

Comprehensive identity management

Balancing cost, risk and convenience
in identity management

Contents

Executive summary	3
Variables shaping identity management	4
Business costs to the organisation	4
Compliance	4
Technologies and approaches	4
Society at risk	6
Becoming sophisticated about risk	7
Balancing costs and risk	7
The importance of convenience	7
Users in the risk equation	8
Diversity and usability	8
Convenience, privacy and security	8
More advanced technology and solutions	9
Sharing responsibility	11
Moving towards an identity-centric society	11
About the authors	12
BT as your security partner	12
References	13

Executive summary

The need for more careful identity management is an inevitable outcome of a variety of changes that are compounding together into a perfect storm of change. These changes are making today's world increasingly dependant on digital identities to enable transactions, allow access to services, information sources, communication networks, applications, and even to enter buildings. As a result, the volume of data and personal information that is stored and harvested is growing rapidly, with personal information required for every aspect of our lives from home, work, healthcare and government. In addition to the significant user advantages and cost efficiencies from effective identity management (IdM), the increasing use of digital media and the web can also make personal information more easily accessible, placing our privacy and security as well as the resultant inappropriate exploitation of our identity at serious risk.

Compromising an identity is the modern equivalent of holding the "key's to the kingdom." Our identities underpin numerous critical transactions and life events; once an identity is captured it can quickly unravel into many unintended and damaging consequences, reflecting its many uses.

Identity theft can happen to anyone. Statistics from the Home Office in the UK indicate that identity theft affects at least one in four adults, and the UK's Credit Industry Fraud Avoidance Scheme (CIFAS) reported a 17% increase in identity fraud in the past year. In the US, The Identity Theft Resource Center reports that 19 people become a victim of this crime every minute, with 10 million people affected each year.

Business is becoming more successful at detecting fraud early and stopping criminals in their tracks, according to recent figures released by CIFAS, but identity fraud and theft are still a major threat. Despite efforts to fight this crime, business, governments and individuals are still not adequately geared to cope with the consequences of identity theft, according to research conducted by BT and HP Labs with the University of Plymouth, and published as the Trustguide.

Research in the US, by the Ponemon Institute, shows that a lack of accountability and resources are at the root of the corporate data loss problem. Therefore, organisations need to guarantee effective risk management and provide maximum protection to mitigate the threats. Certain sectors are also under market and regulatory pressure to provide tactical solutions, such as the deployment of strong authentication, but this is expensive and needs to be set within complex longer-term social, business and economic dimensions, such as public trust, and technologies that are accessible to all. Balancing risk and cost is therefore compounded by the need to provide a diverse base of users with solutions appropriate for their intended purpose, but still providing easy and convenient access to services. Achieving the perfect balance is further challenged by the need for organisations to maintain pace with the rapidly advancing technology landscape and increasingly sophisticated identity threats within a framework of legislative constraints.

Variables shaping identity management

Business costs to the organisation

The cost of inadequate identity management

Over the last three years, identity theft and crime cost the UK economy at least £1.7 billion, according to the Home Office. This amount includes £504.8 million the UK payments association, APACS, lost from plastic cards being used by criminals. The Department of Constitutional Affairs in the UK lost £29.9 million due to unpaid fines related to tracking problems, plus £5.9 million in unpaid fines due to identity problems. The Association of British Insurers lost £22 million due to identity fraud, while other financial association and government departments also incurred significant losses.

In 2006, The Ponemon Institute reported a 35% increase in the cost companies incur for each lost information record. At a cost of US\$182 a record, the Ponemon Institute calculated the average cost of notifying customers and indirect fallout, such as high customer turnover, to cost and average company \$660 000. The same study says each business is losing around \$2.5 billion in lost business, setting up call centres, legal and auditing expenses, and other costs.

