CHAPTER 1

Power to the people

The power is out there . . . somewhere

What is power? And who holds its key? Many seek it. Some try to seize it. A few get to exercise it. Not all are successful. Power is an elusive goal.

Most people imagine power in terms of a kind of force or strength being exerted. That might be true for some types of power. But it's the wrong perspective for understanding power over *people*. Because in practice, such power is less about personal status, physical strength or money – though these things help – but more about how other people respond to you. Power over people is in the eye of the beholder. And you can't always buy that or gain it through status or force of arms.

It's harder to manipulate people when they're joined up through networks. And that trend is growing. That's why, these days, even prime ministers and presidents can appear powerless. And it's why captains of industry find it difficult to drive change across their organizations.

I asked a top CEO what it felt like, today, to be in charge of a big modern organization. He replied:

> *'It's like driving a big bus, except that the wheels aren't connected to the steering wheel.'*

If you work in a large enterprise, you'll already have noticed this phenomenon. It's becoming harder to make an impact on your fellow managers and staff. That's never been easy of course. But it's more challenging today. And the situation on

Managing the Human Factor in Information Security David Lacey

the ground is much worse than you imagine. You'd be shocked if you carried out a review of how many company staff actually understand and follow your corporate policies.

I know this because I recently carried out such a survey, across dozens of organizations. The results made grim reading. The fact is that many corporate policies are not understood, communicated, implemented or enforced. Yet policy is the basis of information security. So either we've failed to get the message across, or for some reason, it's being widely ignored. But that's not just down to our own lack of competence. In fact, it's a characteristic of a modern, networked society.

An information-rich world

In today's fast-changing, information-rich world, people have many distractions. The relentless flood of e-mails is only the tip of the iceberg. A typical information worker will check his or her e-mail at least 50 times a day. But they will also look up a similar number of websites. And even more disruptive is the growing flow of real-time, instant or text messages.

Lost productivity from such distractions is estimated to be costing many hundreds of billions of dollars a year, though nobody seems to have measured the corresponding increases in efficiency that the technology brings. The jury is therefore still out on the balance of the benefits and costs presented by new network technologies.

But new technology is necessary to attract young graduates. And that provides a major edge in the growing competition to attract new talent. It's not surprising, therefore, to find that top companies that aim to attract the best staff, such as Goldman Sachs, until recently are amongst the most advanced companies in introducing the latest network technologies.

The end result is that people today have to be selective about what they pay attention to. They will concentrate on the issues that are most relevant to their immediate, personal needs.

Modern managers have little time for quiet reflection about speculative, security risks and their consequences. And, increasingly, they will prefer to consult networked colleagues or public websites for advice on new issues, rather than asking official advisers.

It's also hard to get subtle points across on complex subjects. And it's virtually impossible to communicate lengthy policies and procedures with any real degree of success. When, for example, was the last time you read an instruction manual? Yet that's what information security managers expect from company staff. And even if you can find the time to read it, how much of it would you remember? And what would prompt you to apply it?

In fact, traditional approaches to information security, such as publishing a thick manual of policies and standards, no longer work. They might be fine for enabling you, and your management, to tick your compliance boxes, to demonstrate that you're discharging your corporate responsibilities. But lengthy edicts are ineffective as a means of influencing staff. They should be consigned to the corporate dustbin.

We need to rethink and re-engineer the way we communicate and enforce our security policies. And that's no trivial feat, because the content is getting lengthier, and ever more complex. At the same time, many employers claim that literacy rates in the West are plummeting. It's becoming an enormous challenge to communicate complex security policies to a volatile organization that's constantly restructuring.

These are major challenges. We don't have all the answers. But there's quite a lot of change and improvement that needs to be applied. In particular, we need to shift from implementing security less on the basis of a 'tick-the-box' culture of defensive policy setting, and more on the basis of how people now think and behave.

We need to embrace, understand and exploit the social networks that are increasingly used by our colleagues and staff. Electronic networks are, in fact, both the source of the problem and the key to its solution.

When in doubt, phone a friend

Social networks empower managers, staff and customers. They don't operate on the same lines as traditional organization structures. They resist dominance, and they erode the traditional, hierarchical power bases in organizations. Social networks are disempowering head offices and corporate centres, weakening the influence of corporate security policy in organizations.

The nature of decision-making is changing, decisively, and for good. It's now much more a bottom-up, rather than a top-down process. Our thought leadership is no longer in the exclusive hands of a privileged group of central policy makers, and their consultants. It's out there in the peer-to-peer networks running across our enterprise infrastructures. Power is moving to the people.

Forrester Research, an independent technology and market research company, has been tracking this trend for several years. Amongst other things, they've noted that trust in institutions is progressively weakening, and that social networking is undermining traditional business models.

We can see this in many types of business. You no longer need a travel agent to sort out your holiday arrangements. You don't need to buy a copy of the *Good Food Guide* to find a decent restaurant. There are plenty of free opinions available on the Web. And they're just about good enough for most people.

The same holds true for most other sources of independent advice. Professional, independent experts are on the run. In fact, social networking might even make obsolete research analysts, such as Forrester themselves. At a Chief Information Officer Summit in Monaco a few years ago, I put this observation to Brian Kardon, their Chief Strategy Officer. 'Yes, that's a very good point. We've grasped that and are already working on the challenge,' he admitted.

In fact, the future of research is likely to be one that favors the specialist, niche operators. The broader, more general stuff can be freely accessed on the Internet.

The phrase 'The Long Tail', coined by Chris Anderson in a *Wired* magazine article, describes the tendency for business products, especially intellectual ones such as information services, to increasingly fragment in order to satisfy the individual needs of customers. The future of business is selling less of more. And

the same is true of security. We need to develop a broader portfolio of tailored advice that caters more closely to people's specific needs.

Engage with the public

Smart stakeholders instinctively respond to this trend and seek to engage with their customers. Forward-looking companies increasingly seek the views of the general public on their activities.

The Royal Dutch/Shell Group, for example, tries to engage with citizens by encouraging people to pose questions to Shell executives. They learned the importance of such public dialogue many years ago, following a high-profile media campaign mounted by Greenpeace in reaction to their proposed method of disposal of the Brent Spar oil storage buoy.

Politicians are also well advanced in embracing and exploiting web technologies and other forms of social networking. Most have their own websites. Some engage in daily web chats and invite electronic petitions. Number 10 Downing Street, for example, has, for some time, run a website where e-petitions can be created by the public. And most political parties religiously consult focus groups of citizens before taking a view on any aspect of public policy.

Even the Royal Society now spends as much time engaging with the public as it does debating the finer points of scientific developments. This famous institution firmly believes that science is a wider part of our culture and cannot flourish without the support of the wider community. Their 'Science in Society' program consults with members of the public from all walks of life and all geographic regions across the UK. That's something that could not have been contemplated a hundred years ago.

The power of the blogosphere

All corporate communications managers monitor the 'blogosphere'. It's an evolving network that links huge numbers of personal web logs, enabling them to connect, interact and amplify the thoughts of popular individuals.

A few years ago, Reuters encountered the power of the blogosphere when bloggers discovered that a photograph of an Israeli F-16 firing missiles on Lebanon had been slightly doctored, in order to make the photo appear more sensational. This incident had a major impact on Reuters' reputation, forcing them to rethink their news gathering strategy and to review the way they authenticate photographic images from their agents.

But more significant is the greater challenge that news agencies, such as Reuters, face as they contemplate moving towards a future news gathering process that is increasingly based on images captured by members of the public, rather than snapped by their trusted agents.

Blogging is very different from journalism. It's more conversational and it has a greater focus on personal views than objective reporting. And, unlike newspapers, blogs are interconnected, resulting in a powerful network aggregation effect.

Karl Schneider, a former executive editor of *New Scientist* and an expert on new forms of media, sees major changes in the role of journalists. He believes they will progress from being 'creators of news', to acting in a role similar to a 'disk jockey', becoming 'curators of information' and 'sowers of seeds'. Professional news gathering is changing, and will never be the same again.

The future of news

It's interesting to speculate on the longer-term future of professional news services. Several years ago a flash movie called EPIC 2014 appeared on the Internet. It provided a fascinating glimpse of how news gathering might evolve over the next decade, shaped by competition from the progressive mergers and increasing dominance of big Internet companies.

The film also introduced a new word 'Googlezon' to the English language. As we'll see in a later chapter, it can be a useful marketing trick to invent a catchy word or phrase, if you're aiming to make a lasting impact with a memorable message.

In the film, Googlezon is a fictional company created when Google merges with Amazon. Eventually the company creates a news product called EPIC, the 'Evolving Personalized Information Construct', which automatically creates news that is tailored to individuals, without the need for journalists.

This eventually leads to the 'news wars' of 2010, in which Googlezon triumphs, triggering the downfall of the *New York Times*, which is forced to move offline, becoming 'a print newsletter for the elite and the elderly'.

