FREEFORM DYNAMICS

Open Research and Analysis

Managing Access Securely

Authentication that works for the evolving organisation

Freeform Dynamics, June 2006

You've probably heard the stories, there are several each year, of employees who are prepared to part with logon and password information for a free caffè latte or an Easter egg. This highlights that security of information systems is not just about technology, the human factor is important too, and one of the obvious places in which security meets the user is authentication. This short report looks at some of the trends and developments in this area based on the findings of an online research study during which information and insights were gathered from 1,464 respondents, primarily IT professionals.

KEY RESEARCH FINDINGS

Fragmented authentication leads to user frustration, business risk and IT cost

The continuous introduction and evolution of new business systems has led to a proliferation of authentication methods and credentials such as usernames, PINs and passwords. Two thirds of large enterprises and over half of small and midsize organisations report significant fragmentation of authentication requirements within their systems. This leads to user frustration, risk to the business and increased cost of IT support.

More flexible and diverse access makes managing the risk more challenging

Since many newer applications are web-based, they may in principle be accessed from any browser based device, including home PCs, machines in Internet cafés, PDAs and smartphones. The study reveals that users are taking advantage of this, with almost two thirds of organisations participating in our study endorsing access from uncontrolled PCs, and over 40% supporting personal mobile devices … then there is the unofficial access the IT department is unaware of.

And the challenge doesn't stop with employees

Two thirds of large and midsize organisations allow customers and or suppliers direct access into their systems, extending the need to manage authentication beyond the company boundary. Furthermore, developments in Web Services and Service Oriented Architecture (SOA) are accelerating the direct connectivity between systems over company boundaries, creating a whole new set of security considerations.

SSO use is ramping up, with advanced authentication appearing on the radar

Developments in authentication technology are helping organisations to respond to some of these trends from a security risk management and business efficiency perspective. Already, 55% are active with Single Sign-On solutions to one degree or another and the use of advanced authentication technologies, particularly biometrics and smartcards, is predicted to increase sharply over the coming three years. Organisations are also telling us that multi-factor authentication will become more broadly adopted.

RSA SECURITY®

The research upon which this report is based was designed, executed and interpreted on an independent basis by Freeform Dynamics, with sponsorship from RSA Security.

Introduction

As enterprises continue developing and acquiring new business applications to replace the manual processes and paper-based workflows of the past, authentication methods and credentials such as usernames and passwords are proliferating at the same pace.

Additionally, an increasingly mobile and gadget-equipped workforce is evolving that expects unfettered access to key applications from any location, and increasingly from a range of web-enabled devices. The wider availability of broadband access technologies such as WiFi hotpots, 3G etc, has fuelled activity in this area.

There are then developments around the concept of the Value Chain as a description of the production flow within a company, which increasingly extends backwards to materials suppliers and onwards to downstream customers. Enterprise applications that deal with logistics and production are increasingly being made available to external companies that form part of the value chain. Evolution here is being greatly helped by the concept of Service Oriented Architecture (SOA), which allows separate systems to be linked together much more easily using standard service and data interfaces.

Put these trends together and you have more users from more organisations connecting to more applications that exchange data in more sophisticated ways.
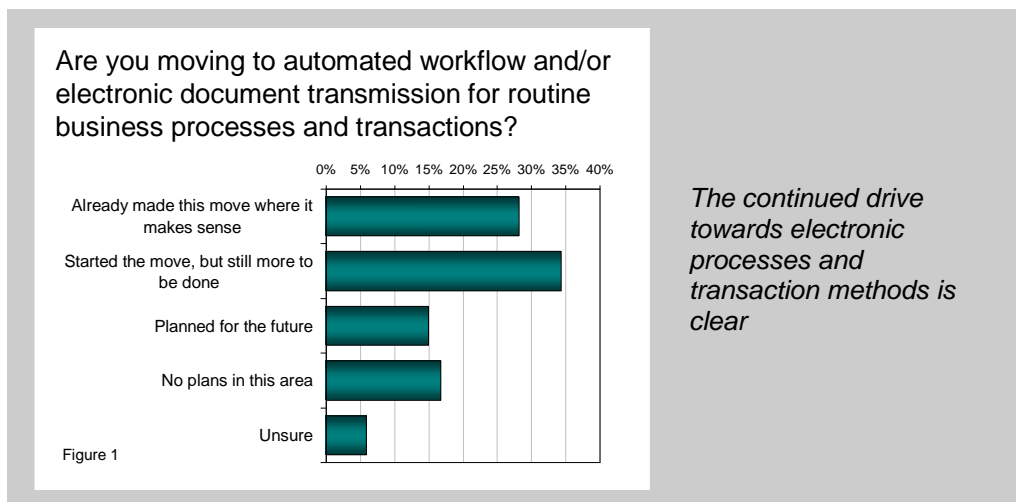
The challenges across the business are clear. Internal and external users are often left to cope with the proliferation of authentication methods themselves, while network managers have to struggle with new forms of vulnerability that arise with each new application and method of remote access introduced.

