

Information Security

...let's talk business



Information security is not about hackers and viruses. Neither is it about firewalls and Public Key Infrastructures. All of these new, exotic threats and tools are certainly part of the information security environment – but information security is essentially something much more familiar. Information security is business risk management.

Defaced web pages are risks to a organization’s reputation. Denial of service attacks are similar to the kinds of business disruption caused by protesters. Unauthorized access to data is similar to physical theft. There is nothing *fundamentally* new here – CEO’s have always had to balance the drive for higher returns against protection of the investment, while keeping a healthy eye on potential risks and threats to facilities and shareholders.

What *has* changed is the dynamic between operational and business risk – a change driven by the information revolution.

New economy or new risks?

In a strict sense, there wasn’t any risk – if the world had behaved as it did in the past.

Merton Miller, Nobel Laureate, referring to the spectacular demise of investment firm Long Term Capital Management.

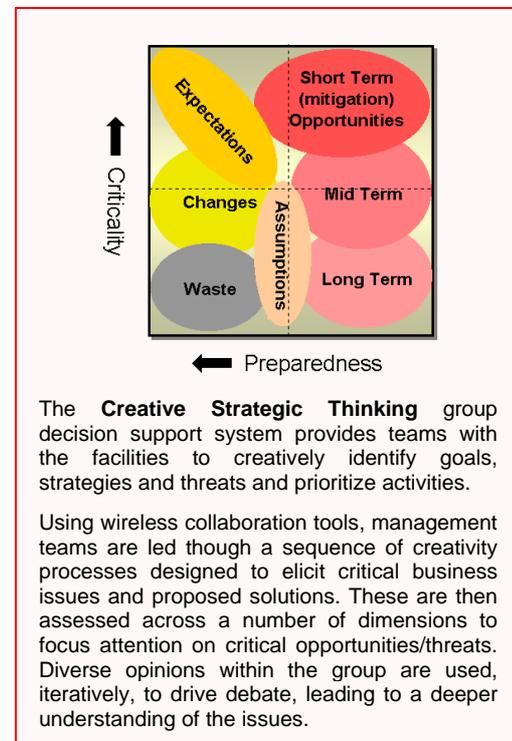
Companies are relinquishing control of their key assets. In the past, we could understand, and manage our assets - our land, facilities, machinery, computers, people, databases, etc. Intangible assets, such as reputation, were more complicated, but we still had protection mechanisms (e.g. PR).

Life is no longer that simple. Our organizational nervous systems are increasingly composed of open, "inclusive" systems – often reliant on public infrastructure (e.g. the Internet). Reputations can be made or lost via undetectable, *uncontrollable* "chatroom" gossip. Assets are becoming amorphous, emergent phenomena as competitive companies exploit networks of global expertise and knowledge systems to deliver customer value. Efficient electronic business services are lashing companies together, creating fragile, unpredictable, commercial eco-systems.

Couple these new sources of risk with the *pace* of business in the electronic age and you start to get *real* problems... Modern organizations need to respond to unpredictable events that unfold much, much faster than ever before. Today’s organizations need "real-time" risk management.

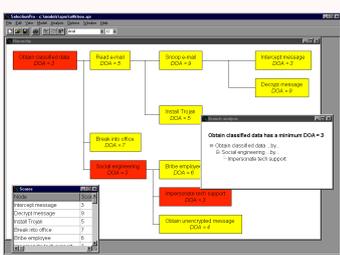
If we are to succeed in the face of these new challenges, it is essential that we

maintain our perspective in the face of current media, and industry, scaremongering. Information security risk is just business risk. Our existing tools still apply. We just need to be more creative in our identification of information security risks, and our development/deployment of mitigation strategies.



Capability is largely addressed by the “Who?” and “How?” questions – i.e. could this agent technically deliver this threat? Opportunity is addressed by the “Who?”, “What?”, “How?”, “When?” and “Where?” questions – e.g. does this person have access to the facilities needed to deliver this threat? Intent is address by the “Why?” question – i.e. “OK. So she can do it, but why would she *want* to?” Without this final element, the majority of your staff are active threats!

In order to determine the severity of a risk, it may be necessary to decompose it. A denial of service attack may be conducted in many ways – by an individual with the resources to install computers at multiple Internet access points; by a programmer who has installed Trojan horses on third party machines or; by a coordinated group of activists. Which attack is easiest to mount (given the anticipated attacker and intent)? This is the one we have to stop first.



