THOUGHT LEADERSHIP FORUM

# RISK & DATA SECURITY:
## From NetWars to Networks... Finding the right balance

**24TH JUNE 2003**

FIRST TUESDAY ZURICH

GDI for economic and social studies

## Results and Findings

**Think Tank > Panel & Discussion > White Paper**

**design:** andrianameyer@bluewin.ch / www.desartes.com

## Foreword

An introduction to the Thought Leadership Forum and Topic

## Thought Leaders

The 20 leading experts who brainstormed about Risk and Data Security
Some views on Risk and Data Security from the Thought Leaders (Interviews)

## Thought Starter

Commissioned research providing industry background information

## White Paper

Results of the Risk and Data Security Thought Leadership Forum

## Keynote

**"Protecting business in the 21st Century – a look into the future"**
Evening Keynote Speech by David Love, Head of Security Strategy EMEA, Computer Associates

## Annex

- Full results of advance Thought Leader Survey
- Closed Thought Session: Results & Findings

## Producers

The producers behind the Thought Leadership Forum

# Foreword

# Foreword

## Foreword

The Thought Leadership Forum is more than just a conference. It is a learning process which includes preliminary research, a structured software - supported brainstorming session, bringing together a relatively small group of Thought Leaders, an evening presentation and discussions with a larger audience and finally the publication of the key findings in a White Paper.

## The Question

Today, not only CEOs and senior management, but also vendors, service providers and public administrations must be accountable for and recognize security management as indispensable for corporate management and economic growth. As organizations face regulatory compliance obligations, or have adopted standards and best practices to manage their information protection programs, Boards of Directors and executive management will pay closer attention to their governance responsibilities as related to the protection of information assets.

What are the winning combinations that balance highly principled and responsible corporate governance with executive commitment to sustainable company growth? Who will be in the driver's seat on the data security questions of the future, in reference to the protection of the private sphere of the public citizen? Who will draw the new battle lines between the isolationism of the "netwar" mentality to the open networked approach? And who will make sure that the lines are not crossed?

These and other questions were debated during the Thought Leadership Forum. The key results are presented in this White Paper.

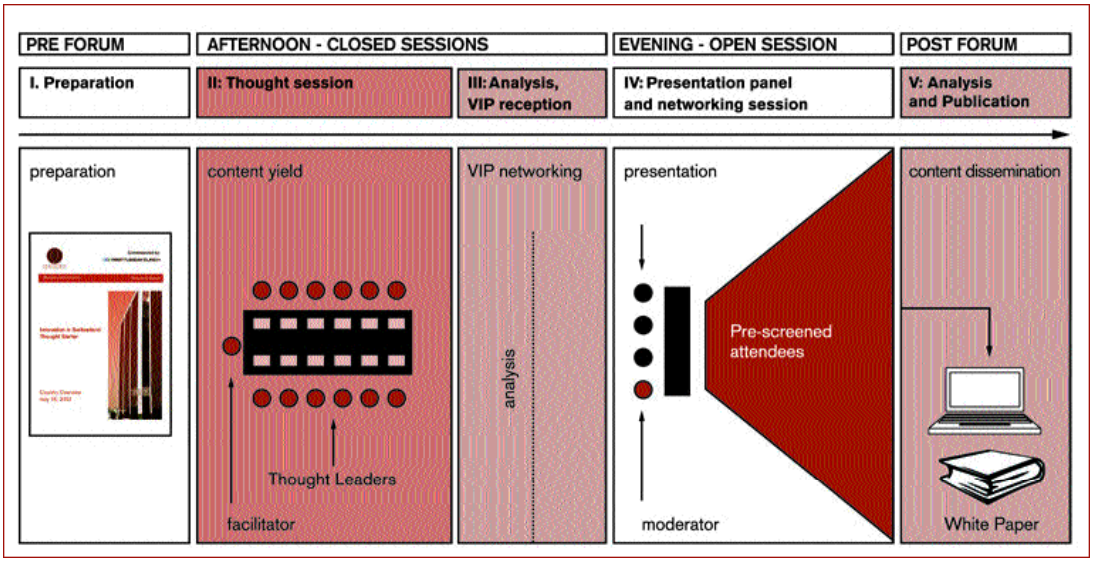
## Thanks

A very special thanks to our Presenting Partner Computer Associates, our Knowledge Partner PricewaterhouseCoopers and our Forum Partner T-Systems. Many thanks as well to our Software Partner groupVision and our Media Partners Financial Times and Netzwoche. We would also like to extend our thanks to the Thought Leaders and the evening attendees for their participation and contribution.

Susan Kish
First Tuesday Zurich

Samuel Dubno
Gottlieb Duttweiler Institute

# Foreword




## The Format

Prior to the Thought Leadership Forum, a Thought Starter Report providing background information on the topic is commissioned and distributed to the participants. The Forum begins with a structured brainstorming session bringing together a relatively small group of Thought Leaders focusing on the topic in the afternoon. Decision-makers from various sectors, backgrounds and with differing perspectives are gathered to accelerate the development of new and meaningful insights and ideas.
Following the Forum, the results of the afternoon session are analysed. These results are presented and discussed with a larger evening audience. A second round of analyses including the evening discussion and feedback is performed and the results are published in a White Paper.

## The Results

Included in the results from the Forum are the following papers:

Thought Leader Interviews: Thought Leaders express their personal view on the topic.

Thought Starter: Provides background research about the topic and current trends.
It is commissioned by First Tuesday Zurich and the GDI, and written by Evalueserve.

White Paper: The key analysis of the results of the afternoon think tank among the Thought Leaders and, as well as the input of the evening VIP audience.

Keynote: Transcript of the keynote address from David Love, Head of Security Strategy EMEA, Computer Associates.

Annex: Results of advnace Thought Leader survey
Closed Thought Session: Results and Findings

Thought Leaders

# Thought Leaders – Interviews

**Data Security focus: Hannes P. Lubich**

*Hannes is part of the group who literally connected Switzerland to the internet. Hannes P. Lubich currently works as an IT Security Strategist for Computer Associates. Prior to that, he was Chief Security Officer at Bank Julius Bär, and co-founded SWITCH, where he headed the SWITCH Computer Emergency Response Team. He curently serves as a lecturer in Information Technology at the ETH Zurich.*

*You've been involved with the internet since very early on. Over time, what were the major steps in the evolution of the data-security issue?*

At first, the internet was a purely academic thing, and there was a tremendous trust level between people using it. None of the protocols were designed to be secure because nothing legally binding was done over the internet. That went on for a long time, until the point where the Morris worm infected the net in 1989. And that was a wakeup call to the core internet community - things had changed: People had started using the Internet as a productive service and they trusted an incredible amount of confidential, important information to be sent by email or stored online. So there was a real gap between the security of the internet and its actual usage.

The internet protocols running today were defined as early as 1981, and there have been few operational changes there. People have invented security fixes like firewalls, but they only cure the symptoms, not the problem--which is that you cannot trust what's transmitted because there's no digital signature or encryption on a data packet as it travels across the internet. The newer version of the internet protocol (IP version 6) has a lot of security elements embedded in it, but rolling it out will take 5 to 10 years, because everyone - especially on the provider side - has to use it before it's effective.

*Working with Computer Associates, you have many clients. What's the range of attitudes toward data-security that you see among them?*

It's a bell curve, with the very highly regulated companies such as banking and finance in the middle. Since they face legal and regulatory requirements, they have a very precise understanding of risks and countermeasures and have allocated a substantial part of the budget toward it. And then on either side you have two extremes: some are over-the-top on IT security, although these are fading away, because they can't really prove the effectiveness of those cost-intensive measures. And then the larger group are the ones who are unaware, who have the attitude "If it hits me, it hits me," or "I'm not in finance, so why should I bother?" Most have some basic understanding that they might have a risk, but they have no real idea of how to analyze their risks and avoid them without spending all their money.

*How much of the problems that you try to solve are technical and how much are behavioral?*

We find that many of the risks are not technical at all. They involve careless employees, or traveling employees, or remote offices. In most cases we find that people are more willing to solve technical things, because those fixes are easy to measure and the implementation can be affixed to an IT asset or an operations procedure. Whenever we find ourselves crossing the border into rearranging parts of the organization or running an awareness program, everyone will agree on the importance, but they usually hesitate to do it. That's a corporate culture issue and it takes a lot of cooperation from people not involved in IT security, like human resources or legal departments. But it's harder to measure, it's harder to implement, and it involves a lot of people. They find it easier to just push the whole problem back to IT and say, "figure it out."

# Thought Leaders – Interviews

*From the data-security standpoint, how do you see the issue of people working wirelessly or remotely developing?*

There are two security factors influencing mobility. One is that more and more devices are becoming multifunctional, with a lot of processing power. Look at a telephone: this used to be just a telephone; now it's Java-enabled browser machine that also allows you to make a telephone call. On the other hand I just bought a new PDA and found it has wireless LAN, Bluetooth and infrared connectivity. So it has three sorts of networks, from very local to remote. And that really poses a problem, because their extended processing capability allows these devices to replace computers. They can run Excel sheets, Word Documents, or databases. So it's an extension of the workplace, but it's not secured by any physical security parameter. These systems also tend to interface with each other without any control by the user. You can have two notebooks sitting side-by-side in the train with the infrared ports activated and they'll interface. They might send a virus, or private files.

There's no way of stopping the mobility, so you need to have proper security deployed with the devices. But most people today are happy just to have connectivity at all. They're not so worried about the security of the wireless LAN they're using in an internet café or WiFI hotspot.

This evolution is part of our culture regarding risk taking: We make mistakes, learn from them, adapt our behavior. Look at the example of the car: We should have built roads, invented traffic rules and so forth, and only then put the first car out on the road, but we did it the other way round. The problem is that with abstract, global risks such as those that corporations face in IT, we don't have a real chance to learn from mistakes, because the first mistake could be fatal. Also, we do not have enough time to learn from our failures, since the time allowed for a new technology to be reflected in our behaviors and societal rules is becoming shorter and shorter. Before, technologies with impacts on the social contract were invented and introduced over 2 or 3 generations - like the car, phone or TV. Now the payback for technologies is more like 2 to 3 years.

*Looking forward, what are the new data-security issues that you think will be critical 5 years from now?*

The whole area of mobility, including devices like cars, household appliances, medical instruments and other things that have not previously been networked outside of their local environment. If that's not done properly these systems will all become vulnerable. Five years from now, your car, your front door, your refrigerator could all be talking IP and be connected to the outside world. People are working on interactive streets that will track your car as you drive. And if someone hacks a system like that the privacy issues are major. It's also true for planes, for hospitals, for mass transport systems. That's going to be a big threat.

There's also the whole range of cyber terrorism and threats to the critical infrastructure of the country. Here in the Switzerland, but also in the Unites States and in the UK, the governments have all added an IT part to existing efforts in protecting critical infrastructure like power supply, public transportation, air traffic control or food distribution. Because the systems are so interconnected, it doesn't even take a suicide attempt to bring them down. This could effect things like traffic control, radio telephony for emergency services and power plants, which are all controlled by IT systems. For terrorists it's a low-cost, low-risk attack and it can have a devastating effect on networked economies.

# Thought Leaders – Interviews

**Data Security focus: Pierre Brun**

*As a partner with PricewaterhouseCoopers, Pierre Brun manages the Financial Services Industry Team and leads the Technology Risk Management specialists in Switzerland. Holding a degree from University of Zurich and having completed postgraduate studies at ETH Zurich, he has written on IT security issues for publications such as Neue Zürcher Zeitung and Netzwoche .*

*Working with clients, what is the range of attitudes toward data security that you encounter?*
It depends a bit upon whom you talk to inside the company. Usually the people on the board are very concerned but then quickly delegate things to the management. The management again is very concerned, but delegates further to the risk or security officer. That person is usually left alone with the problem, facing limited budgets and a lot of work.
So on the one hand we try to help the dedicated security people find their way through the maze of vendors, standards, technologies and products. But also, we help them raise the awareness about the importance of what they're doing with their management. A lot of these security officers are good at their jobs, but perhaps could do better with communication. With companies, where we are also the auditors, we are in a better position to point out problems that we spotted and then clearly recommend how they be fixed.

*Do you see differences between clients as well?*
Regulated industries like banks are very concerned and very sensitive to anything that has to do with security. The Pharma industry, subject to FDA regulation, is also very concerned and very open to improvements. The same basically hold true Government agencies. Industries like manufacturing are usually less concerned—unless they own a certain patent or production secret that they want to keep secure. During the dotcom hype, the concerns over internet security were the most pronounced. Then this switched more towards internal concerns over things like fraud, security policies and governance. Now, after the latest wave of viruses, the pendulum will swing back to more on the focus on external problems.

*When you deal with a new client, what are the key indicators you examine when checking how well they've dealt with the issue?*
We follow our Enterprise Security Business Model, ESBM. Roughly speaking, we'd look at how they planned their security strategy. We'd analyze their readiness to deal with eventual problems. We'd check how well they implemented their strategy in terms of controls and technology - is it shelfware or have they actually configured it to fit their company correctly? We'd see how they operate it day-to-day - are they updating their viruses database, and are they installing patches on the critical systems? And then, finally, how they respond to incidents or catastrophes - how they repair damage, recover data, stabilize the systems and investigate the causes.
Corporate culture is also important, because technology plays a part in securing an enterprise, but awareness and organization process issues are at least as important. It's harder to change the people than the technology in a company. When it comes to fixing people's attitudes, we're still at the very beginning. A lot of people see the internet as a kind of El Dorado where everyone can do whatever they want. It's new terrain and has a feeling of adventure, so people want to explore it freely. That's a deep-rooted mentality, but that attitude has to change.

