

## Securing the benefits of globalisation • Part III, Chapter 7

Insights  
from  
Unisys

**Bart de Maertelaere,**  
*EMEIA Security Services Lead*

**Bertrand Bouteloup,**  
*EMEIA Security Business Development Director*

### Global security management

Information technology can be viewed as a key driver of globalisation or a deadweight, depending on how progressively one views the term. Either way, IT is undeniably one of the contemporary CEO's primary concerns as it supports global business, whether in a centralised or decentralised manner. It should be addressed on cost basis as well as with security and / or compliance with regulatory requirements.

#### | Drivers for global security

Yet, as companies open their information platforms to the external world (so as to adapt to new customer needs, business requirements and competitive pressures), the threats that these infrastructures face augment extensively. If, in its earlier moment, hacking was a contest of gamesmanship – a demonstration that one could break any IT security – it is now political, commercial *and* criminal: hackers attack organisations, and their distributed infrastructures, from anywhere and at anytime, to gain political advantage or profit. Information and com-

## **Securing the benefits of globalisation**

munication technologies (ICT) are the weapons of choice for today's endlessly inventive Internet desperados. Amongst other examples, their recent exploits include the distributed denial of services attacks through botnets<sup>1</sup> or phishing attacks<sup>2</sup> – the latter of which is especially worrying for banks as it threatens to restrict the development of online banking (the withering confidence of online banking customers equals its potential diminution as a financial service).

### ***Proactive and reactive regulations***

As with globalisation, so with regulation. Consider, for example, what UK financial institutions must now comply with (chronologically):

- The 1998 Data Protection Act
- The Turnbull Guidance for the Combined Code (1999)
- The Freedom of Information Act (2000)
- Sarbanes-Oxley Act (2002)
- Anti-money Laundering Regulation (2003)
- Privacy and Electronic Communication (EC directive) Regulations (2003)
- Basle II (Financial Services, circa 2004)
- The Companies Act 1985 Regulations (2005)

Many of these standards and regulations have been written proactively so as to enable and support globalisation. In so doing, they have pushed public and private organisations to adopt a holistic and global security framework. Basle II is exemplary in this regard as it mandates banks to identify, assess, monitor and mitigate operational risk. Hence, IT security operational risk management are now day-to-day board preoccupations.

### ***Technology has evolved***

Banks are not the only organisations with security concerns as the development of connectivity and networks raise new threats that apply to diverse infrastructures. Not long ago, personal computers were hooked up to a serv-

1. A botnet is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet.

2. Act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

er using local area network (LAN), limited to single office buildings. When branch-offices got interconnected, wide area networks (WAN) developed. Now, virtual private networks (VPNs) support global business by interconnecting people across the Internet.

Over the last decade, point solutions from firewalls to intrusion detection systems and antivirus protections have been developed for companies and their subsidiaries. Monitoring and management consoles have likewise been created to administer these solutions. However, these are seldom perfect as the millions of logs they supervise make it virtually impossible, in practice, to assess risk. In a global business scenario, a *master* management view is required.

Technology vendors have thus developed new solutions entitled SIM (Security Information Management) and SEM (Security Event Monitoring) that enable the correlation of huge amounts of security events across technologies, and generate meaningful security incidents to support effective action. They also offer advanced reporting technologies to provide a clear vision of the security service delivered for the entire network.

### ***Taking stock of the global ICT infrastructure***

Ceaseless waves of innovation in the ICT domain have enabled both private and public organisations to run their operations from anywhere, anytime. This new generation of technologies lives by one fundamental slogan: *the world is your home*.

The available functionalities have drastically shifted the position, and importance, of the ICT layer. Initially no more than a supportive platform, ICT now stands at the core of an organisation's operations. Indeed, if communications between enterprises and their customers / partners are no longer supported by ICT, they are nevertheless enabled by it. The same holds for public organisations as interactions between the administration and its citizens are becoming ever more digital. Hence the need for ICT to be available without interruptions. Mergers and acquisitions, small and large, occur daily, a theme echoed throughout the pages of this book. This creates heterogeneous infrastructures that are costly and difficult to manage, whilst the demand for availability and flexibility is high.

Trust has also become a primary focus, especially online. Tantamount to Internet transacting is a belief (on behalf of end users) in the integrity and security of a company's solution.

