

# Case for investment in information security

Sukhendu Pal and Jon Fuller

October 2005



*The battle against internet crime is intensifying as fraudsters step up activity. The IT security industry is fighting back, but customers are unconvinced that companies are taking good care of their personal data; companies' reputations are on the line. Enterprises need to consider carefully what to protect and how to invest wisely in security. An integrated security management against risks and threats (SMART) framework can help them make those decisions and protect their major assets effectively.*

Threats to internet security come in many forms: phishing, pharming, pherretting – the list goes on. A degree in philology and a blind eye for misspelling are becoming essential to keep up with the latest trends. In fact, new kinds of threat are proliferating more rapidly than security experts can create a decent glossary to define them.

However, business executives are less likely to care about the nomenclature than the consequences. UK companies lost more than £500 million to internet crime during 2004<sup>[1]</sup>. US companies were stripped of more than £9.7 billion (\$17 billion) in the same year by computer fraudsters<sup>[2]</sup>. These figures may not represent the whole picture: it is not uncommon for companies to keep quiet when their security is breached and only a few spectacular frauds or attempted frauds hit the headlines. One incident that did make the news during 2005 was a report that police in London had foiled a gang planning to steal £220 million from Sumitomo Bank of Japan by hacking into its computer system and electronically transferring cash to bank accounts around the world.

For a glimpse into the future of internet security, just take a look at a nasty piece of software known as Troj/BankAsh-A. Designed to be secretly downloaded to a person's computer, this "Trojan Horse" lies in wait until a user tries to connect to one of the several banking websites. It then springs into action, hijacking the web browser and displaying a fake log-on page. The fraudulent web pages are so convincing that the web browser address bar still indicates that the user is logged on to a legitimate banking site. When the victim types in account information, it is recorded and sent to the fraudsters' computers. According to recent media reports, Barclays and Bank of Scotland are just two of several banks targeted by Troj/BankAsh-A.

We already could not trust the sender's address on incoming email, and now we cannot trust the address bar of our browser. Troj/BankAsh-A points to a new breed of automated malicious software, or "malware" designed to infiltrate PCs, collect specific personal information and deliver it to internet fraudsters. Automated malware is much more insidious than "phishing" scams, which rely on social engineering through bogus emails to lure in unsuspecting victims. That's because automated malware can be seeded in computers across the internet with much greater stealth, through downloads or email attachments. This tactic, known as "pharming", makes it more difficult for customers or security experts to spot an unfolding scam.

### **Internal breaches on the increase**

These new threats reflect the fact that, after years of mediocre performance, online retailers and auction sites are finally turning profits and banks are discovering the advantages of internet transactions. But fears of account hijacking and identity theft have once more made customers wary of e-business, while companies worry that security breaches will affect their brand and reputation.

Moreover, automated malware, such as Troj/BankAsh-A, highlights how a growing group of organised hackers are working together to stay few steps ahead of companies' security measures in order to steal large amounts of data which can then be used to defraud customers of billions of pounds. This loose-knit community, scattered around the world, gathers in a handful of secretive internet chat rooms to buy and sell stolen information ranging from bank details to national insurance or social security numbers, or data from birth certificates, passports and drivers' licences, that can be used to commit identity theft and other

types of fraud. As a UK tabloid reporter recently found out in New Delhi, a batch of a thousand customer bank account numbers is available for anything from a few hundred to a few thousand pounds.

In fact, the proposed deal in New Delhi is part of a trend which is even more difficult to control: cases in which employees sell insider information. There are signs that gangs are approaching employees with financial incentives that some find too good to pass up. These internal security breaches have now become a greater threat to financial institutions than external hacking. A recent survey of the world's top 100 financial institutions by accountants Deloitte found a sharp drop in external IT attacks, but security breaches inside organisations more than doubled.

While less than 33% of those surveyed had experienced an external attack in the past 12 months, compared with 83% a year earlier, some 35% of companies had suffered an internal attack, compared with just 14% the previous year. The UK's Financial Services Authority also warned last year that there is increasing evidence that criminals are placing staff inside banks and there are suspicions this was the mechanism used in the attempted raid on Sumitomo. It seems that, after financial institutions have spent a great deal of effort making their information systems secure from external threats, with firewalls and anti-virus programmes, criminals have responded by reverting to older and less high-tech forms of attack.