Whatever your views on the conduct or capability of the media, it's clear that the death of professional news services would be a major blow to society. Whether or not professional journalists can survive, it's certain that the future of news will be based on assemblies of citizen information, of varying accuracy and reliability, increasingly personalized to meet consumer tastes, defined by their historical network activity.

Leveraging new ideas

Social networks are surprisingly powerful, perhaps more so than most people realize. They threaten to undermine any long-standing institution that fails to engage with them. Networks are a powerful leveller, with little respect for status or authority, and a potent means of leveraging individual ideas and initiatives.

Some people can single-handedly transform organizations, cultures or countries. Great men like Gandhi and Nelson Mandela seem to effortlessly change the mindset of huge numbers of people. In the field of technology Bill Gates, Tim Berners-Lee and Steve Jobs have also driven through large-scale culture change. They were exceptional individuals, of course. But how did they do it? Were they lucky, timely, charismatic, or did they discover a magic formula for persuading people to follow and support them?

Perhaps it's a combination of all or most of those things. But one thing is certain. However they approached it, their success was achieved by creating a critical mass

of support across a social network. Either by chance or by design, they acted in a way that appealed to people, they created a compelling message. And at the same time, they were able to harness the power of social networks. They created a virtuous circle, a positive feedback loop that grew and grew.

In an increasingly networked society that's the key to success. Whatever you're trying to achieve, you have to find an effective means to capture people's attention, develop a compelling justification, communicate in the language they understand and exploit their support, not just on an individual, one-to-one basis, but across a networked community.

Changing the way we live

Networks are the engine of the information age, arguably the modern equivalent of the factory to the industrial age. Wherever you look, digital networks, and the flows of knowledge and ideas they convey, are transforming the balance of power across business, society and politics.

Networks are flattening organizational structures, extending supply chains beyond traditional borders, enabling the globalization of markets, businesses and beliefs. They're making billionaires out of twenty-something, Californian geeks. They're changing the way we live and work, and they're upsetting the balance of political power in the world. And there's a lot more change to come.

Where will it lead? What will be the long-term impact on our everyday life? In fact, there are numerous dimensions to the impact of networks. And many are uncertain or unknown. But we already know some of the implications.

Urban planners, for example, have long experience of studying the impact of disruptive infrastructure changes such as the introduction of roads, railways, electricity and piped water. So it's not surprising to find that leading experts in this field have already assessed the impact of the Internet on urban life.

Around 10 years ago, Professor William Mitchell, Dean of the School of Architecture and Planning at MIT, published an illuminating book called *e-topia*, setting out some of the implications of digital networks for urban planning. In particular, he spotted a number of interesting trends in US planning.

Technology companies, for example, have been progressively moving out of cities, in search of knowledge workers who prefer leafy suburbs. Millionaires prefer to migrate to upscale resorts, with good airport connections. That leaves the cities to young, single people and the businesses that need to employ them. 'Sex brings cities alive', as he puts it.

Observers in Seattle have already spotted radical, new patterns in commuting, such as the 'reverse commute' where male computer scientists, from Microsoft's suburban complex, race downtown after work each day in search of females.

I wondered how these trends might play out across in other countries, such as the UK, so I asked a logistics professor at a London university whether he expected to see the same type of changes. 'No,' he replied, 'that won't happen here, for all sorts of reasons, such as planning restrictions.' 'What might it be like then?' I asked. 'Just a lot more urban sprawl,' he replied.

But however the land lies, mobility, and the nomadic working style it enables, will have a progressive impact on our working methods, and our office and social life. Multi-tasking – checking our e-mails, sending text messages and answering telephone calls, whilst travelling, cooking a meal or attending a meeting – is here to stay.

Dilbert-style cubicles are no longer necessary for staff that can hot-desk or access everything they need while travelling. Who needs an office when there are plenty of Starbucks coffee houses and wine bars in which to meet or touch down?

William Mitchell also suggests that 21st century building design and aesthetics will probably turn out to be the exact opposite of the sci-fi chic that futurists of the past imagined. Modern architects are now thinking more in terms of light, air, trees and gardens. And future building designs will also need more nooks and crannies, in order to provide privacy for individual laptop workers.

One of the most significant impacts of the growth of the connected society is a major shift in focus, from networking with people who happen to be within physical reach, to cooperating more with on-line, distant colleagues. People are becoming more dependent on the stronger ties they develop over networks, rather than the increasingly weaker ties they make through physical encounters.

We can reach many people through networks, but, perhaps paradoxically, digital networks also encourage the growth of isolated, always-connected, virtual cliques, making it harder for outsiders to gain attention. They strengthen digital families and established communities and weaken the influence of strangers. This phenomenon introduces both threats and opportunities for security managers aiming to make an impact on a workforce that is increasingly networked and mobile.

Transforming the political landscape

Networks, and the globalization they enable, have also transformed the international political landscape. The World is now positioned at a crossroads, where political power is shifting to new regions and countries, and existing regional and international institutions are struggling to exert their traditional level of influence.

The US National Intelligence Council regularly conducts long-range research and consultation exercises, to provide their policy makers with a view of how global developments might evolve over the next 15 years. Their recent report *Mapping the Global Future*, published in 2005, considered global trends up to the Year 2020. Amongst other things, they noted that:

> *'At no time since the formation of the Western Alliance system in 1949 have the shape and nature of international alignments been in such a state of flux.'*

Futurists Alvin and Heidi Toffler were amongst the first to understand the transformational power of technology and networks. They set out their theories in a classic series of books published in the seventies and eighties. The ideas set out

in these books were decades ahead of their time, so few business managers and citizens paid much attention to them.

But the Tofflers made a deep impression on governments and political stakeholders. Their book *The Third Wave* became a bestselling book in China, the second ranked bestseller of all time just behind a work by Mao Zedong, and an underground cult book in countries such as Poland. It helped transform US military doctrine, encouraging smarter tactics and weapons. And it transformed politic thinking across the globe, even though these days you'd be lucky to find a copy in a British bookshop.

I experienced a flavour of this book's influence when I visited Romania in the mid 1990s. My driver, like many locals, was naturally inquisitive about my lifestyle. He asked me what I did. I told him I worked in information technology. 'That's great,' he said, 'I'm just reading Alvin Toffler's book: The Third Wave.' I was impressed. 'It's also one of my favourite books,' I confided. Then, as he dropped me off at the airport, he leaned over and asked 'Will you ever meet Alvin Toffler?' 'I don't know,' I replied, 'it's possible. And if I do, I'll pass on your compliments.' 'No,' he said, 'please convey to him the thanks of one million Romanian citizens.'

I never did get to meet Alvin Toffler, but I did manage to close the loop. Several years later, I was having a beer in an Amsterdam Hotel with John Perry Barlow, founder of the Electronic Freedom Foundation and one-time rancher and Grateful Dead lyricist. I commented on how much his ideas aligned with Toffler's. 'That's because I admire him, and he's a good friend of mine,' he replied. So I told him the story about my experience in Romania. 'Wow, that's cool,' he said, 'I'm seeing Alvin next week. I'll tell him. He'll be knocked out.'

It's remarkable to think that a driver in Romania could be a mere three steps away from his literary hero, a person who inhabits an entirely different business and social world, in a continent many thousands of miles away. And that's just through the power of a physical, social network. Just imagine what electronic ones could do.

Network effects in business

The concept of a 'network effect', the idea that a product or service can grow in value as more and more people adopt it, is an old one, first pointed out by Theodore Vail, president of Bell Telephone, around a century ago. It's fairly obvious, of course, that the more people who have a telephone, the more calls you can make. But it took many years for the idea to be studied seriously by economists.

In fact, academics who study network effects, such as the former Stanford University Economics Professor Brian Arthur, have been both in and out of fashion in recent years, with theories of how positive feedback loops in networks might channel global wealth into the hands of a handful of first-mover, electronic commerce conglomerates.

As with many other dot-com predictions, that didn't happen as fast as many investors had hoped, so much of the excitement about network effects in business

and economics has now calmed down. But there's a strong tendency for people to overestimate what will happen in the next year and underestimate what will happen in the next decade.

Many economists believe Brian Arthur got it wrong. Positive feedback loops present difficulties for economics. And there's little hard evidence to support his theory. But a lot of people didn't listen closely enough to the points he made. He differentiated *collaborative* networks, which grow more powerful with each new member, from others. There's plenty of the latter but few of the former.

For example, if we all buy a book from Amazon or a similar website, there's little collaborative value generated. In contrast, networks like e-Bay, Skype, Wikipedia and Facebook, get more useful with each new member or transaction. But there aren't enough examples of such sites, even though they are fantastically successful. The truth is that we've not been sufficiently imaginative to conceive, develop or exploit collaborative network effects. But that will, undoubtedly, come with time.