## Global Trends

### ***The need for a 'follow the sun' security management***

Global business is a fact, and it is manifest 24 hours per day, 365 days per year, worldwide. Similarly, the enabling ICT infrastructure has to be continuously available. Any service interruption has a direct business impact and will result in missed revenues, if not more severe costs.

Of course, the 24 / 7, globally distributed enterprise is a target for intruders and mischievous hackers who seek to exploit the infrastructure's weakest link. The chain is only as strong as its weakest part, an ever-pertinent adage at a moment when the impact of an intrusion or a denial of service is potentially irreparable.

As a consequence, public and private organisations are required to manage their IT security on a continuous basis. Several responses have emerged:

- Full outsourcing of security monitoring and management. In this scenario, companies rely on a Managed Security Service Provider (MSSP) or an outsourcing firm to administer their critical infrastructure;
- In sourcing or building their own Global Security Operation Centre. Here, both the monitoring and the management will be ensured by the organisation in question;
- A hybrid solution where a MSSP, or an outsourcing firm, performs the monitoring and recommends actions to be executed by the organisation, itself.

Most of organisations, whether local or global, are now looking at these solutions to mitigate their operational risks and to reduce the operating costs of security. For example, French organisations have generally stuck to insourcing, while outsourcing dominates in the UK. Whatever the chosen option, the points of emphasis from a security perspective are shifting from network, to application- and data-centric.

As companies become virtually diffuse, effective workflow management will rise in importance. This requires flexible connectivity that can be quickly modified to accommodate new information and work groups.

These evolutions make security event and incident management a complex matter, as many decisions will have an impact on both the application level and business environment. Delegation of authority and swift reactions to constantly evolving incidents need to be addressed proactively; escalation paths and chains of decision need to be predefined.

### ***A new generation of CSO***

The first generation of IT security officers witnessed the regime of Chief Security Officers (CSOs) who were often members of an organisation's IT staff. The CSO was technical and he / she was network-centric. Budgets were missing or limited. A holistic and integrated approach was not institutionalised. CSOs tended to be reactive, implementing point solutions for point problems. They were mostly isolated from the company's core business and human resources concerns. Their policies and procedures were built on a zero-tolerance approach. The eventual principles of governance were solely inspired by IT, not by the business.

With the global and distributed business environment, a CSO's skill-set has changed: an understanding of compliancy and risk management is necessary; sensitivity to business interests, paramount. This has spawned a new generation of CSOs. The operational risk manager is firmly connected to the business, human resources and financial dimensions. He has a seat in the boardroom, or at least reports to a member of the boardroom. The policies and procedures are based on a balanced and proactive approach, inspired by operational risk management. There is a company-wide holistic approach that covers network, applications / data and people / process. The operational risk manager operates under a corporate governance model and addresses the security requirements in a phased and prioritized approach.

The 2004 *Global Information Security Survey* (conducted by CIO Magazine and PWC) exemplifies the altered terms of the game: in 2004, half as many security executives reported to IT as they did in 2003; significantly more reported directly to the CEO; and, three times as many reported to high-level business functions or groups.

## Securing the benefits of globalisation

### *Identity and access management*

In this new world, it becomes more and more difficult to monitor and manage 'who has access to what information'. For this reason, the interest for identity and access management solution is growing.

Chart 1 lists some examples of auditor objectives and their logging and reporting.

**Chart 1**

<b>Examples of auditors objectives</b>	<b>Logging and reporting</b>
1. Determine if access rights granted to users are consistent with policy	List of users and their access privileges
2. Determine who has access to particular systems	List of resources and the users who are authorized to access them
3. Ensure user accountability	For a particular user, list actions over a period of time
4. Ensure that terminated employees access rights are revoked in a timely manner	For users who are terminated employees, list access rights and note when they are revoked
5. Validate that attempts to gain unauthorized access to systems are logged and are followed up on a timely basis	List all unsuccessful attempts to gain access to a particular system

Identity and Access Management (IAM) solutions deliver clear answers to these needs, through:

1. Building an effective information security strategy based on implementing best practices with leading IAM solutions;
2. Meeting the requirements of multiple current regulations as well as pending regulation;
3. Lowering the ongoing costs of compliance;
4. Reducing complexity through consistent approaches across the enterprise; and,
5. Promoting commerce, which, in turn, enables more online access to information against a backdrop of increasing threats.