Clearly the older practices of leaving users to remember all their credentials and their consequent use of Post-it notes doesn't scale to fit this model, and this, along with the multiple modes of access, has much broader security implications for the organisation, as well as ramifications within the new compliance culture sweeping through business.

Against this background, this short report is based on a recent online research study, during which feedback was gathered from 1,464 IT professionals on a series of questions related to the access and authentication technologies used within their organisations and the way they expect the industry and their own plans and activities to evolve in this area over the coming three years.

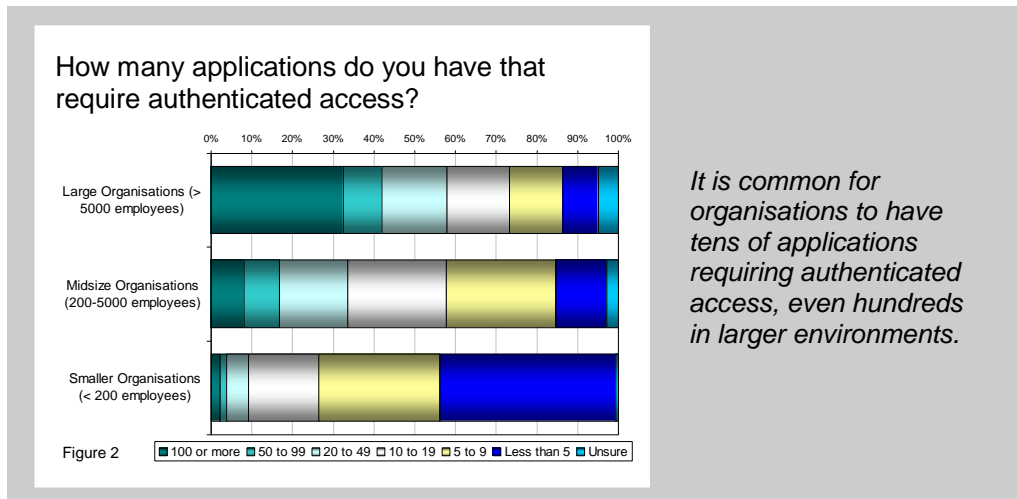# Consequences of evolving processes and applications

While it has become fashionable to dismiss the paperless office as an unachievable goal, over three quarters of the organisations in our study still say they are committed to moving their routine business activities away from paper wherever possible (Figure 1).

Are you moving to automated workflow and/or electronic document transmission for routine business processes and transactions?