Moreover, the focus by management on implementing corporate governance rules, such as Sarbanes-Oxley in the US, seems to have made companies more lax about internal security. The same survey found that only 65% of companies were training staff to spot suspicious activities. Financial institutions are also failing to keep control over the IT they outsource to suppliers. Almost 75% of companies have outsourced at least one IT function, but 27% do not conduct regular assessments of how their outsourcers are complying with security requirements.

### **Personal identity theft gathers pace**

This stolen information is not just used for account hijacking but also for identity theft. A more elaborate scam than account hijacking, identity theft involves fraudsters using stolen personal information to sign up for new credit cards or mobile phone accounts, or to borrow money, apply for social security benefits and conduct other fraudulent business in a victim's name (see Figure 1).

These frauds are not entirely new, but new technologies and tactics are enabling internet fraudsters to steal vast amounts of information from enterprises and customers. No one really knows how much money is being siphoned off into cyberspace. According to the Federal Trade Commission (FTC), more than 635,000 people reported that they were victims of identity theft and fraud in the US in 2004, with losses totalling more than £312 million (\$547 million). But the FTC pointed out that they cannot measure unreported frauds and have suggested that internet fraud runs into billions of dollars in the US. In the UK, security experts suggest identity theft of all types is responsible for about 10% of fraud, accounting for some £1.3 billion of losses in 2002.

### **Corporate identity theft is also on the increase**

Corporate identity theft is also estimated to cost the economy millions of pounds each year. Fraudsters are abusing a loophole in the system for registering changes of business address with Companies House, which is limited by law to acting merely as a repository for information on the two million companies whose details are held there, with no powers to question the thousands of applications it receives each week to change corporate details. A company's trading address can be moved to a different location simply by submitting a single form, downloadable from the Companies House website and requiring little more than a business name, its registration number and a signature. Cars, computers and other big-ticket items are then ordered, apparently on behalf of the legitimate company, for delivery to the changed addresses. Then the fraudsters make off with the goods without paying.

The biggest losers from corporate identity fraud are usually not the companies whose addresses are changed but those that are duped into sending items to the fraudsters. According to Companies House, the cost to the UK economy is £50m a year. However, the Metropolitan Police believes that the true figure is likely to be higher, with an average loss for each incident of corporate identity theft of £2 million. Perhaps of equal concern is the impact that these growing losses have on customer confidence and the

reputation of companies in the marketplace. The Federation of Small Businesses is so concerned by these developments that it has been prompted to write to Companies House calling for tougher action.

Date (2005)	Reported by	Type of breach	No. of individuals affected ('000s)
Feb 15	ChoicePoint	ID accessed by thieves	145
Feb 25	Bank of America	Lost backup tape	1,200
Feb 25	PayMaxx	Details exposed online	25
Mar 8	DSW/Retail Ventures	Hacking	100
Mar 10	LexisNexis	Passwords compromised	32
Mar 11	Uni of CA, Berkeley	Stolen laptop	98.8
Mar 11	Boston College	Hacking	120
Mar 12	NV Dept. of Motor Veh.	Stolen computer	8.9
Mar 20	Northwestern Uni	Hacking	21
Mar 22	CA State Uni	Hacking	59
Mar 23	Uni of CA, San Fran	Hacking	7
Apr 8	San Jose Med Group	Stolen computer	185
Apr 11	Tufts Uni	Hacking	106
Apr 12	LexisNexis	Passwords compromised	280
Apr 14	Polo Ralph Lauren/HSBC	Hacking	180
Apr 18	DSW/Retail Ventures	Hacking	1,300
Apr 20	Ameritrade	Lost backup tape	200
Apr 21	Carnegie Mellon Uni	Hacking	19
Apr 26	Mich. State Uni	Hacking	40
Apr 26	Christus Hospital	Stolen computer	19
Apr 29	Oklahoma State Uni	Missing laptop	20
May 2	Time Warner	Lost backup tapes	600