Being there

Electronic networks might be based on technology, but the resulting behaviour they generate bears more resemblance to an ecological system than a Swiss watch. Man-made, hub-and-spoke designs can create networks of surprising complexity and unpredictability. They are part of a class of networks called 'scale-free' networks, and they exhibit many unusual topological characteristics. They are, for example, more resistant to random failures than natural, organic networks, but they're also more vulnerable to deliberate attacks that target big hubs or spokes.

We are only just beginning to understand the strange properties of complex networks. Many researchers are now looking at parallels between network activity and other scientific fields. One interesting theory proposed by Ginestra Bianconi, a graduate student, is that, under certain conditions, a single node in a network can become dominant. This theory, which is based on an analogy with gaseous condensates in physics, suggests that some of the phenomena we observe in competitive networks, such as the 'first-mover advantage', the 'fit get richer' or the 'winner takes all' outcomes might actually be phases in the underlying evolution of networks.

A consequence of this theory is that the largest or fittest node, at any one time, does not always end up as the eventual, dominant participant. Networks appear to favour certain members at particular times, accelerating their influence to positions of high dominance. It's an advantage gained by being in the right place at the right time.

It might, in fact, be that large-scale success in networks is as much down to luck, as it is to skill, judgment or hard work. Networks are a great leveller. But they can also be a powerful kingmaker, under the right conditions.

Value in the digital age

Identifying value at risk is a key element of modern security and risk management. It shapes our priorities, countermeasures and enterprise programs. But where is

the value in business today? It's not just in the fixed assets and bank deposits. Increasingly it's in our intellectual assets: the brands, reputation and the knowledge and skills of our employees.

For many years, technologists and economists have been studying the nature and value of intellectual capital. Much of it resides in social networks. But how do you recognize it or measure it?

At the height of the dot-com boom in May 2000, a few months after the NASDAQ hit its peak, I attended a conference in Washington DC on 'Value and Values in The New Economy'. The conference was organized by TTI Vanguard, a private technology circle advised by luminaries including Gordon Bell, Alan Kay, Nicholas Negroponte, David Reed and Peter Cochrane.

The conference was attended by technology directors, economists and academics, and it focused on the shift of economic emphasis from 'things' to 'connections between things'. Amongst other things, the speakers and attendees debated how we could measure the true value of dot-com companies.

At that time it appeared that the main reason for the huge valuations placed on Internet companies was their potential for leveraging large numbers of customer relationships. Various formulae were proposed to quantify the future potential of a start-up company. For example, by calculating the number of customers they might be able to win, the value of each relationship they control, and the capability of the company to exploit these relationships. There were some fascinating theories and algorithms put forward to help assess intellectual value. But they were largely discredited when the dot-com bubble burst.

There were also some interesting ideas on security and risk management put forward at that conference. Professor Peter Strassman, for example, suggested that security effort should be exclusively focused on employees that generate the maximum intellectual value. This might turn out to be a trader, researcher or strategist, for example.

It's an interesting view, unfortunately too far ahead of its time. I could see it being impractical during a period when most organizations were struggling to patch up the weakest links in their infrastructure, rather than harden the protection around their crown jewels. But in the future, when basic security measures become pervasive, intellectual assets become easier to identify, and security threats become increasingly targeted at our most valuable assets, Peter's ideas will certainly be worth revisiting.

Hidden value in networks

Nevertheless, there is huge theoretical value lurking in networks, at least in theory. Metcalfe's Law, named after Robert Metcalfe, co-inventor of the Ethernet and a founder of 3Com, claims that the value of a network is proportional to the square of the number of users of the system.

This assertion is based on the number of relationships between individuals, the number of pairs that you can make. It assumes of course that some form of value can actually be derived from each relationship.

The way that pairs of relationships increase with the size of a network is quite unexpected. We often experience this phenomenon when we clink champagne

glasses at a celebration. When there are only three or four people, it's quite easy. Just a handful of clinks and it's done. But if you have a dozen people, it's surprisingly harder, requiring more than sixty clinks. And if you have than twenty people, it then rises to a couple of hundred clinks.

Robert Metcalfe was one of the most influential technologists of the 20th century. He's attained near legendary status in the industry. But he didn't always get his forecasts right. Amongst other things, he predicted the imminent collapse of the Internet and the death of open source software! When the Internet failed to collapse, Robert was compelled to eat his words, literally, by placing a paper copy of his forecast in a blender.

In fact Metcalfe understated the network relationship potential. Reed's Law, named after David Reed, an adjunct professor at MIT Media Lab and former Chief Scientist for Lotus Development Corporation, points out that the value of social networks scales exponentially with the number of members. That's because network relationships are not just confined to pairs. We also need to take account of larger sub-groups.

Exponential growth is a much faster rate of growth, proportional to the function's current value. For any exponentially growing quantity, the larger the quantity gets, the faster it grows. It's the sort of growth you get by progressive doubling, or even tripling. It's a sneaky form of growth, starting low and rising fast.

For example, if you place a single grain of wheat on the first square of a chessboard, then two grains on the next square, and so on, then by the time you reach the last square, you'll have reached more than a thousand times the total annual wheat production of the Earth. Early in the doubling sequence, the true power is not apparent to an observer. But after a few dozen operations the numbers become enormous.

Figure 1.1 overleaf illustrates the difference in growth between these two laws.

Theories, such Reed's Law, are purely academic if we don't know how to exploit them for real business value. But the potential prize is massive. There is huge latent value, perhaps waiting to be tapped in any large social network. This is why venture capitalists have been paying so much attention to investments in social networking technologies.

How hard can it be to exploit the power lurking in networks? That's the 64 dollar question. If we could find a way to tap just a small percentage of this power, then it would be valuable. In fact, there are some features of social networks that suggest it might be easier than we imagine.

For example, it's a rather surprising fact that the average path length between any two people in a human network is quite tiny, in comparison to the total number of network members. Most people have encountered this phenomenon as the 'six degrees of separation', which describes the counter-intuitive claim that you might be just six relationships away from anyone else on the Earth.

The idea of six degrees of separation was conceived by Stanley Milgram, a social psychologist, after experiments in which he sent out a set of packages to a random selection of people for onward transmission to a common recipient. Some observers have questioned the reliability of this claim, but a recent study of 30 billion instant messages by Microsoft researchers confirmed that the vast majority of people appear to be linked by seven or fewer acquaintances.

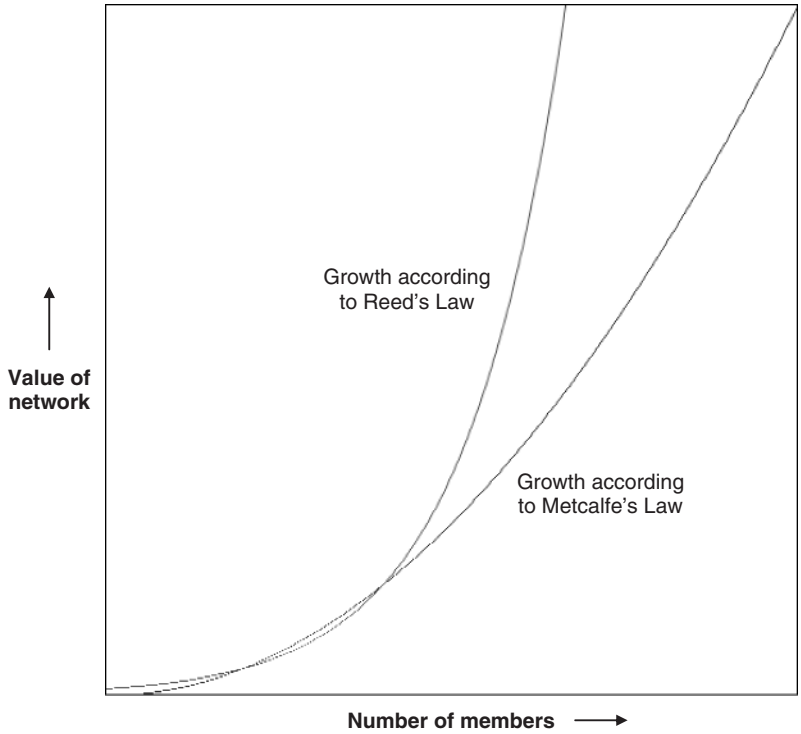

Figure 1.1 How value increases in networks with increasing membership

This surprising phenomenon explains why my Linked In account can proudly boast that I now have a staggering 27 000 professional connections just one step away from my small group of directly linked friends. Friends of friends are a powerful force that can be exploited for many purposes. It's a useful fact to know if you're seeking new employment, for example. Experienced human resources advisers will advise you that, statistically, you're far better off e-mailing your CV to friends than applying for advertised positions.