Properly verifying identities and subsequently authenticating users to the appropriate degree of certainty can be complicated and expensive. This is particularly a challenge with the current influx of foreign workers into industrialised countries, with limited resources to validate identities. This proper verification and authentication of users is critical for both the external citizen or consumer facing channels and the internal back-office systems. More specifically, the consumer facing channels may suffer a fraudulent registration or authentication that can result in immediate direct loss to the organisation and the innocent consumer in terms of damage to reputation. Moreover, the access to back-office systems by internal theft may incur no direct cost for a company as stolen information might be used to perpetrate attacks elsewhere.

The cost benefits of effective identity management

CIFAS reports that the financial benefits of detecting fraud early, for example at the account applications stage – before serious losses and consequences have been incurred – saved UK business £579 million from January to September 2006, which is a 12.86% improvement on figures for the same period in 2005.

According to Forrester, provisioning solutions have reduced annual organisational expense by nearly US\$500 per employee:-

Annual benefit per employee

(1) Improved IT efficiency	\$70
(2) Reduced help desk cost	\$75
(3) Quicker access	\$350
TOTAL	\$495

This data is reflected in BT's own client experience. BT clients with effective identity management will reduce organisational expense by about US\$540 per internal user as IdM solutions improve quality and reduce security exposure, which lowers user administration and IT costs while increasing productivity.

To illustrate, the creation of a single BT enterprise directory, using sound registration, remote access, and reduced SignOn saves BT £88 million a year in direct cost savings around reduced administrative expenses, as well as the indirect advantages of user convenience. The scale of soft benefits can go well beyond these near-certain cost savings which in themselves are considerable.

Compliance

Compliance with laws and regulations is currently the most important driver of security expenditure, according to the DTI. Companies are subject to more regulations than ever before. Laws such as Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Federated Information Management Act of 2002 (FISMA), and the European Union Privacy Act (EUPA) mean companies have dramatically increased spending on the growing requirements for greater data security and improved corporate accountability and transparency to ensure regulatory compliance. The cost of compliance is high, but it is significantly less than the costs and losses that could result from a lack of compliance.

Furthermore, if compliance laws are aligned with best practices, such as Control Objectives for Information and related Technology (COBIT) and ISO 17799, implementation of identity management can significantly improve the overall quality of business. In a recent Interactive Data Language (IDL) survey of 163 Heads of Compliance IT and Finance, 69% of those surveyed found that complying with SOX helped assist in wider requirements. When asked for specifics, 82% referred to improved speed of management reporting and 79% to better information sharing supporting faster decision making.

Organisations are turning to identity management solutions to meet their data security needs and improve accountability, as well as increasingly recognising the positive business impact through best practice.

IdM solutions, such as single sign-on, strong authentication and Federated Identity Management (FIM) enable organisations to enforce control over access, providing reporting and auditing capabilities and enhancing compliance, as well as improving the agility and quality of collaboration.

Technologies and approaches

Technologies and solutions in use

Identity management systems have traditionally been delivered as tailored solutions to cater for the internal requirements of an organisation. These solutions have covered specific technological areas or extensive professional services and have been intended to address the internal requirements of authentication, authorisation, user provisioning, business process automation and more recently the requirements of audit and regulatory compliance.

Identity management systems that underpin a variety of products and services, a cross section of which are listed in the table below, have often developed in a piecemeal fashion over time. The complexity and diversity of today's computer systems as well as the growing ambiguity of users which often extends to third parties, makes effectively managing identity and access a major challenge. A 'fragmented' infrastructure introduces duplicated administrative processes, increased business and technical risks, inconsistent user experience and also restricts the development of improved IT architectures, systems and business processes. To address these issues, a more consistent and rigorous approach to the management of identities is required.

