# STRATEGIC DIALOGUE ON RISK AND SECURITY

Results of the Swiss Think Tank on Risk & Security in the light of current IT-security research

Risk & Security EXCHANGE powered by Microsoft

# INTRODUCTION

## HOW IS THE THINKING ON RISK AND SECURITY DIFFERENT IN SWITZERLAND THAN IN OTHER COUNTRIES? DO WE HAVE DIFFERENT PROBLEMS OR JUST DIFFERENT SOLUTIONS?

The publication you have in your hands compares the outcome of a number of Swiss Think Tank sessions – Risk & Security Exchange – with the current status of research on IT Security worldwide. In three short research papers Forrester Research compares their current knowledge with what a number of Swiss leaders from government, private sector, academia, research and IT suppliers have developed during three intensive, highly focused debates.

The three topics discussed are:

1. **Risk and Security: Who's in charge?**
2. **Identity, Security and Privacy: from the «e-Citizen» to the «Networker»**
3. **Real and Virtual War: CIIP & the Public/Private Collaboration**

After three successful and fruitful sessions we decided to not only concentrate the results in one place but also to compare them with the current status of research on IT Security worldwide. How are the results of our Swiss panel different than what researchers find all over the world? What are the main differences and where do the opinions converge?

# WHAT IS THE RISK & SECURITY EXCHANGE AND WHO STANDS BEHIND IT?

Risk and Security Exchange is a series of Think Tanks that brings decision makers and strategic thinkers together around the table on the topic of Information Security and the complex risks it implies. The Think Tanks are not only based on IT issues; Information Technology is the backbone of all modern business and society, but what it does, and how risks pertain to it, is what is at the centre of the debate.

The Think Tanks are based in Switzerland and deal with issues important to Swiss business decision makers, but they also bring the issues into light through a European and international filter. This kind of exchange brings a new dimension to the topics at hand and creates a business dialogue with a much wider scope.

## INFORMATION SECURITY IN THE COMMUNICATION SOCIETY

Data security and net security are becoming more and more important. In the age of the communication society, the volume and importance of information traffic are constantly increasing. An ever-growing proportion of the activities of public authorities, military agencies or commercial businesses is represented or supported by information. Consequently, the ability to assess, decide and act depends increasingly on the availability of reliable net security systems to ensure secure communication. Given the high value that information can represent these days, the supplier of information security and net security systems takes on great responsibility. As a partner, he must enjoy the user's trust.

## WHY IS MICROSOFT ENGAGED IN THIS SERIES OF THINK TANKS ON STRATEGIC SECURITY ISSUES?

Contributing to the dialogue and the knowledge about making a more secure and trustful environment in which and information society can grow and prosper is the basis of Microsoft's engagement in Risk & Security Exchange. As information technology is pervasive in every business, Microsoft's growing relationship with its customers implies great power to make things move ahead. But with great power also comes great responsibility to fully engage in the changes that lie ahead.



While Microsoft powers the Risk & Security Exchange, it reaches out to its community network in Switzerland, in Europe and internationally, to identify the best leaders to be involved in the process. Other partners, as First Tuesday and Computer Associates, are involved and supporting the initiative.

## HOW DO THINGS WORK IN THE THINK TANKS?

Each Think Tank is made up of a select group of leaders, who work together on the assigned topics during a timed work session of 4 hours. They are being helped in their work by a facilitator and individual group coaching to collect the ideas and bring them together. At the end of each session we create a to-do list, which will define steps that must be taken in order to get closer to important change in the topic area.

At the end of a session, a working paper captures the high points of the discussions. After a series of sessions, an overall paper – the publication you are holding in your hands - resumes the combined work. During this time, leaders are encouraged to further study the issues at hand, with the group or outside the group, and to keep up the Exchange.

## WHO IS PART OF THE THINK TANKS?

Leaders, decision makers, influencers who are contributing to the strategic dialogue in making business and information society a fruitful environment of growth and progress are engaged in the Think Tanks. The groups are combined of leaders from enterprises, academia, research, consulting and government to ensure a broad focus on the topics at hand.

A joint initiative to engage in strategic dialogue on Risk & Security

Microsoft® FIRST TUESDAY ZURICH

With the support of:

ca Computer Associates®

# Forrester Consulting

## Risk & Security – Who's In Charge

**Prepared for:**
Microsoft and the Risk & Security Exchange
July 2004

**Project Director:**
Steve Hunt

European Research Center
Forrester Research B.V.
Rijnsburgstraat 9–11
1059 AT Amsterdam
Netherlands
Tel.: +31 20 305 43 00
Fax: +31 20 305 43 33

FORRESTER®

HELPING BUSINESS THRIVE ON TECHNOLOGY CHANGE



## WHAT TO EXPECT FROM THIS DOCUMENT

The Risk & Security Exchange (RSE) is powered by Microsoft. In the spring and summer of 2004, the RSE hosted three Think Tanks on various risk and security topics in Switzerland.