And in the security field we can use the power of social networks to cascade warning messages, or to request information about a current threat or event, or perhaps carry out a survey, or to seek assistance with a search operation. The potential of networks is only limited by our imagination. Unfortunately, in the security field, it's been the bad guys who've been first to recognize this potential. Mass mailers hijacked our address books and contact lists a decade ago, and social networks are already being exploited to distribute malware.

Network innovations create security challenges

Ever since their invention, developments in electronic networks have transformed day-to-day business life. At the same time, they've heightened security risks. It's interesting to take a step back and reflect on the impact of these changes on both

Table 1.1 The impact of network innovations on organizations and security

INNOVATION	ORGANIZATIONAL IMPACT	SECURITY IMPACT
Telegraphy and telephones	Changed the balance of power between head offices and their satellites	Heralded a new era of communications intelligence gathering
Electronic mail	Generated an explosion in person-to-person communications	Caused the collapse of traditional paper filing systems and security classification schemes
Joining up local area networks	Enabled enterprise knowledge sharing and rationalization of datacentres	Shattered the traditional security perimeters that protected many application systems
The Internet	Opened up a new world of electronic commerce	Introduced a 'Wild West' landscape of new security threats to retail systems
Secure remote access	Enabled home working and mobile access	Triggered the erosion of the barrier between personal and business lifestyles
Extranets	Enabled extended-enterprise working	Created new dependencies on the security behaviour of third party organizations
Wireless	Enabled high speed business contact from any location	Radiated company information outside the office environment
Social networking	Enables collaborative decision making and networking	Opens up new sources of information leakage and erodes authority of central security function

organizations and security, ever since William Sturgeon first laid the foundations for large-scale electronic communications.

Table 1.1 above lists the organizational impact, as well as the security impact of successive network innovations. You can see a common thread in these changes. Networks cut through barriers of all kinds, whether geographic, within organizations, between enterprises or between lifestyles.

We now call that 'de-perimeterization', a term originally coined by Jon Measham, my chief security researcher at Royal Mail Group. It's a word that is intended to encompass both the problem space and solution space, associated with managing security across boundaryless network environments. It's an inevitable and unstoppable consequence of modern technological progress.

Each advance results in a major breakthrough in business productivity. But at the same time they introduce lasting problems for the security of information, and the protection of critical infrastructure.

In practice, we never fully recover from the legacy impact of the earlier changes. Most of the effort in information security today is concerned with addressing problems created by unanticipated changes to the context of application systems and infrastructure that weren't originally designed to operate within a more hostile network environment.

You've been de-perimeterized!

In the early years of the 21st century, it seemed as though the future lay in hardening all business systems to operate across the Internet. But it was clear that the journey would be a long one, requiring new design principles and architecture.

I asked my security researchers at Royal Mail Group to develop a practical security architecture that was able to support the transition from a private network infrastructure to a public one. They delivered as promised, but the problem was that it made no sense to apply this in isolation. We would be able to operate securely outside the constraints of the enterprise. But unless other enterprises followed a similar model, we would have nobody to communicate securely with.

With this in mind, I persuaded Cisco to lend me a conference room at their executive centre near Heathrow Airport, and I invited a group of top information security managers to explore the possibility of working together to develop a common, security architecture for a de-perimeterized business world. The result was the formation of an informal, private circle of senior professionals, which helped to sow the seeds for the subsequent foundation of the Jericho Forum.

The Jericho Forum is an organization dedicated to developing solutions to meet the business demands for secure IT operations in an open, Internet-driven, networked world. Originally conceived as an invitation-only circle for large user organizations, this forum is now open to all organizations, including vendors. The aim is to get the user members to define the problem space and the vendors to fill in the solution space.

Many people misunderstand the mission of the Jericho Forum. They imagine we're advocating the removal of corporate perimeters and firewalls. That's not the case. Our perimeter defences are already leaking. We're simply stating the fact that:

> *'You've already been de-perimeterized. You'd better do something about it.'*

The Jericho Forum has published a set of 11 principles for the planning and design of systems and infrastructure for a de-perimeterized business environment. These are judged to be the quintessential design principles for moving towards a secure, collaborative extended-enterprise business model.

Many people ask why we picked 11 principles. The group set out, in fact, to produce 'Ten Commandments' for de-perimeterization. But the outcome was 11 principles. We simply felt it to be inappropriate to leave any out. Ron Condon, former editor of *SC Magazine Europe*, suggested that we must have been inspired by Spinal Tap, the spoof rock band, whose amplifier volume controls were based

on a scale of one to eleven in the expectation that it would make them a touch louder.

One of the most important Jericho Forum principles is to 'assume context at your peril'. Security solutions have limitations. Technology and controls designed for one environment might not operate effectively when transferred to another. An information system developed for a private, secure network environment is unlikely to have the controls and strengths of mechanisms to be secure when operating across the Internet. And these limitations are not just technical. Changes in context create problems from a variety of sources, including geographic, legal and risk acceptance considerations.

The collapse of information management

Electronic networks have created huge challenges for all organizations. Many of our traditional information management systems, designed for a paper-based industrial age, are no longer appropriate for controlling today's horizontal information flows.

Many IT directors will privately agree that their information management has all but collapsed, and that their networks are no longer under control. But they'd probably be sacked if their Executive Board believed that.

In fact, our intellectual assets are out of control. And most of us are apathetic, or in denial. We've completely lost track of our corporate information as it's moved from the filing cabinet to the desktop. Who files minutes of meetings today? The answer, in many cases, is everyone and nobody. Plenty of copies might be flying around for a while, but can you find them when you need them?

Yet it's our intellectual assets that represent the enterprise's primary future source of revenue, profit and market capitalization. The great challenge of the next decade will be to regain control of these intellectual assets, in order to maximize their worth, and safeguard their value.

These assets include not just the valuable information resting in company databases and documents, or in its brands and reputation, but also the added value provided by the know-how, skills and relationships that are embedded in the organization's networks, both inside and outside of its corporate boundaries.

We need to develop new models for valuing, exploiting and safeguarding these increasingly important assets. But the starting point is to identify them, recognize their value, and aim to secure them. And not just for the purposes of regulatory compliance, but also because it's good for business.

The shifting focus of information security

The nature of information security changes regularly. Each decade brings a new focus through the extension of electronic networks.

The 1970s introduced the concept of risk assessment for individual information systems. New methods were developed to help determine the specific requirements of systems that were generally isolated and dedicated to a particular

business application. Some worked. Others didn't. Methods based on annual loss expectancy came and went. They proved impossible to deploy because of the absence of any reliable information on incident rates and losses.

Throughout the decade the focus of attention for security controls remained on individual systems and machines. Even the most advanced military research was focused primarily on the problem of achieving better separation of users of different clearance levels sharing a common machine, or from preventing an individual terminal from radiating information to a nearby location. Most organizations managed without professional security expertise. Local computer managers looked after security.

The 1980s encouraged business units to establish secure, glasshouse datacentres in order to safeguard and showcase their growing collections of valuable hardware. The focus of security had moved, from individual machines to collections of machines. Physical security, disaster recovery and mainframe access control systems were the new priorities of the first generation of information security managers, who generally operated from the bowels of the datacentre rather than the corporate centre.

The 1990s moved the primary focus of security to the enterprise infrastructure. Local area networks were joining up at a frightening pace. Uncontrolled connectivity threatened the security of previously isolated systems. Firewalls and rules for enterprise sharing of information were the big issues for information security managers.

We developed new security standards for the whole enterprise, not just individual systems. The British standard BS7799 was created in the early nineties to support this new standardized approach to enterprise, and inter-enterprise, security.

The introduction of the World Wide Web persuaded organizations it was more important to share company information, rather than to keep it under lock and key. As one enlightened Shell business director put it to me, 'We're a big tanker, we can afford to lose a few drops.' I was inspired to develop the slogan, 'Share your knowledge with Shell, not the rest of the World.'

The early years of the 21st century introduced a much stronger external perspective. Networks stretched beyond enterprise boundaries to embrace the Internet. Security also became a business in itself. Electronic commerce was the future. Internet 'pure plays' suddenly became investments worth millions of dollars. Some businesses viewed security as a unique selling point.

For a brief moment in time, electronic security became the poster child of the marketing function. SRI International caught the mood and shocked both its clients and staff by rebranding its security research unit as 'Atomic Tangerine'. Shares in Baltimore, a UK vendor of digital certificates, rocketed and briefly entered the FTSE 100 index.

But the business fascination with electronic security dissolved with the dot-com crash, leaving a few individuals as millionaires, most investors out-of-pocket, and many employees out of a job.

The post dot-com years have been a necessary time of consolidation for information security. Most leading enterprises have used it to catch up with new processes,

technology and architecture, to establish professional functions, and to adopt the more disciplined approach demanded by the regulatory compliance.