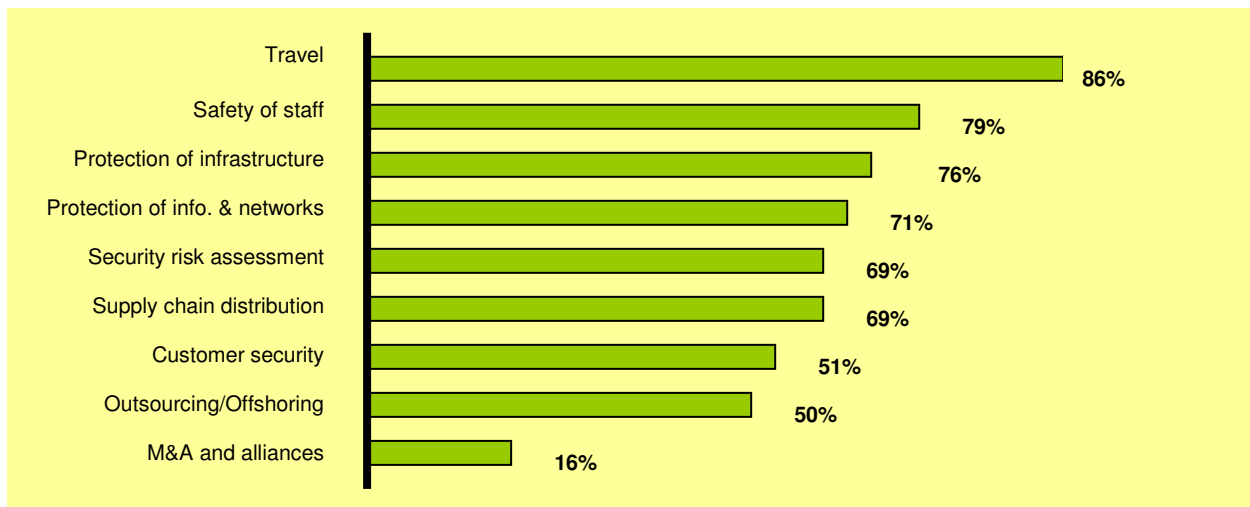
**Figure 1:** Selected data breaches in the US in three months of 2005 (source: Piracyrights)

### Policy makers and business executives are concerned

Policy makers do seem to be stepping up efforts to tackle internet crime. The National Hi-tech Crime Unit, a team of 58 computer experts and crime analysts, was set up in 2002 in the UK in response to the growing sophistication of the internet fraudsters. Companies are also putting more effort into tackling these threats. However, a number of factors make it difficult for them to protect their data and their customer information. It is impossible to know what targets and mechanisms hackers will focus on next, while ratcheting up security measures requires significant investment, especially as most companies have reacted in an ad hoc manner to threats as they arise. Moreover, companies have typically spent 80% of their security budget on protection against external hackers, despite the fact that 80% of attacks come from internal breaches by their own employees. The challenge facing most corporate executives is how to assess the vulnerability of their organisation to each kind of attack for each major class of asset: physical assets such as office buildings, plant and operations; information and network assets such as computer systems and network infrastructure; and human assets such as employees, partners or suppliers, and stakeholders. These threats don't just come from internet fraudsters concerned with profit. Today they also include terrorists who see economic strength as a source of power and industry as the target.

A poll in April 2005 of 100 UK chairmen, CEOs and senior executives – conducted by Mori on behalf of the Confederation of British Industry (CBI) – found that 57% were particularly worried about information and network security. A further 41% were concerned about their ability to continue with business after an attack from terrorists and 40% pointed out protection of their brand and reputation as a big concern, while 38% said they were concerned for the safety of their employees.

In addition, a short survey carried out by Centrix after the terrorist attacks in London on 7 July 2005 found increased concern for travel and for protection of staff, customers and information and networks, (see Figure 2).



