporate security. If they do not take

this threat seriously, their business—not to mention share price—is likely to suffer in the long term.

● **Effective identity authentication can eliminate redundancy, reduce human intervention and cut costs.** Proper digital authentication can reduce cycle times and make transactions more seamless by, for example, minimising the number of credentials that must be presented or authenticated for account opening or changes, and enabling a single credential for identity authentication across banks. At the same time, digital authentication can deliver cash management benefits. Corporate payables are already more electronic (and therefore usually faster and more seamless) than receivables, so companies could suffer a negative cash-management impact unless they improve digital authentication to facilitate cash flows, especially as the electronic-payment trend becomes more marked in the future.

E-commerce is fraught with liability risks for companies that cannot authenticate the identity of counterparties.

● **Identity authentication enables companies to better exploit market opportunities.** E-commerce is fraught with liability risks for companies that cannot authenticate the identity of counterparties. As a result, companies tend to limit their dealings to parties they already know to protect themselves. In the process, however, they are potentially missing out on opportunities to profitably expand their pool of suppliers and customers. Proper digital authentication will allow companies to trawl safely throughout the entirety of cyberspace to optimise their dealings, whether they are issuing requests for proposals, buying raw materials or selling into a new region.

● **Companies should look to existing trusted advisors for identity authentication support.** Outsourcing the mechanics of identity authentication is a viable (and preferable) option, given the capabilities and expenditures involved, but proper due diligence of providers is critical. More and more potential providers are likely to emerge as identity authentication matures, but companies must always aim to maintain proper control of security and minimise their liability risks. Companies are well advised to look first at existing providers that have a track record of trustworthiness and a formal and publicly verifiable set of controls.

● **Banks are a natural partner in authentication strategies.** Banks already provide authentication and guarantees to companies along the financial supply chain, and may be able (and can be urged by companies) to do the same along the physical supply chain. Around the world, banks must already authenticate identities, and verify fund flows, to meet various laws, such as those targeting money-laundering and terrorism. Banks can similarly endorse e-commerce activities, issuing digital certificates to validate identities and providing non-repudiation, or verifying the authenticity of the origin and delivery points in a transaction so that neither party can disavow their participation. In this way, banks assume the liability associated with e-commerce risk from participating companies, a process in keeping with their traditional role of assuming and managing risk. Furthermore, banks already collect most of the customer information they need to provide digital authentication, and unlike most non-bank authenticators, they are legally bound to collect, house and protect that data responsibly.

● Whatever the provider, companies looking for digital-identity authentication solutions should expect providers to commit to the following:

(1) Understand and manage the challenges of authentication across borders, and in governmental interactions.

(2) Provide a clear set of operational standards today, and commit to continually pursue global interoperability and multi-party acceptance in the future.

(3) Explicitly guarantee to:

- validate counterparties properly;
- provide protection if transactions go astray or awry;
- protect corporate data;
- offer non-repudiation; and
- provide legally enforceable contracts in all participating countries.

Conclusion

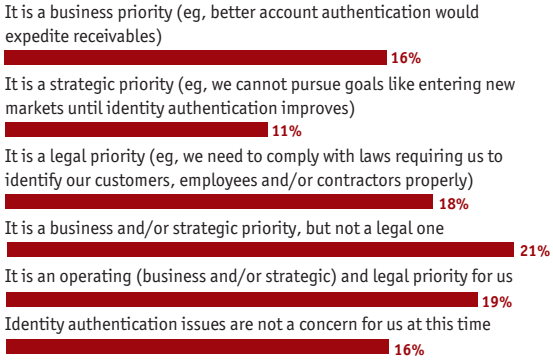
Digital authentication, while nascent, is a critical issue facing all companies today. The immediate focus for most is on managing the mechanics of digital authentication, especially across borders. However, companies must start to think strategically about positioning themselves to capture the potential business benefits of secure authentication. Those that take a wait-and-see attitude will soon find themselves at a competitive disadvantage.