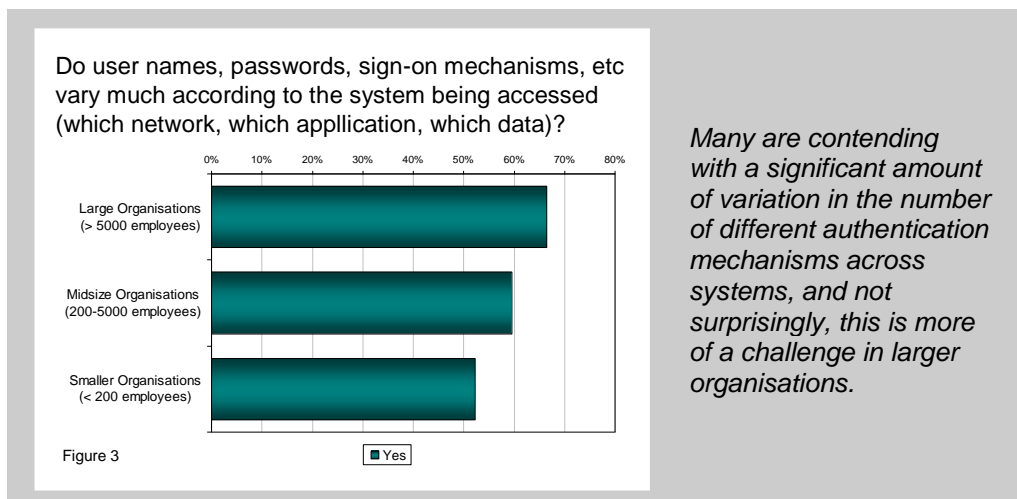*The continued drive towards electronic processes and transaction methods is clear*

Figure 1

The broad availability of tools and applications for straightforward web management of the business process is having a profound effect on the way business works. Instead of printing multiple copies of a document and placing it in pigeonholes or internal mail, or having a single document placed on a circulation list, taking an indeterminate amount of time to reach all necessary readers, information is increasingly being moved around electronically, often in parallel, depending on the requirement. The addition of collaborative elements, such as editing, discussion and chat, further enhances and streamlines the way we work with information. All of this activity can be captured and tracked to satisfy increasing compliance requirements.

Such electronically enabled collaborative working, with properly constructive document control and communication systems, can be a powerful way for companies of any size to speed up the process of communication. This has benefits in terms of rapid and flexible response to market factors, better service and support of customers, and fuelling of the innovation process.

Companies that are introducing new applications into their portfolios to drive effectiveness and flexibility are sensibly making them available to a managed pool of users through authenticated access. These applications are a mix of off-the-shelf programs, as well as in-house developments that may involve the use of application, middleware and database layers, all with separate authentication requirements. As new applications and components have been introduced that require authentication, most organisations have accumulated a significant management challenge (Figure 2).

How many applications do you have that require authenticated access?

It is common for organisations to have tens of applications requiring authenticated access, even hundreds in larger environments.

Figure 2 — legend: 100 or more | 50 to 99 | 20 to 49 | 10 to 19 | 5 to 9 | Less than 5 | Unsure

An indication of the drawbacks of the evolutionary nature of the growth in application portfolios is the fact that over 50% of those polled report a wide variation in the sign on mechanisms that users have to contend with (Figure 3).

Do user names, passwords, sign-on mechanisms, etc vary much according to the system being accessed (which network, which appllication, which data)?

Many are contending with a significant amount of variation in the number of different authentication mechanisms across systems, and not surprisingly, this is more of a challenge in larger organisations.
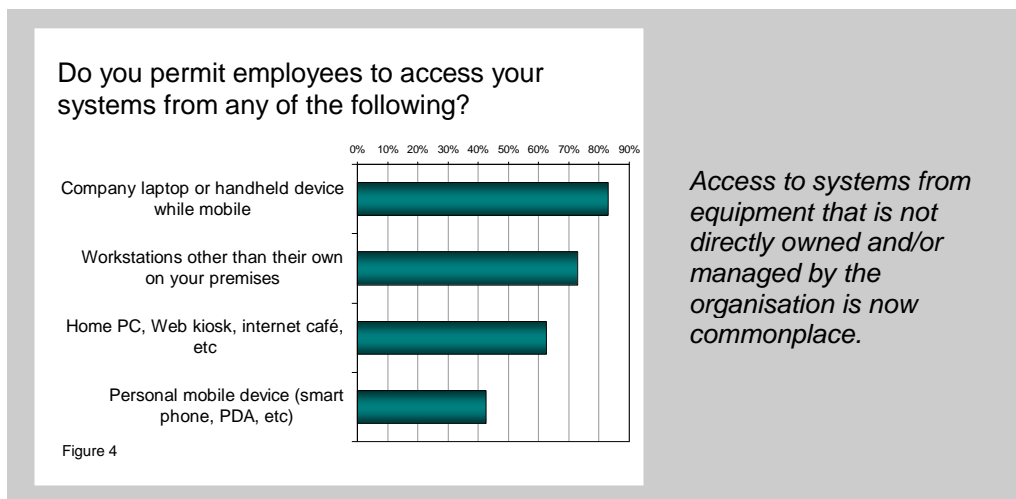
Figure 3 — legend: Yes

When you are buying off the shelf equipment there isn't always a lot that can be done about this proliferation of sign on mechanisms, no company wants to be tied to one vendor.