**Figure 2:** How security has reshaped the post-July 7 executive agenda (Source: Centrix Analysis)

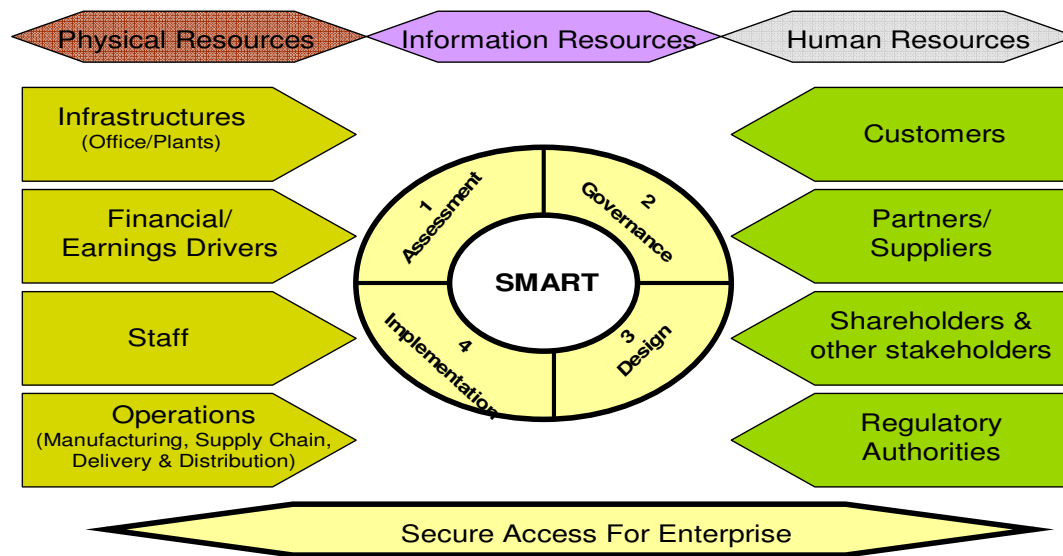
### Software vendors talk about uniting – but where are the integrated solutions?

Providers of network security products have often not done a great job of talking to each other, and their solutions to complex information and network security problems sometimes conflict. Leading technology vendors, including Microsoft, Symantec, IBM and Cisco, recently announced an initiative called the Network Admission Control (NAC). This aims to get vendors to work much more closely to solve the interoperability problems that customers face in keeping their networks and information secure. Yet corporate executives are not just looking for “point solutions” – which solve particular issues – to play nicely with other point solutions. They want solutions that unite that interoperability with best practices, tools and techniques and an overall governance framework.

Moreover, security risks have not traditionally been perceived by product vendors or users in the context of key earnings drivers. This means they have been managed in a functionally isolated way. For example, financial risks were the province of the chief financial officer (CFO); operational risks were the responsibility of the chief operating officer (COO); and information technology and network security was the task of the chief information officer (CIO). Rarely do these executives or their security programmes link together in support of strategic objectives such as the need to transact business openly yet securely across organisational boundaries.

Defining security in the traditional way – as protection of property and people, with a business continuity programme bolted on – is no longer sufficient. Neither is it acceptable to delegate management of security risks down the chain of command to individual business units, or to hand over security concerns to an external service provider as part of an outsourcing contract. Companies need an integrated framework (such as SMART) to ensure they can maintain operations in spite of damage or stress caused by attacks or the threat of attack (see Figure 3).

SMART is an integrated framework, incorporating a set of proven techniques, processes and tools that underpins the overall management of security within a business. It enables a company to resiliently withstand both systematic and unexpected threats and to adapt quickly to new security risks. It aligns an enterprise’s business strategy, operations, information systems, governance structures and decision-support capabilities across all its different assets (physical resources, information and network resources, and human resources) so that the company can identify and respond to continually changing security risks and successfully survive disruptions to its primary earnings drivers. The result is that the company can derive competitive advantage over less adaptable and resilient rivals.



**Figure 3:** Framework for Security Management Against Risks and Threats (SMART)

The plain fact in today's business environment, is that it is no longer possible, practical, or even effective to build a wall around a company by posting security guards outside office buildings and plants, and installing firewalls, intrusion detection, encryption, authentication and anti-virus software to protect the enterprise's information systems. Modern trading practices – such as IT-enabled supply chain integration – have created new interdependencies. Companies need to understand these interdependencies and ensure that all their resources and processes – including security – are aligned throughout this greater enterprise. For example, they need to conduct stricter due diligence amongst partners and suppliers to identify weaknesses in areas such as data security, physical protection of facilities and potential for supply chain disruption. SMART goes beyond the traditional boundaries of the company to protect these broader systems, infrastructures and interdependencies.