Appendix: **Survey results**

In January 2007, the Economist Intelligence Unit conducted an online survey of 246 executives from Europe, the Americas and the Asia-Pacific region. Our sincere thanks go to all who took part in the survey.

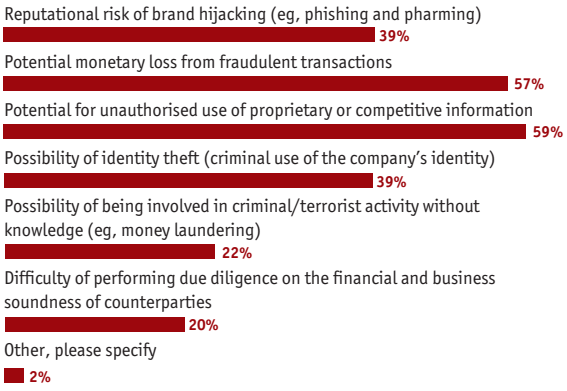
Please note that not all answers add up to 100%, because of rounding or because respondents were able to provide multiple answers to some questions.

1. Is it currently a business, strategic or legal priority for your organisation to address issues of identity authentication?
Select the one statement that is closest to your circumstances.
(% respondents)



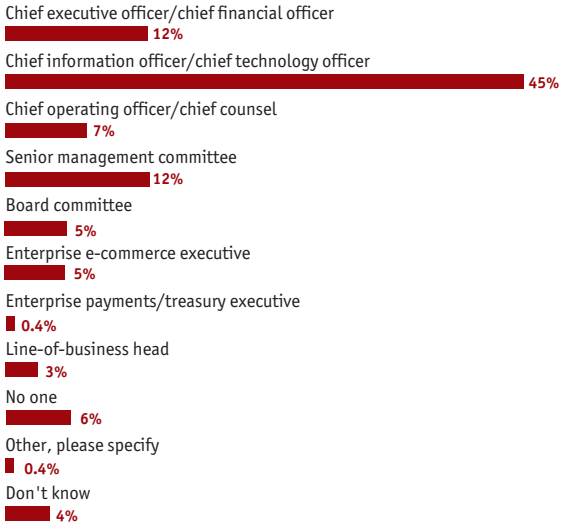
Source: Economist Intelligence Unit survey

2. What are the greatest e-commerce security threats your company faces today?
Select up to three responses.
(% respondents)



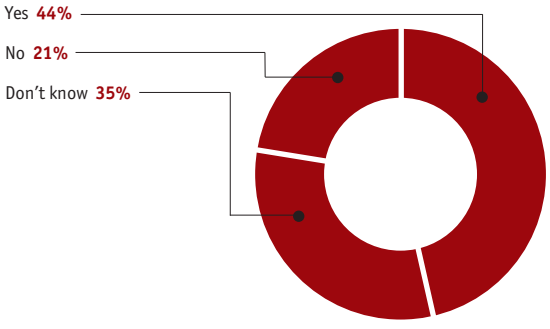
Source: Economist Intelligence Unit survey

3. Who is chiefly responsible in your company for shaping the identity authentication strategy?
(% respondents)

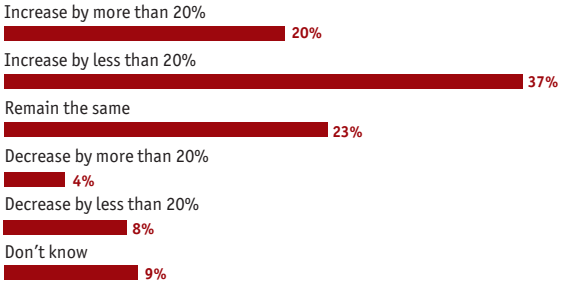


Source: Economist Intelligence Unit survey

4. If identity authentication were more effective, would that enable your business to grow more rapidly over the next three years?