This document covers one of those Think Tanks, which was on the subject: «Risk & Security: Who's In Charge?» This document:

- **Describes the current understanding («What Most People Think»).**
- **Summarizes the outcomes and discussions that were held at the Think Tank («What We've Learned»).**
- **Provides Forrester's perspectives on the implications for interested stakeholders («What It Means»).**

## WHAT MOST PEOPLE THINK TODAY

**IN RECENT YEARS, IT SECURITY HAS BEEN EVOLVING INTO A CRITICAL SHARED SERVICE WITHIN MOST ORGANIZATIONS, WHICH MEANS THE HEAD OF SECURITY HAS ALSO BEEN EVOLVING INTO A CRITICAL LEADERSHIP ROLE.**

Trends in Europe show that the new security leader has responsibilities not merely to IT, but to improving the operational efficiency of the business and implementing cost-effective risk management measures. Those bottom-line improvements come most easily when companies treat security as a business process, assigning a single individual to coordinate the various risk management processes of that organization.

For those reasons, the role of chief information security officer (CISO) has burst onto the corporate scene in Europe in the past three years. Before 2001, such a position was unique and considered rather peculiar. Today, there are more than 200 CISOs in Europe, but their respective job descriptions, reporting structures, qualifications, and compensation are wildly diverse. Therefore, despite some clear indications that organizations are adopting the role of CSO more frequently, there is little agreement on the nature of the position.

In the discussion on «Risk and security: Who's in charge?» Forrester completely expected to hear confirmation that the CISO role is solidifying in the European corporate culture, and that the role is rising in organizational importance and influence.



## WHAT WE'VE LEARNED

**THE GROUP BEGAN DISCUSSIONS ALONG THE LINES OF DEFINING THE NATURE OF THE CISO ROLE AND RESPONSIBILITIES, BUT ENDED UP IN A VERY DIFFERENT PLACE.**

The group determined that information security management is in a state of transition. The pressures of regulation, legislation, and increased liability are driving information security to become an operational risk management function outside of the IT department.

Organizations face pressure from privacy, identity theft, cybercrime, physical and cyber-terrorism, regulatory requirements, increased oversight and reporting requirements, and the threat of liability from security breaches. Legislation like Sarbanes-Oxley, California Senate Bill 1386, Basel II, Health Insurance Portability and Accountability Act (HIPAA), GLBAm and the Patriot Act have become corporate mandates to manage information security to specific requirements. This is driving information security to come under the umbrella of operational risk management.

In response to these demands, many organizations are beginning to evaluate the establishment of a chief risk officer (CRO) role, responsible for managing overall operational risk. Information security, physical security, privacy, compliance, and insurance are the roles that will report to the CRO.

The CRO, in turn, will report to the COO, CFO, or, in many cases, directly to the CEO. Information security is not often included in executive meetings today, but the CRO will be responsible for managing operational risk; this is a more intriguing position that plays a vital role in today's high-stakes environment and that will be an integral part of many executive teams.

The financial services sector is leading this trend to establish a combined enterprise operational risk management function. In large financial services firms, a CRO is integrating information security, physical security, privacy, and compliance. Additionally, an audit and legal function may report to the CRO. With the Basel II Capital Accords that require the management of information security as a part of operational risk coming soon, this will become more commonplace.

The typical CISO does not do true risk management, but as more pressure comes through regulations and legislation, this is starting to change. The trend is to manage information security as a part of operational risk, and this will drive the CISO out of the IT organization. There most often will be a security presence in the IT organization, labeled IT Security, with a dotted-line reporting relationship to the CISO, who reports to the CRO.

## WHAT IT MEANS

**WITH ACCOUNTABILITY AT THE TOP AND GOVERNANCE THROUGHOUT THE ORGANIZATION, THE FACT REMAINS THAT SOMEONE NEEDS TO LEAD AND MANAGE THE RISK MANAGEMENT AND REGULATORY COMPLIANCE EFFORT. THE QUESTION IS WHO?**

There is no model that is perfect for every organization. Some organizations break compliance management across different business roles. The CIO, or a designee, may head up the information technology and data aspects of compliance; the CFO may lead the financial integrity compliance requirements; and the COO may lead the operational requirements.

However, this fragmented approach is ineffective because organizations and regulatory challenges demand a coordinated role to facilitate compliance across the enterprise. Requirements cross different parts of the organization and require collaboration and monitoring of compliance centrally. A compliance program involves a mixture of information security, privacy, physical security, business continuity, integrity, legal/contractual issues, business partner relationships, insurance, and assessment roles.

This intersection of complex requirements that span the organization is best facilitated through a central role – a role best served under someone responsible for operational risk. Large organizations, particularly in financial services, often designate an executive as the chief risk officer responsible for operational risk. Although this title is not necessary, a central role for operational risk management, with compliance as a function, is becoming more relevant.