# Thought Leaders – Interviews

*Can you actually stop all data risk, or is it better to accept a certain degree of vulnerability?*
To do risk management, first you have to understand the nature of your risks. There will be some risks that your company cannot afford running, so those are the ones you focus upon preventing. Then you have certain risks that may be hard to quantify, but they are so rare and the impact is so small that you just live with them. Then there are the ones that could have a big impact but are either impossible or too expensive to defend against, so companies consider buying insurance to mitigate such risks.
We talk about two distinct forms of security. One is the "security of inclusion," where you specifically allow certain people in. For example, some companies want their suppliers to connect to their inventory control and manage their own section of inventory, so you have to deploy things like identity management. That has an immediate business benefit. On the other hand you have the "security of exclusion" - keeping the bad guys out by using things like threat and vulnerability management and incident response. It's always harder to make the case for this, because here the issue is preventing bad things from happening and the benefits are harder to quantify.

*Looking forward, what are the issues you expect to be handling for your clients five years from now?*
We are convinced that the identity-management discussion will be very important. People talk about the internet as a highway system. But if you want to go onto the real roads, you have to pass a driving test. And then you have a license plate, so if you behave badly it's easy to figure out who you are and take you off the road. On the internet, anyone can do anything.
In the future, I think we will want to know who the surfers on the internet are, and managing that will be a big challenge. For our clients, knowing who they want to deal with and keeping everyone else out of their network will be the task at hand.

## Data Security focus: Bernhard M. Hämmerli

*Bernhard M. Hämmerli's activities extend into both the public and private sectors. He is vice-president of Fachgruppe Security (www.fgsec.ch), serves as the scientific consultant on the advisory board for the InfoSurance Foundation and is involved with several federal working groups on the topics of data-risk and critical- infrastructure issues.*

*What is the role of government and academia on the issue of Data Security?*
It involves a lot of research in technical areas - especially in the precompetitive stages, because the competitive research is mostly done by security-products companies. There is also a lot of methodological support from academia, helping the private sector to address new topics. The federal administration has supported work on data-security topics for about six years now, and there is a convergence today toward creating standards and procedures. On the legal front, there is also the issue of developing laws for the prosecution of cybercrime.

# Thought Leaders – Interviews

*How does the Fachgruppe Security fit into the picture?*
We have two main tasks. One is organizing meetings or conferences presenting new security research or the ideas of national opinionmakers, focusing on topics such as managed-security services or human security aspects. Another activity is the working groups, where we handle specific topics - for instance, there was a guide to preparing penetration tests, or a paper on how corporations can initiate forensic investigations. We also help people – sometimes competitors – to meet each other and understand each other's positions and goals. In the future, we'd like to be an official player in the political opinion-building process and to professionalize the organization.

*In the time that you have been dealing with data security, how have you seen people's attitudes change?*
At first there was only a device and that device was a single point of security. So people encrypted certain lines and secured the data by using backup tools. Physical security was added as the next step. And then later there came codes of practice and some more general security thinking. A lot of corporations tried to evaluate all the security problems through a security officer. But that person could encounter real problems unless he had full support from the management, which led to another phase: trying to raise the issue to the executive level. Now, companies understand that data security is something that involves all the various processes within the corporation. This approach - which has not yet been fully deployed - is the final solution, because these various process interact and have common infrastructures. At the moment security architecture is much more important than before. Certain architectural rules are being developed, which everyone must follow to put security into a framework. So, in this sense, information security has changed and become part of overall corporate-risk management, and data security is an important part of that work.
Another topic, driven by the federal organizations, is examining the role of IT as part of the state's critical infrastructure, and understanding how it differs from the infrastructure needed by corporations. Today, nations think hard about what needs to be running to avoid our society collapsing. So there has been an evolution from data security at first only involving individual machines to now involving the entire society.

*How much can you control risk and how much do you have to accept it?*
For me, this is a perception issue. We have done experiments on this topic, trying to determine "What's critical?" and we found that it depends on the scenario. Most of the time, acceptance of certain risks is based on the premise that we have a normal economy and a functioning state. But that can change. The larger the crisis, the less important minor details become. For example when the bombs are falling around you in Iraq, you do not worry so much about your data-backup systems. So there are always acceptable risks, but they change depending on the scenario.
Ultimately, what companies can accept is a financial issue. We can always create defense strategies and parallel defense systems that are impenetrable. But putting in place something as strong as the Swiss banks have – which means a lot of expense and a lot of training for the personnel – is not for most corporations. Unless a company has an enormous amount of money, it must accept that there will be some risk that remains because of unnoticed vulnerabilities to the viruses and malicious code constantly attacking their system. Data risk is a part of the company's destiny, in the same way that when we have a highway system there will be 500 people a year dying on the roads.

# Thought Leaders – Interviews

*How important is the human aspect for data security?*

People need to be aware of their security responsibilities- and of the potential consequences involved if they fail to fulfill them. It is very important that we have permanent education and continual security checks. If someone wants to hack a corporate system, the easiest way is to find one person inside who is willing to give them the information they need. In that way, corporations are very vulnerable; therefore, they need to be able to check on people, which means that sometimes they will come into conflict with privacy regulations.

But society also needs to start dealing with the human aspect of data risks earlier. Young people now are taught using computers and benefit from using the machines, but most of the time they are not educated at all in acceptable security measures. Even the teachers at the 5th-grade to 9th-grade level are not aware enough of proper information security. But the training needs to already start when people are that young. It's logical: If you use a device, you have to be familiar with using it safely. When a parent gives a chainsaw or a motorcycle to a 14-year-old boy, they require them to get training and certification. Yet with computers we are too far behind in this thinking. So on the Infosurance Foundation steering committee, one of the projects we are pursuing is getting this sort of education into the curricula from a very early age.

# Thought Leaders

| Name | Company Name & Title |
|---|---|
| **Juan A. Avellan** | WISeKey (e-voting Geneva), VP Corporate Development and Policy Chief |
| **David Basin** | ETHZ, Professor Information Security, Dept. of Computer Science |
| **Martin Bosshardt** | Open Systems, CEO |
| **Hellmuth Broda** | Sun Microsystems, Chief Technology Officer EMEA |
| **Pierre Brun** | PricewaterhouseCoopers AG, Partner Global Risk Management Solutions |
| **Alfred Büllesbach** | Daimler Chrysler AG, Chief Officer Corporate Data Protection |
| **Rafael Cruz** | consul&ad, Partner |
| **Anja Dingenotto** | SonicWall, Marketing Manager (Germany, Austria, Switzerland & Benelux) |
| **Peter Fischer** | Fed. Office for Communications (BAKOM), Deputy General Director |
| **Bernhard M. Hämmerli** | FGSec, Board Member |
| **Thomas Kohler** | UBS, Head IT & Information Risk Control |
| **Maya Lalive d'Epinay** | National Councillor & President ICTswiss, Founder sederwäl AG |
| **Hannes P. Lubich** | Computer Associates, IT Security Strategist |
| **Peter Saladin** | Les Hôpitaux de Suisse Tarmed, President |
| **Paul Schöbi** | cnlab AG, CEO |
| **Wolfgang Straub** | Deutsch & Wyss Attorneys-at-Law, Partner |
| **Peter Waser** | Microsoft AG, Director Microsoft Services, Switzerland |
| **Uwe Wehrle** | T-Systems, Member of the Core Management Board, Head of Service Line |
| **Frank Zimmermann** | Hewlett Packard (Switzerland), Consulting Manager |
| **Marc Zweiacker** | eVersum GmbH, CEO |

| | |
|---|---|
| **Facilitator:** | |
| **Paul de Ligny Boudreau** | IT Leadership/Management, Business/IT Strategy Alignment and Trends |
| **Keynote:** | |
| **David Love** | Head of Security Strategy EMEA, Computer Associates |
| **Executive Producer:** | |
| **Maria Finders** | Senior Project Manager, First Tuesday Zurich |
| **Moderator:** | |
| **Susan Kish** | First Tuesday Zurich, CEO |

Thought Starter

# Thought Starter


Business Information – Market Overview 24/06/03 – Research Expert

**Evalueserve India**

Marc Vollenweider
Marc.Vollenweider@Evalueserve.com
Tel: +43 67683115394
Austria

Vikram Suri
Vikram.Suri@Evalueserve.com
Tel: +91 124 256 1770
Fax: +91 124 256 2393
India

India Team
Pankaj Sharma
Sandeep Sonpatki

**Evalueserve Research Expert:**

## **RISK & DATA SECURITY:** From NetWars to Networks... Finding the right balance

# Thought Starter

## EXECUTIVE SUMMARY

Information powers modern-day business. It is a source of competitive advantage to many businesses and the basis of existence for many others. With technological advances, reliance upon information is only rising.

Therefore, information, if unavailable, can wreak havoc upon the networked global economy that relies upon it. It can also be used to the disadvantage of those who own it, upon breach of its confidentiality. Further, if it is inaccurate or tampered with, it can result in incorrect decisions with immeasurable impact.

The risks of massive business and financial losses and myriad regulations have made it incumbent upon top management to recognise these risks and implement a concerted data security management strategy to deal with them.

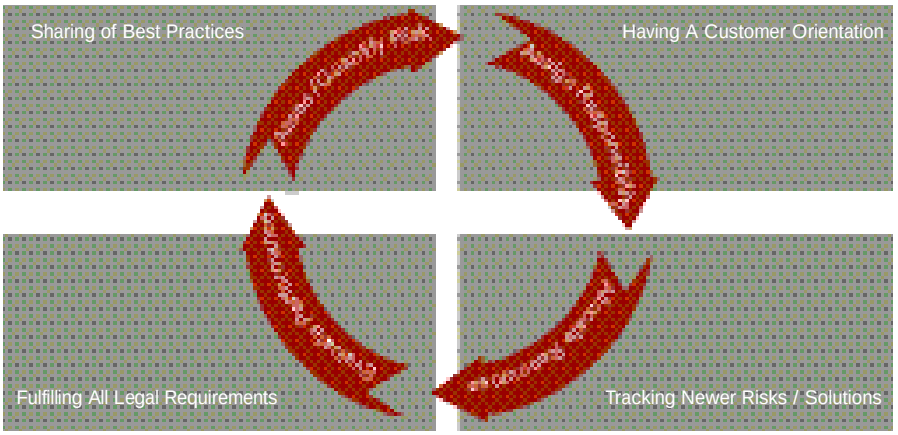
Such a strategy could be formulated by following a four-step, cyclical process.

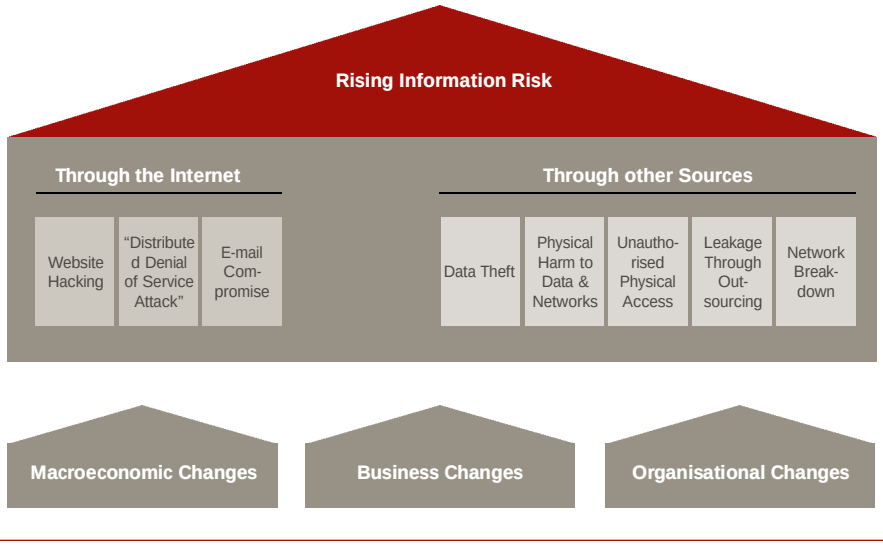
- All the sources of risk should be identified and ranked according to the threat that they pose.
- An entire hierarchy of responsibility and accountability should be put in place to assess and deal with each risk source.
- Resources will need to be allocated to those responsible to meet the data security objectives.
- The performance of these measures should be continually evaluated. This possible strategy would need to be re-assessed and fine-tuned to fit new challenges or opportunities, as they would arise.

The success of such a strategy can be measured by its influence on sharing of best practices of data security management across the organisation. It will be judged on its customer orientation and ability to anticipate and adapt to newer risks and solutions thereto. Finally, such a strategy must ensure that the organisation fulfils the provisions of the complex web of data security regulations that surrounds businesses today.

# Thought Starter

*Figure 1: Risk and Data Security*




Source: Evalueserve

# Thought Starter

## SIGNIFICANCE OF DATA SECURITY

Fortune 1000 companies lost more than $45 billion from proprietary information theft in 1999, and such incidents, which result in an average yearly $15 million loss, are increasing.[1]

Two out of five enterprises that suffer a disaster go out of business within 12 months.[2]

In the credit card business, MasterCard and VISA are losing about $5 billion a year due to security breaches.

In 1998, there were about 17 million people globally with the skills to launch an attack on the information infrastructure. Losses due to theft of proprietary or confidential information cost U.S. businesses an estimated $300 billion in 1997.[3]

## INFORMATION "RISK"

Information is the most critical asset of an organisation in today's business. As the examples show, information so vital to the brand image and shareholder value of the company, is vulnerable to:

- Risk of breach of confidentiality: Information accessed by unauthorised means.
- Risk of breach of integrity: Information exposed to being manipulated with or without malicious intent, hurting accuracy and reliability.
- Risk of unavailability of information: Information unavailable when networks crash and essential stakeholders are denied access.