Technology area	Products and services
Networks and infrastructure	WiFi Voice over IP Converged networks incorporating session and access protocols Voice and Data convergence De-perimeterisation
Software	Distributed computing and virtualisation Device proliferation Web and thin client
Applications	Security Supply chain Customer relationship management (CRM) Simplicity Service oriented architectures
Security	Virtual Intranet Trusted computing Federated Identity Management (FIM) Managed Transaction Security Logical and physical convergence
Bio and nanotechnology	Biometrics Radio Frequency Identifier (RFID)

Focus on first point of registration and authentication

Initial registration precedes authentication and, if an error regarding identity occurs at this starting point, all subsequent authentication transactions will be false. Consequently, government has led the way in stressing the importance of the first point of registration, even though the correct processing of identity related information during the authentication process is still vital. The financial services sector is also re-enforcing the importance of accuracy, verification, good practice and security at this initial registration or account opening stage. It is here that an individual establishes his or her true or false identity – the real or stolen representation of the physical person – that will be used repeatedly to access services and complete transactions. A failure at this initial point will impede the authentication process and threaten the validity and trust in the entire system.

Subsequent authentication ensures that users are who they claim to be, and technology is constantly advancing to find:

Stronger authentication

- Personal factors: your voice, face, eyes, fingerprint
- Possessive factors: one-time number generator tokens
- Knowledge factors:
 - something you know, such as a password, PIN or secret
 - something someone else knows about you, such as your footprint on society
- Deployed factors: a unique programme you have installed or modified
- Your location
- Feedback loop: informing registered individuals each time their identity is verified

Improved validation

- Multi-factor validation
- Threat analysis and response

Increasingly this information is being used dynamically to evaluate the risk of a requested transaction based on previous usage patterns. Out of pattern behaviour could lead to further requests for proof of identity, human intervention or potentially a refusal.

Reduced complexity of administration

- Adaptation policies
- Identity and access management (IAM) integration

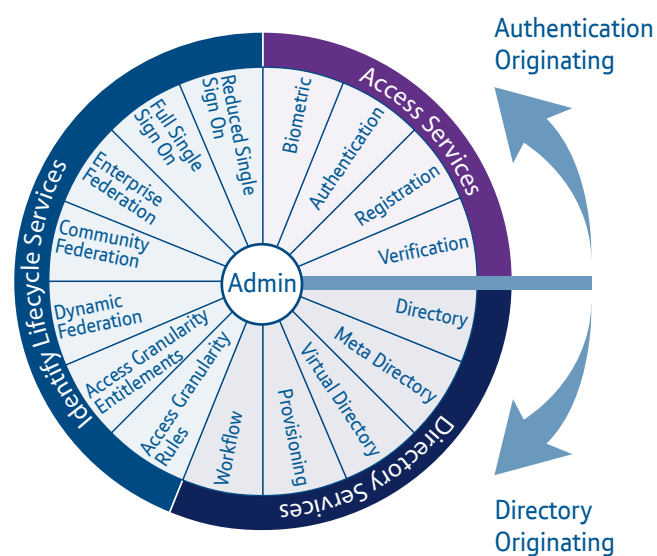
Auditing

- Archive, Analysis, Assessment, Audit

Usability and convenience

- Single Sign-on and Federation

All other application and service components of an identity solution depend fundamentally on this foundation layer of physical verification, good registration and binding. Subsequently, establishing that you are who you say you are in a consumer, commercial or citizen context depends on good authentication as well as joining up with identity lifecycle and directory services.



Society at risk

The changing landscape and growing complexity of information technology, business and regulatory compliance creates an ever-changing risk that needs to be managed and mitigated. Organisations recognise the need for identity management in their businesses as identity theft and fraud can have devastating long-term consequences for individuals, businesses, and governments. Moreover, identity theft can be a precursor to other crimes, including organised crime, human trafficking, money laundering and terrorist activities, posing a threat to national security.

Failure to prevent data breaches, identity theft, and fraud can result in serious financial and brand capital losses. If a company incurs an identity theft incident, customers could be directly or indirectly impacted. Consequently, customers will lose trust and confidence in the company, move to a competitor and even sue the company for damages. If the crime receives significant media coverage, an organisation risks significant and irreparable losses to its customer base and brand capital. In addition, failure to comply with regulations can also result in legal and financial penalties.