Regulations mandate requirements across information security, privacy, physical security, business continuity, and integrity. Furthermore, the requirements to protect information do not stop with the organization itself, but extend to the organization's business partners and contracts as those relationships interact with regulated systems and data. Centralized responsibility for compliance brings different organizational silos under one umbrella to manage.



This is illustrated in the guidance given to banks by the Basel Committee on Banking Supervision:

**«An independent function that identifies, assesses, advises on, monitors, and reports on the bank's compliance risk, that is, the risk of legal or regulatory sanctions, financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with all applicable laws, regulations, codes of conduct and standards of good practice together 'laws, rules and standards'.» (Excerpt from the Basel Committee on Banking Supervision consultative document «The Compliance Function In Banks» issued for comment on January 31, 2004.)**

Success in meeting the complex web of business and regulatory requirements involves establishing a formal compliance program in the organization. Because compliance involves many aspects of the organization (technology, privacy, business continuity, financial and business integrity, and business partner relationships), this is best served under an individual who is responsible for operational risk management and who has the power to coordinate the requirements and functions across the organizational units involved in meeting requirements. The individual in charge of compliance is responsible for establishing the compliance control architecture and continuously assessing that it is in place and functioning. However, for this role to succeed, senior management and the board need to establish a culture of governance that involves accountability for compliance.

# Forrester Consulting

**Risk & Security: Identity, Security and Privacy**
**From the «e-Citizen» to the «Networker»**

**Prepared for:**
Microsoft and the Risk & Security Exchange
July 2004

**Project Director:**
Steve Hunt

European Research Center
Forrester Research B.V.
Rijnsburgstraat 9–11
1059 AT Amsterdam
Netherlands
Tel.: +31 20 305 43 00
Fax: +31 20 305 43 33

FORRESTER®

HELPING BUSINESS THRIVE ON TECHNOLOGY CHANGE



## WHAT TO EXPECT FROM THIS DOCUMENT

The Risk & Security Exchange (RSE) is powered by Microsoft. In the spring and summer of 2004, the RSE hosted three Think Tanks on various risk and security topics in Switzerland.

This document covers one of those Think Tanks, which was on the subject: «Risk & Security: Identity, Security, and Privacy, From the «e-Citizen» to the «Networker.» This document:

- **Describes the current understanding («What Most People Think»).**
- **Summarizes the outcomes and discussions that were held at the Think Tank («What We've Learned»).**
- **Provides Forrester's perspectives on the implications for interested stakeholders («What It Means»).**

## WHAT MOST PEOPLE THINK TODAY

**THERE ARE TWO PREVAILING AND SEEMINGLY CONTRADICTORY ATTITUDES ABOUT SECURITY AND PRIVACY TODAY. PEOPLE SOMETIMES SAY THEY WANT MORE SECURITY AND WANT TO PROTECT PRIVACY, AND OTHER TIMES THEY SIMPLY IGNORE RISKS.**

One Global 500 company is removing water dispensers in order to save money, but it has increased its security and privacy budgets. Stories like that are not unique and tell us that security and privacy are top concerns of executives and shareholders.

However, consumers willingly sacrifice privacy for convenience at every opportunity. Loyalty cards and online transactions record personal information, freely offered by consumers. Nevertheless, when asked directly, most people will claim that privacy and security are very important to them. Mainly, individuals want to have control over how information about them is used.

Losing control over that information is a violation. More than 5% of all online consumers have experienced identity theft. These higher-income and more-experienced online shoppers remain technology optimists, but they tread the online world cautiously. Their concerns about theft and fraud pertain not only to identity theft, but also to credit card theft and purchasing fraudulent products. But retailers should still market to these consumers: 42% of identity-theft victims would purchase more online if they were more assured that their data was being protected. Consumers:

- **Don't think the privacy issue is overblown. When asked if the online privacy issue was a lot of hype, the answer was an unequivocal «no» for 97% of consumers. It doesn't matter how concerned people are about online privacy – everyone thinks that it matters.**
- **Feel like the tradeoffs aren't fair. Almost half of those surveyed feel like their privacy is more at risk since venturing online. And 94% percent of consumers we surveyed – including those claiming not to be very concerned about online privacy – feel that the risks of providing personal information over the Internet don't outweigh the benefits.**



## WHAT WE'VE LEARNED

In response to these issues, our group in Bern assembled a proposal for a directive on privacy and identity management. The directive proposed ways to protect business, government and personal privacy objectives from the perspective of consumers, employees, government, and business, respectively.  Some of the recommendations included clarification around who actually owns personally identifiable information, who has rights over it, and who may use it. That line of questions reflects similar struggles in many multinational organizations. Those organizations which want to comply with European data protection legislation have found cross-border data transfers within their own corporate entities a thorny issue if those transfers were going to countries that are not recognized by the European Union (EU) as featuring a level of data protection similar to the EU.A variety of options – outlined below – has been created over time to address the issue, but none of these has been optimal for ensuring data protection compliance for intra-company transfers of personal data. This is why a new proposal by the Article 29 Data Protection Working Party at the European Commission should be of interest to multinational organizations in this situation. While only a proposal at this stage, it is nevertheless worth scrutinizing, since it may meet a multinational's requirements better than the existing options.