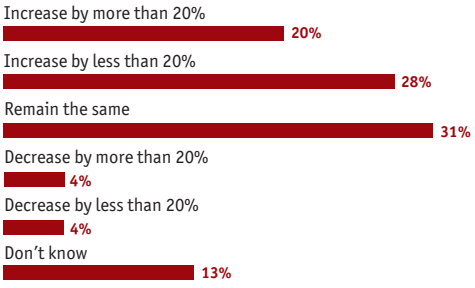


5. What increase or decrease do you expect in the next three years in the number of suppliers your company uses??
(% respondents)



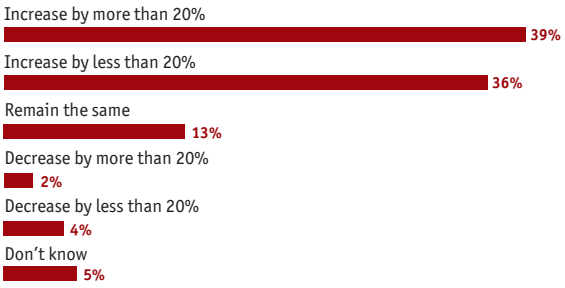
Source: Economist Intelligence Unit survey

6. If identity authentication were more effective, how would you expect the number of your organisation's global suppliers to change in the next three years?
(% respondents)



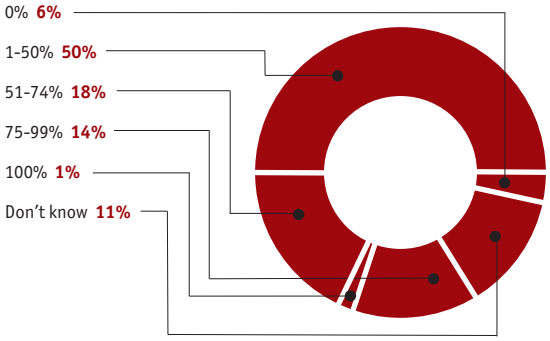
Source: Economist Intelligence Unit survey

7. How do you expect your customer population to change in the next three years?
(% respondents)

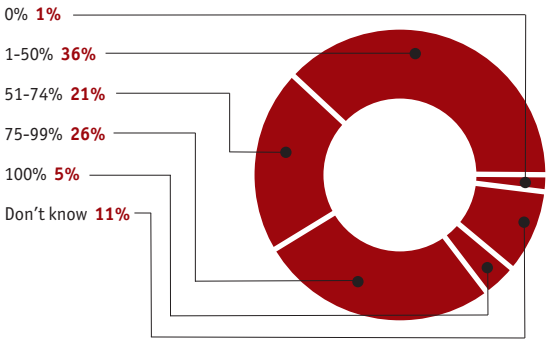


Source: Economist Intelligence Unit survey

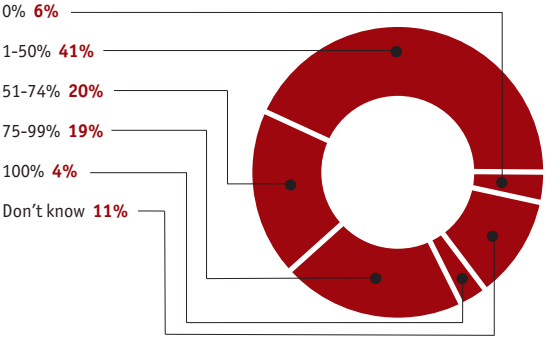
8. Approximately what percentage of your company's receivables currently arrives electronically?