With SMART, companies are in a position to assure employees, customers, partners, shareholders and regulatory authorities that their operations are robust and will be there to serve them in difficult times as well as good ones.

### How is SMART different?

Most companies have some form of security and risk management procedure. Rarely have these procedures kept up with the shift from centralised to decentralised organisations, and the move to closer working with partners. In addition, most security and risk management procedures rely on “point solutions”, which attempt to mitigate security risks by “hardening” vulnerable spots against attacks. This is a futile exercise in a decentralised company. It cannot simultaneously harden all the nodes, and threats will simply migrate from a hardened node to a more vulnerable point, perhaps within a partner's operations.

In contrast, SMART enhances a company's speed and agility by combining two things. One is an integrated set of processes and practices that provides a firm line of defence. The other is an offensive strategy to protect the whole decentralised organisation against the new and unavoidable security risks that are the by-product of working in an interdependent fashion with partners and suppliers. SMART gives companies the agility to adjust to new security risks and threats, while taking into account the priorities and operational momentum of the business. It allows executives to make educated decisions about trade-offs when they develop their risk mitigation strategy, balancing the costs and benefits of solutions with the need to meet overall security targets and maintain or improve earnings.

## Earnings drivers versus investment in security risks

CEOs have been under increasing pressure in recent years to keep their profit marching “to the northeast corner”. However, investment in information and network security doesn’t sit well in that context.

Suppose a CEO invests aggressively to protect his company against the possibility of a serious security breach, but his competitors do not. If no one in the industry experiences a major security breach for two or three years (admittedly unlikely, given the trend of incidents shown in Figure 1), the CEO will have nothing to show for his investment, while the company’s earnings may not be as attractive as those of competitors. So the CEO who invests in security is likely to be punished by the stock markets and may be out of a job for failing to achieve or maintain the share price the board is looking for.

Moreover, the way investments are justified discourages investment in security. Traditional financial analysis scales the costs associated with serious risks in terms of “expected value”, taking into account the likelihood with which they will occur as well as the absolute cost of such events. A £10 million loss that is judged to be only 0.1% probable will be entered into the decision-making process as only a £10,000 loss ( $£10,000,000 \times 0.001$ ). Yet it is difficult to judge the probability of such an event occurring: it could easily be out by an order of magnitude in either direction – and that makes it even harder to justify investing a lot of money to avoid the loss. On top of that, those strict calculations rarely reflect the loss of reputation and brand value that a company typically suffers as a result of serious security breach. Policy makers, business executives and stockmarket investors need to begin placing as much emphasis on the value of companies investing in security as they have started to do on companies efforts at complying with corporate governance directives.

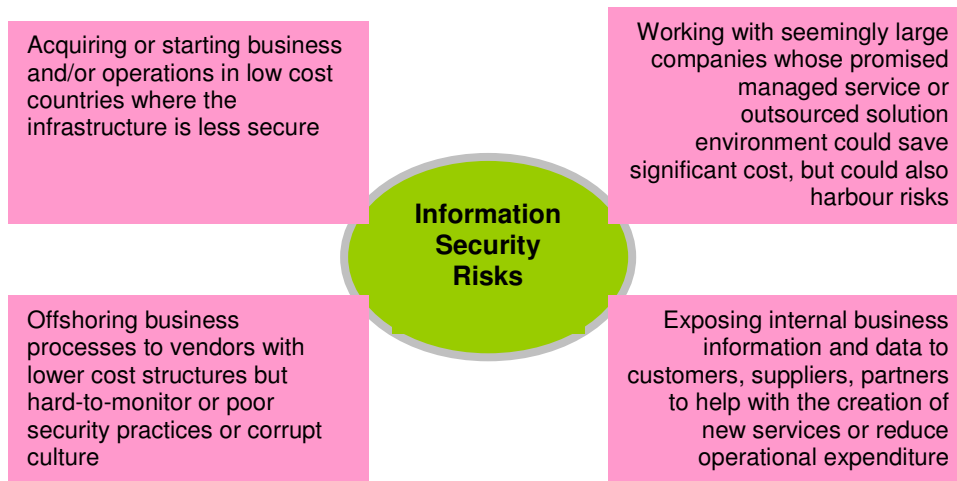
## What does all this mean for senior executives?