The following are options available to multinational companies needing to ensure compliance with European data protection legislation when transferring personal data to non-EU and non-EEA countries that are deemed not to offer an equivalent level of protection for personal data:

- **A so-called «White List» of countries that qualify as having an equivalent level of data protection has been around for a while, but so far has few entrants (Hungary, Canada, Switzerland, and, most recently, Argentina). The list can be accessed at http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm**
- **Specifically for the United States, there is the Safe Harbor agreement, but this has its own problems and has not been widely taken up.**
- **A potential alternative option is using «model contracts,» which get third parties to agree to EU-level data protection principles. But this is a rather cumbersome method and not ideally suited to intracompany data transfers.**
- **Obtaining consent is also a potentially cumbersome method, in particular because the specific requirements for obtaining consent differ between EU countries.**

## WHAT WE'VE LEARNED

The lack of suitability of these compliance methods for intra-organization transfers was recognized some time ago, hence this proposal by the Article 29 Data Protection Working Party. The group advises the European Commission, and its members are representatives from EU countries' data protection authorities. Rather cumbersomely titled «Working Document:

**Transfers of personal data to third countries: Applying Article 26(2) of the European Data Protection Directive to Binding Corporate Rules for International Data Transfers,» the full text can be found at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp74_en.pdf (French and German also available).**



## WHAT IT MEANS

The fundamental difference between privacy protection in the US and Europe lies in the contrast between the laissez-faire attitudes to legislation in the US versus active passage of protective regulations in Europe. The fundamental difference between consumer perceptions of privacy and those of corporations is that consumers want control over information they believe to be personal property, while corporations want to protect their brand, efficiently manage identities and privileges, and comply with regulations.

### THE US AND EUROPE

The existing US Data Protection laws against the misuse of personal data by nongovernmental organizations are restricted to especially sensitive data, including financial information, personal data on children, and health information. The only general data protection act, the Privacy Protection Act of 1974, merely provides protection against the misuse by the government.

As a consequence, all-embracing data protection against nongovernmental entities is still left up to the private sector. Organizations are asked to regulate themselves by posting privacy policies and implementing privacy-enhancing tools.

This situation is consistent with the traditional reactive approach and wait-and-see attitude of the US legal system. It also mirrors the US constitutional background. The US constitution does not include individual rights protecting all personal data. It does not include constitutional rights against the misuse by nongovernmental entities either. As a result, the US legislature is not obligated to enact such general privacy laws.

European countries, on the other hand, have been forced by the European Union (EU) Directive on Data Protection to offer a unified standard of legal protection against the misuse of all personal data by government and nongovernmental organizations. The European countries have implemented General Data Protection Acts accordingly.

The attempt to forestall problems like the misuse of personal data before they occur with the prior enactment of general protection laws is consistent with the traditional regulatory approach of most European countries. As in the US, this follows the constitutional background in Europe. Most European constitutions protect the individual against the misuse of all personal data by the government and private parties. The national legislature is therefore obligated to enact laws to accordingly guarantee such protection. The general Data Protection Acts are the result.

The increasing use of the Internet will cause an increasing approximation of the US and Europe. The difference in approaches described above will decrease during the next 12 months to 18 months accordingly. The likely enactment of general privacy legislation in the US within this year and the growing promotion and implementation of self-regulation tools in European countries are steps in that direction.

## CONSUMERS AND CORPORATIONS

Companies – specifically, marketing, sales, and IT departments – should keep in mind the principles behind regulations in order to avoid errors when modifying content and processing personal data. As people have become more sensitive to personal data protection and their corresponding rights, it is time to build, inform, and train teams that may be involved in this issue and to develop specific skills to support them – even to create a «privacy department,» if necessary.

Privacy should also be taken into consideration regarding identity management. For example, when hiring a new employee, the company should use processes and technologies to ensure that the new user has access to everything he ought to and no access to those assets that are restricted. Simply granting a password is not good enough.

Although IT budgets remain tight, organizations are continuing to invest in identity management because it addresses critical business issues and delivers a quantifiable return on investment (ROI). The specific, measurable ROI associated with identity management is a distinct departure from traditional security products that focus on value in terms of managing risk, deterring attacks, and avoiding security breaches.

Identity management delivers direct business value and measurable ROI in four key areas:

1. **User productivity and empowerment, by giving users: timely access to the data and applications they need; the ability to personalize the content and delivery of services and data; and control of their environment through self-service processes.**
2. **IT management efficiency and help desk cost avoidance, by streamlining the efforts required to keep the data consistent and up to date. This often simplifies user sign-on, which, combined with self-service features, also reduces calls to the help desk associated with forgotten passwords and other basic issues.**
3. **Application development agility, by accelerating application development cycles through reusable integration and security components and improving business competitiveness by helping organizations build new services and expose existing applications more quickly.**
4. **Security auditing and compliance, by assisting organizations in evaluating compliance to access-control policies as well as in consistently enforcing such policies throughout the enterprise.**

Of course, not all security issues can be reduced to the challenges of managing user information. Yet the fundamental elements of security – authentication, authorization, administration, and audit – cannot be effectively addressed in large-scale environments without examining the methods in which user data is managed, accessed, and interpreted by applications and resources that organizations wish to secure.