SelectionPro, a multi-criteria decision-making system, can be used to design, and analyze, **attack trees**. Attack trees recursively decompose a threat into its constituent activities – highlighting the alternative ways in which a threat can be implemented. Software then calculates the lowest “cost” implementation path – i.e. the weakest link in your security.

Using this approach, investment can be made where it will be most effective. Extending the analysis, via the underlying multi-criteria approach, allows the attack tree to be directly integrated into the wider business planning.

Ideally, the impact of a threat can be estimated in financial terms – even if it’s just a rough order of magnitude. This allows for direct comparison of risks – and the evaluation of mitigation measures.

Starting with the key risks (i.e. high probability, high impact), we can begin to identify mitigation strategies/activities. The impact of each mitigation strategy must be mapped onto the identified risks *and* the

business strategies. For example, a comprehensive Public Key Infrastructure should reduce fraud, but is likely to inconvenience customers and staff. Such a mitigation activity reduces risk, but has an adverse impact on existing business operations.

As with risks, it is important to model the dynamic impact of mitigation activities. For example, enforced password changes (e.g. every three months) make it difficult for users to remember complex passwords. As a result, they may progressively simplify passwords – *increasing* the level of risk in the system!

Each mitigation activity must also be evaluated in the light of established risk behavior patterns. Risk homeostasis hypothesizes that people embrace a constant (but personal) level of risk. For example, if an organization introduces high profile physical security measures, employees may start leaving confidential documents on their computer screens while they are away from their desks. Putting their desks on the sidewalk would be likely to encourage a “clean-desk” policy!

Many risk reduction programs actually translate into increased performance – with *no* decrease in the level of risk exposure. Theories such as risk homeostasis help identify “unexpected” effects.

The “balance sheet” (benefits accruing from risk reduction versus impact of constraints on operations) must be drawn up for each mitigation strategy. If these are defined in financial terms, a portfolio of mitigation strategies can be assembled that maximizes the overall benefit to the organization.

Accurate risk assessment is impossible without considering the **psychological and social dimensions of risk**. This is particularly true in the area of information security where the threats are largely intentional, and the defenses often rely on personal discipline.

“People issues” must be addressed at all stages of risk analysis. CoNexus has developed a body of expertise in this area – addressing risk communication, risk culture, risk appetite and psychological phenomena (e.g. risk homeostasis, Prospect Theory).

Balancing risk reduction with business performance

Turning “gambling man” into “zero risk man”...is just one of the challenges...

Koos Visser, Shell Oil

Risk reduction should never be a goal. Intolerance of risk is intolerance of business. Balancing risks with the pursuit of effective business goals is the challenge. This is achieved by clear, explicit models addressing:

- business goals;
- strategies, and their relationship to these goals;
- risks/threats, and their impact on strategies and;
- risk mitigation activities, and their impact on strategies (both directly, and through risk reduction).

These models must support a quantitative assessment of the impact of risks and mitigation activities – even if these are no more than rough estimates. Financial considerations are a necessary, although not sufficient, component of robust investment planning. In addition, accurate risk modeling needs to address the *dynamic* nature of strategies, risks and mitigation activities. Dynamic behavior has a considerable impact on business performance. Static analyses will lead to ineffective decisions.

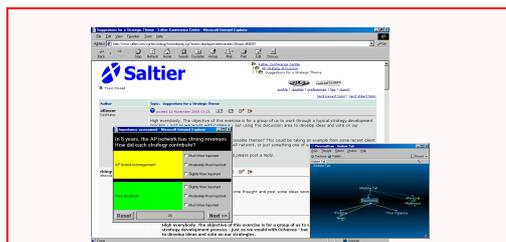
Due to the technical nature of information security, and the general lack of familiarity with the issues, any modern risk

management team must be comprised at least one expert in the field – not just an “IT person”, but an information security professional. However, information security *must not* be divorced from the general risk management activities of the organization – it is an *integral* part of these activities. Just as information security issues must be tempered by the overall needs of the organization, other functions (e.g. finance) must address information security issues in their own planning.

Risk No.	Risk Name	Risk Description	Risk Category	Risk Rating	Risk Mitigation Status
45	High	...
35	Medium	...
38	Medium	...
39	Medium	...
39	Medium	...
40	Medium	...
71	Medium	...
74	Medium	...
37	Medium	...
33	Medium	...
46	Medium	...
47	Medium	...