There are significant risk and cost issues here from a business perspective, however. Many organisations find that forgotten passwords are the biggest burden on their help desks, and this situation is naturally made much worse when multiple login methods are required as well as different passwords. As a workaround, many users will attempt to have the same password for all applications, although password ageing and different syntax requirements by various systems will naturally cause users to have more things to remember (and therefore forget), which brings us right back full circle to the password reset problem and the burden on IT this represents. It is a classic Catch 22 situation and we will be discussing ways around this later. In the meantime, though, we need to discuss a couple of other trends that should be considered when formulating authentication strategies.

The challenge of the unknown client

Once applications are available online, access from equipment that is not directly controlled by the organisation becomes possible, and is certainly attractive from a user productivity perspective. Since many newer applications are web-based, they may in principal be accessed from any browser based device, including home PCs, machines in Internet cafes, PDAs, smartphones, and so on. This is revealed clearly by our survey, with over 60% of all companies allowing access from uncontrolled PCs, and over 40% supporting personal mobile devices (Figure 4).

Do you permit employees to access your systems from any of the following?

Access to systems from equipment that is not directly owned and/or managed by the organisation is now commonplace.

Figure 4

And this is just what organisations "permit", i.e. know about. It is impossible to quantify the amount of unofficial access that goes on, but we can guess that this would elevate the figures even higher.
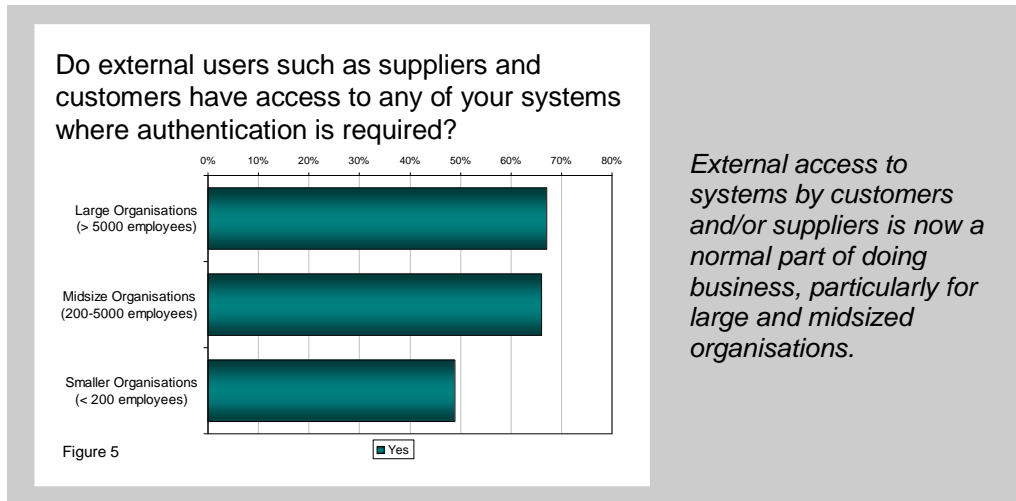
The potential for key-loggers and caching software, such as Google Desktop search to actively or inadvertently capture sensitive company data is an important consideration for IT departments when enabling remote access; as are permissions for printing and saving (as opposed to merely viewing) documents. There are now classes of application gateway products which are seeking to help mitigate these problems, but when evaluating these, organisations should be sure to give a comprehensive examination to potential suppliers on this subject, and make sure that the features in question are available on shipping products, not merely as slideware, which is a potential problem in this space at the time of writing.