But the primary focus of most security managers remains largely an internal one, focused on the security needs within the enterprise. It's failed to keep up with a problem space that's been progressively moving outside of the corporate boundary.

The external perspective

Our network perimeters might be full of holes, but they're still needed to help protect our insecure legacy systems. In fact, for many years to come, we will need to shore up the security protection around our enterprise networks.

But an inward focus is no longer sufficient. Current technology trends, such as mobility, grid computing, and software-as-a-service, are moving the focus of corporate data flows outside of the corporate perimeter. That demands a more outward-looking security perspective. We need to shift our attention away from merely securing our own backyards, towards working together with business colleagues to build community solutions, for an emerging business environment that is based on open networks and shared services.

We also need to start paying more attention to the extramural security behaviour of users. That might seem invasive to many people. But trends such as home working, portfolio careers and social networking are removing the traditional barrier between business and personal lifestyles.

Networks have transformed our perspective of work. The view of work that we have inherited was designed to meet the needs of mass production, a legacy of the industrial age. That model required every aspect of business life to be standardized, classified and synchronized. Business was something that took place in a dedicated building, during set hours, using business equipment. What you did outside, and how you did it, was of no direct concern to your employer.

Now it's all mixed up. People instinctively grab the nearest communication channel to conduct either personal or business transactions, at any time, any place, anywhere. You can't separate business and private activities. The result is a steady drift towards a more flexible way of conducting business, using consumer devices and external services.

We are also in the midst of a steady, unstoppable march towards consumerization, a trend by vendors to develop IT products for consumer, rather than business markets. The first telephone was a functional, black device, owned by the telephone company. Progressively, consumer demand has encouraged greater and greater user choice in the styling, features and ownership of client devices.

This trend is irreversible. Vendors are now building features that appeal to consumers, not business, though some consumer devices, such as the Apple iPhone, now incorporate a range of business features, in order to appeal to both markets. And our business users now expect and demand the same functionality and personalization in their business devices as they already have in their personal ones.

Like it or not, we're going to have to take more interest in what our staff get up to outside office hours. We need to encourage them to take extra precautions when

they're conducting business in insecure environments. We need to take steps to ensure that the work they carry out at home is adequately protected from security threats, and that any personal content they introduce into the office environment is free from damaging malware.

The challenge is to understand, accept and manage the consequential security risks of a business environment that's now everywhere but nowhere in particular. It's no less than a major paradigm shift for business and security.

A new world of openness

Networks enable instant communication and large-scale sharing of information and knowledge. These are powerful business capabilities. But they're also fraught with danger. Espionage and identity theft are becoming more attractive to criminals. In the past, only hostile foreign intelligence services would take the trouble to invest in stealing your information or identity. Now any criminal can make a fast buck out of it. And they have far more opportunities to get hold of it.

But organizations still need to maintain secrets. The problem is that it's becoming harder to keep them from leaking out. Employees like to share their information with colleagues, friends and acquaintances. What people do at work is no longer a secret. They advertise it in their CVs and their Linked In entries. Few people today think to keep corporate secrets to themselves.

And sharing makes perfect sense in a networked environment. It's logical that pooling your knowledge with others will gain you a bigger return. The only problem is sorting out the wheat from the chaff. Perhaps only one in a hundred items might be actually useful. The consequence is that, in practice, few staff will be bothered to search for those valuable nuggets of information in a sea of irrelevant data. But be assured that hackers, spies and fraudsters will. They think and behave in a different way from honest members of staff.

Many companies are concerned about the increasing use of social networking sites by company staff in business time. One survey carried out at the start of 2008 suggested that, in the UK alone, more than £6.5 billion a year is wasted in lost productivity. That should be balanced, of course, against the gains in productivity by enabling collaboration and knowledge sharing. The survey makes no mention of this.

But lost, or changed, productivity is just the tip of the iceberg. The use of social engineering to hijack sensitive information from companies is real and growing. Social networking sites provide a means for criminals to identify and target employees, and to connect with or impersonate them. Companies have been slow to address these new threats. Corporate policies lag far behind user behaviour, and security education and guidance in this area is generally weak or non-existent.

There are also big political and commercial issues yet to be addressed. For example, how far should we monitor employee activity? Who owns the intellectual property generated by networked relationships on social networking sites? And how can enterprises maintain the necessary control and direction across its empowered, networked groups of staff.

And it's not just cyberspace that's been affected by this new spirit of openness. During the eighties, millions of business executives were moved from the privacy and comfort of their own private offices to new, open-plan environments. It wasn't just because of economics. It was a symbolic gesture, a sign of the times, and a salute to the new culture of equality, teamwork and information sharing.

But open-plan environments have left a legacy of free access that's a dream to an insider spy or thief. Once you find an excuse to enter a building, and there are many, you can generally wander around with little challenge, grazing away at the faxes and print-outs waiting to be collected from printers, and the papers that executives are forced to leave out on their desks, because their office furniture can't accommodate the mass of paper documents that the paperless office has singularly failed to eliminate.

A new age of collaborative working

The World Wide Web has revolutionized business, but it's yet to prove itself to be a good medium for collaborative working. It might be perfectly fine for publishing, but it certainly doesn't lend itself to interaction. That wasn't the original intent of its inventor Tim Berners-Lee. As he puts it in his paper *Web Architecture from 50,000 feet*:

> *'The original idea of the Web being a creative space for people to work together in seems to be making very slow progress.'*

Many would consider that an understatement. It's clear we have a long way to go before we can tap the latent, exponential power that might be lurking in the Internet, the enormous value suggested by David Reed's law. That requires a step change, in both the skills and technologies applied to collaborative working.

Nevertheless, collaborative tools are improving. Vendors of enterprise applications are incorporating Web 2.0 features into their platforms as fast as they can. The term Enterprise 2.0 has been coined to describe the application of technologies for collaborative working in organizations. A few academic models are also slowly emerging to provide some much-needed structure to the use of what is basically a rag-bag of unconnected tools for manipulating unstructured information.

Harvard Business School Professor Andrew McAfee, for example, has coined the acronym 'SLATES' to embrace the six components of Enterprise 2.0 technology: search, links, authoring, tags, extensions and signals. Hopefully, that might be a start in the development of a basic framework and taxonomy to underpin the development and application of the necessary management controls. But we have a long way to go before we can impose an effective governance structure for these emerging technologies and services.

New business services are also emerging to encourage collaborative support for business operations. The term 'crowdsourcing' was coined by Jeff Howe, in a June 2006 *Wired* magazine article, to describe the process of outsourcing work to an

undefined, large group of enthusiasts, through an open call. You can, for example, invite members of a social network to help you to design a new technology, to build or test a piece of software or to collect or analyse a large body of data.

In their book *Wikinomics: How Mass Collaboration Changes Everything*, Don Tapscott and Anthony Williams explore how companies have exploited mass collaboration and open-source technology to business advantage. It's a compelling book written with great enthusiasm. And there's no doubt that mass collaboration is an important business trend. But real collaboration success stories are, as yet, few and far between. They have yet to capture the imagination of mainstream business organizations.

The reluctance of business to take up these new ways of working is not only due to the conservative nature of most organizations. It's also because we have yet to develop and promote the new, professional business models, architectures and methodologies that are needed to underpin this approach. But the fundamental principles are clear; they are: openness, peering, sharing and acting globally. And these principles also represent major challenges in a business world that's facing up to tighter regulatory compliance, as well as a sophisticated security risk landscape.

Collaboration-oriented architecture

In fact, the real future of business is one of increasingly deeper, faster and more volatile collaboration, underpinned by secure electronic networks. It's about companies that come together more purposefully and quicker, to develop new, compelling products that the marketplace cannot deliver.

That demands a substantial degree of trust between consenting business partners, to allow or block connections between sensitive or critical information systems and infrastructure.

How will this be achieved? In the past, we largely kept our fingers crossed and hoped for the best, or relied on legal contracts to compensate us for any consequential losses, caused by a rogue third party. These options are no longer realistic, though, unfortunately, they might reflect typical practices today.

The only sensible option is to develop common architectures that enable secure, extended enterprise business operations to be established with minimal risks to either party.

Developing such solutions is a painfully slow process, but progress is being made. The Jericho Forum, for example, is developing a common 'collaboration-oriented architecture' to provide guidance for building systems that can operate securely with users sited outside of the corporate perimeter. This mode of working is already a reality for many enterprises. Many Jericho Forum members are migrating users and services to operate or connect across the Internet.

Companies such as BP, for example, have tens of thousands of users communicating securely over the Internet, rather than across a corporate network. ICI has implemented an Internet-based content monitoring and filtering system to enable mobile users to drop in and connect through any convenient access point, with full security screening of access and content. And KLM has cut its support costs

substantially by giving thousands of staff special allowances, to buy and manage their own personal computers.