According to the Trustguide research, customers value companies' fraud prevention efforts, such as a helpline set up by a bank to assist customers in the event of fraud or identity theft. At the same time, too many fraud prevention efforts give clients the impression that such crimes are likely to occur. Industry has to strike the correct balance of providing assurances of security, without making customers feel too vulnerable or threatened. User confidence and trust, which enable transactions, needs to improve to diminish the risks unobtrusively.

Tactical attempts, such as secure payment mechanisms and strong authentication, are the main ways in which identity management solutions have tried to control risk.

These technologies are constantly changing, from the first application of Public Key Infrastructures (PKIs) to smart cards, and new and evolving technologies such as biometrics, device fingerprinting, geolocation and transaction footprints. However, this is not enough and identity theft still remains a problem.

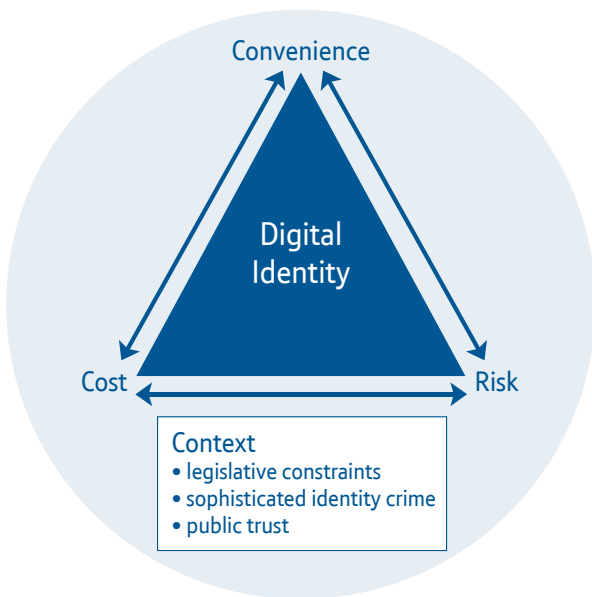
Becoming sophisticated about risk

There is no one definitive approach to identity management. Instead, the ability to adapt in an immature but profoundly important and developing space is required. The evolving threat landscape is a challenge that requires a radical new approach to cost-effectively manage change, processes and the migration to new technologies.

To meet the challenges of identity theft and fraud businesses need to take a more holistic view, which focuses more on:

- Developing risk calculation and assessment methods
- Monitoring user behaviour to calculate risk
- Building trust and value with the user or consumer
- Engaging the cooperation of the user or consumer with transparency and without complexity or shifting the liability to the consumer
- Taking a staged approach to authentication deployment and process challenges, using more advanced technologies

In other words, business is faced with the challenge of managing the interconnected variables of authentication costs, risks and convenience to users.



Balancing costs and risk

There are many IdM solution vendors trying to sell authentication and IdM products to business based on initial upfront costs, but BT advises business to consider the costs across the entire lifecycle of identity management.

Choosing the right authentication mechanisms for your business depends on several factors and one product might not be the right answer for every business or for every user or consumer.

For example, the proposed type of authentication mechanism could differ depending on the:

- Frequency with which users need to access an application or service
- Access to and familiarity with IT resources
- Level of security required
- Technical ability or range of physical ability of users
- Constantly changing interaction of the risks, costs and convenience

Stronger authentication alone is not enough to protect against identity theft and fraud, and other technologies that develop customers' feelings of trust and confidence are also necessary. Therefore, the most suitable authentication methods for your business will be those that provide the best balance between strong authentication and security, cost, and customer convenience.

The importance of convenience

To tackle identity fraud, the convenience and usability of a system in the users' view should be the primary consideration and one of the major factors affecting the choice of technology used. Even if an IT system is secure, customers will be deterred from using it if it has low usability.