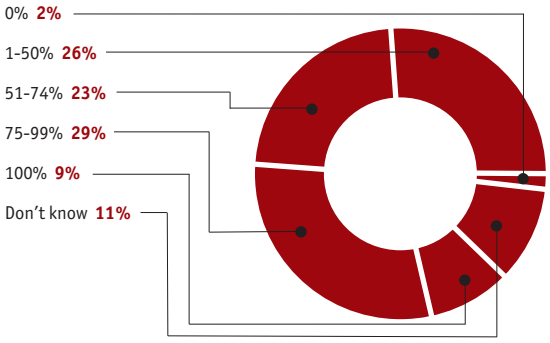
9. Approximately what percentage of your company's receivables do you expect to arrive electronically in three years?



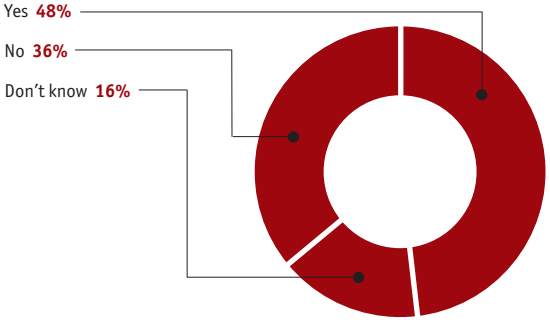
10. Approximately what percentage of your company's payables is currently settled electronically?



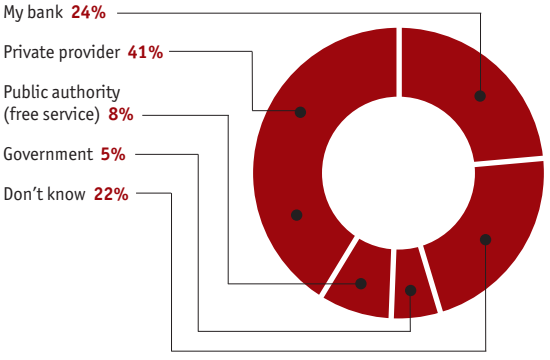
11. Approximately what percentage of your company's payables do you expect to be settled electronically in the next three years?



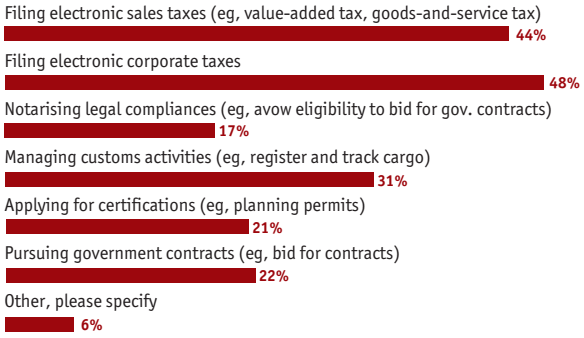
12. Does your company currently employ Internet-based digital certificates for e-commerce (communications or transactions)?



13. If so, who is the major certifying authority?

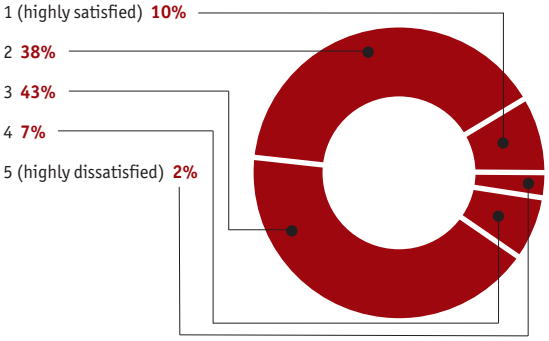


14. For which of the following interactions with local or national government agencies does your company currently employ Internet-based digital certificates? Select all that apply.
(% respondents)



Source: Economist Intelligence Unit survey

15. If you utilise internet-based digital certificates for any reason, how satisfied are you with the security they provide?
Rate on a scale from 1 (highly satified) to 5 (highly dissatisfied)