Porous perimeters

The Value Chain as penned by Michael Porter in his 1985 book *Competitive Advantage* is described as "a systematic way of examining all the activities a firm performs and how they

interact". In today's internet enabled global economy, this increasingly means the coordination of activities between upstream and downstream companies to create a "value system".

From a communication and automation perspective, online systems allow suppliers and vendors to integrate their individual value chains more tightly together, sharing information to improve the efficiency of the value system. This is a compelling business driver that has caused a majority of companies in our study to allow their suppliers and/or customers access to their computer systems directly in one way or another (Figure 5).

Do external users such as suppliers and customers have access to any of your systems where authentication is required?

Figure 5

External access to systems by customers and/or suppliers is now a normal part of doing business, particularly for large and midsized organisations.

The way in which technology developments and standards in the areas of XML, Web Services and Service Oriented Architecture (SOA) are simplifying the integration of applications and information is accelerating activity in this area. The opening of what has been termed the Enterprise Service Bus to third party companies goes to the heart of a strategic approach to the integration of Value Chains within a Value System, tightly integrating suppliers and customers to mutual benefit.

As the middleware industry evolves to support this business need, the potential arises for a new class of security threats that will require management. Because an SOA is built on a set of open and interoperable standards, it becomes an application layer that by default is equivalent to the exchange of plain text. New initiatives such as Security Assertion Markup Language (SAML) and eXtensible Access Control Markup language (XACML) are beginning to emerge to deal with the new vulnerabilities that are emerging, and IT departments not yet familiar with such developments are advised to get up to speed on them sooner rather than later.

With the business-to-business access model come some other important questions the organisation needs to consider. The first is to make sure that only information that is absolutely necessary to the business transaction can be accessed by the third party company. A common example of this is the Demilitarized Zone, or DMZ, that is established using a firewall that allows a web server to sit on the Internet and be available for transactions, yet still be manageable from within the corporate network by IT staff. Users are able to enter transaction information, but they can't get at the database and application software that is presenting that capability to the outside world.
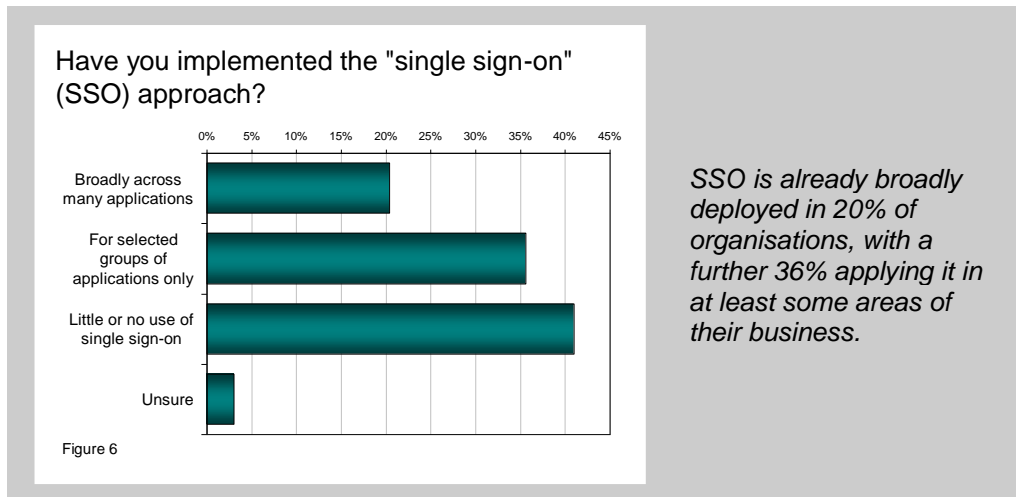
The second important consideration is identity management of people in the external company that have access to any sensitive information that is made available to enable the business transaction. Simple examples might be wholesale prices for products or lead times on popular components. This and other information could be potentially valuable to a competitor, so the supplying company may wish to have protection in addition to the simple contractual one to participate in the identity management of the third party company.