Consumers are motivated by convenience and control when performing transactions and other day-to-day tasks that involve authentication. Users look for the quickest, easiest and cheapest way to achieve their goals, such as completing a purchase or accessing a bank account. This is not to say that individuals ignore security issues altogether. On the contrary, they are aware of a risk and the need for security measures, but also feel somewhat responsible for the security of their personal information.

If there is a trade-off between the risk and convenience, consumers will take the easy option – and this is why individuals sometimes write down passwords, give cards and pins to partners, and use personal information over the phone. Users only perceive new security positively when the convenience factor is high. The consumer will determine whether the effort is worth the risk by judging how much time, money and effort is necessary in order to use it. The user will then weigh this up against how secure the system appears to be and how difficult it would be for his/her personal information to get into the wrong hands. If a new technology is perceived to be much more secure, consumers are likely to accept and adopt it, even if a little bit of time, money and effort is required.

It is also interesting to note that various countries and cultures have different reactions to the intervention of security technologies. In many countries in continental Europe, for instance, users are prepared to pay for security devices. In the UK, on the other hand, the consumer perception is that these should be free, while in the US market concern is about convenience.

Users in the risk equation

The general public underestimates the risk, perceiving less risk than there really is or believing that it will not happen to them. Even when individuals recognise the risk, they often do not react or behave in ways to protect themselves from identity theft and fraud. This is partly because users have had generations of experience in attuning themselves to physical risks, but logical risk is a relatively new and abstract concept surrounded in layers of uncertainty and misinformation. For instance, credit card users are aware of the risks of credit card theft and fraud, but often give out their details over the telephone. Consumers believe that unless they are genuinely negligent they will get their money back. As a result, consumer concerns about fraud have to be thought about in the context of companies, such as banks, providing a safety net. This perceived safety gives many consumers the confidence to use interactive banking and shopping products where they might otherwise avoid them. It is usually only when this security breaks down that consumers start to be more cautious and learn from their collective experiences in ways which gradually enhance the sense of personal responsibility.

Despite the safety net, consumers recognise that they too have a responsibility to keep their passwords safe and PC-based information secure. Securing personal information is a shared responsibility in which consumers have to keep informed about scams, take steps to keep personal information secure, and remain vigilant – while banks and organisations have to keep personal details secure, offer secure banking and transaction processes, and also provide insurance and protection in the event that identity theft and fraud do occur. They must strive for the perfect balance between letting go and keeping control: trust and caution.

Diversity and usability

Creating secure systems that are convenient to use is complex, given the heterogeneous nature of users. When developing an identity management solution plan, a business must have an intricate understanding of its users. Not all demographic groups have the same technical ability. Young users are more comfortable with messaging, Web applications, downloads and sharing – while the ‘silver surfers’ tend to stick to technology for basic functions, such as email and checking their bank balance online. Even within the same demographic group, technical ability can vary considerably and authentication mechanisms must also be accessible to people with physical and mental disabilities. IdM solutions must, therefore, avoid widening the gaps between the technological haves and have-nots and strive to be inclusive. Furthermore, selecting inappropriate technologies can adversely impact helpdesk and lifetime support costs.

Usability is also influenced by the education and awareness of users. As a result, organisations are challenged with the need to properly convey the intent of a managed and interoperable identity system and its relevance to the citizen or customer. Users need to understand how a system operates, but should not be placed at risk or exposed to other liabilities if their understanding is incomplete.

Business can ensure user convenience through a variety of process and architecture mechanisms, such as single sign-on and workflow. The goal is to provide the right access to information to the correct people, with appropriate workflow in an auditable way. Providing a range of authentication mechanisms into a single authentication platform – in particular using the new authentication capability derived from combining voice and data on a single network – can also offer high usability.