## EFFECT OF INFORMATION RISK ON BUSINESS

Information risk, unless managed, might lead to the following:

- Productivity losses
- Disruption of services to customers
- Loss of proprietary information
- Legal liabilities
- Loss of brand equity
- Loss in shareholder value

**Productivity Losses**
Security breach of data networks within the organisation can lead to a complete shutdown, directly affecting productivity.

As much as 97 percent of virus costs are productivity related. Of CodeRed's (virus) estimated $2.6 billion damages worldwide, Computer Economics attributes $1.5 billion to the negative productivity impact.[4]

**Disruption of Services to Customers**
Attacks on vulnerable networks flood a web server with false requests for information, overwhelming the system and ultimately crashing it.

Losses traced to denial of service attacks were only $77,000 in 1998, and by 1999 had risen to just $116,250. However, by 2000 the figure had grown to more than $8.2 million.[5]

[1] ASIS / PWC "Trends in Proprietary Information Loss" survey report
[2] Gartner report
[3] 1998 Computer Crime and Security Survey, conducted by the Computer Security Institute (CSI) and the FBI's International Computer Crime Squad
[4] Information Security magazine - Year 2000 survey
[5] 2000 Computer Crime and Security Survey, conducted by CSI and the FBI's International Computer Crime Squad

# Thought Starter

**Loss of Proprietary Information**
The company that has not secured its data is vulnerable with respect to its proprietary information.

On average, business loss of $6.6 million can be incurred each time proprietary information is stolen (including costs of research and development and branding), and anywhere from $1,000 to $9 million per virus attack.[6]

**Legal Liabilities**
Quite often, firms exposed to digital risk are legally liable to the extent of loss or inconvenience caused to its clients or other stakeholders. As a result the management needs to allocate resources to handle these contingent liabilities.

In May 2003, more than 75 customers of Bank of America replied to a fraudulent email asking for personal information. However, the entire liability of fraudulent activity on the affected accounts was the responsibility of the bank because of the "zero-liability" guarantee that it offered.

**Loss of Brand Equity**
Digital risk mismanagement can often result in the company losing its brand equity. In certain cases, the entire business could get wiped out.

In the background of the collapse of Arthur Andersen and Enron, also lies the lack of coherent and integrated enterprise-wide policies concerning destruction of documents and computer records. This led to Andersen losing its key customers initially and then going out of business completely.

**Loss in Shareholder Value**
Losing proprietary information reduces competitiveness and in extreme cases, may lead to bankruptcy. Shareholders and other stakeholders alike are quick to abandon companies once an information-loss incident is publicised.

Egghead.com, an online retailer, lost 25% of its stock market value in December 2000, when hackers struck its customer information systems and gained access to 3.7 million credit card numbers. Egghead had security systems in place and claimed that no data was actually stolen. However, the response lacked co-ordinated effort from the organisation and could not convince customers and shareholders that their sensitive data were actually secure.[7]

## REASONS FOR RISING SIGNIFICANCE

As the dependence on information rises, information risk is becoming increasingly significant. This can be explained by:

- Macroeconomic changes
- Business changes
- Organisational changes

**Macroeconomic Changes**
The share of the services sector in the overall economy has been rising. Data and information are driving this. The need for information and data security is critical in today's world.

In the industrial economy in the past, failure to adhere to standards resulted in problems that were localised. To deal with these problems, rules and regulation were put into place. However, failure to do so in the global digital economy has potentially far reaching consequences and a much larger impact due to the breadth and depth of networked relations.

[6] 2002 Computer Security Institute / FBI Computer Crime and Security Survey
[7] News.com article

# Thought Starter

**Business Changes**
Significant changes in the way business is conducted today have brought information to the forefront, making it one of the key assets of a company. Some of these fundamental changes converge on the following issues:

- Businesses going online
- Increasing dependence on technology
- Outsourcing
- Demanding customers

*Businesses Going Online*
Companies can no longer afford to neglect the impact of the Internet on their business. Online business is a common phenomenon requiring a company to transact over the Internet. Others use the Internet to exchange information. This makes the company prone to various attacks on its websites, servers etc. and thus vulnerable to losses.

*Increasing Dependence on Technology*
Advances in technology have benefited businesses by enabling the sharing and utilisation of information at a scale that was previously impossible. However, with increasingly complex systems, the risks associated with maintaining digital data security have also increased.

*Outsourcing*
Although outsourcing, as a strategic objective, controls costs and improves operational efficiencies, companies sharing their internal processes and data with third party processors are particularly vulnerable to loss of critical information.

To deal with this risk, the Indo-American Chamber of Commerce has stressed the need for data protection legislation to protect the privacy of data outsourced from other countries.

*Demanding Customers*
Increasing competition has led to a definite shift in the balance of power in favour of customers. This has resulted in businesses having to cater to increasing demands of customers. It is almost mandatory for firms to share more data and information about their products and services. Online access and 24 hours connectivity are some of the other features that customers demand.

For example, almost all major banks offer ATMs, Net banking and 24 hour phone banking features to its customers.

**Organisational changes**
Information has become a critical asset from an organisation point of view. Knowledge is the key driver for an organisation. Proprietary information is the source of competitive advantage and any compromise on that front can lead to serious consequences.

According to one estimate nearly 70% of a typical US company's market value resides in its intellectual property assets.[8]

[8] "Trends in Proprietary Information Loss, Survey Report", American Society for Industrial Security/ PriceWaterhouseCoopers LLP, 1999

## SIGNIFICANCE OF DATA SECURITY

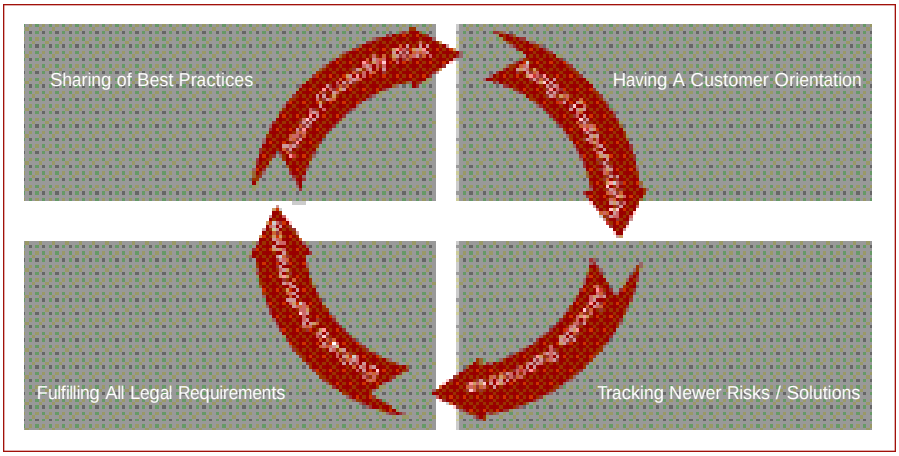
Data Security Management is the aggregate of all activities that aim to:

- Maintain confidentiality of information
- Maintain accuracy and reliability of information
- Ensure continuous availability of information

## CORPORATE GOVERNANCE AND DATA SECURITY

The CEO and the senior management of an organisation are accountable and must recognise security management as an indispensable part of corporate management. Top management commitment is of paramount importance if companies have to counter information risk. The overall direction in which the organisation is moving largely dependent on the willingness and competence of the chief executive.

*Figure 2: Figure 2: Data Security Management*




Source: Evalueserve Analysis

As Figure 2 shows, CEOs could consider a 4-step cyclical process for Data Security Management, guided by certain principles. Both of these are described in the following sections.

## THE DATA SECURITY MANAGEMENT PROCESS

The commitment of the CEO, the senior management and that of the entire organisation is critical to manage information risk and maintain data security.

CEOs could consider addressing this risk by following a cyclical process. This four-step process is described below:

- Assess / Quantify data risk
- Assign responsibility
- Allocate resources
- Evaluate performance

# Thought Starter

**Assess / Quantify Data Risk**
Each source of risk must be identified so that measures can be instituted to deal with it. Organisations could also consider quantifying the magnitude of risk from each to help prioritise their efforts. A proactive approach would go a long way towards pre-empting the losses.

Potentially, information risk could arise:

through the Internet

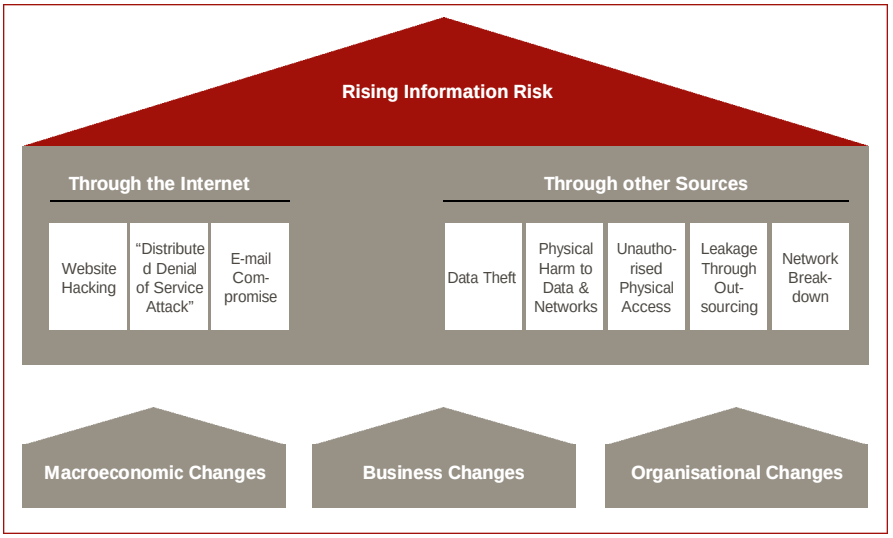
- Distributed Denial of Service (DDOS) attack
- E-mail compromise
- Web-site exposure

or through other means

- Physical Destruction of Data
- Data Theft
- Leakage due to Outsourcing
- Physical breakdown of networks

Figure 3 illustrates these issues and their impact on information risk.

*Figure 3: Rising Information Risk and its Sources*




Source: Evalueserve Analysis

*Distributed Denial of Service Attack*

- How can we be sure that the company networks are secure?
- Are the networks vulnerable to hackers, who could compromise the security weakness?

An insecure network could fall victim to attackers, who would gain access and use it to launch attack on other networks. The attackers can then use the victim's IP address to initiate denial-of-service assaults on a target.

The DDOS attack launched in October 2002 against all 13 of the Internet root servers made use of hundreds of such insecure networks. These victim networks are also referred to as "zombies".

# Thought Starter

### *E-mail Compromise*

- What are the risks that the organisation as a whole faces from the exchange of e-mails among the employees and with the outside world?
- Do we have adequate security to check the spread of virus or Trojans?

E-mails could be one of the biggest culprits of virus and spam attacks across the world. Many times, unknowingly legally sensitive unprotected e-mail harbours virus or Trojans and are the cause of large-scale infections. Fraudulent e-mails are also a source of threat to the brand equity of many firms.

By the year 2005, there will be 1.2 billion e-mail boxes (growing at a compounded growth of 138%) and 36 billion person-to-person emails daily.[9]

### *Web-site Exposure*

- How is the company addressing the threat of hacker attacks on the company web site?
- How often in the last year was the corporate web site unavailable and what were the causes?

Corporate web sites are a very common phenomenon these days. Equally common is the issue of hacker attacks, which render the web site either unavailable or maliciously altered to include erroneous information.

### *Physical Destruction of Data*

- How safe is the customer information in our databases located in the office building? Do we have a backup at another, safer location?

The impact of physical destruction of data resources was shown in sharp relief in the events of the September 11, 2001 incident.

Even now, many US companies are not capable of withstanding business and IT outages caused by a severe calamity. In fact, one in three US businesses would lose critical data or operational capability if a major disaster occurred.[10]

### *Data Theft*

- How many employees (including the system administrators) have access to sensitive information within your organisation? Do you perceive a threat?
- What will be the impact of lost employee morale when internal hackers gain access to private human resource records?

An organisation is at threat of losing sensitive data or proprietary information due to theft by either insiders or outsiders. Adequate procedures need to be in place to ensure that critical data is protected against such a threat.

Internal employees commit an estimated 70 percent of unauthorized access to information, and more than 95 percent of intrusions that result in significant financial losses.[11]

### *Leakage Due to Outsourcing*

- How should we ensure that crucial information and company documents do not leak out to a competitor?
- Have we taken adequate measures in the service level agreement (SLA) with the outsourcing vendor?

[9] IDC report
[10] Gartner-Dataquest survey
[11] Gartner Report

# Thought Starter

Companies outsourcing processes are always under the threat of losing sensitive information to their competitors. Companies consequently need to ensure that all eventualities have been taken care of at the agreement stage itself, and award the outsourcing contracts to those vendors which assure data security.

This due diligence includes a security survey, a comprehensive audit and ongoing penetration testing. In fact, ISO has come out with an ISO 17799 standard for Information security management. This standard attempts to outline the broad level categories, which an outsourcing company can refer to before awarding a contract.

### *Physical Breakdown of Networks*

- How often does the network shutdown in our organization?
- Have we been able to identify the cause for it?
- What is the impact on our business?

Over and above the external risks that the networks face, the risk of a network breakdown due to internal causes always exists. Such a breakdown could result in reduced productivity and affect the continuous availability of information to the customers.