These projects have to be global and must comprise the organisation's complete identity (employees, contractors, customers, etc.). Over the last year, the largest banks have started to implement the first phases of an IAM solution. Some have started with 'Single Sign On' to both improve productivity and reduce security risks due to multi-password use; others have begun to experiment with provisioning solutions to reduce operation costs, and so on.

### ***Addressing network complexity***

In 'Converging Technologies: the Future of the Global Information Society'<sup>3</sup>, Christopher Altman discusses: 'An omni-linked world populated with intelligent artefacts [that] will bring sweeping changes to virtually every facet of modern life – from science and education to industry and commerce – leaving no segment of society unaffected by its advance.'

Following Altman's observations, the Internet is gradually becoming the underlying architecture and informational foundation of global business, whilst the notion of the 'Network' emerges as a central theme of our time: networks of politics and education; networks of collaboration; telephone and mail networks; power and industrial networks; commercial networks comprising vertical market groupings; peer to peer networks; networks of terrorism; river and transportation networks; neural networks; ecological and food networks; corporate ownership networks; and a variety of communities of interest – not withstanding cooperatives, consortia, and diverse alternative associations, ever yet.

Because the Internet so fundamentally transforms the global economy, traditional systems do not suffice to manage these complex adaptive systems. This observation has profound implications for the ownership, management and control of business – in particular, an increasing dependence of corporate network architectures on the Internet, and network boundaries, which no longer reflect archetypal commercial infrastructures. Most corporations still use deterministic models to build their protection mechanisms – building, controlling, structuring and managing – whereas network behaviour is closer to that of biological ecosystems rather than business architectures.

At the structural level of ICT, as businesses recognise that the Internet will

3. Christopher ALTMAN, "Converging Technologies: The Future of the Global Information Society" (UNISCA, First Committee Chair Report to the UN General Assembly, 2002).

## **Securing the benefits of globalisation**

become their underlying network architecture, they may feel the need to 'let go' and 'lose control' of the existing monolithic command and control approaches to expansion. However, we need to conceive of the business and underlying ICT architecture more as shifting sands – an advancing of business solutions that appropriately balance flexibility with diagnosis, prediction and, most importantly, accountability.

### ***Identity networks***

Identity is emerging as the most tangible mechanism for conversation and exchange in commercial and social relationships; it will soon become the mechanism for understanding responsibility, context, and interaction, for establishing accountability, and for distilling order from the chaos of the tightly coupled connections of today's proprietary architectures.

Due to the scale with which networks are growing – in terms of the number of users, devices, services, back-end systems, and so on – their underlying complexity has exploded so exponentially that efficient management is no longer possible (the variables are simply too many). Moreover, businesses are finding that the complexity problem is now being compounded by limitations in the underlying architecture, both in terms of costs and flexibility. This places unacceptable limitations on a 'global business' agility seeking to capitalise on the increasing diversity in their business environment – and which consequently results in lost opportunity and reduced growth.

The continuing explosion in complexity is causing businesses to hone in on the cost of managing and maintaining support infrastructures. However, the current solution of incremental expansion is no longer sustainable from a cost perspective, a reason why more and more businesses try to capitalise on the apparent advantages of IT outsourcing. In so doing, they have ironically inherited an unknown 'scala' of potential security issues.

But the available technology cannot sustain the incremental expansion either. So, we also see a simultaneous uptake of distributed computing driving a degree of availability and readiness. Security has everything to do with a proper understanding of who users are (e.g. confirmation of their identity), what they can access and how / when they retire that privilege.

Evolving the role of security from defensive to proactive naturally results in models that enable businesses to unlock the value of information stored in their IT systems and to get that information into the hands of the right end-

user – customers, employees, business partners, contractors, whomever – when they need it, securely.

Identity and access management are thus becoming key to security management, as:

- Collaboration and trading amongst multiple business entities accelerate;
- ‘Vitalising’ initiatives – such as outsourcing and off-shoring, or diverse consortia and joint ventures – hasten. These factors combine to make ownership of the underlying infrastructure less clear, and more thinly spread amongst the business constituents;
- Competition intensifies, driving the need for faster market responsiveness and fulfilment. In a growing and economically unstable environment, the business extends *virtually* rather than *physically*. Companies must aim to ‘do more with less’, and to reduce costs in the face of new competitors;
- Regulatory requirements imposed upon companies encourage them to track the action of end-users of their information system so as to ensure that their actions will be auditable. Regulation serves to define, and advance, roles and profile definitions.