Today, security breaches have become a significant risk for senior executives and threaten intellectual property and brand equity. Information security is not just an issue for retailing organisations and banks – all companies face new risks, ranging from industrial espionage to sabotage. Compounding these concerns, compliance fears created by Sarbanes-Oxley and the forthcoming Basel II accord have fostered an environment of risk aversion inside many companies (see [Linking CEOs Corporate Governance agenda to CIOs agenda](#) by Pal and Hammond).

Building stronger walls around a company’s information systems can help to keep out some unwanted guests, but those clever invaders and unhappy insiders who find their way to into the fortress discover a treasure trove of information once they have gained access. But many risks lie deeply hidden within the de-parameterised organisation. While many companies have taken actions to strengthen their own internal security, their partners often harbour risks that open the entire company to vulnerability.

In September 2005, HM Revenue & Customs issued an apology to UBS after it lost a CD Rom containing sensitive financial information on some of the private bank’s well-heeled customers. As a result, UBS had to implement additional security measures around their lost customer accounts. The customer information lost included names and addresses, dates of birth, national insurance numbers, UBS account numbers and the value of their holdings. It is worth noting that processing of the CD Rom was outsourced to a well-known and large outsourcing company (see [Offshoring: Saviour or Value Destroyer?](#) by Pal and Hammond). The lesson is clear – senior executives must consider the security risk management practices of their partners, suppliers, and other stakeholders. For example, where does sensitive data flow when it leaves the company? How is it protected, and what are the risks? Equally importantly, do those partners, suppliers, and stakeholders have the right incentives to make the necessary security investments? It means that senior executives must factor their partners’, suppliers’, and other stakeholders’ risk into their own risk portfolio.

In addition, senior executives must incorporate information security risk into an overall company’s risk management strategy, before spending money with security software vendors and their alliance partners, who have quickly capitalised on the security fear along with new compliance measures. Like any other risks within a company, security risks must be identified and balanced against the benefits and costs of mitigation. Too often, information security risks arise from amateurish and corner-cutting practices so common in companies and government departments. Many information security risks occur within the context of larger business strategy with anticipated rewards (see Figure 4).



**Figure 4:** Information security risks occur with a larger context of business strategy

Becoming aware of the information security risks is just the first step in building an effective management strategy. Based on our experience, we found that companies in every industry are struggling to develop effective ways to measure and manage information security risks across their de-parameterised company. More worryingly, few admit that they have problems.

### Security risk is reality – get SMART

Companies have always faced security risks, but the events in London in July 2005, coupled with rising internet fraud and a growing number of hacking incidents, provide evidence that security risks in today's economy are greater than ever. Not all risks can be anticipated, but the impact of even unforeseen risks can be managed more effectively by senior executives and stakeholders working together to implement a SMART approach to security. While shareholders' expectations are high, companies that are more secure are also more likely to succeed over the long term and deliver premium earnings, because of increased customer, employee, and partner loyalty.

#### About the authors

Jon Fuller is the Operations Director of Centrix and Sukhendu Pal is a consultant.

#### About Centrix

Centrix is a leading independent consultancy that brings together the best of business, service and technology to create lasting value for its clients.

#### What Centrix Brings

Centrix designs effective operating formulae built on both innovative technical solutions and the practical realities of running a successful business. We help companies protect and grow their earnings by working with them to deliver effective information security management strategies, carrying out a current state assessment, and designing and implementing an integrated framework that secures their information and network assets. We also help companies to design secure strategic offshoring and outsourcing platforms and shared services organisations. Centrix's approach is set apart by capabilities that help companies tie security decisions to business drivers. When our clients align their security strategies and frameworks to the needs of the business, they achieve performance breakthroughs.

#### NOTES

1. "Ever classier forms of pherreting", Alan Cane, Financial Times, 9 May 2005.
2. According to Computer Economics, a consulting company.