### Assign Responsibility

- Who is in charge of identifying data security challenges and building the strategy to deal with them?
- Who decides the appropriate level of security for your enterprise?
- Who will determine standards of data protection within your company and who will control the process?
- Who is responsible when your system crash causes productivity losses?

Clearly, the risks are significant and continually rising. The organisation must act in an orchestrated manner. The CEO would need to put together an entire hierarchy of responsibility and accountability to deal with specific sources and types of data security risk.

In 2002, The US government created the National Infrastructure Advisory Council (NIAC) to advise the President on issues surrounding the security of information systems that support the US's critical infrastructure.

Indeed, many organisations now have a hierarchy under the leadership of a Chief Security officer (CSO). In a survey involving financial institutions, 61% of the respondents had a well-defined CSO with another 14% having more than one of such positions.[12] This chief liaison between IT and the business side of the firm would ensure that implementations of technical measures meet the business requirements.

### Allocate Resources

- How deeply should you be committed towards managing digital risk?
- Do you balance the risk with the cost of managing it?
- Has your budget for security products, services and strategy consulting increased since September 11, 2001?
- What have been the areas of this increase if any?
- Do you see your e-security budget increasing next year? In which areas will it increase if any?

Resources, both financial as well as human, need to be allocated across the hierarchy of responsibility. The level of security for an organisation would largely depend on the risks and the corresponding costs. A Risk vs. Cost assessment would reveal how deeply the management should be committed to the endeavour to manage digital risk.

[12] Deloitte Touche Tohmatsu 2003 Global Security Survey for financial institutions

# Thought Starter

The penetration of security technologies among financial services institutions (FSIs) is shown in Table 1 below:

*Table 1: % of FSIs Adopting Various Security Technologies, 2003*

| SECURITY TECHNOLOGY | PENETRATION % |
|---|---|
| Anti-virus solutions | 96% |
| Virtual Private Networks (VPNs) | 86% |
| Intrusion detection systems | 85% |
| Content filtering / monitoring | 77% |
| Public key infrastructure | 45% |
| Smart cards | 43% |
| Biometrics | 19% |

Source: Deloitte Touche Tohmatsu 2003 Global Security Survey for Financial Institutions

The expenditure on IT security by organisations has grown at a CAGR of 28% since 2001.[13] In the 2003 survey of financial institutions, the IT security budget was found to be 6-8% of the total IT budget[14], which as a percentage of the overall revenue was 9% in 2002[15]. Thus, the overall expenditure of organisations on IT security comes to 0.6% of the revenues.

The overall IT security market, including hardware, software and services, is expected to increase to $45 billion in 2006 compared to $17 billion in 2001.[16]

### Evaluate Performance

- What are you really buying when you invest in highly priced Information Security tools and services?
- If you are making major investments in this area, does this directly relate to your clients / public perception of your brand? How can you make your commitment visible?
- How will you evaluate the performance of employees who have been assigned these responsibilities?

The efficacy of enterprise-wide controls needs to be investigated, lest the entire process of ensuring data security should result only in escalating costs.

The top firms in the UK have a security network in place, but still around one-third suffer from 'bad housekeeping' with unacceptable levels of basic flaws, leaving them vulnerable to external attack.[17]

## GUIDING PRINCIPLES

While following the process described above, management must be guided by the following principles:

- Share best practices of data security
- Have a customer orientation throughout the data security process
- Track environment for new security challenges and solutions
- Fulfil all legal requirements

### Share Best Practices of Data Security

- Is the top management aware of any industry platform that enables mutually beneficial sharing of best practices? What benefits could the organisation derive from such an alliance?
- Would the organisation benefit by sharing its best practices of data security, if sharing were against the company's professional interests? How much information should an organisation share?

[13] Gartner Report
[14] Deloitte Touche Tohmatsu 2003 Global Security Survey for financial institutions
[15] InformationWeek
[16] IDC report
[17] NTA Monitor's Fifth Annual Security Audit

# Thought Starter

Data risk affects all businesses today. Learning and innovation by one can help prevent losses elsewhere. If businesses join hands to combat this threat, risk management is likely to be more effective. It is imperative for an organisation to share its best practices of data security with its vendors and other links in the value chain to ensure mutual benefit.

Work is underway in the Information Technology-Information Sharing and Analysis Centre (IT-ISAC), an industry organisation established by 19 leading IT companies to report and exchange information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures. The objective is to establish mechanisms for systematic and protected exchange of highly sensitive business information and develop methods to protect business and personal privacy.

**Have a Customer Orientation throughout the Data Security Process**

- How can you own your customers and use information about them without encroaching upon their privacy?
- What do customers expect from your information security network?
- Can technology deliver the twin benefits of enhanced privacy and efficiency of process?

Organisations around the world now need to guarantee customer privacy as part of their service offering. Stringent regulations and heightened consumer activity ensure that any breach in customer privacy can prove devastating to organisations. To protect against unauthorised access and security breaches, organisations have to constantly devise newer identification and authentication procedures.

Microsoft has spent $250 million to date on protecting the rights of user privacy and preventing unauthorised file sharing. It recently announced the introduction of a security service for Windows 2003. The Microsoft Windows Rights Management Services works with applications to help customers protect sensitive Web content, documents and email.

**Track Environment for Newer Security Challenges and Solutions**

- How do the new security challenges, thrown up by rapid technological evolution in a connected economy, impact your company?
- Do these new challenges make it to the agenda of your board meetings?
- Do you have a system in place to monitor data networks at all times?
- What will be the future of user identification and authentication procedures? What role would biometrics play in future technologies?

With progress in technology and information processing, novel environments with complex systems are emerging. At the same time, organisations need to maintain the older technology and systems to maintain backward compatibility. This implies that the risks associated with an upgrade in technology would always be additive.

Meanwhile, the threat to data networks from the internet is ever increasing with the emergence of a new breed of cyber attackers having varied motivations. The list now includes terrorist groups, intelligence communities and disgruntled employees, each having their own objective.

The viruses of the new age are faster and “better”. According to a study conducted by a group of experts, the Slammer or Sapphire worm appeared to double its infection base every 8.5 seconds. The same study compared this infection to CodeRed in July 2001, which doubled its infection base every 37 minutes.[18] Along with newer risks, organisations also need to be abreast of newer solutions that are available in the market. New encryption techniques like “Palladium”, at COMDEX Fall 2002 and a Microsoft proposal to create Trustworthy Computing are efforts to secure hardware and software systems from newer risks.

[18] Cooperative Association for Internet Data Analysis (CAIDA), International Computer Science Institute, Silicon Defense, University of California at Berkley and San Diego study report

# Thought Starter

Similarly, biometrics is a difficult technology to forge, steal or abuse. Biometrics make use of a person's unique characteristics like fingerprint, face, voice or retina to prevent unauthorised access. The issue of Biometrics, Security and E-Government were central to the G8 in Evian in May 2003.

**Fulfil All Legal Requirements**

- Should information security be a public / private initiative?
- How do you think existing and emerging global and local information security policies affect your company's bottom line?
- How would the cost structure of your organisation change because of these?

Globally, governments and regulatory authorities are now more aware of cyber crimes and attacks. In order to secure data and reduce information risk, these agencies come out with security policies and guidelines.

In the US, for example, new regulations and recently updated Federal Sentencing Guidelines created mandatory corporate governance environments, making the business leaders personally liable for privacy and information security violations.

Even within a specific vertical such as financial services, the complexity to meet security requirements is brought on through an onslaught of different regulations (e.g. the US Gramm-Leach-Biley Act of 1999 (GLBA), Basel Accords, Security and Exchange Commission (SEC) requirements, USA Patriot Act). Moreover, five of the twenty-eight proposed resolutions for the G8 in Evian were related to security of information and data protection.

Organisations need to be abreast of each legal requirement that affects or will affect them and fulfil each of them. These issues would require increasing attention as the number of such regulations rise varying by each industry, business or geographic area that the company operates.

## Evalueserve Disclaimer

White Paper

White Paper

# Risk & Data Security: From NetWars to Networks.... Finding the right balance

Summary, results and quotes

*"Considering 2002 as an anomalous year in IT security, Giga forecasts for 2003 a 30% decrease in IT security spending relative to 2001 levels. The successive years 2004-2006 will each see a modest 15% annual growth. Therefore, we do not expect IT security spending to match 2001 levels until at least 2005."*

Giga Group Research, 2003

## Introduction

In the age of ever-increasing digital pervasiveness, there are words that strike fear in the hearts of business leaders: Slammer, Blaster, SoBig, worm, virus, hacker, corporate espionage. Among people charged with deflecting such attacks, the greater fear involves the cost of constantly implementing IT security and the difficulty of justifying security measures. The effectiveness of such measures are hard to gauge, except when they fail. So before a crisis, it's hard to get the necessary budgets; afterwards, it's too late.

Yet the more we depend upon computer systems, the more vulnerable we become when they are compromised. And the more those systems become interconnected, the greater the avenues for potential entry, both sanctioned and unsanctioned. Hacker attacks are only the most visible problem; more than 50 percent of security breaches are internal. Moreover, for companies active in the United States new corporate-governance regulations create a situation in which business leaders could potentially be held responsible for their company's information-security flaws; likewise in Switzerland the country's "Obligationenrecht" makes board members and other executives directly responsible for both non-compliance and gross negligence when doing business.

### An Overview

In order to explore this mission-critical issue within today's information society, First Tuesday Zurich and the Gottfried Duttweiler Institute convened 20 Thought Leaders for a one-day forum at the GDI in June 2003. These participants work at top-level positions within a wide range of companies, from global leaders to startups representing IT, Finance and Insurance, Health, Industry, Law, academia and the Swiss Federal Government.

Before the forum took place, the Thought Leaders had been asked to read a Thought Starter on the topic (also included with this report), and also to submit a list of the three most significant data-security challenges they face. The event started with each Thought Leader discussing those challenges. Several issues came to the foreground:

- The tension between always-on machines and risk of intrusion by outsiders
- The need to balance user productivity versus data security
- The proper management of security, including risk assessment and risk management, return on security investments etc
- Security as a moving target: Each new type of attack creates new defenses; each new defense sustains new types of attacks.
- Technology representing only part of the solution, because generally a system's security ultimately relies upon the practices of users. Also, technology can sometime even make things worse, because just piling more security technology on top of a complex IT environment adds to the problem.

# White Paper

**Risk and data security: Corporate Governance**

For the first of three sessions, the Thought Leaders tackled the issue of corporate governance, specifically: "What should be the rules and who should oversee the information-security system in the enterprise?" Broken into four groups, they were asked to select the 10 most critical data-security aspects from the standpoint of corporate governance. Two groups were assigned to think in terms of a horizon stretching to 2006, while the two other groups were asked to look forward to 2010 - the medium forward timeframe considered to involve "educated speculation" rather than indulging in pure science fiction.

*Looking toward 2006*

As they discussed the aspects important in the near-term future, Thought Leaders examining the next three years focused on corporate culture, concluding that:

- Liability for information security has to delineated and enforced throughout the organization.
- Security has to be constantly stressed and shown to be valued by high-level executives.
- Awareness of risk and data security has to be pushed downwards through the company from the executive board. "The problem is that if security strategies are to be realized, the order has to come from the top," analyzed one Thought Leader. "You can't just delegate it to operations."

Of course, this will not be easy. As one Thought Leader remarked: "There's always going to be a tension between the board's authority and the operational issues involved in executing their orders. It's not possible for someone at CFO level to be constantly evaluating IT risks."

*Looking toward 2010*

"The problem is that if security strategies are to be realized, the order has to come from the top… you can't just delegate it to operations."

"We often have the notion that we can find something to make data-security problems go away. That won't happen…"

The Thought Leaders predicting further-away concerns, naturally, had different issues:

- As the security sphere matures, much more will be bought rather than built in-house, entailing major integration issues.
- Concerns surrounding issues such as transparency and privacy will rise in visibility, and officers will probably be held more personally liable.
- Some companies will create a new position, perhaps titled the Chief Risk Officer, assigned to deal with risks of all sort, although data security will be a major and increasingly critical focus of any such position. As part of the operational risk management, which in turn is part of a company's overall risk management, this person's role could also be enforced by sector-wide regulations, in the same way the Basel II Accord requires banks to detail their risk-management practice.

Speaking more globally, the Thought Leaders expect that attitudes toward risk and data security would evolve over time. "When cars first came to London, someone had to run ahead ringing a bell and carrying a red flag, in order to warn pedestrians," pointed out one Thought Leader. "Now people know the risks. In the same way our acceptance and understanding of data risks will grow." Along similar lines, another offered this analysis: "We often have the notion that we can

find something to make data-security problems go away. That won't happen, so we just need to learn to deal with these difficulties and prepare for them."

Another Thought Leader predicted that security would be geared around multiple access levels. "Right now a lot of companies are like buildings where once you make it past the front door all the floors and offices are unsecured. That will change." (In the evening session, David Love of Computer Associates would make the point even more bluntly: "If you have 1000 points of access and only one is vulnerable, you're not 99.9 percent safe, you're 0.1 percent safe.")

In general, the Thought Leaders predicted the issue of information security will no longer function as an isolated wing of the company, but rather come to be a pervasive part of its overall business and risk management practices.