One of the initiatives that is being pursued by a number of vendors for inter-company identity management is the Liberty Alliance project http://www.projectliberty.org. Companies considering sharing sensitive data may want to ask suppliers about this and other initiatives that can protect them without placing an unreasonable burden on themselves, or their suppliers and customers.

Trends in authentication technologies

The background of business and systems evolution we have been discussing helps to put some of the trends in the area of authentication technologies into perspective.

The activity we are seeing in the area of Single Sign-On (SSO), for example, is very relevant to organisations trying to manage the proliferation of usernames, passwords and other authentication mechanisms. Indeed, over half of the respondents in our study are already doing something with SSO (Figure 6).

Have you implemented the "single sign-on" (SSO) approach?

SSO is already broadly deployed in 20% of organisations, with a further 36% applying it in at least some areas of their business.

Figure 6

SSO addresses the problem of multiple logins by placing a proxy between the user and the various systems they need to access. The SSO solution manages the multiple login and password requirements of the different applications and presents the user with a single login for everything. A key feature of an SSO solution is obviously going to be its own security, since it represents a potential single point of failure (and attack) on the network.

The ease with which the system can be set up and maintained by the IT department through login scripts, password reset procedures, entering users into the system, synchronising with corporate directories, etc is also an important consideration. If a lot of this has to be hard coded, the effort of setting up a new SSO system would be considerable, not to mention the overhead of maintaining the system subsequently as things change over time. When evaluating SSO solutions, organisations must therefore pay particular attention to this area of automation, integration and flexibility.

Note that SSO is not to be confused with the way in which credentials are authenticated. All it does is allow that authentication to take place just once for all systems rather than many times for each individual system.

Of course an obvious consequence of this is that if authentication is compromised, the impact is much broader. Stealing or otherwise acquiring one of an employee's multiple user names and passwords in a traditional fragmented authentication environment only provides illicit access to a single system (putting to one side user attempts to make all passwords the same for a minute). In an SSO environment, however, you just need to acquire one login to gain access to all systems the employee is authorised to use. This brings the importance of effective authentication into particularly sharp focus.

Our survey reveals that many users have realised that the simple use of passwords and PINs is not sufficient to protect sensitive data. This is not to say that they do not trust users with the data, just that they recognise that they must takes steps to reduce the chance for inadvertent release of login credentials, as well as preventing casual harvesting of the information (using keyloggers or social engineering for example). The end result is that reliance on simple passwords and PINs looks set to drop dramatically over the next few years, with a sharp increase in the use of smartcards and biometric methods and a continuing rise in the use of security tokens (Figure 7).

Which of these methods are used to authenticate employee access to systems today and which will be important in 3 years time?
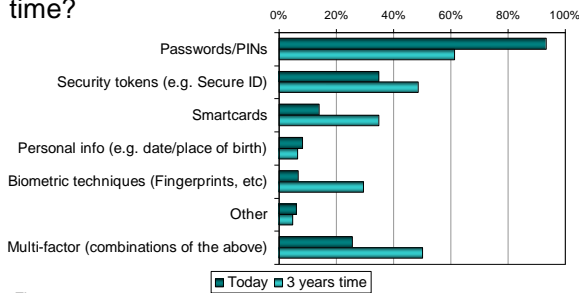
Traditional passwords and PINs will be de-emphasised over time in favour of a mixture of tokens, smartcards and biometric based authentication, with many more organisations combining methods and taking a multi-factor approach.

Figure 7

Smartcards have the drawback of being physical items that the user must have with them in order to access the system, whereas biometrics, in essence, rely on information that is essentially encrypted on the body of the person themselves. Having said this, the two will often work together, with biometric information stored securely on the smartcard so relevant systems can authenticate without the need to maintain or access a sensitive database of biometric data.

In terms of specific technology, the strongest form of biometric authentication is currently iris recognition. This isn't as scary as it sounds, and does not require the use of lasers or the pulling back of eyelids! It simply relies on using a video camera to examine the surface of the eye. By way of comparison, this provides much stronger authentication than a fingerprint scan, and has the added advantage that it doesn't require the user to physically touch the sensor.