SmartRisk is a powerful, intuitive risk management system. Using “traffic light” displays to represent risk exposure pre- and post- mitigation, it allows managers to rapidly assess the effectiveness of risk planning and can be used as an on-going management tool.

SmartRisk has a non-technical interface that uses visual scoring facilities, and customizable “riskbases”, to produce quick, comprehensive risk assessments. For more detailed analyses, SmartRisk has a built-in simulation capability, allowing the quantitative assessment (e.g. financial) of total risk exposure.



Virtual conferencing helps maintain the multidisciplinary teams required for effective risk management and provides an organizational framework for deliberating risk issues.

While the technology is relatively low-cost it is only 10% of the solution. Successful virtual conferencing requires trained, experienced facilitators who can maintain interest and coherence in a distributed, text-based environment. CoNexus provides technology, facilitation, consulting and training to organizations wishing to conduct a virtual conference.

Modeling tools can help make information security an integral part of business management – especially tools designed to support business decision making, in addition to specific risk assessment. Tools that assist in the creative task of “searching” for new opportunities are also invaluable when identifying threats and risks - and can capture the complex interactions between risk management and business operations. Likewise, tools that help in “scanning” to pick out the critical strategies can be deployed to identify high impact risks.

Groups using tools build common language and analysis methods that begin to bridge the needs of business development and information security.

Continuous assessment

I didn't know that our [Lotus] Notes keys were deposited [with the US]. It was interesting to learn this.

Attributed to (an admirably understated) Jan Karlsson, Data Security Chief at the Swedish Defense Department, on learning that their recently deployed organizational communications system had a deliberately weakened encryption mechanism - making their confidential documents transparently readable to the NSA.

Information security requirements must be continuously revisited due to the constant evolution of business requirements, threats and defensive technologies.

This mandates a risk assessment model that evolves in parallel with the environment. As a new threat begins to approach, analysts must be able to "slot it into" the existing business model, devise mitigation strategies and identify the appropriate (i.e. cost-effective) organizational response. This requires a "living" modeling approach – an approach that can be updated in real time, without having to start from "scratch". Without such an approach, information security planning becomes an "annual event" – an unacceptable situation in an environment that evolves by the day.

Continuous, interactive information security assessment relies on integrating the elements of business planning/risk assessment with an envisioning or gaming capability. Potential threats or major security incidents are modeled before they become reality. In this manner, participants develop "memories of the

future" that can be recalled to identify an emerging opportunity or threat.

	SE	UN	f
SERBS			
attack enclaves	✓	x	✓
withdraw heavy weaponry from enclaves	x	✓	x
UN			
use artillery against Serbs	x	x	✓
use air strikes against Serbs	x	x	✓

Confrontation Analysis provides a powerful framework for developing "alternative futures" in competitive or defensive situations.

Extending the mathematics of game theory, it allows events to be couched in terms of intent/strategy, and guides the development of robust defensive strategies.

Plans are evaluated against the anticipated counter-measures (and counter-counter-counter measures, etc) of other parties.

Developing a continuous assessment capability for information security can be greatly facilitated by on-line collaboration. Wider employee participation can be engendered, providing better planning, better awareness of risk, and much better implementation of new procedures and measures.

Communication

I remain stunned at the number of companies that invest real money in firewalls and elaborate intrusion detection systems, only to continue letting their employees send confidential e-mail over the Internet (e.g. to clients, suppliers, traveling colleagues).

IT manager in the defense industry

Effective, swift communication is essential when besieged by new and evolving threats. As technology advances, so do the threats. Each uninformed individual in your organization is a vulnerability in your "system". Commandments from the IT department have, again and again, failed to "encourage" secure behavior.

Security policies need to come from the users. Having the IT department draft a fifty page report telling people how to do their jobs is an ineffective way of promoting information security. IT specialists need to provide businesses

with the technical background they need to develop effective security, and business, policies. While information security specialists continue to lay down laws, users will continue to break them.

Communication is also an essential prerequisite to *understanding* information security threats. Desktop PCs may be considered a low risk area in the overall information security strategy. It's relatively easy to switch one PC for another, with minimal business disruption. However, when you realize that sales staff are using Palm organizers to hold client details, and

synchronizing them with Outlook, you may change your assessment!

It is impossible to comprehensively assess the severity of information security risks without engaging the entire organization. Given that these threats are changing daily, effective information security necessitates an *ongoing, organizational* dialogue around the issues, and how they impact business operations.