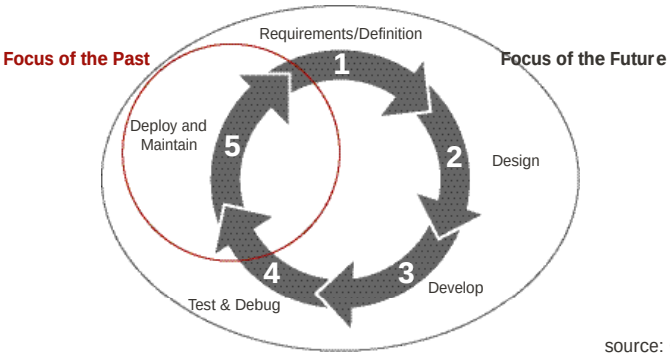
Finally, asked to vote on the most critical aspects for risk and data security today, the Thought Leaders as a whole stressed the need for leadership on the issue. The two factors judged most important were "Foster executive/board awareness of security imperatives and governance responsibilities" at 76 percent, and "Assign responsibility and accountability for all security aspects," close behind at 72 percent.

"Right now a lot of companies are like buildings where once you make it past the front door all the floors and offices are unsecured. That will change."

"If you have 1000 points of access and only one is vulnerable, you're not 99.9 percent safe, you're 0.1 percent safe."

**Risk and data security: Needs Assessment and Best Practices**

Once a company decides to invest in upgrading its information security, how does it make that happen? Paul de Ligny Boudreau of the Giga Group consultancy, who acted as this Thought Leadership Forum's moderator, described the necessity for an information-security architecture that moves the problem through a company, starting with the business units spotting security needs, continuing with the CIO developing a response strategy and then ending with deployment and maintenance via the operational and technical teams. De Ligny Boudreau described a new paradigm for looking at risk and data security in the age of "moving target" data-security work, explaining, "It's a much more iterative process than before."




source: Giga Information Group Inc.

As before, the human element raised its head. Major points of discussion involved a) the need for keeping employees happy, to avoid data-related sabotage due to disgruntlement and b) the importance of having a good plan for dealing with a data-security disasters, via effective media handling and unleashing rapid response with customers and clients.
Having built their own list rankings of best practices, the Thought Leaders debated and then voted as a group. Again, their answers raised the idea that risk and data security will fast become part of the company's fundamental procedures: The top two answers, almost tied, were "Consider information security risks as part of your business risks" at 84 percent, and "Integrate information security into the business process engineering" at 82 percent, followed closely by the related "classify and control access to information, and assign residence/ownership of all business info" at 78 percent.
Aside from companies re-thinking how they handle this issue, global or national standards are another solution. But they were seen by some Thought Leaders as a double-edged sword. "Large corporations will look for those kinds of certifications," said one Thought Leader. "But small companies may get pushed out of the market because they can't afford to go through the certification process." Regulators and rating agencies can also come to be a factor here, if they require certain practices (as with the banking world's Basel II Accords, which is enforced by the Bank of International Settlements but also required as part of Moody's or S & P ratings).

"Large corporations will look for those kinds of certifications…but small companies may get pushed out of the market because they can't afford to go through the certification process."

**Risk and data security: Technology's Opportunities and Challenges**
Obviously, technological developments will play a key role in the evolution of the risk and data security environment. Role-playing as members of a forward-looking company's governance board, the Thought Leaders were again split into four groups - with two looking toward 2006 and two looking toward 2010 - and asked to create a ranked list of the top information-security challenges.

*Looking toward 2006*
The increasingly wireless workplace was a recurrent theme here, not surprisingly. Many aspects present problems:

- The surging number of different devices - e.g. laptops, PDAs, phones - each with different security issues.
- As these devices become more powerful, they hold more critical information locally (files, spreadsheets, databases etc).
- The fact that these devices can also be misused as entry points into a corporate network, especially due to their network capabilities.
- Because these devices are often private property and viewed as personal performance tools (datebook, address lists, etc) and can be taken in and out of a company with ease, these devices are hard to control.
- These devices can form a spontaneous network without central controls to verify users and grant proper access.
- It's not enough to secure these devices against viruses and other dangers. When in "nomadic" mode they must have sufficient security-context information to be able to decide questions such as "Should the guy sitting next to me have access to my files, and if yes, which? "

# White Paper

*Looking toward 2010*

The Thought Leaders looking further forward predicted that inter-operability of systems would continue to be an issue. “The system is only as strong as the weakest link,” one Thought Leader pointed out. “Once you start networking, it doesn’t matter if you have the latest encryption systems in place. If your colleagues don’t have them running as well, then it does nothing for you.”

After these forecasting exercises, the Thought Leaders as a whole voted on the most important technologically related issues facing data security players today. Once the votes were tabulated, de Ligny Boudreau observed an interesting pattern: “Most of the top ones are not so much about technology. They’re more oriented toward trust, identity and anonymity.” Indeed, in the voting, “Management of trust relationships between companies, intermediaries and customers” ranked first at 83 percent; “Implementing identity management and newer biometrics” came in at 79 percent; “Anonymity, data and privacy protection” followed closely at 77 percent.

But managing the flurry of new devices was also ranked very important: “Nomadic / ad-hoc mobile (Wi-Fi) networking” and “Integration of user devices” tied for fourth place at 76 percent. In the end, observed one Thought Leader: “The real issues isn’t the new technology, it’s how we handle that technology.” In other words, the fundamental issue here is developing security management, not just adding complex security technology to already overly complex IT environments.

> “The real issues isn’t the new technology, it’s how we handle that technology.”

**Risk And Data Security: Brainstorming Results**

The Thought Leadership Forums are intended as brainstorming sessions to draw out and discuss the important themes and tensions surrounding an issue, rather than reach conclusions per se on the topic. Over the course of the Risk and Data Security forum, several things became clear:

- The public is starting to demand security as a built-in feature of IT products, much as it demands security in cars or household devices.
- There will be no clear winner – neither attackers nor defenders will be able to gain a decisive advantage, regardless of what technologies will be invented.
- Data security will become a pervasive part of business practice, not merely the domain of the sysadmins and technical terms, but rather touching everyone from the board-level executives who must spearhead the efforts to the lower-level employees whose daily work will be infused with new data-security technologies and practices.
- A tension exists between data security and a company’s other needs, including productivity, accessibility, and information flow. Each company will have to decide how to balance the two, as a function of its business and of its perceived risks.
- Technology is no cure-all, but rather one part of a dynamic system, engineered to avoid security being compromised and minimize potential damage when it is compromised. Creating and maintaining trust between all the different elements of the business is the foundation upon technology must be deployed.

Keynote

# Keynote

## "Protecting business in the 21st Century – A look into the Future"

**by David Love, Head of Security Strategy EMEA, Computer Associates**

You'll see from the programme that I've changed my job title since I agreed to do the presentation. I was Head of Security Strategy for Europe, the Middle East and Africa, and I've now moved to an EU area, still very much looking at security. I think it's important that people understand what sort of company we are: we are the third largest global software house after Microsoft and Oracle. We are one of the leaders, if not *the* leader, in Enterprise Management and in Integrated Solutions.

As you will see, we have very much of a security background, but we have to understand what the threats are before we can protect them. I know of no faster way of throwing your money away in IT security, than if you don't understand the threats from which you're trying to protect yourself. Similarly, from our perspective, we have to try to understand those threats in developing our software.

My presentation today is very much looking to the future. I do enjoy playing with PowerPoint, (and I was in the office long enough, about 5 minutes), so I make no apologies in saying when I'm doing a presentation looking to the future that I have used the latest toys to do so.

My background: I spent 28 years in counter-intelligence in the Royal Airforce. I was Head of Counter-intelligence and Security, Head of Defence in information warfare, Head of Military Security for NATO in Europe (which has given me the understanding of what happens right across the European perspective – a little more tricky for Switzerland because for some reason you've been neutral for 800 years or so).

We very much live in the global village. I'm a New Zealander by birth (I'm proud of that) and I've got a son currently at university in New Zealand. I bought him a car for his 21st birthday present – which has gone wrong – and I'm now able to select a mechanic who actually fixes it, on the internet (and I'm doing this from the opposite end of the world).

This is the power of the Internet; what it means for you is that the world is now your oyster. You have the capability of doing business with everybody in Europe, not just Switzerland. Equally, it means that people can compete with you because they have the opportunity of doing their business in Switzerland – which was your business in the past. This is the European overview.

Erkki Liikernan is from Finland. He's the commissioner responsible for IT and he presented to the rest of the commissioners about 2 weeks ago some recent survey findings. It's quite worrying, that this is the state of Europe. I know that Switzerland isn"t in the EU (I'm not quite sure whether the UK is or isn't, but that's another matter). Where we are in Europe: no security

# Keynote

strategy for 75% of companies. I take issue with what somebody said this afternoon:" How important is a security strategy?" It is my belief, unless you start with a security strategy and understand what you actually need; you're going to waste your time in this area by either under-protecting yourself or spending more money than you ought to.

IT security investments: only 1.8% of overall IT investments – however 25% increase and improving. Less than 1% spent on security for 18% of companies – I'm not so worried about that. People say to me:"What is the right percent I should be spending on security?" I say: "If you're asking that question, you don't understand the problem". It all depends on what your individual requirements are and unless you've set those in your individual strategy, you can never answer the question. That should tell you how much you ought to be spending to protect your level of investment.

Underestimation of core business risks, I tend to find to be a major obstacle for investments in IT security by 59% of companies. Perhaps even more frighteningly, they found that security was not yet strategic for 90% of companies. What this means, is that those companies view security much in the same way as providing cafeteria services and gate guards (and everything else). It has not yet got to the collective psyche of the board of directors –although we are seeing some changes in that .

We know about Security in the Headlines: we all know about the 16 year old boys sitting in the attic thumping away on their computers –funnily enough, there are very few girls involved in hacking; it is a male and boy thing. The only place we see them (girls) active is in the USA and that is because they believe it is wrong that it should be male dominated.


Security not in the Headlines: what is really frightening is the move of organized crime into this area. I can give so many examples (if time would permit) of what is happening. A question, which was asked to me earlier:" Where is this crime coming from?" If you had asked me this question 3 months ago, I would have said it was coming from Russia, the Ukraine, Hungary, and Romania. What we're now suddenly beginning to understand is that the servers where the attacks are coming from may be in those countries. There are reasons for that - the police force in Russia has better things to do, and it's an under-funded state which doesn't protect its people outside Russia. What we're beginning to understand is where those strings are being pulled from: quite a lot from the USA and the UK, some from Germany. And that's something we have only recently begun to understand.

# Keynote

Commercial Espionage: another thing that greatly concerns us – a multi billion dollar business. It is one of the things, which prevents business from being done – it makes it close up on itself. There's commercial espionage going on in all sorts of areas: in research and development in particular, in contract bidding (in the EU we've seen some major examples).


This is what I call the Cyber Crime Threat Spectrum: espionage, sabotage and deception. I could probably spend a month speaking on this slide alone, but I'm just going to go from the two opposite extremes. One of them is EMP (electro magnetic pulse), a bi-product of a nuclear explosion, which wipes and destroys magnetic storage. I was speaking at a forum, which included delegates from India and Pakistan in June last year. They had not understood the enormity of what a nuclear attack (and they were threatening each other with nuclear weapons at the time) would mean to their countries. If an explosion took place near their banks, it could devastate their country.

The other is HERF (high energy radio frequency). These new weapons give that burst of pure energy, which you get from EMP but without the nuclear explosion. That's why many banks today are beginning to put their data bases underground, storing them in Faraday cages.

Social Engineering: this is when you get a telephone call saying: "Hi, it's the IT engineer – if you give me your password, I'll give you the latest version of XP". And of course, 90% of people do. Quite frightening! It's a little more pernicious than that, and it shows how organized crime has moved into the area.

We're dealing with a case (3 or 4 months old in the UK), where an insurance company was subject to a massive fraud. What organized crime wanted to do was to keep making a number of claims on the same policies but always wipe the records so that it was never seen that the claim had been made before. It's quite brilliant, isn't it? The only reason they got caught was because they got greedy. What they actually did was go up to where the data was stored, got to know who had supervisory access and hooked 3 of them (who had supervisory access) on cocaine – and kept feeding them cocaine provided they carried out changes to the system. This is how organized crime is moving in this sort of area. If you were working for banks here, what would happen if your people with supervisory access were subject to that kind of pressure? What systems have you got in place? We've got to have those systems in place, so that when somebody is put under that pressure he says: "I cannot do what you want me to do – what you are blackmailing me to do – because I will be found out". That's the level of computer security which we're going to have to get to.

# Keynote

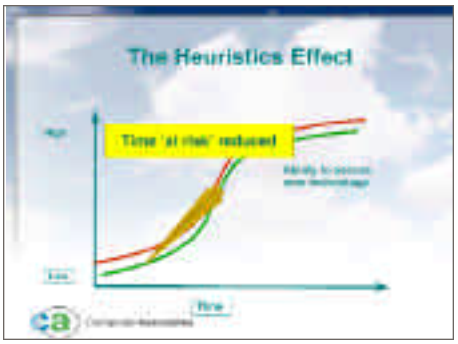
The Insider Threat: the biggest problem we're going to have to face are people with legitimate access on the inside. And today, what that means is we have to have Big Brother look at some people and try to persuade some people, and some MPs at the EU parliament, that this isn't the case. It's seen now that Big Brother, now, needs to look at people all the time to monitor their actions. Not quite true – but there is a philosophical debate, which we all have to have: where do the rights of individuals, and where do the rights of society (made up of individuals) balance? Where should the pendulum stop in the swing?

Terrorism: the other major threat. I've sat at a couple of terrorist conferences recently, and I've had the pleasure of being briefed on where we are: I was one of those people who made the decision that there was no risk from terrorists flying aircrafts into high-rise buildings - I was wrong then. But, as we see it at the moment, terrorists are not interested in mounting on-line attacks. It's a perception they're trying to achieve as a terrorist organisation and they don't think they get the bang for the buck from an IT attack that they would from a physical attack. We know that many terrorist organisations and Al Queda have been sending people to university to study these areas, but at the moment we do not believe an attack is imminent.