Consumers have the opposite challenge: not managing many users, but managing multiple «identities.» For example, when the consumer engages in online banking, he has a particular identification and password, with associated privileges. But when he later buys a book online he is known by his profile, his past purchases, and his credit card number. In other words, subsets of his personal information are collected by perhaps 10 or even 50 companies, which in return grant privileges.

The consumer in general is growing in his awareness that his personal privacy depends on how responsibly these businesses manage his personal data. Therefore, the standard we created in Bern reflects a trend: to return control of personal data and its usage to the consumer, to give the consumer oversight of how his data is used, and to give the consumer recourse. Forrester sees the trend growing for three to five more years until the employee, corporation, government agency, and consumer each for its own reason respects privacy, ensures security, and protects the identity of everyone.

# Forrester Consulting

**Real and virtual war: Critical Information Infrastructure Protection (CIIP) and the public/private collaboration**

**Prepared for:**
Microsoft and the Risk & Security Exchange
July 2004

**Project Director:**
Steve Hunt

European Research Center
Forrester Research B.V.
Rijnsburgstraat 9–11
1059 AT Amsterdam
Netherlands
Tel.: +31 20 305 43 00
Fax: +31 20 305 43 33

FORRESTER®

HELPING BUSINESS THRIVE ON TECHNOLOGY CHANGE



## WHAT TO EXPECT FROM THIS DOCUMENT

The Risk & Security Exchange (RSE) is powered by Microsoft. In the spring and summer of 2004, the RSE hosted three Think Tanks on various risk and security topics in Switzerland.

This document covers one of those Think Tanks, which was on the subject: «Real and virtual war: Critical Information Infrastructure Protection (CIIP) and the public/private collaboration.» This document:

- **Describes the current general understanding («What Most People Think»).**
- **Summarizes the outcomes and discussions that were held at the Think Tank («What We've Learned»).**
- **Provides Forrester's perspectives on the implications for interested stakeholders («What It Means»).**

## WHAT MOST PEOPLE THINK TODAY

Information security and the protection of critical information infrastructure is a hot topic these days. However, opinions vary regarding what the critical infrastructure is and whose responsibility it is to protect it. Government, commercial organizations, and regulated commercial organizations all have different perspectives on implementing critical information infrastructure protection.

Forrester monitors trends related to business continuity around critical information infrastructures and reports on those trends frequently. The most recent trends in government and commercial organizations are the following:

**A moderate increase in business continuity (BC)-centric product and program implementation rates.** As predicted at the end of last year, the BC market trends show a transition from the strategy development, planning, and technology evaluation that characterized the market calendar year 2002 to more of an implementation-centric phase in 2003 and 2004. Organizations are now spending real money and committing resources to BC programs. Across all industries, Forrester Research's recent technology spending research indicates a spending commitment to disaster recovery (DR) products and services of 59% – the highest level of IT budget commitment among all categories identified in our survey.

**Operational efficiency initiatives will continue unabated.** Despite the continued commitment to BC and DR programs, maintaining profitability in a bearish economy is still priority one. We have seen no slowdown in initiatives to reduce costs through data center, server, and storage consolidation efforts, even though these initiatives can increase BC expense.

**A reduction in production-recovery-site separation.** The trend toward reduced but still responsible site separation policies continues largely unchanged from last year. The only significant market event in this area in recent years was the relaxing of minimum distance policy from the initial Securities and Exchange Commission (SEC)/Office of the Comptroller of the Currency (OCC)/Federal Reserve Bank (FRB) draft in October of 2002 (applicable only to a limited number of financial services organizations).

**Increasing popularity of internal recovery site provisioning.** This trend continues, and appears to be accelerating based on the recent development of capacity-on-demand offerings from leading platform vendors. The basic concept is that cost savings from on-demand platforms allow an IT organization to purchase a very minimal hardware configuration that is sufficient for logical testing of the recovery plan, but with the flexibility to quickly (in minutes) activate much greater capacity in the event of an actual disaster or any other sudden need for additional capacity. The economics of many hardware components now make it feasible for vendors to "park" spare capacity on the customer's floor for such purposes. Most, but not all, software vendors support this dynamic capacity upgrade capability. The bottom line is that for many leading platforms, IT is no longer forced to make large capital investments in hardware and associated software carrying costs for idle recovery resources – rather, they can make much more modest investments sufficient for testing, with the knowledge that the additional capacity is already on the floor. This improves the economics of internal recovery site provisioning.