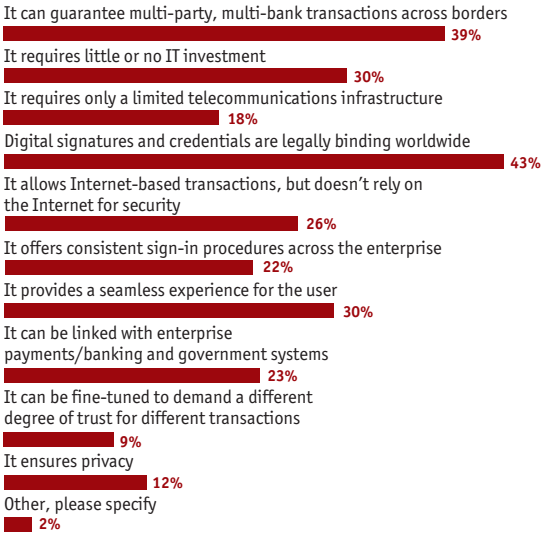
16. If you do not use Internet-based digital certificates, what is the single biggest reason?
(% respondents)

Source: Economist Intelligence Unit survey

17. What do you see as the biggest disadvantages with existing Internet-based digital certificates (whether you currently use them or not)? Select up to three responses.
(% respondents)

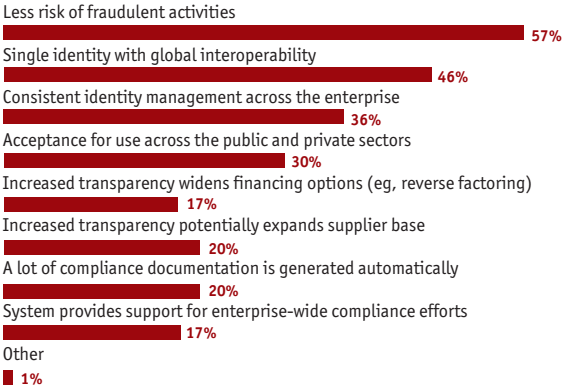
Source: Economist Intelligence Unit survey

18. What are the most important features of your ideal identity infrastructure? Select up to three responses.
(% respondents)



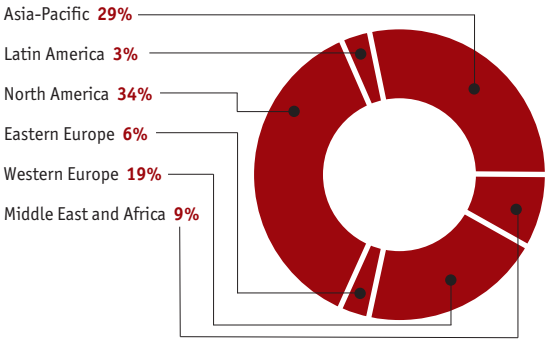
Source: Economist Intelligence Unit survey

19. What would be the greatest business benefits of using the ideal identity trust infrastructure? Select up to three responses.
(% respondents)