Organization Trends: back in the 20th century companies were based on a hierarchal structure, with the accompanying organization and information flow. Now, we've got (especially with e-mail) an organism where information flows on the outside as much as on the inside. The big question today is, when we talk about perimeter defence, do we actually know what our perimeter is? If we've got a thousand doors into our system and 999 are well secured but one isn't, does that mean we've got 99.9% security? Does it mean we've got 0% security? In IT terms, that one door means you've got 0% security. As you move in that direction (as I say, it's e-business that's driving us) the threat and vulnerability both rise. That's something we're going to have to accept as businessmen: there is a cost of doing business. There are some cheaper ways of getting a competitive advantage, but overall, we have to understand that if we want to move to e-business, there is a cost involved.

Security Legacy: we started off with the humble mainframe. When I was in the air force we were paranoid about our mainframe security. I laugh at myself now because we had armed guards on the door; everybody had a positive vetting security clearance to get inside the building; and we weren't connected to anyone in any case. Of course, as life went on we got the various distributive systems – the different platforms connected together – and then with the Internet, and then to the outside. What you've got is a plethora, a whole host of systems, standards and applications all joined together. And, you must provide security across the total platform if we are to be secure.

# Keynote


One of the other problems, is that in the past we introduced a new technology and had to wait until the hackers had had a go at it to understand what was happening. After that, we could plug the gaps and holes. That's the danger zone that the criminals are trying to attack. We need to reduce that time of risk. We don't want to wait for a system to go out, put it in a vulnerable state and wait until we can secure it. We have to be able to use the predictive power of Artificial Intelligence (A.I ) in our systems. All the top vendors are now beginning to do that. We are going to have to use the power of A.I to predict what might happen. We've never seen this event before, but the last time we saw something looking like this it was malicious, and therefore, we're going to examine it again.

Equally, what we've got to try to do with systems is not say "pass / fail"; "up / down"; "working / crash". We've got to create resilience in our systems. To this effect, when it is under attack, it gradually closes down onto itself so it can control what is happening. This is what we're going to have to do in the 21st century.

I was speaking to the Vice-President of the EU parliament the other day, and she was trying to convince me that spam was the next thing we should legislate. I said: "Why legislate? We've solved the problem". Solved to a certain extent, there will always be a new form of attack: what really worries us is organized crime. It has been spotted in the States actually funding primary research in the leading research institutions. That research has only been taken out to create new tools, and I don't think they're putting those tools on the net for everybody to use. We must have a way of spotting attacks which we've never seen before.

Pornography is a very interesting subject from this perspective, in that there are two major banks and an insurance company in Europe (and one of the biggest banks in the UK is one of them) which have been found to be the biggest repository of child pornography on their data bases. It was put there by people working on the inside who didn't want to be caught with the material at home, and who of course needed that enormous data base (pedophile material is so expensive on storage capacity). The only reason they were caught was because advanced intrusion detection tools were put in place.

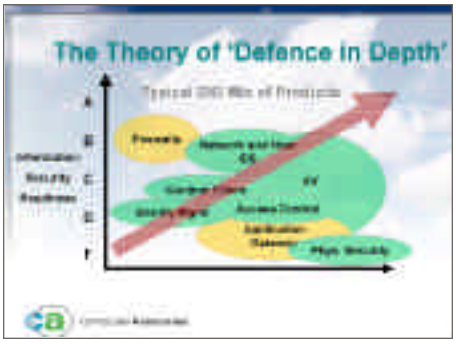
Socio-Economic Phenomenon: May 1, 2002. The Anti-Capitalist Brigade, instead of (or as well as) going down and knocking off McDonalds in London and having all the riots, clubbed together

## Keynote

and had a sophisticated attack on the global financial system – which hit very hard in the EU and the USA. It's threats like that (amateur information warfare) which are as much a concern to us as anything else. For example, if the Greens decided that something was of overriding and fundamental importance, they might decide not to allow this anymore – and they can use these tools. We have to understand this capability.

Critical National Infrastructure: these are the systems that are required to run a modern state - banking and finance. Obviously in Switzerland this is highly important (it's important everywhere) – 84% in private ownership. The big question is: Who pays? Who's going to provide the security that the state requires over and above what the shareholder provides? That's a question which is required of all of us.

Information Warfare: ever since man clubbed together as a society, if you wanted to attack a state you first had to defeat the standing army. The standing army was a defense. That model has held good for the 2-3000 years man has been organized in that way – until we hit the digital era. Now the armed forces have no real role in this area. So who is it that protects the state in relation to this? Most police forces are under-resourced and not able to do it. Is it the security services? Most security services are too small. It's easy for me to stand up here and ask the questions. I don't know the answers either. What I do know, is that the security industry is going to have a major part to play in providing the tools and working with the government and with commerce; and we have to work together if we're going to protect those vital organs which make our combined life possible in the crowded way we now choose to live together.




You've all heard over the recent years about Defense in Depth – this is how you achieve security: you've really got to have everything working together. Unfortunately, it was a good idea. It failed because it's too difficult to manage. It's become a nightmare to actually control those systems, and yet what you need is an extended view across the enterprise if you're going to achieve security. So, where we were in the past was very much with security monitoring. It was really a look backwards – an audit capability – but where we're going to have to move in the future is security management. It's pro-actively looking at our systems - looking for attacks, for problems. And it's a different way of looking at the entire problem. How do we achieve security? Integration is the key.

When I worked for NATO, trying to put all the military systems together and get 16 different nations to agree on a common way of doing business was an absolute nightmare, and something

# Keynote


which I never achieved (in my time). When I decided to leave the military environment at the end of the Cold War, I joined CA because they had started this integrated approach. For the first time, I had begun to see a solution for the way ahead. At the time I joined CA (3 years ago), if you had an integrated system you virtually had to apologize for it. Now, if you're a single source of supply, you're the apologist: everybody has begun to understand that integration is the key for getting all this together.


There are a number of things we have to integrate together. Identity management is absolutely critical: if we're going to do e-business, we have to know who it is tapping on the other end of the computer. Yet identity thefts are exploding as crimes right across the world.

Threat Management: the traditional way of looking at the viruses will always remain the key element. But the real key is access management – management on the inside. It's not just the access, it's how you manage everybody together. How can you use your system to the best advantage? How can you alternate your processes? How can you alternate your administration? The biggest cost to running most systems is personnel, and one of the biggest costs to running that system is the help desk. One of the biggest problems a help desk has to face (75% - 80% normally) are problems with password re-setting. If you could alternate that process and provide it on a self help basis, there's a massive saving to be made. Equally, if you can manage your administration in such a way that it just takes one single key stroke to get a person to join a company and give him the conditions he requires, there is so much saving to be had (which people are now beginning to appreciate). It's this sophisticated approach where we're going to see the return on investment in the future.


Overall, if we have those areas in big systems, unless we can pull all that information together, we're not going to be effective at all. So the key is to have those three areas but have the portals which have the capability of pulling that information together: to use A.I; algorithms; to use whatever is appropriate to understand what is happening. This is just an example of one of the slides, which I use in other presentations of Full Identity Life Cycle Management, which shows how complex the whole thing is.

# Keynote

One thing I will disagree with from the results I have seen so far is Biometrics: Biometrics is just a means to an end – another way of authentication – it's nothing magic. The first time we came across it was in the state of Louisiana, which introduced it for social security payments. They used retina scanning and then discovered it didn't work on blind people: they had to pull the system out because it was discriminatory.


Security Best Practices: this is the real way ahead. Are we talking about technology here or business? What we've done for years is let the technologists and the computer engineers have their hour, while where we have failed is at the board level, and elsewhere. We have not understood that what we're trying to protect isn't technology, but the business process. Having the capability of understanding the business process is protecting it. The Basel II Accord is a very good example of that – it's not based on technology, but it's giving us standards and concepts which will enable banks to do better business in the future. The pharmaceutical industry has just started that as well. It's a business process more than the technology where we have to look to provide cost effective security for the future.

Antiviruses: standard antivirus with A.I enhancement is where we are at this stage of the game- but it's no good. When we had the slammer attack a couple of weeks ago, the antivirus people claimed (to the board of directors) it wasn't a virus. But the CEO said: "I don't care if it's a virus or not – it's something which is bringing our system down". So therefore, we have to have an understanding that we've got to put all these threats together and understand them.



We have to link e-mail security and Antispam, Web Security, URL filtering, Malicious Code Defense (that's the mobile code), to provide the defense we need – not against a particular technological area, but against attacks against business. So, the three things needed to counter the threat are: the integrated tool sets; A.I; and the centralized view of the extended enterprise. What we want to achieve is lower cost. What's the bill at the end of the day? A well-constructed

## Keynote

and effective strategy for computer security, worked out against a business process, need not be a cost killer. On the other hand, it can be a competitive driver. Lowering costs must be a part of what we do.

Managing Risk: we have spoken of risk management for the last 10 years. Have we really understood what we've been talking about? Were we capable of deciding what risks we were facing when we didn't have the tools to understand what was happening in our systems? I suggest we didn't. It was risk avoidance – or blindness – we were practicing (it was taking a "close-your-eyes-and-hope" guess). We've now got the tools to get us into managed risk and security control from the centre.


Finally, if there's one message I want to leave you with tonight, it's IT. Security protection is not the major focus. The aim is to protect the business process and summary of IT, enterprise management, security, storage management (and everything else). What they have to do is work with the purchasers of those tools to understand the business case, to build a bespoke system – a tailored system –, which meets the requirements of a business. That is the direction for cost effective computing, not just cost effective security.

# Annex

# Annex

## ANNEX 1 : THOUGHT LEADERS PRE-SESSION SURVEY

Summary, results and quotes

### Question No. 1

**Information Security / Corporate Governance**
*What should be the rules and who should oversee the information security system in the enterprise?*

**Overview:**
Information security has evolved from an area primarily for technical (IT and Security) specialists to an integral operational component of Risk Management and Corporate Governance for corporate executives. This requires on the one hand that highly skilled experts are increasingly involved in business risk assessment and decision-making processes, and on the other hand that the business decision makers acquire sufficient knowledge on handling operational security risks and appropriate methods and technologies for risk recognition and management. Bridging these reciprocal information gaps and developing a common understanding of security threats and counter-measures is a significant challenge. It is not only critical for enterprises to manage; it also commands the immediate attention of legislators and regulatory bodies, and the public at large.

**Instructions:**
1. On the list below are a number of items pertaining to corporate governance in information security. Please study the points, Please rank these points with respect to the following criteria:

A. Absolutely Critical
B. Important and being considered
C. To be considered

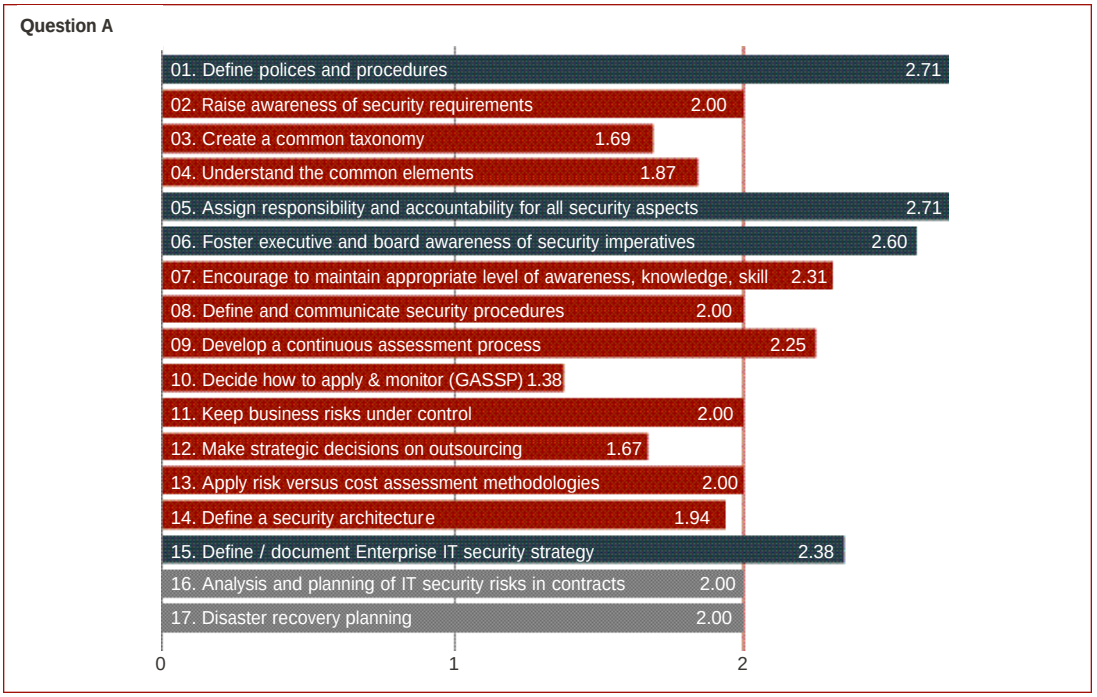
**Items:**
- Define polices and procedures that meet industry and international standards, and comply with legal and policy requirements
- Raise awareness that security requirements are brought on through different regulations (e.g., the US Gramm-Leach-Biley Act of 1999 (GLBA), Basel Accords, Securities and Exchange Commission (SEC) requirements, USA Patriot Act, among others), new security and storage technologies, increasingly pervasive networks and specific business needs and partnerships that are unique to each Enterprise.
- Create a common taxonomy in order to manage and validate compliance to the myriad of standards and regulations, and set up and communicate on compliance and management practices for information security
- Understand the common elements in all of the standards/regulations that the
- Enterprise has to comply with and show compliance to the common elements, which then can be mapped back to individual standards/regulations.
- Assign responsibility and accountability for all elements/aspects of Information
- Security throughout the organisation
- Foster executive and board awareness of security imperatives and their governance

# Annex

responsibilities as related to the protection of information assets.