Increasing volumes of data are being centrally controlled in databases, making users feel more vulnerable. This vulnerability can be offset by giving users greater control. Identity management solutions that put users at the heart of the business relationship enable them to control their privacy in business relationships and the information and preferences shared with a business or organisation. For instance, self-service gives users transactional rights into applications, information assets and physical assets.

User control creates a feeling of confidence and trust which, in turn, reduces risk.

Convenience, privacy and security

Collecting and using identity data presents risk, but it is key to providing access to services, customer service, verifying identity in transactions and preventing fraud.

The convenience of standardised passwords across channels and the concept of mobile payments and centralised databases appeal to consumers. But, according to the Trustguide, harvesting information from a variety of sources and amalgamating it into a single database poses new dangers to privacy. On the one hand, a centralised patient information database might provide healthcare workers with lifesaving information. On the other hand, it could create a greater risk of abuse if information were to fall into the wrong hands. Consequently, organisations are struggling to make the conflicting variables of security, confidentiality, privacy and convenience co-exist harmoniously.

In fact, the technologies are mature enough to manage most of the conflicts. For example, approaches to directory management are becoming increasingly virtualised and distributed. This enables user information to be managed and recorded without the need for a physically centralised and vulnerable information silo. However, the only way organisations can achieve a perfect balance between conflicting variables is to go beyond adopting sophisticated technology. To do this organisations must develop trusted and secure information-gathering environments that maximise social benefits in terms of convenience to customers, and minimise the risks of any threat to a person's identity and information.

More advanced technologies and solutions

Organisations are increasingly driven to work collaboratively with their customers. As a result, they need to move away from point solutions, consider their requirements in terms of a wider business process and also as part of an ongoing roadmap of services in the context of evolving threats.

This dynamic nature of the business environment is leading organisations to consider outsourcing all or part of the services required. The movement towards an outsourced service also allows organisations and businesses, particularly small- and medium-sized businesses, to exploit identity management solutions for which there was previously no justifiable ROI on the basis of direct cost. However, without the infrastructure they were unable to engage with the evolving collaborative identity-centric networks and services, and reap the resultant benefits.

The provisioning and management of IT devices on a service basis minimises capital investment and operational costs through:

- Economies of scale
- The introduction of subscription based services
- Minimal upfront costs
- Reduced risk
- Access to an evolving service portfolio to meet evolving threats and to provide new services
- A common trust framework to verify and trust each others identities
- The ability to control and audit who has access to what information
- Self Service administrative interfaces or automated interfaces where appropriate
- Network infrastructure access with greater visibility to combat fraud and other threats
- The ability to create collaborative and federated communities enabling individuals to use the same personal identification mechanism to sign-on to the network of more than one organisation and conduct transactions

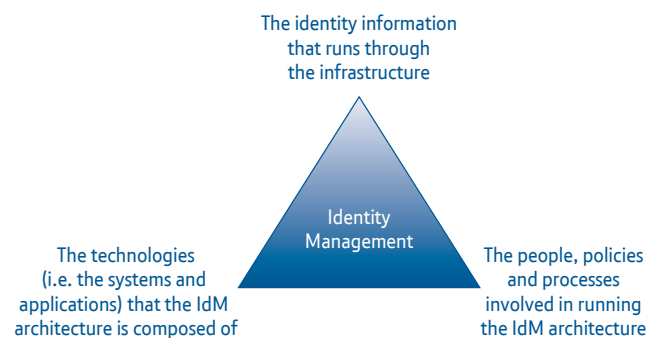
The first step to achieving this is to review and assess seven IdM architecture components across the following three areas of the business:

- 1) The people, policies and processes involved in running the IdM architecture
- 2) The technologies (e.g. the systems and applications) that the IdM architecture is composed of
- 3) The identity information that runs through the infrastructure

If any one of these three areas is weak, then the overall IdM infrastructure will perform poorly. While there is a tendency to focus on specific projects to deliver new technologies and software solutions, optimised business benefits in IdM can only be achieved by taking a holistic approach.