Therefore, we fully expected the conversation in Geneva to be an investigation of disaster recovery best practices from the respective points of view of government agencies, regulated private industries (like banking), and other commercial organizations. Such best practices include the following:

- **Facilities cost.** The cost of real estate is an obvious consideration in site selection, but not necessarily the primary consideration. The cost of raised floor is a high priority for machine-room environments, but lower on the list of priorities for "people centers," where quality-of-life issues and staff retention concerns outweigh the value of inexpensive floor space. Put more simply, you can put machines in very low-cost locations but you may well have a problem convincing skilled IT professionals to live in those same communities. The total cost of expected relocation expenses for employees who must be relocated should be included in the cost model for situations where this applies.
- **Quality-of-life factors.** Expanding on the point above, for people centers, selecting a location that has good quality-of-life factors like climate, affordable housing, good school systems, low crime rates, etc. is important for retaining quality staff in relocation projects. Further, the availability of an educated workforce, population growth, and «talent feeds» from quality technical schools, colleges, and university programs should be considered in the ability to maintain quality skills over time.
- **Physical security.** In addition to the personal security of employees mentioned above (crime rates, political stability), the exposure to natural disaster threats (tornado, hurricane, flood, earthquake, etc.) as well as human-made disasters (toxic spills, terrorist attacks, etc.) needs to be assessed for each location.
- **Infrastructure.** The use of existing locations with excess space – especially owned property or property under long-term lease commitments – is an intuitively attractive option. It is not unusual to see site selection activity for data center consolidation projects initially consider existing locations exclusively. Only after these sites are deemed unfit are other options considered. Often, the use of an existing facility is the correct and obvious choice – especially when smaller locations are being absorbed into large, efficient class-A data centers. However, there are many situations where the exclusive consideration of existing sites will result in suboptimal results. Examples include situations where all of the existing centers are located in substandard facilities or where consolidation into existing sites will create unacceptable risk by exposing too much IT infrastructure to a single disaster event.

## WHAT MOST PEOPLE THINK TODAY

- **Use of existing facilities.** The use of existing locations with excess space – especially owned property or property under long-term lease commitments – is an intuitively attractive option. It is not unusual to see site selection activity for data center consolidation projects initially consider existing locations exclusively. Only after these sites are deemed unfit are other options considered. Often, the use of an existing facility is the correct and obvious choice – especially when smaller locations are being absorbed into large, efficient class-A data centers. However, there are many situations where the exclusive consideration of existing sites will result in suboptimal results. Examples include situations where all of the existing centers are located in substandard facilities or where consolidation into existing sites will create unacceptable risk by exposing too much IT infrastructure to a single disaster event.

- **Recoverability.** Following on from the previous point, data centers can only get so large from a capacity perspective before they become «unrecoverable». Large IT organizations can create «mega-center» locations through consolidation of data centers to the point that they exceed the capacity of the largest commercial recovery site providers and make internal recovery site provisioning financially impractical. There are many factors to be considered in the «how many data centers should I have» question that are beyond the scope of this discussion. There are practical limits on absolute capacity for a single site that will come into play if risk is responsibly managed.



## WHAT WE'VE LEARNED

Our discussion regarding protection of critical information infrastructure seemed to reflect a general feeling of disconnectedness between public entities and private companies. During a power blackout or flood, each organization initiates its own disaster continuity program, relying very little on public infrastructure.

The group in Geneva reached consensus on the top 10 infrastructures underpinning the overall information infrastructure:

1. **Human access, including transportation systems, motorways, public transport vehicles, transport systems, and traffic lights.**
2. **Electricity, power, and water.**
3. **Internal and external communications systems: voice networks, mobile, cable – email.**
4. **Key IT infrastructure: management systems, physical workstations.**
5. **Key production processes.**
6. **Key human resources and procedures.**
7. **Corporate internal network – all the fiber and copper connections, routers and switches, and wireless access points.**
8. **Employees need access to the work place – therefore, critical infrastructure for those individuals includes public transportation, roadways, food and drinking water, and personal health (plague, flu).**
9. **Global money and securities transfer, settlement systems from central banks.**
10. **Cooling systems (computer rooms).**

Notice first of all how the information infrastructure was not perceived as a single, clearly defined group of systems. Instead, many different systems seemed to affect and support the information infrastructure. For example, some of the non-obvious subordinate infrastructures were motorways, public transportation, and traffic lights. After all, if employees cannot get to work, the information infrastructure likely won't work.

The threats to the information infrastructure, then, can be very indirect. That is, something like a disease or anthrax scare can inhibit access to post offices and thereby interfere with the transfer of information.

## WHAT IT MEANS

### «PEOPLE» CONTINUITY IS DIFFERENT TO «MACHINE» CONTINUITY

It is important to understand that somewhat different considerations apply for «people center» and «machine center» locations. Historically, data center machine rooms and the associated support staffs have been collocated, but the state of systems management technology today is such that there is less and less need to have people and machines in the same physical location. Clearly, there are certain functions that require a local presence, but these tasks represent a small subset of overall IT staffing needs – typically only facilities management and physical hardware configuration administration. Functions like technical support (systems programmers), network operations control centers (NOCs), DBA, etc. have no compelling reason to reside with hardware resources.