- Encourage management and staff to maintain an appropriate level of awareness, knowledge and skill to allow them to minimise the occurrence and severity of Information Security incidents.
- Define and communicate security procedures for stakeholders (customers, shareholders, senior management and board of directors, employees, suppliers, services providers and contactors)
- Develop a continuous assessment process to assess business needs as they pertain to information security, and manage business and operational risks, and compliance in the face of on-going technological change and complexity.
- Decide how to apply and monitor Generally Accepted System Security Principles
- (GASSP) or Generally Accepted Information Security Principles (GAISP) in the Enterprise
- Keep the business risks associated with information systems under control
- Make strategic decisions about possible outsourcing of business or support processes
- Apply risk versus cost assessment methodologies (a cost/benefits analysis in information security) to all areas of the business
- Define a security architecture that gives the Enterprise something to manage and measure against as well as a road map to “destination”
- Define/document the Enterprise IT security strategy, policy and standards

**The Results:**



# Annex

## Question No. 2

**Information Security / Needs Assessment / Best Practices**

*The "how's" and "what's" of defining Enterprise requirements and abiding by the rules.*

**Overview:**

The costs incurred in managing information security represent a delicate balance between preventing risk and managing disaster. In times of peace, the costs of prevention are too often conveniently set at the zero level. Many enterprises still regarded prevention as an annoying obligation and a potential source for cost savings, since an absolute proof of impending crisis is hard to assess. In contrast to this, cost models to manage actually incurred damages are practically non-existent and hardly ever reflect the varying degrees of urgency, from the most benign breach to the worst-case scenario. This lack of clarity makes it often impossible to arrive at a methodical base to allow the estimation of a "real threat" situation from that of just a "perceived" threat. Without improved application in enterprises of generally accepted and applicable best practices in this area, it will be difficult to assess opportunities to better balance information security risks and costs in an increasingly complex and fast changing environment.

**Instructions:**

1. Confronted with increasing information security risks, risk versus cost imperatives and requirements for corporate governance, which items from the list below can you identify as best practices based on your organization's needs today. Please rank these points with respect to the following criteria:

A. Absolutely Critical
B. Important and being considered
C. To be considered

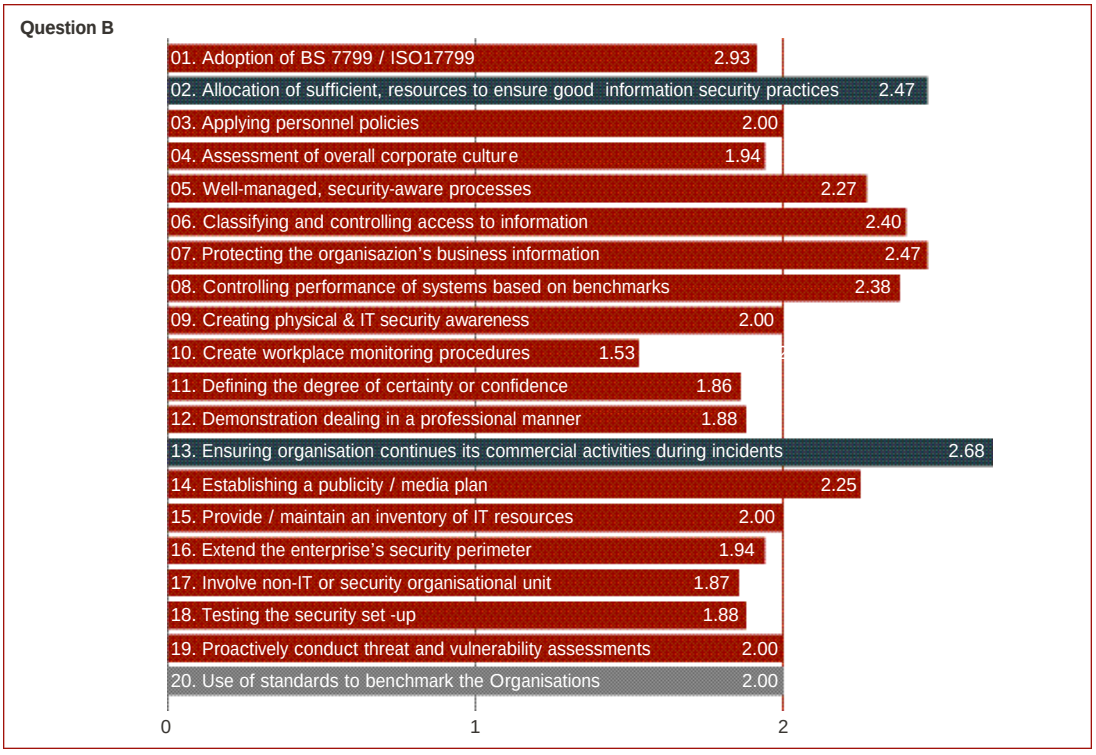
**Items:**

- Adoption of BS 7799 / ISO17799 and its upcoming revisions, or similar standards, and enterprise-specific additions / modifications, baselines, checklists etc.
- Allocation of sufficient and adequate resources, and effective arrangements to ensure good information security practices across the organization.
- Applying personnel policies that incorporate specific measures to support the implementation of approved information security policy across the enterprise.
- Assessment of overall corporate culture in terms of information security
- Well-managed, security-aware processes for realising business requirements (including changes), based on formal service level agreements (internally and externally) and considering direct an indirect development and operations expenses
- Classifying and controlling access to information, data and systems according to their criticality, sensitivity and vulnerability, as well as to residence and ownership of all business information
- Protecting the organization's business information and any client or customer information within its custody or safekeeping by safeguarding its confidentiality, integrity and availability.
- Controlling performance of systems based on benchmarks, detecting and responding to security incidents, identifying key vulnerabilities. Monitoring of security violations.
- Creating a physical and IT security awareness program and basic grid of security strategies for all employees delivering training and staff awareness

# Annex

- Creating workplace-monitoring procedures that comply with internal policies and privacy laws, making sure that electronic evidence handling procedures meet legal requirements
- Defining the degree of certainty or confidence you need to know about other party's identity (customers, suppliers, business partners...)
- Demonstrating to third parties that the organisation deals with information security in a professional manner.
- Ensuring that the organisation is able to continue its commercial activities in the event of significant Information Security incidents. Establishing a business continuity plan/ disaster recovery plan, guaranteeing business continuity after prolonged unavailability of critical computer facilities or equipment, communications services, personnel, buildings or access to buildings, establishing a security incident response plan
- Establishing a publicity/media plan in the event of a security breach becoming public in order to limit damage to the reputation of the enterprise.
- Provide and maintain an inventory of IT resources and active life-cycle management of IT assets, including information about the respective IT services / Service Level Agreements, and criticality.
- Extend the enterprise's security perimeter to other parties (customers, suppliers, partners, regulators etc.) or locations (home office, mobile employees).
- Involve non-IT or security organisational units (human resources, legal, compliance, audit) in security-critical decisions, development, procurement or operations processes.
- Testing the security set-up and organisation by periodic realistic tests and simulations.
- Proactively conduct enterprise-specific threat and vulnerability assessments, participate in industry / sector working groups etc.

**The Results:**



# Annex

## Question No. 3

**Information Security / New Technologies, Challenges and Opportunities in the Connected Economy**

*Dealing with new tools and new rules*

**Overview:**

In an increasingly connected and interdependent world, private and business privacy spheres collide; a deeper understanding of the balance between personal and enterprise privacy interests, and the ways new information technology will affect these is required. While today many enterprises are already somewhat overtaxed with current threats, it is difficult to foresee exactly what the future holds (cyber terrorism, super viruses, information warfare, etc…) or how existing threats will evolve (industrial espionage, hacker attacks etc.). As the innovation cycle becomes shorter and the surrounding environment becomes more complex, the reaction time to deal with new threats becomes even tighter. The bottom line is that risks increase with complexity, and the whole IT industry is busy inventing new, complex systems / services, while many enterprises still have to retain their old / current systems & services (either for backward compatibility, or because their customers actually use them). So the cost/risk side of new systems / services is always additive. We're struggling to keep the current landscape under control, while at the same time; we are havi ng increasing difficulty controlling the speed of introduction of new opportunities and challenges.

**Instructions:**

1. Given the new risks and constant change, which items from the list below can you identify as new opportunities for information security (even though, as per above introduction, capitalising on these opportunities may be challenging in itself). Please study the listed points. Please rank each of these points with respect to the following criteria:

A. Absolutely Critical
B. Important and being considered
C. To be considered

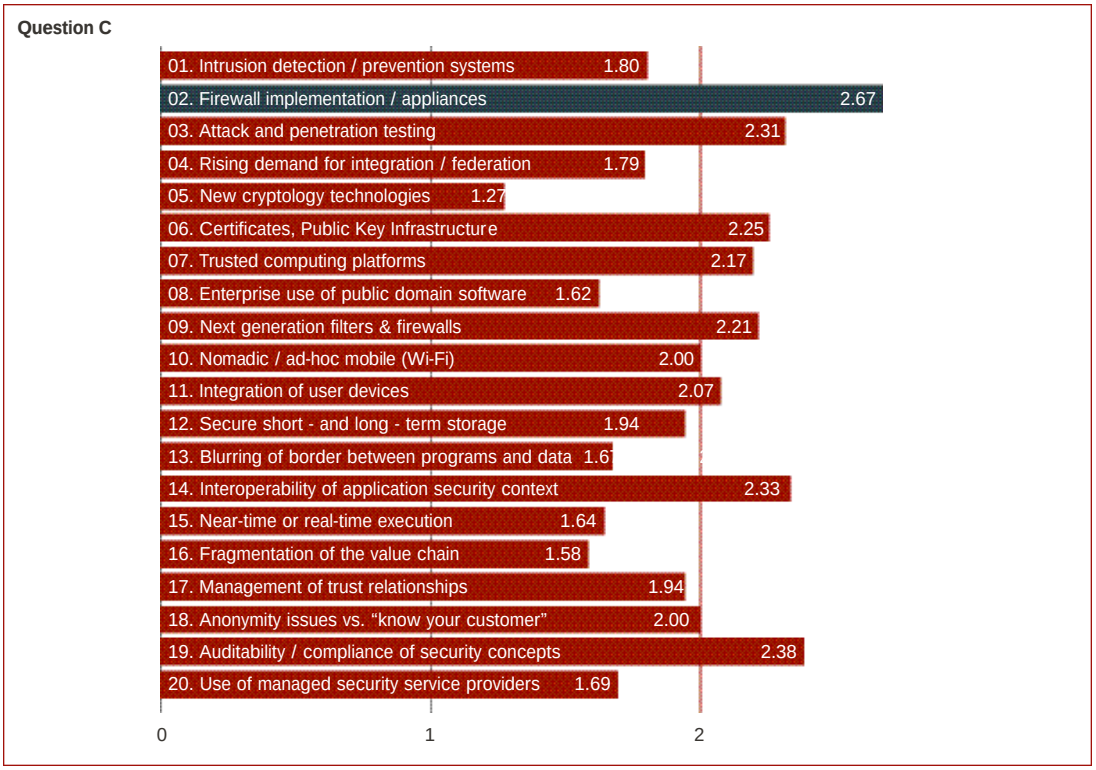
**Items:**

- Intrusion detection/prevention systems, based on Artificial Intelligence / knowledge/behaviour-based systems
- Firewall implementation/appliances for critical systems and networks, deep packet inspection etc.
- Attack and penetration testing, including response/ forensic testing
- Rising demand for integration/federation among identity management solutions, biometrics, PKI and single sign on
- New cryptology technologies (quantum cryptology, advanced steganography & digital watermarking...)
- Certificates and Public Key Infrastructures
- Trusted computing platforms, trusted software components & secure distribution / use
- Enterprise use of public domain software / shareware / freeware / public license software (i.e. GNU)
- Next generation filters & firewalls, advanced virus protection
- Nomadic / ad-hoc mobile (Wi-Fi) networking (i.e. without central control structures), ubiquitous "always on" Computing

# Annex

- Integration of user devices (home / mobile phone, PDA, notebook, tablet, household appliances, car, chip cards, RFID tags...)
- Secure short- and long-term storage, new storage management technologies and archiving of information
- Blurring of border between programs and data, effects of Java, XML etc., licensing / royalty / fee Issues, especially in “pay per use” scenarios
- Interoperability of application security contexts, integration of complex application frameworks (SAP, Notes, Siebel, Oracle...) into existing security frameworks
- Near-time or real-time execution of rationalised business processes across companies, “deep” mutual embedding of business processes (“just in time delivery”...)
- Fragmentation of the value chain along different companies with un-coordinated security contexts
- Management of trust relationships between customer and companies or between companies and intermediaries on behalf of clients
- Anonymity issues versus “know your customer” requirements / regulations
- Auditability / compliance of complex, but fragmented security concepts & contexts
- Use of managed security service providers

**The Results:**



# Annex

## Annex 2: Closed Thought Session Full Results

Summary, results and quotes

### Session A - Information Security / Corporate Governance

*What should be the rules and who should oversee the information security system in the enterprise?*

**The instructions:**

*Part 1*

*Please choose on the available list on your screen, the 10 most critical aspects of corporate governance as it applies to information security. You can add points to this list if necessary.* ·

Group 1& 2 must make a top ten list based on today and the next 3 years·

Group 3 & 4 must make a top ten list based on what they think will be critical 7 years from now and beyond

*Part 2*

Once you have make the list of top 10, attribute one lead role to each item.