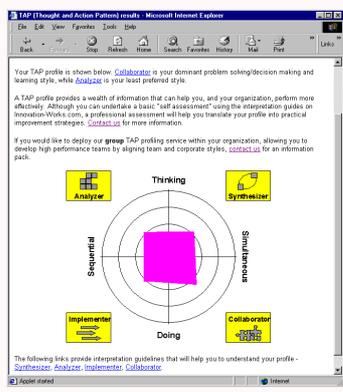
One area of communication almost universally overlooked by organizations is that of risk appetite. Organizational strategies are founded on a certain appetite for risk – a startup will be willing to embrace options that a corporate CEO would never take to her board.

It is important that employees understand the risk appetite of the organization, and align their individual activities behind it. If the planned risk appetite is not supported by the organization's risk *culture*, problems will arise.

Risk appetite varies across functional areas (e.g. R&D versus legal departments), but everyone needs to be aware of how their own appetite for risk effects the organization. For example, an ultra-cautious legal department may congratulate itself on keeping the company's nose clean, while marketing is

unable to react to e-business fuelled competition due to a laborious product screening process.

Organizations need to make their risk appetite explicit, and communicate their expectations to staff.



Thought and Action Pattern (TAP) profiles the communication preferences, and styles, of individuals or groups. Dominant approaches can be isolated and used to design effective communication plans. TAP can also be used to design targeted briefings for selected individuals or teams.

Based on decades of "whole brain" research, TAP comprises an electronic (web-based) assessment tool, and a database-driven reporting and analysis suite.

Conclusion

There are risks and costs to a program of action, but they are far less than the long-range costs of comfortable inaction.

John F. Kennedy

Ever increasing reliance on information systems is a reality for competitive businesses – and we must accept the ensuing risks.

Any business that relies on the flow of information through its own internal systems and external networks has to create an information security capability that can be managed by *business* managers – a capability that is in sync with its business objectives. In tandem, it must develop the capability to actively envisage, and react to, the evolving commercial landscape that characterizes the information society.

Balancing business requirements with information security requires:

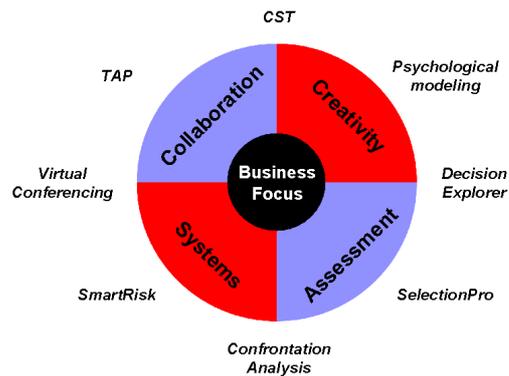
- an understanding that information security is just another part of business risk;
- assessment techniques that are grounded in, and focused around, business performance;
- creativity in the identification of threats and defenses;
- structured, comprehensive dynamic, quantifiable, "living" risk modeling approaches;
- a greater focus on "intent" in evaluating threats;
- knowledge of "risk psychology" and;
- access to information security professionals.

Let's talk business

Take calculated risks. That is quite different from being rash.

George S. Patton

CoNexus' business modeling and analysis solutions provide a context for client's wishing to exploit SAIC's class-leading information security capabilities. Our tools and process provide a comprehensive information security planning service that ensures investment is aligned with business requirements.



In our discussion, we have illustrated the importance of creativity, appropriate assessment, organizational systems and collaboration/communication in developing effective information security. We have also attempted to illustrate, through selected components in our toolkit, how CoNexus can support organizations in these areas.

Using our toolkit, we provide organizations with complete, structured, "concept to implementation" information security planning processes - processes that guide you from vision statement to technology selection! As our toolkit captures assumptions and arguments, it creates an evolving model of the "business case" for every information security investment decision.

We look forward to talking business with you...

Contact

CoNexus – North America

Mary Crannell

SAIC

Mary.E.Crannell@saic.com

Tel. +1 703 676 7795

CoNexus – Europe

Andrew Flower

SAIC

Andrew.Flower@saic.com

Tel. +44 178 881 7302



www.CoNexus.com



The information in this document is the property of Science Applications International Corporation (SAIC) and may not be copied, or communicated to a third party, or used for any purpose other than that for which it is supplied, without the express written consent of SAIC.

While the content of this document is given in good faith, based on the latest information available to SAIC, no warranty or representation is given concerning it. This content does not establish any contractual or other commitment binding on SAIC or any of its subsidiary or associated companies.