### EUROPE: STILL ASLEEP IN THE FACE OF TERRORIST THREATS AND THEIR CYBER EQUIVALENTS

There is one significant difference between the US and Europe on this matter. The US has formed a Department of Homeland Security, while the European Union has not. Instead, each country has networks of first responders and incident-response teams at various degrees of maturity and readiness. Otherwise, it is fair to say that both continents are woefully unprepared to defend against cyber attacks, as well as physical terrorism. There is too much dependency on core infrastructure or on specific vendors or simply on corporate and government IT. That leaves companies and government agencies open to attacks.

### NATURAL DISASTERS ARE STILL THE MOST COSTLY

Consider that:

- **The direct costs of Sept. 11 are estimated at $25 billion to $29 billion.**
- **The direct costs of the 2002 floods in Europe are estimated at $25 billion.**
- **There have been 15 natural disaster events since 1980, with direct costs estimated in excess of $10 billion – the most costly being the 1995 earthquake in Kobe, Japan, estimated at $131 billion.**

(Source: EM-DAT: The OFDA/CRED International Disaster Database, www.md.ucl.ac.be/cred)

### IT'S DEPENDENCE ON POWER AND WATER

The catastrophic failures of the power grid in North America in August 2003 and in London on August 28, 2003, on the heels of the less-sensational rolling brownouts and blackouts in California during 2000 to 2001, underscore the critical dependency of IT services on reliable power sources. In Switzerland, data centers rely on low water temperatures in lakes and rivers to cool computer systems. When temperatures rose some years ago, many data centers had to shut down for lack of cooling systems. When primary utility providers cannot deliver service, or when other dependencies on utilities are challenged, it is incumbent on the IT organization to identify this risk to the organization, and where justified, invest in internal power generation capabilities.



### GOVERNMENTS OVER-REACT WHILE PRIVATE ORGANIZATIONS OFTEN UNDER-REACT

The other key takeaway from the Geneva session is relative not to the threat of events themselves, but rather to the behavior of the commercial and government sector to these threats. The net is that:

- **The media love a potential disaster and will promote worst-case possibilities as long as the public will tune in.**
- **In a very litigious society, public and private organizations may cancel critical services merely on the basis of a threat of a natural disaster**

We certainly do not encourage a cavalier attitude toward the potential impact of predictable natural disasters like hurricanes, but business continuity planners must anticipate that the community will not always behave rationally in advance of such events and must plan accordingly. For example, in the case of hurricane Isabel, US federal government offices were closed for two days, and public transportation was shut down in the Washington, D.C., area – despite the fact that, with almost near-certainty, the storm was forecast to hit 350 miles to the south and with only 40 mph winds expected in the US Capitol. With greater justification, 7,000 flights were preemptively cancelled. School districts in Long Island, NY, were closed, although there was no appreciable impact of the storm in this region (which again, was known well in advance of the school closings). Clearly such disruptions in public services may compromise the ability of employees to commute to work, either because of a lack of public transportation or unexpected responsibility for child care, and again these underscore the value of remote access in business continuity planning efforts.

### THE VARIOUS VERTICAL VIEWS OF CRITICAL INFORMATION INFRASTRUCTURE

- **Government agencies see information infrastructure protection as meeting requirements that have been mandated to them. For example, a civilian-facing federal agency may be primarily concerned about simply conducting the obligated security assessments rather than working out systems of interdepartmental communication in preparation for a disaster.**
- **Commercial organizations think of critical infrastructure as protecting their own assets and want to focus on internal security and disaster recovery.**
- **Regulated commercial organizations look at critical infrastructure protection as a balance of two views: They have to meet requirements (e.g., Basel II, Sarbanes-Oxley, etc.) but also need to keep the business perspective in mind and meet those needs as well.**

Our group listed several ways to harmonize the contrary perspectives. They suggested that sector influencers, like professional associations, should take the lead in creating positive information and best practice in view of achieving CIIP. Already independent associations are working on awareness, but now large market holders in the sector should take over the process from there and create a more concrete way to contribute information and declare incidents to establish sector weaknesses and specific solutions. Vendors are also among those influencers. Considering that vendors have access to critical customer information about every level of security issue, it is imperative that they become instrumental in information gathering and public communication. For example, vendors and users must publish and share best practices in order to standardize business continuity plans. But the public sector has a role, too. The European Union should form a committee responsible for regulating critical infrastructure protection. However, that regulation must be done by an accepted, trustworthy, neutral authority. That authority may even establish a public code of conduct in order to test skills, for example a «license to surf» or some other crednetial authrizing people to deal with electronically connected activities.