The long journey to a de-perimeterized, collaborative business world has begun, though the security and management models are far from mature. Organizations are naturally proceeding slowly and cautiously. In fact, few enterprises are ready to manage the degree of anarchic interaction that contemporary collaborative tools might unleash on business systems that are already struggling to meet tight regulatory compliance demands.

There are exceptions, of course. Goldman Sachs, until recently one of the more profitable and confidential investment banks, is a pioneer of Web 2.0 applications. They are managing the balance between security and innovation. But smaller, newer companies generally have the edge. They are not tied down by legacy systems and infrastructure, governance models, bureaucratic processes and restrictive enterprise licenses and procurement deals.

Nevertheless, as with any new technology, there will come a point when user power overturns corporate objection. Personal devices, aimed primarily at the consumer market, will eventually become the basis of mainstream business. We've seen it happen in the past. Security considerations and business economics initially resisted the introduction of the mobile phone, the Internet and the Blackberry. But executive power triumphed. Similarly, Web 2.0 technologies will become an essential part of business-as-usual.

Business in virtual worlds

Virtual worlds present a new and different set of challenges for security managers and corporate policy makers. I'm often asked by security managers what the acceptable use policy should be for employees who wish to experiment with sites such as Second Life, whether for research or business purposes. It's a good question, with no simple answer.

In fact, it's easy for business units to make a case for establishing a presence in virtual worlds. Customers can be reached; products can be promoted; new ideas for brands can be floated; press conferences can be held; virtual business meetings can be arranged; new extensions of IT systems can be tested. You can even make investments in virtual assets, though the business case might prove to be quite difficult for most managers.

We need limits and rules to govern the behaviour of people's avatars, the virtual representations of people in virtual worlds. Regardless of how much of a game it might seem, behaviour in any public space has security and legal implications, and an impact on corporate reputation and brand perception.

Context is especially significant in determining the appropriateness and legality of any actions. And, as we'll see later in the book, environments also help to shape people's behaviour. Staff will be compelled to act very differently in a novel environment.

We need new thinking to respond to these challenges. In the early years, the nature of the solutions will depend on what companies make of their early experiments. Will they view it as a major new marketing channel, an essential internal communications tool, or a valuable new form of collaborative working?

All of that is an unknown quantity. But one thing seems clear. It's unlikely that many companies will generate major revenue from virtual worlds, at least in the early years. Few traditional companies will view this new space as a serious basis for strategic business investment, though there might be opportunities for the niche operator.

Information security will, therefore, largely be operating in a defensive mode, aiming to keep business managers out of trouble and to safeguard corporate reputation, rather than in an enabling manner, aiming to build, develop and support a major new business channel.

Nevertheless in the longer term, virtual worlds will become a serious business environment, and we will need to adapt our traditional security governance approach to fit the new environment. How should approach this? A common theme in this book is to suggest security solutions that match the problem space. That means that we should be planning to engage with, and build solutions within, the virtual worlds themselves.

Democracy . . . but not as we know it

In February 2008, the media reported that three leading UK Internet service providers, with 9 million households between them, had signed up with Phorm, a provider of a new form of advertising service, aiming to match advertisements to customer habits, but designed to keep customer's identities anonymous to advertisers. The publicity resulted in an unprecedented backlash from privacy campaigners.

An e-petition requesting the Prime Minister to investigate the Phorm technology was launched on the 10 Downing Street website, attracting 10 000 signatures in the first two days and reaching the 'Top 10' list within two weeks. It was 'in with a bullet' as they used to say in the music industry.

At first sight, this appears to reflect a massive amount of public support. But is it really? Can 10 000 signatures really be interpreted as representing a significant slice of public opinion? It might be big in relation to other petitions doing the rounds. But it's a long way from being a majority vote of the UK population.

Civil libertarians, in particular, present a dilemma for politicians. On specific issues they often reflect a minority viewpoint. But it's a very substantial one. And they are articulate and well-organized, especially when it comes to campaigning.

Peer-to-peer collaborations sound all very healthy and democratic in theory. But they're far from perfect in practice. Minority interest groups can hijack thought leadership and collective opinion across networks. Democratic voting is an integral function of modern social networks. But not everyone wants to take part in on-line debates. And you don't need a majority of the population's voters to create a wave of change.

Social networking creates a new form of minority democracy. It's inevitable. We're just going to have to get used to it. Political activists are generally concerned about defending minority rights from the tyranny of the majority. But this time it looks like we're heading for the opposite problem, safeguarding everyone's interests from the tyranny of the minority. There are deep implications for both

politics and business. Few political and business leaders, however, appreciate what's really happening.

What are the implications for politicians? I asked Lord Errol, a rare example of a peer of the Realm who actually understands technology and its implications for politicians. Lord Errol rightly pointed out that 'much of the present work of politicians is defending minority interests'. In fact, the truth is that politicians are already champions of minority concerns. The future will be business-as-usual for politicians.

But as Alvin and Heidi Toffler pointed out more than a decade ago in their 1994 book *Creating a New Civilization*, it's clear that there's a mismatch between the current political system and the emerging demands of the information age. Eventually we will need to align the two, to create a new political system that's more attuned to the structure of the Information Age.

Unfortunately, public interest in political elections in the UK appears to be waning, though there are an increasing number of attempts to mount single-issue demonstrations. In fact, many people would now prefer to select their issues and politics, in a personalized manner, just as they might select goods from a store, or order a special cappuccino from a coffee shop.

This 'Starbucks-style' politics, as the *Economist* terms it, has not so far had a major impact on mainstream politics. But it undoubtedly will. Consumer choice is an unstoppable force that's slowly penetrating politics, as well as every other aspect of modern life. It just requires campaigners to learn to exploit the power of social networks to change majority opinion.

In fact, the implications for business are more challenging. Politics has always lived with a degree of short-term anarchy generated by events and media coverage. But business needs a clearer, longer-term focus. Minority voting might be fine for local quality improvements, but it can be a dangerous distraction for an enterprise that's operating to a demanding business plan.

Corporate centre plans have rarely been popular because they aim to optimize the efforts of the whole enterprise, generally at the expense of the individual parts. In contrast, lobbyists tend to focus on single-issue arguments in support of short-term, local interests. Quiet thinkers and sensible strategists will be ignored. It will be the survival of the fastest, the loudest and the best networked.

The consequence is that, for better or worse, decision-making will become increasingly democratic, based on minority opinions. And there's nothing we can do about it, other than to get stuck in and join the debate.

The influence of top management and corporate centre directors will progressively die unless they change. In the future, the ability to craft a compelling e-mail will become more useful than a commanding physical presence. Whether people like it or not, it seems inevitable that good bloggers will eventually have the edge over traditional company men.

Don't lock down that network

Many security managers ask me whether we should be closing down risky network transactions, or learning to live with the risks the present. It's a growing dilemma for network security managers.

No long ago, I was asked to speak at a big European conference in London on the subject of 'Locking down social network vulnerabilities'. The title was chosen to attract delegates and to appeal to the media. But it's an ironic one, because locking down any feature of networks is a futile objective. And vulnerabilities also exist in real-world social networks. People have a tendency, for example, to blab to their friends and family. The differences on-line are the visibility and, more particularly, the scale.

We do, of course, need to address the security vulnerabilities presented by social networks. But constraints on network flows are rarely a sensible idea. Networks should be designed to be free-flowing, and to resist attempts to block, filter or divert traffic. In fact, resilience of flows is a primary security feature, one of growing significance. And, anyway, the best security measures to control social networking lie outside of the network.

My advice to the audience was not to lock anything down, but to pay more attention to supporting the free flow of networks. In particular, it's important to appreciate the real intellectual value that might be present in a network. Increasingly, that will be tied up in the intangible know-how and personal relationships in the information flows, rather than in the static stocks of legacy data in the connected databases.

Getting to grips with the ownership and management of personal relationships is much more important that blocking or filtering an ad hoc selection of passing data. And in most cases, educating users will be more effective than monitoring their traffic. These should be the new priorities of the modern security manager.

We need, of course, to be mindful of the risks from the insider threat. But countering such a threat requires a broader, richer set of solutions than we can achieve at the network level. To detect an inappropriate or illegal user action, we need to appreciate the full context of that behaviour, which requires much more than an inspection of data and transactions. And when it comes to deterring or detecting fraud and espionage, the most effective controls lie outside of the network environment.

That doesn't mean that network security is dead. Filtering and blocking of network traffic will continue to be a practical reality for many years to come. And monitoring of traffic will continue to provide an increasingly useful source of security intelligence, as well as delivering the essential evidence to support breach investigations.

The future of network security

So what exactly is the future of network security in a world that values information flows above security barriers? Not long ago, I was invited to contribute a thought leadership column to *Network World*, on behalf of the Jericho Forum. I chose to write about this subject. The focus of my article was the implication for network security in a de-perimeterized world, an environment in which the focus of security controls migrates from the infrastructure towards the application and data level. What will be the longer-term role of network security? Will it eventually become redundant or will it grow even more powerful?