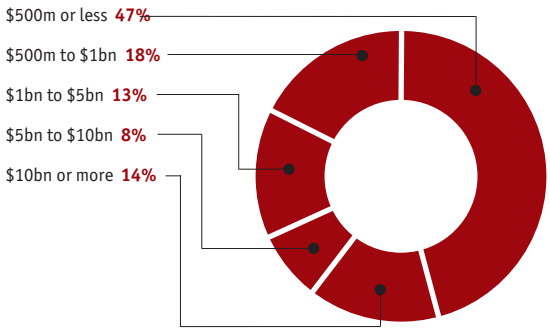


Source: Economist Intelligence Unit survey

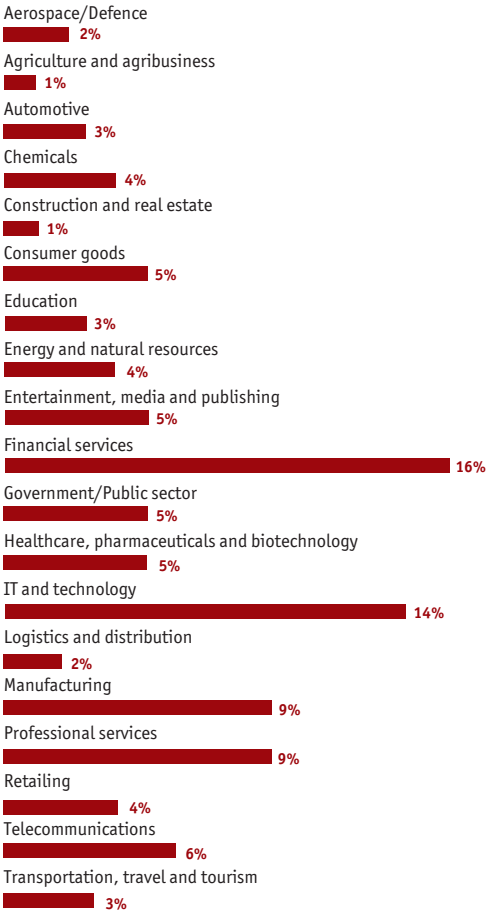
In which region are you personally based?



What is your organisation's global annual revenue in US dollars?

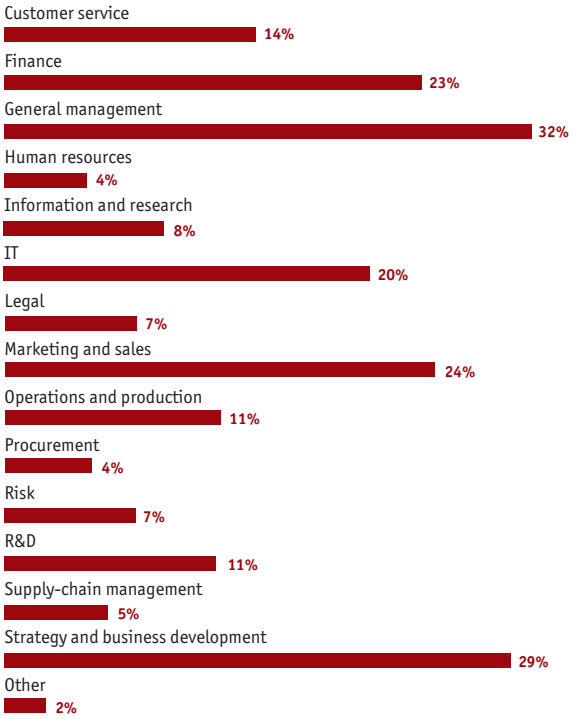


What is your primary industry?



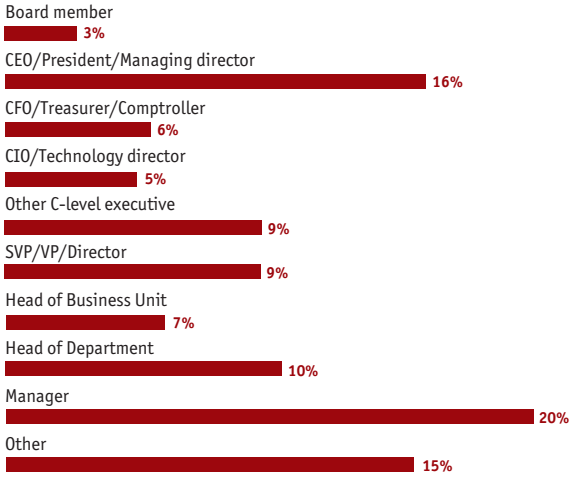
Source: Economist Intelligence Unit survey

What are your main functional roles?
Please choose no more than three functions



Source: Economist Intelligence Unit survey

Which of the following best describes your title?



Source: Economist Intelligence Unit survey

While every effort has been taken to verify the accuracy of this information, neither The Economist Intelligence Unit Ltd. nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this white paper or any of the information, opinions or conclusions set out in the white paper.

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