Those more active recommendations could be complemented by longer term awareness-building. When the public and private sectors work together, we collectively increase knowledge, combine information and set forth best practice. Chances are that someone has already dealt with your issues, or is struggling with them right now, so we ought to share the information. Security should be part of education, for children but also for business managers. The earlier in we learn about good practice in information security the better, however, it is never to late to learn. But above all, be patient. It takes time, maybe even 50 years, to fully integrate CIIP in public and private consciousness.





### FIRST TUESDAY

First Tuesday Zurich is an independent Business Think Tank, encouraging and supporting the creation of knowledge where business intersects policy, technology and innovation. We are experts in creating strategic dialogue, leveraging the power of different perspectives and experiences to develop new insights. We believe that the knowledge of networks is more powerful than the knowledge of the individual. Today, creating a common ground for ongoing leadership dialogue is greatly needed when it comes to global issues of Information Security. Bringing together a strong peer-to-peer leader group was, for us, the cornerstone of the Risk and Security Exchange for it insured a dynamic investigative process and guaranteed the quality and integrity of the group's findings.

Responsible for RSE session content:
Maria Finders, Senior Project Manager,
Executive Producer of the Risk & Security Exchange.

### COMPUTER ASSOCIATES

As IT security is a complex, interdisciplinary and fast-moving area, security solution providers need a trusted basis to exchange viewpoints and to share information with a broad range of security stakeholders, such as research and development, regulation, standardization, law enforcement, user groups etc. The Risk and Security Exchange has proven to be a valuable, neutral platform for such in-depth coverage of security topics – the results of the various RSE sessions contain valuable information and guidance for Computer Associates, and its customer base.

Computer Associates International is the world's largest management software company, delivers software and services across operations, security, storage, life cycle and service management to optimize the performance, reliability and efficiency of enterprise IT environments.

### MICROSOFT

Microsoft is the worldwide leader in software, services and solutions that help people and businesses realize their full potential. As information technology is pervasive in every business, Microsoft's growing relationship with its customers implies great power to make things move ahead. But, with great power also comes great responsibility to fully engage in the changes that lie ahead. Contributing to the dialogue and the knowledge about making a more secure and trustful environment in which an information society can grow and prosper is the basis of Microsoft's engagement in Risk & Security Exchange.

Responsible for RSE session content:
Joanna Stefanska, Security Solutions Manager
Roger Halbheer, Chief Security Advisor

## RISK AND SECURITY EXCHANGE PARTICIPANTS

| | |
|---|---|
| **Juan Avellan** | Chief Policy Officer, Wisekey |
| **Kevin Blackman** | Chief Technology Officer, Wisekey |
| **Adar Eyal** | Founder and CEO of iTcon |
| **Roger Halbheer** | Chief Security Advisor,<br>Microsoft Switzerland Ltd |
| **Bernhard Hämmerli** | Vice President FGSec Association, HTA Luzern |
| **Kurt Haering** | President, EFSI AG |
| **Martin Hauser** | Head of Information,<br>Security & Risk Management,<br>DHL Global Information Systems |
| **Charles d'Heureuse** | Chief Technology Officer, Bluewin AG |
| **Ralph Holbein** | Chief Information Security Officer,<br>Information Security and Operational Risk,<br>Credit Suisse |
| **Steve Hunt** | Vice President Research Director Security,<br>Forrester Research |
| **Stéphane Koch** | Advising & Training in<br>Competitive Intelligence and strategic<br>management of the information, Intelligentzia |
| **Vladimir Kulhavy** | Project Manager, DS, Consultant, Siemens |
| **Hannes Lubich** | Information Security Strategist,<br>Computer Associates |
| **Ernst Messmer** | Partner, Affentranger Associates Ltd. |
| **Rolf Oppliger** | Swiss Federal Strategy Unit for<br>Information Technology, FSUIT |
| **Heidrun Pollmann** | Business Technologist, Computer Associates |
| **Carlos Rieder** | Head of Competence Center IT Security,<br>Business University Lucerne, HSW |
| **André Schmid** | Director, Infosurance |
| **Alexander Stüger** | General Manager, Microsoft Switzerland Ltd |
| **Giampaolo Trenta** | Group Chief Security Officer,<br>Julius Baer & Co. Ltd |
| **Lilia Vogt** | Head of Information Security,<br>World Intellectual Property Organization, WIPO |
| **Ralf Winzer** | Head of Information Security,<br>Swisscom Enterprise Solutions AG |
| **Andreas Wuchner-Bruehl** | Head Global IT Security, Novartis Pharma AG |
| **Reto Zbinden** | Director, Swiss Infosec |
| **Pius Ziegler** | National Security Officer, KPMG Switzerland |

## WHERE DO I FIND MORE INFORMATION?

All dates, information and result papers, as well as this current publication can be found under **www.riskandsecurityexchange.ch**.

If you have any questions please contact **rsech@microsoft.com**.

**www.riskandsecurityexchange.ch**

Risk & Security EXCHANGE powered by Microsoft