The IdM architecture components that should be assessed in this approach can be broadly grouped as follows:

- 1) **IdM architecture itself** – a higher level collection of policies and processes that are essential for the effective inter-working of the specific areas
- 2) **User Management** – the collection of technologies and processes that allow an identity to be created, maintained and distributed in a consistent and auditable manner
- 3) **Authentication** – the collection of technologies and processes used to determine that users are who they claim to be
- 4) **Authorisation** – or ‘Access Management’ – establishing a user is authorised to perform the action they wish to undertake
- 5) **Audit** – reviewing and ensuring all operations involving identity are properly and securely undertaken according to company policy and external legislation
- 6) **Extended Enterprise** – working with business partners and internal separate organisations in an ‘extended enterprise’ e.g. through Federated IdM
- 7) **Application Exploitation** – how effectively the business applications and other services are exploiting the IdM infrastructure



This assessment of IdM architecture components across the business enables organisations to understand any risks involved in their IdM strategy and current implementation. This also enables the organisation to more clearly identify areas of improvement and the benefits these changes will bring. With a comprehensive understanding, an organisation can build a business case. This can be presented to stakeholders and budget holders to secure investment and enable the development of an IdM architecture and transformation of IT processes aligned with business priorities. New technologies that offer more offensive threat response are key to IT transformation that can better address identity management challenges. In approximately three to five years, the new types of products and services underpinned by a critical requirement for good identity management will be as follows:

Technology area	Products and services
Networks and infrastructure	Converging services Broadband wireless Everything over IP Grid
Software	Web as platform Social technologies Semantic technologies Web 2.0 Open systems
Applications	Location Ambient intelligence Business process automation Internet protocol television (IPTV)
Security	Internet Protocol / Multiprotocol Label Switching (IP/MPLS) control plane security Border Gateway Protocol/routing protocol security End-end VOIP/multimedia security Traffic analysis and visualisation Mobile/wireless security Ambient Networks
Bio and nanotechnology	Genomics and Proteonomics

The appropriate technologies do not end here and BT predicts that, within five to ten years, there will be a need for completely new business and technology reflecting a growing emphasis on users as the “network nodes”, which are detailed below:

Technology area	Products and services
Networks and infrastructure	Open Spectrum Gigabit Ethernet anywhere Neural networks and artificial intelligence
Software	Web 3.0 Automatic software Generation
Applications	Intelligent and aware systems Virtual worlds become economically important Ubiquitous computing Quantum computing
Security	Heterotechnochronicity (old and new coexisting) The end of reusable passwords Firewalls are dated – layered defences in applications, networks and devices Perimeterless networks will become the norm Log file analysis to be real-time and the response proactive Emergence of independent stochastically operating software agents
Bio and nanotechnology	Human enhancement — logical and physical identities continue to merge

Sharing responsibility

Business and society's defence against identity theft should be one reflecting a culture of shared responsibility in which everyone plays their part:

Governments have introduced many data security laws, but there is still scope for improvement. For instance, the theft of identity in the UK is still not a crime: it is only the subsequent use of the identity information for gain that is a crime. Furthermore, there is no central facility for responding to and recovering from identity theft. Changing this would send a clear signal of intent.

Industry must strive to better understand how information is gathered and used, educate users and make it easier for them to take preventative action without any unexpected shift of liability. Evaluating vulnerabilities across all aspects of the business, and developing consistent and enforceable policies are required. However implementing more offensive, yet compliant, threat responses and best security practices are most important.

Identity management solution providers need to continually develop more advanced technologies that effectively balance risk, cost and convenience in context.

Universities and research bodies need to further the body of research on how to effectively mitigate the risks in context through more interdisciplinary cooperation between social and computer scientists as well as collaborative partnerships between academic institutions and business.

Individual citizens also have a responsibility to become more aware of the risks and how they can take personal responsibility to better protect and control their personal information. For example, keeping personal information secure and regularly obtaining a copy of your personal credit file from credit card agencies.