These questions are often raised when de-perimeterization is discussed, because there is an assumption that placing security closer to the data and applications, might remove the need for controls in networks. My conclusion, however, is that there is huge potential for delivering value through security features in networks. But it will be very different from what we see today. And it will be increasingly focused on the human factor.

Networks are a convenient place to apply many types of security control. They're a good place to position controls that need to be less invasive or more transparent to users. But they also present limitations. Geography, topology, ownership boundaries and legal jurisdictions are all major constraints. It's often hard to find a convenient choke point in a network, at which you can view or control all of the traffic you might be interested in. But, on the other hand, network gateways are a great place to secure central databases. And the latest gateway platforms offer a huge range of security features. Topology can work for or against security.

Valuable security intelligence can also be derived by profiling and mining network content, traffic patterns and user behaviour. Psychological profiling offers huge potential for the future detection of fraud, espionage or terrorism. But privacy considerations are a major, growing concern. Controls will need to be designed in, from the ground up, to preserve anonymity for intercepted traffic of people who are not the subject of a security investigation.

In fact, you can monitor a user's behaviour either from within the network, or from its endpoints, such as the client and server platforms. Each option provides a very different, complementary perspective. The network view, for example, has the advantage of being able to compare or contrast an individual user's behaviour with those of a broader community. In contrast, the endpoint perspective enables comparison with historical activity. Both viewpoints are useful.

Network gateways are also a vital source of security intelligence because they can see many failed or blocked transactions, providing a greater degree of insight into near misses and attempted attacks. And as we'll see in Chapter 3, it's important to keep an eye out for near misses, because they're a potential indicator of incidents to come.

Can we trust the data?

Peer-to-peer collaboration and consultation is progressively becoming a mainstream business tool. But the integrity of knowledge to support business decision-making will be under threat if managers rely solely on the views of networked colleagues, rather than expert advisers. Networks don't always get things right. In some cases they can be positively dangerous.

'Chinese whispers', a process in which a story gets distorted as it's passed on from one person to another, can distort the true facts and figures.

I once asked a media relations director what his biggest information problem was. 'Establishing the right numbers,' he replied, 'If the correct figure is 67.5, some will round it to 67, others to 68, or perhaps even 60 or 70. And as these numbers get passed on, they get further distorted. You will end up with a range of different estimates, ranging from 50 to 100.'

The process of rumour has been studied by psychologists for many years. Early research, by Gordon Allport and Joseph Postman in 1947, examined how messages travel by word of mouth. They found that about 70% of the details of a message were lost in the first five or six exchanges, and concluded that as rumors travel, they grow shorter, more concise and easier to tell and grasp.

Allport and Postman identified three key processes that shape the development of rumours: levelling, sharpening, and assimilation. Levelling is the progressive loss of some of the details of the original message. Sharpening is the process that selects and highlights particular details. And assimilation is the unconscious (or perhaps subconscious) distortion in the details of the message.

Internet discussions, however, are quite different. They are interactive, and the original postings are also available. More recent research suggests that there is often a collective, problem-solving process at work, in which new ideas are introduced, further information is volunteered and discussed, and then a resolution is drawn, or interest tails off.

A few years ago, James Surowiecki, a columnist with the *New Yorker* magazine, published an articulate and influential book on networked behaviour, called *The Wisdom of Crowds*. The concept of the book is a hypothesis that collective group behaviour is smarter, wiser and more innovative than individual efforts. Surowiecki cites entertaining anecdotal examples from history and everyday life in order to demonstrate how this principle operates.

In fact, the title of Surowiecki's book was inspired by a 19th century book by Charles Mackay about human follies, called *Extraordinary Popular Delusions and the Madness of Crowds*. That book cites examples of the opposite phenomenon, such as witch hunts, crusades and financial bubbles.

Both these books illustrate the potential for good and bad decisions in networks. Unfortunately, you can't rely on collective voting to get it right all the time. But the more people that accept an idea, the stronger it becomes.

'Three men make a tiger' is a Chinese proverb based on the phenomenon that if three or more people mention an observation then it's likely to be believed. The proverb is reported to have come from a speech by a Chinese official called Pang Cong, in around 300 BC.

Pang Cong claimed that he'd asked the King whether he would be inclined to believe a single citizen's report that a tiger was roaming the markets in the capital city. The King replied that he wouldn't. He then asked the King what he would think if two people reported it. The King said he would begin to wonder. He then asked what he would think if three people claimed to have seen a tiger. The King replied that it must be true if three people say it.

The word of three different people might have seemed credible in an ancient society, at a time when people travelled much less on a daily basis. But it's statistically insignificant in the context of a large network such as the Internet.

Urban myths, fictional tales passed on as true stories, are an interesting feature of social networks. They have proliferated with the growth of the Internet. And it's not surprising, as it's so easy to invent a story and to spread it across a network. Someone, somewhere, is bound to believe it. And if one or more people accept it, then it will begin to gain credence. Eventually it might become accepted by a majority.

Urban myths abound in security. The wealth of hoax viruses is an example of this. They cause anxiety and waste people's time. Several years ago I received a report from a police force about a new technique that was being used by thieves to help steal laptops from cars. Using a cheap electronic scanning device, bought in the High Street, they were reportedly able to detect the presence of a laptop in the locked boot of a car. Like all good stories it sounded unlikely, but just about possible. We had to try it out. It failed, of course, to work as suggested.

The learning point is not to believe everything you read or hear over a large public network. But that's the way the world is going. And many people are surprisingly trusting of information that's generated by technology. Electronic data all looks perfectly genuine at first sight.

The art of disinformation

The real secret of disinformation, the promulgation of false information for military or propaganda purposes, is to mix a few lies with some genuine information. Such techniques have long formed a part of military strategy.

They were heavily used by MI5 during World War II to deceive German intelligence about British intentions. The Cold War turned them into an art form. At its height there were thousands of people on both sides secretly engaged in creating false trails for the other side. Today we can see a certain amount of disinformation practiced by all stakeholders in the War on Terror.

Disinformation is a complex business, a rich blend of truth, lies and opinions. Sorting out the real truth from a range of facts that have been invented, massaged, exaggerated or just selectively reported, perhaps by a multitude of players, is certainly not easy for the recipients.

In his book *Disinformation: 22 Media Myths That Undermine the War on Terror*, Richard Miniter, an experienced journalist, points to six sources of media myth: honest errors, government spin, disinformation by foreign intelligence services, historical amnesia, leaks and media failures.

The concept of 'spin', presenting facts in a distorted way to promote a particular cause, has long been a skill practiced by the media. Now it's become endemic in most government communications. And as we become accustomed to its use, it's likely to spread further. Most company communications functions also apply a small about of spin to their press releases, though much less than their government counterparts. Spin includes a range of techniques: suggestive phrasing, selective reporting and downplaying of bad news.

The potential for spin has been progressively growing with the continuing increase in analogue media to communicate news and knowledge. Images are much less precise than words for conveying information, and they can substantially alter the context and interpretation of a message. In the past, we relied primarily on factual sources, such as books and classroom lectures to gain our knowledge of a subject. Today, our knowledge is gained through a haze of sponsored images and advertising through television and the Internet.

Some spin is subtle, disguised and unconsciously absorbed. Other types of spin are less covert forms of persuasion. It can, for example, be an obvious, indirect,

form of criticism, as encapsulated by Alexander Pope's famous quote in his epistle to Doctor Arbuthnot in 1733:

> *'Damn with faint praise, assent with civil leer, and, without sneering, teach the rest to sneer.'*

Fear, uncertainty and doubt, or FUD for short, is a highly effective form of deliberate, undisguised spin, used extensively in the computer industry to cast doubt on the wisdom of buying a rival product. The term was coined by Gene Amdahl after he left IBM to found his own company:

> *'FUD is the fear, uncertainty, and doubt that IBM sales people instill in the minds of potential customers who might be considering Amdahl products.'*

IBM's marketing people were certainly highly successful at planting a simple but powerful perception in their customer's minds: that nobody ever got fired for buying IBM equipment. Whether or not it was actually true did not really matter. It was enough to make purchasers think twice about the downside risks in selecting a less established product.

In fact, it's surprisingly easy to spread fear, uncertainty and doubt about any new thing that looks promising. Just float a few negative comments such as: 'But is it proven?', 'Can they deliver?', 'What's the catch?' and 'What about the hidden costs?' People will quickly begin to form doubts. Every business decision involves a degree of uncertainty. But it's not generally at the forefront of our minds. FUD is that slight nudge that reminds us to place those risks higher in our mental selection criteria.