The new global business generation needs to conceptualise novel approaches to designing operational platforms that will emphasise flexibility, responsiveness, collaboration and co-opetition, and that will be centred on identities (people, devices and applications) and their mobility, both in physical and contextual terms.

Global businesses must operate successfully within a virtual network of mobile and remote employees, business partners, consultants and outsourcers. The days of businesses as self-contained entities are ending; the core network is shrinking and there is a growing reliance on more open, fluid and dynamic business supply chains that run on technical architectures extant outside of the core.

The global business needs to adapt to conditions of high velocity, innovation and change. *Agility* has become a buzzword, signalling the ability to permanently update business models, operational processes and technical architectures. But *accountability* is as key. In these fluid and dynamic models, businesses will need to know who did what, to whom, and why – and whether it occurred within their business domain or responsibility, or not.

In this world, *security* is becoming synonymous with *identity*.

## **Securing the benefits of globalisation**

- *Risk, trust, brand* and a more holistic, and actuarial, approach to managing your business globally are key.
- Now constituting a central organising principle, *identity* solves many of today's problems: complexity, collaboration, accountability, availability, etc.
- Envisioning people as the *real* network nodes (behind the device or application, travelling across the network) and the 'way-points' in extended business process – irrespective of boundaries and physical locations – has many commercial and logistical advantages.
- Standards now evolve more quickly and comprehensively than during any former historical moment. SAML, Liberty and WS 'Identity Standards' are maturing, and converging. This will enable an open and service-oriented world based on business processes and peoples' roles therein. Loosely coupled and portable identities will replace applications and platforms, the latter of which are poor proxies for real value-exchanges.

Security, as applied to an extending and traditional infrastructure, is required to stretch beyond its original design parameters, and it must adapt likewise. However, appropriate security measures often require considerable, and costly, administration when applied to multiple access paths, multiple methodologies, blurred boundaries and differing protocols. The network security approach of an organisation needs to be rethought. Today's objectives include: reducing costs, improving usability and delivering on the promise of flexibility. This new attitude reflects the identity-centric view. The dynamics impacting the security allow for IAM to support the business benefits whilst facilitating the requisite risk reduction and assurance.

IAM begins by establishing and providing a strong identity, ensuring that 'you are who you say you are' – irrespectively of device, location, or application. This, alone, stands as a powerful and cost effective asset. A strong identity increases transactional confidence and can be enriched by adding other static and dynamic attributes that empower the enterprise. The value of identity can be passed into an enterprise's applications through 'Single Sign On', and carried across domains through the extension of a 'virtual and global organisation' which encompasses business partners and other affiliated parties worldwide. Brands can be strengthened in association, and customer loyalty increased; the business benefits are staggering, indeed.

The emphasis on *identities* is accelerating and is reflected not just in chang-

ing consumer behaviours or evolving business models, but so in every one of the major platform vendors unified around a core competence of IAM. This applies unilaterally from 'apartment block to nomad' – from a bastion / perimeter approach to a mobile / nomad approach with an undefined perimeter – and requires a shift from infrastructure-based security to application / data and identity security.

### ***The fabric of our lives is changing***

Signals of a (technological) revolution are present. The fabric of our economic, commercial, and recreational lives is up for grabs. 'Identities' are now being emphasised at every level.

This groundswell is triggered by unique dynamics coming together in a perfect storm of change. Newfound life is being given to our biological selves. Levels of automation, informational perfection, and connection are enabled in previously inconceivable ways. The momentum is accelerating and is reflected not just in changing consumer behaviours and evolving business models, but also in all of the major platform vendors unifying around IAM.

Three-letter acronyms have come and gone, but none has impacted the landscape so quickly, so fundamentally. The sheer scale of investment on the enabling technology brings a richness and meaning to our online persona. More importantly, it has accelerated issues of trust, privacy, regulation and control. These themes are counter-points to the looseness and agility of web-based models, but they represent a fundamental catalyst without which the real technological potential cannot be realised. Effective mechanisms have evolved to balance the conflicting needs of security and openness; freedom and control; privacy and invasiveness. For the first time, the high degrees of control are within our grasp.

As identity-centric models increase momentum, and as the blur of transactions and information exchanges crackle across the complex arrangement of network 'neurons' at light speed, the game moves into another dimension...