Standards need to evolve in a way that incorporates policy and best practice as well as to converge towards one consistent technology framework.

Moving towards an identity-centric society

Since identity theft threatens the core of society's wellbeing, the place of identity as a central organising principle to create secure cost-effective environments that offer a competitive advantage is growing. This is likely to lead to a new cultural and economic model built upon the foundations of identity as the network node in tomorrow's 'network of networks.' The transformation resulting in a 'new world' revolving around our logical selves, or digital identities, will not occur overnight. Policy frameworks, technology approaches, legal readiness and the associated social and economic repercussions will unravel across a number of generations.

The key to achieving successful identity management solutions is to become more sophisticated about risk, carefully balancing the risk, costs, usability, and compliance issues across different sectors and in context. Embracing fresh approaches to risk and cost-effectively managing the transition to more secure identity management over appropriate timescales are critical. A business focus involving cost and risk is not enough, however, and a consumer-focus is vital to ensure easy and convenient use of services. The sheer scale and complexity of networks coupled with a need to enable user interactions and information sharing across a wide range of platforms and business services further complicates matters. The issues will gradually extend all business models right down through the supply chain to the consumer or citizen. It is in this way that the shift to identity-centric approaches will change the face of society and business as we know it.

About the Authors

John Madelin, Head of UK Practice for Business Continuity, Security and Governance, BT, is a Chartered Accountant with an MBA from Manchester Business School. He is also a Board Member of the Information Assurance Advisory Council, a member of the Institute of Information Security Professionals (IISP) and has held advisory board positions for a variety of start-ups in the technology sector.

Richard Baker, IdM Lead Consultant, Business Continuity, Security and Governance Practice, BT, has worked with product vendors, end-user organisations and systems integrators. He also contributes to international standards development in communications and identity solutions.

BT as your security partner

BT has been managing, operating and deploying complex global Identity Management Infrastructure solutions for more than a decade. This experience of delivering Identity Management is supplemented by administering BT's own network, the largest in Europe. Our Enterprise Directory Management solution, for instance, delivers savings of £88 million a year.

References

Allan, Ant., Heiser, Jay., Litan, Avivah., Newton, Alistair and Wagner, Ray. (May 2006) State of the Art for Online Consumer Authentication. Gartner

CIFAS (11/2006) Identity Fraud Rises but British Business is Winning the Fight. Available at http://www.cifas.org.uk/press_20061108.asp

Home Office Identity Fraud Steering Committee (2006) Identity Theft www.identitytheft.org.uk

Lacoehe, Hazel., Crane, Stephen and Phippen, Andy. (October 2006) Trustguide: Final Report Available at: <http://www.trustguide.org.uk/Trustguide%20-%20Final%20Report.pdf>

Lacoehe, Hazel., Crane, Stephen and Phippen, Andy. (October 2006) Trustguide: Response to the Lords Science and Technology Committee to Investigate Personal Internet Security

Ponemon Institute (08/2006) Press release: Ponemon Institute Study Shows Lack of Accountability, Resources at the Root of US Corporate Data Loss Problem. Available at http://www.ponemon.org/press/Ponemon_Port_AuthorityDetectPr.pdf

Ponemon, Larry (10/2006) Ponemon Data Breach Study. Ponemon Institute

UK Department of Trade and Industry (DTI) Information Security Breaches Survey 2006: Identity and Access Management Available at: <http://www.dti.gov.uk/files/file28343.pdf>

Identity Theft Resource Center. (10/2006) Find Out More About the Nations Fastest Growing Crime. Available at: http://www.idtheftcenter.org/factsandstats_1006.pdf

Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

© British Telecommunications plc 2007
Registered office: 81 Newgate Street, London. EC1A 7AJ
Registered in England No. 1800000.

Designed by Unigraph Limited 22872/02/07.

PHME 52223