NB: Most companies attribute all roles pertaining to Information Security to the CSO. However, we would like you to take the broader perspective of corporate governance to assign these roles.

The roles available are: Board of Directors, CEO, CFO, CIO, CSO, Admin, LOB, External Supply Chain Partners, External Service Providers, Chief Operating Officer, Audit (internal/external), Legal Services, Compliance Services, Human Resources

**Priority of Consolidated Corporate Governance Issues (Vote Results)**

| Top 5 Ranking Corporate Governance | Ranking |
|---|---|
| 01. Foster executive/board awareness of security imperatives and governance responsibilities. | 76% |
| 02. Assign responsibility and accountability | 72% |
| 03. Define polices/procedures | 64% |
| 04. Define a security architecture, as well as a road map to "destination" | 59% |
| 05. Apply risk versus cost assessments to all areas of the business | 56% |
| 06. Continuously assess business needs in the face of on-going technological change/complexity | 50% |
| 07. Analysis and planning of security risks in contracts (i.e. IT) | 48% |
| 08. Keep information security business risks under control | 48% |
| 09. Document Enterprise IT security strategy, policy and standards (PRAGMATIC APPROACH) | 47% |
| 10. Staff education on information security | 44% |
| 11. Disaster recovery planning | 41% |
| 12. Encourage staff to maintain an appropriate level of awareness and corporate culture | 40% |
| 13. Raise awareness on complexity of security issues | 37% |
| 14. Vulnerability Intelligence (Management and Monitoring) | 34% |
| 15. Insurance coverage for security liability | 30% |
| 16. Identify common elements in all standards/regulations | 24% |
| 17. Infrastructure resilience (technology, people, processes, etc.) | 22% |
| 18. IS as a tradable commodity / SLA | 21% |
| 19. Create a common taxonomy and communicate on compliance | 19% |
| 20. Require to hire MBAs with IS knowledge | 08% |

# Annex

## Corporate Governance – Today to 3 years

**Ten Most Critical Aspects of Corporate Governance + roles**

| Group 1 | Group 2 |
|---|---|
| 01. BOD Foster executive/board awareness of security imperatives and governance responsibilities | 01. BOD, Foster executive/board awareness of security imperatives and governance responsibilities |
| 02. Audit, Raise awareness on complexity of security issues | 02. CSO, Define a security architecture, as well as a road map to "destination" |
| 03. LOB, Admin, Audit Define polices/procedures | 03. BOD, Assign responsibility and accountability. |
| 04. Legal, CIO, CSO, Compliance, Analysis and planning of IT security risks in contracts | 04. BOD, Define polices/procedures |
| 05. CEO, CFO, CIO, CSO, COO, Admin, LOB, Audit, Legal, HR, Compliance, Assign responsibility and accountability | 05. LEGAL SERVICES (CRO) Analysis and planning of security risks in contracts (i.e. IT) |
| 06. HR, Encourage staff to maintain an appropriate level of awareness and corporate culture - Document Enterprise IT security strategy, policy and standards | 06. COO Disaster recovery planning |
| 07. CEO, CIO, COO, CSO, CFO Disaster recovery planning | 07. CFO, Apply risk versus cost assessments to all areas of the business |
| 08. CSO, COO,LOB Keep information security business risks under control | 08. CIO, Continuously assess business needs in the face of on-going technological change/complexity |
| 09. CSO, CFO, CIO, LOB Apply risk versus cost assessments to all areas of the business | 09. CIO, Staff education on information security |
| | 10. CIO, Document Enterprise IT security strategy, policy and standards (PRAGMATIC APPROACH) |

## Corporate Governance - 7 Years & Beyond

**Ten Most Critical Aspects of Corporate Governance - 7 Years & Beyond**

| Group 3 | Group 4 |
|---|---|
| 01. CEO, Foster executive/board awareness of security imperatives and governance responsibilities | 01. BOD, Assign responsibility and accountability |
| 02 CRO, Identify common elements in all standards/regulations | 02. CEO, Define polices/procedures |
| 03. CRO, Vulnerability Intelligence (Management and Monitoring) | 03. CSO, Raise awareness on complexity of security issues |
| 04. CRO, Create a common taxonomy and communicate on compliance | 04. CSO, Define a security architecture, as well as a road map to "destination" |
| 05. HR, Encourage staff to maintain an appropriate level of awareness | 05. LOB, Encourage staff to maintain an appropriate level of awareness |
| 06. CRO-IS, infrastructure resilience (technology, people, processes, etc.) | 06. LOB, Continuously assess business needs in the face of on-going technological change/complexity. |
| 07. COO, Continuously assess business needs in the face of on-going technological change/complexity | 07. CEO, Keep information security business risks under control |
| 08. CEO/CIO-IS, as a tradable commodity / SLA | 08. CSO, Analysis and planning of IT security risks in contracts |
| 09. HR, Require to hire MBAs with IS knowledge | 09. CFO, Insurance coverage for security liability |
| 10. CRO, Disaster recovery planning | 10. CEO, Apply risk versus cost assessments to all areas of the business |

# Annex

## Session B - Information Security / Needs Assessment / Best Practices

*The "how's" and "what's" of defining Enterprise requirements and abiding by the rules*

**The instructions:**
Please rank the top 5 best practices. Plenary exercise followed by a debate.

### Top 5 Best Practices

| Needs Assessment / Best Practices | Ranking |
|---|---|
| 01. Consider IS risks as part of your business risks | 84% |
| 02. Integrate IS into the business process engineering | 82% |
| 03. Classify and control access to information, and assign residence/ownership of all business info | 76% |
| 04. Proactively conduct enterprise-specific threat and vulnerability assessments | 69% |
| 05. Controlling systems and monitoring of security violations | 63% |
| 06. Implement security-aware processes with formal service level agreements and allocated operations expenses - availability management | 61% |
| 07. Test the security set-up and organization periodically | 58% |
| 08. Design, implement and run infrastructure resilience programs | 56% |
| 09. Certification to an array of industry standards / Adoption of BS 7799 / ISO17799 and its upcoming revisions, or similar standards, and enterprise-specific additions / modifications, baselines, checklists etc | 54% |
| 10. Create physical and IT security awareness programs for all employees | 50% |
| 11. Assess of overall corporate culture in terms of information security | 49% |
| 12. Involve non-IT and security units in security-critical decisions, development and processes | 48% |
| 13. Apply personnel policies to support implementation of approved information security policy | 44% |
| 14. Establishing a publicity/media plan to deal with any security breach becoming public | 41% |
| 15. Extend the enterprise's security perimeter to other parties (customers, suppliers, etc.) or locations | 38% |
| 16. Maintain an inventory of IT and corresponding IT services/Service Level Agreements | 35% |
| 17. Define the degree of certainty and security required about other party's' identity | 34% |
| 18. Create a better work atmosphere and culture to encourage employees to be loyal to the company and respect the systems | 34% |
| 19. Use of standards to benchmark the Organizations | 30% |
| 20. Create workplace-monitoring procedures that comply with internal policies and privacy laws | 25% |
| 21. Demonstrate and communicate to third parties how the organization deals with information security | 25% |
| 22. Being more proactive in the flow and control of communication | 24% |
| 23. If most breaches are internal, we must educate staff to be more vigilant and aware of security issues- we must not only educate, we must also certify that this is done we must not only educate, we must also certify that this is done | 24% |

# Annex

## Session C - Information Security / New Technologies Challenges and Opportunities in the Connected Economy

*Dealing with new tools and new rules.*

**The instructions:**
Please choose on the available list on your screen, the 10 points you think will be top information security technology challenges. You can add points to this list if necessary.

Group 1& 2 must make a top ten list based on what you think will be important 7 years from now and beyond.

Group 3 & 4 must make a top ten list based on what you think its important from today to 3 years from now.

Perspective: You are not a “bleeding edge” high-risk-taking company. But you are a forward-looking, proactive company. Behave like a governance board when answering these questions.

### Consolidated top results for New Technology Challenges and Opportunities

| Needs Assessment / Best Practices | Ranking |
|---|---|
| 01. Management of trust relationships between companies, intermets… | 83% |
| 02. Implement identity management and newer biometrics, PKI | 79% |
| 03. Anonymity, data and privacy protection | 77% |
| 04. Nomadic / ad-hoc mobile (Wi-Fi) networking. | 76% |
| 05. Integration of user devices (home / mobile phone, PDA, notebook) | 76% |
| 06. Anonymity issues versus "know your customer" requirements. | 76% |
| 07. Auditability of complex, but fragmented security contexts. | 74% |
| 08. Integration of complex application frameworks (SAP, Notes…) | 73% |
| 09. Privacy enhancing technologies | 69% |
| 10. Archiving and legal requirements | 68% |
| 11. Trusted computing platforms, trusted software components | 68% |
| 12. Firewall implementation for critical systems and networks | 67% |
| 13. Fragmentation of the value chain among different companies | 66% |
| 14. Adequate technology training for IT professionals | 65% |
| 15. VPN SECURED WLAN = WIRELESS ONLY IN A SECURE WAY | 63% |
| 16. Attack and penetration testing, including response/ forensic | 62% |
| 17. Globalization and Internationalization issues | 62% |
| 18. DIGITAL RIGHTS MANAGEMENT | 62% |
| 19. Implement security certificates e.g. security level agreement | 60% |
| 20. Use of managed security service providers | 59% |
| 21. Next generation filters & firewalls, advanced virus protection | 59% |
| 22. Intrusion detection/prevention systems, based on Artificial inteligence | 54% |
| 23. Secure storage, new storage management technologies. | 53% |
| 24. New cryptology technologies (quantum cryptology...) | 50% |

# Annex

**Top Ten Technology New challenges – 7 year perspective**

| Group 1 | Group 2 |
|---|---|
| 01. Management of trust relationships between companies, intermediaries and customers (Identity Mgmt, DRM, anonymity vs. "know your customer") | 01. Auditability of complex, but fragmented security contexts |
| 02. Trusted computing platforms, trusted software components & secure distribution | 02. Fragmentation of the value chain among different companies |
| 03. Auditability of complex, but fragmented security contexts | 03. Anonymity issues versus "know your customer" requirements |
| 04. Adequate technology training for IT professionals and users | 04. Next generation filters & firewalls, advanced virus protection |
| 05. Integration of the mobile user's devices (home / mobile phone, PDA, notebook, VPN's, etc. including Wireless Lan) | 05. Intrusion detection/prevention systems, based on Artificial Intelligence, etc. |
| 06. Attack and penetration testing, including response/ forensic testing policy and standards | 06. Trusted computing platforms, trusted software components & secure distribution |
| 07. Globalization and Internationalization issues | 07. Management of trust relationships between companies, intermediaries and customers |
| 08. New cryptology technologies (quantum cryptology, advanced steganography & digital watermarking...) | 08. Implement identity management and newer biometrics, PKI and single sign-on solutions |
| 09. Next generation filters & firewalls, advanced virus protection | 09. Digital rights management |
| 10. Implement security certificates, e.g. security level agreements | 10. VPN – secured Wlan = wireless only in a secure way |

**Top Ten Technology Challenges – Today to 3 year perspective**

| Group 3 | Group 4 |
|---|---|
| 01. 1. Anonymity, data and privacy protection including issues like "know your customer" requirements, identity theft. | 01. Firewall implementation for critical systems and networks |
| 02. Nomadic / ad-hoc mobile (Wi-Fi) networking. | 02. Nomadic / ad-hoc mobile (Wi-Fi) networking. |
| 03. Integration of user devices (home / mobile phone, PDA, notebook, etc.). | 03. Integration of user devices (home / mobile phone, PDA, notebook, etc.) |
| 04. Fragmentation of the value chain among different companies. | 04. Implement identity management and newer biometrics, PKI and single sign-on solutions |
| 05. Management of trust relationships between companies, intermediaries and customers (including identity management, PKI, biometrics) | 05. Attack and penetration testing, including response/ forensic testing |
| 06. Integration of complex application frameworks (SAP, Notes, Siebel, Oracle...) into existing security frameworks | 06. Integration of complex application frameworks (SAP, Notes, Siebel, Oracle...) into existing security frameworks |
| 07. Trusted computing platforms, trusted software components & secure distribution | 07. Auditability of complex, but fragmented security contexts |
| 08. Use of managed security service providers | 08. Privacy enhancing technologies |
| 09. Next generation filters & firewalls, advanced virus protection | 09. Next generation filters & firewalls, advanced virus protection |
| 10. Archiving and legal requirements | 10. Use of managed security service providers |
| | 11. Secure storage, new storage management technologies. |

Producers

# Producer

### First Tuesday Zurich

First Tuesday Zurich is a business Think Tank encouraging and supporting the creation of knowledge at the crossing of business, policy, technology and innovation.

We are experts in creating conversations and dialogue among key players in these fields, leveraging the power of different perspectives and experiences to develop new insights.

Insight. Innovation. Impact. First.

**www.firsttuesday.ch**

### Gottlieb Duttweiler Institute

The GDI is an independent think tank for the retailing industry and its economic and social environment. An interdisciplinary team of 30 specialists is developing and providing knowledge and innovative solutions in the areas of management, marketing, e-commerce, POS and consumption. Our services are based on a strong international network of researchers and practitioners, out-of-the box thinkers and farsighted renovators. Our intention is to be geared to the future with our feet on the ground. Our goal is to deliver the latest retailing intelligence to our customers in a competent, attractive and practical fashion. At the GDI it is a tradition to discuss today the issues of tomorrow.

**www.gdi.ch**