In many financial markets, unscrupulous traders can make fast, easy money by floating damaging, false rumours about companies to encourage share prices to fall. But finding evidence of this to support a prosecution is far from easy. The problem is so serious in the financial sector that the US Securities and Exchange Commission has banned 'naked' short selling of shares (which sellers do not yet possess) in the country's major investment banks.

Countering disinformation is simple, though not always easy. The answer is, firstly, never to place your trust in unconfirmed rumours or hearsay, and, secondly to always seek a second opinion when making critical business decisions.

The future of knowledge

Wikipedia is an interesting glimpse of the potential future of many knowledge bases. It's mostly accurate, and like all good disinformation, it encourages a false sense of security. You never quite know whether that key item of information that you've decided to rely on is accurate, mistaken or deliberately distorted.

But it's astoundingly fast at gathering new information. In fact, the work 'wiki' is the Hawaiian word for 'quick'. It's proved itself to be faster than other information channels on many occasions.

On July 7th 2005, London was rocked by four explosions. Within less than twenty minutes of the first explosions, an entry had appeared on Wikipedia. By the end of the day, more than 2500 had collaborated to produce an account that was more detailed than the accounts of any single news agency. Meanwhile, the collaborative website Flickr had been breaking some of the first photographs of the bombings, taken by camera phones.

Amateurs with camera phones will always beat professional news gatherers to new, unexpected stories, simply because they happen to be there at the time. Collaborative websites, run by volunteers, are catching up with, and often overtaking, established sources of news and knowledge.

But the information is not always compiled by people that are experienced, expert, objective or trusted. As the Wikipedia site puts it:

> *'Visitors do not need specialized qualifications to contribute, since their primary role is to write articles that cover existing knowledge; this means that people of all ages and cultural and social backgrounds can write Wikipedia articles.'*

The information on such sites doesn't carry reliability indicators, other than the fact that older information is more likely to be noticed and challenged if incorrect. As Wikipedia cautions:

> *'Older articles tend to be more comprehensive and balanced, while newer articles more frequently contain significant misinformation, unencyclopedic content, or vandalism. Users need to be aware of this to obtain valid information and avoid misinformation that has been recently added and not yet removed.'*

In fact it's not quite that simple. Popular subjects attract faster scrutiny and correction, sometimes in minutes. Less popular entries can remain uncorrected for long periods, perhaps indefinitely. As a legal friend of mine puts it:

> *'Wikipedia is fine for researching your children's homework, but you wouldn't rely on it for a major business decision.'*

Not everyone is that cautious however. It's a percentage game. If it's correct nine times out of ten, then few people will experience or notice a major problem. They will instinctively rely on it. Just as for deliberate disinformation, they will be caught out by the insidious lie that's carefully hidden in a sea of truth.

The next big security concern

Attempts to mislead can cause more damage than espionage. They're also highly complex to uncover and repair. The current big security concern of that nature is identity theft. Repairing the damage to a single compromised account requires an investment of days or weeks of effort.

Identity theft is the bridge between today's obsession with data confidentiality and tomorrow's broader exposure to attacks on data integrity. Integrity of business and personal data will be the most important, future concern for organizations. In fact, it's the next big challenge for all information security managers.

Confidentiality, integrity and availability are the three cornerstones of information security. The balance of significance of these factors has tended to shift over the years. In fact, there is a logical evolution in their visibility and relative significance, though it's been substantially influenced by developments such as the Cold War and the introduction of electronic networks.

Availability is the first thing you notice about information systems. When they stop, which they all tend to do from time to time, it's an obvious problem, with an immediate, but largely temporary, impact. Confidentiality of data is the next security characteristic that comes to people's attention. We rarely experience such incidents in everyday business life, but when we do it, it creates a more sinister, longer lasting impact. Integrity of data is generally the last security characteristic we notice. Few people tamper with data. We rarely experience the impact of a loss, and we don't read much about it in the newspapers. But when a breach comes to light, it's a major concern.

In the old business world of paper documents, confidentiality was a primary concern in most security managers' minds, though the reality was that misfiling of records was probably the biggest everyday problem. Early information security policies from the 1970s are quite an eye-opener, if you ever come across them. Many reflect an obsession with espionage that seems quite surprising today. That was probably due to an early military influence over the development of the subject area.

The end of the Cold War removed much of the paranoia about confidentiality. In the early days of the Internet, the biggest concern of most companies was the availability of information services. It was the most obvious and common risk, and it had a clear business impact. At that time, some security experts even suggested that confidentiality was no longer important, an unnecessary hangover from the Cold War days. But they were wrong.

A breach of customer confidentiality has always been one of the most damaging security risks to organizations. In the early days of electronic commerce, that risk was rarely acknowledged by system managers. A few high-profile breaches have served to change that perception. Today it's clear to everyone that data leakage prevention is a priority for any business process that handles personal data or confidential business information.

As we go forward into the next phase of the information age, we'll find that perhaps the most serious of the emerging risks will be the ones that threaten the integrity of our intellectual assets. This will become clear with the emergence

of new threats, the increase in the value of intellectual assets and our growing appreciation of the potential business impact from such breaches.

Damage to the integrity of business information assets is rarely encountered today, but when it does occur, the impact of a breach is often substantial. Even the suggestion of a small set of unauthorized changes to a critical business database can be hugely damaging to its perceived value, and the reputation of the business services that depend on it.

Uncertainty about the extent of unauthorized changes is a disturbing concern. It's a little like walking into an airport hangar and finding evidence that an overnight intruder has had free access to a passenger jet. You wouldn't dare let it fly, without carrying out a thorough inspection of every single item that might have been affected. Conducting an integrity check of millions of records, however, is a much more challenging task.

Mistakes and bad practices can also be a threat to data integrity. Most citizens would be shocked if they knew just how bad the quality of data was that companies and government agencies held on them. And even short-term data can present major problems. Fast moving, collaborative team working can also result in errors, when team members end up working on different instances of a document.

We have to yet to experience the wake-up call to better working practices and tighter controls to safeguard data integrity. But that will emerge in the next few years. Breaches of integrity are hard to detect, and even more difficult to repair. They are the new nightmare waiting to engulf companies that places high reliance or substantial value on their intellectual assets.

Learning from networks

What have we learned in this chapter? Here's a summary of some of the key findings and conclusions.

We explored the nature of power, and the power of networks. Power and networks are inextricably linked. And both are challenging our approach to information security. Traditional approaches to security are breaking down, as networks break down corporate barriers, and their content displaces existing channels of advice. Social networks are gradually disempowering corporate centre security functions. We will need to rethink the way we communicate and enforce our policy.

Networks are a powerful leveller, with little respect for status or authority. At the same time, they're also a potent means of leveraging individual ideas and initiatives. There is huge value waiting to be tapped in social networks. Reed's Law indicates that the value of social networks might scale exponentially with the number of members. We should be aiming to understand and safeguard that value.

Ever since their invention, networks have transformed business life and increased security risks, by cutting through geographic and organizational barriers, including those between personal and business lifestyles. This is the phenomenon we call de-perimeterization.

Each decade has brought a new focus to security, through the progressive extension of networks. The 1970s introduced risk assessment. The 1980s encouraged business units to establish secure datacentres. The 1990s moved the focus of security to enterprise networks. The early years of the 21st century introduced electronic commerce.

But information security has failed to keep up with a problem space that's moved outside of the corporate boundary. Security managers need to shift their attention towards working together to build community solutions. The Jericho Forum has developed a set of principles, and is building a collaboration-oriented architecture, to enable secure business operations across extended enterprise environments.

Social networking and virtual worlds are new challenges. Lost productivity is just the tip of the iceberg. The real threat is to sensitive information. But corporate policies and security education lag far behind user practice. Social networks also present threats to democracy in politics and business. We now face the tyranny of the minority. Minority voting is fine for quality improvements, but not for an enterprise aiming to operate to a single business strategy.

The integrity of knowledge to support business decisions is also under threat. There might be some wisdom in crowds, but there is also FUD, spin and disinformation. Integrity of data will be the next big problem for security managers. Breaches of integrity are rarely encountered in everyday business but their potential impact is huge. They are hard to detect and even more difficult to repair.

The smart information security manager will aim, not to lock down our networks, but to safeguard information flows. Here are 10 principles that you might wish to consider for securing your intellectual assets in the new, networked, Web 2.0 world.

- Ensure your staff and customers are streetwise
- Understand your real intellectual assets
- Take steps to safeguard the integrity of critical data
- Focus on information flows, not static stocks of data
- Establish ownership and responsibility for valuable assets and relationships
- Engage at the same level as your staff and customers
- Respond to network problems with network solutions
- Use networks to promote awareness
- Exploit virtuous circles to leverage your efforts
- Remember that every change is an opportunity

In particular, we need to think positively. We will experience huge changes over the next decade. Everyone and everything will be affected. We should aim to keep our heads and to stay ahead, to exploit the challenges of the information age, rather than be overtaken by events that are outside our control.