As we can see from Figure 7, we can also expect to see a significant increase in the frequency of authentication mechanisms being combined to implement so called "multi-factor" authentication. This again raises the issue of striking the right balance between the needs of the company for security, and the added nuisance factor that can arrive with multi-factor authentication for users. Certainly introducing SSO in conjunction with multi-factor authentication would represent both an effective and considerate approach, giving more to the user than you are taking back with the extra level of authentication.

Conclusions

We see clear evidence that IT departments are being responsive to the needs of the business by procuring and supporting a broader range of applications. In addition, they are working to make these available to the organisation and its key partners from outside the corporate firewall and using a variety of access methods. These moves are key to building competitive advantage and leveraging the investment in new software systems.

Two trends are clearly identifiable that go hand in hand with these developments. These are the move to Single Sign-On as a way to manage the proliferation of applications, coupled with multi-factor authentication to ensure the identity of the user in a more reliable and secure manner.

As well as taking these steps to establish manageable and auditable trust and identity within the company, organisations must also plan to manage the security concerns related to access from an unknown PC or handheld device that may well be compromised in some way. When doing this, organisations must keep in mind the vulnerabilities of all types of device that are capable of accessing their systems, as well as the security of the communications paths that they use.

In addition, organisations should make federated identity management an integral part of their security policy to extend the circle of trust to outside companies that have access to applications or sensitive data. The starting point for federated identity management is a directory system that can be linked with key third party companies. From this base, application gateways can be deployed in conjunction with multi-factor authentication to roll-out location and machine-based access policies.

Finally, with the increasing mainstream use of Web Services and Service Oriented Architecture for B2B integration, new threats must be anticipated from application-level attacks on the program and data interfaces used by these systems.

The bottom line is that authentication and broader security requirements should be designed into architectural plans wherever possible.

Acknowledgements

We would like to conclude by thanking all of those who participated in our study. Your feedback and insights have been invaluable in constructing this report.

Sample Composition

Sample composition by Geography

Rest of World
11%

UK
36%

US
15%

Rest of
Europe
38%
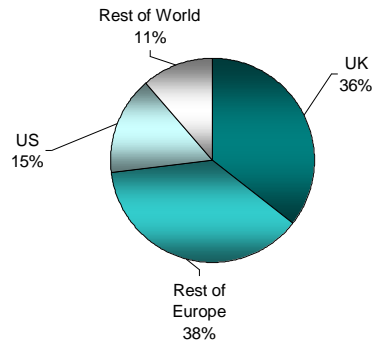
Figure 8

The study was executed in the English language, hence the bias towards native English speaking geographies.

Sample composition by Organisation Size

Undeclared
5%

Large
Organisations
(> 5000 emps)
31%

Smaller
Organisations
(< 200 emps)
39%

Midsize
Organisations
(200-5000
emps)
25%
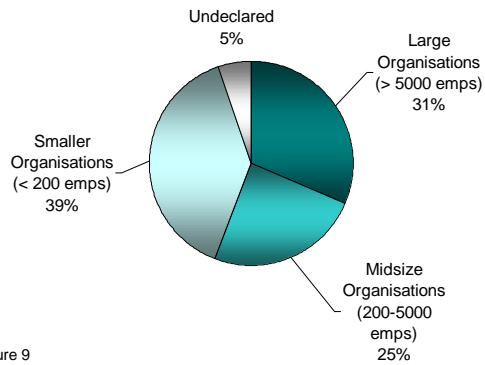
Figure 9

Spread of company sizes from SMB to enterprise

Respondents were primarily IT professionals from a broad cross section of industries.

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in ITC strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.

About RSA Security

RSA Security Inc. is the expert in protecting online identities and digital assets. The inventor of core security technologies for the Internet, the Company leads the way in strong authentication, encryption and anti-fraud protection, bringing trust to millions of user identities and the transactions that they perform.

RSA Security's portfolio of award-winning identity & access management solutions helps businesses to establish who's who online – and what they can do. With a strong reputation built on a 20-year history of ingenuity, leadership and proven technologies, we serve more than 20,000 customers – including financial institutions representing hundreds of millions of consumers around the globe – and interoperate with over 1,000 technology and integration partners.

For further information on RSA Security, please visit www.rsasecurity.com.