JISSec 4(1) 2008

Journal of Information System Security

www.jissec.org

Perceptual and Cultural Aspects of Risk Management Alignment: a case study

Corey Hirsch[1]
Jean-Noel Ezingeard[2]

Henley Management College, UK[1]
Kingston University, UK[2]

Abstract

Understanding how management and functional teams perceive risk, and will decide and act in managing risk, is one cornerstone of an effective enterprise Information Security management strategy. There is evidence in the literature that if managers do not understand the reasons behind an Information Security policy, or do not fully support the rationale behind the strategy, they are unlikely to engage in its development or adhere to it later. Further, if various individuals and management teams in an organisation approach risk management in a non-aligned fashion, their divergent decisions and actions could have the effect of canceling out each other, and rendering the enterprise risk management strategy less effective. Research indicates that a sociological understanding of risk perception as an input to Information Security development is becoming a necessity. We argue this from two strands of literature: the first is the literature in risk assessment in fields other than Information Security. The second strand is the Information Security literature.

How do managers perceive risk in practice? And how might an enterprise foster an aligned approach to risk management? This paper presents the case of LeCroy Corp., a medium size manufacturer of high value electronic testing equipment. We show that whilst there are areas where

A subsequent version of this paper appears in Social and Human Elements of Information Security: Emerging Trends and Countermeasures, edited by Manish Gupta and Raj Sharman (2008).

perceptions toward, and tolerance of, risk are shared within the organization, there are substantial variations between different groups of managers at LeCroy. Groups which routinely work together on information security and risk management related tasks have lower standard deviations in their risk judgments than teams which do not share this working experience, an indication that risk perception alignment is in part a social process. Yet this second group may also have responsibilities that are critical to enterprise risk management. We also find that top executives are "mathematical" in their risk appetite at low and medium stakes, yet highly risk averse when the stakes are higher, such as complete business success or failure, another indication of a social aspect to risk perception and management. The ideal scenario for degree and type of alignment will vary as a function of the type of working team. This case study illustrates one approach for defining and migrating toward a robust enterprise risk culture.

Keywords: Social Aspects of Information Security, Alignment, Case Study, Risk Management.

Introduction

Individuals in a population display variation in their tolerance for risk. A retired widower for example might choose an investment known to offer lower returns than other investments available, because it also presented a lower likelihood of variations in return. A young entrepreneur on the other hand, might be willing to accept a higher probability of surprises, as long as she feels the upside is commensurate with the downside. Willingness to accept a reduction in return, in order to reduce expected variation in return, is defined here as intolerance to risk. Willingness to accept high expected variation in return in order to maximize expected returns, is defined here as tolerance for risk. These are scalar concepts and can be reduced to the question (for intolerance) "how much would you be willing to spend, to reduce uncertainty in a specific context?" Alternatively phrased (for tolerance), it becomes "how much spending do you wish to withhold given your appetite for risk in this specific context?" Developing a clear and aligned Information Security policy requires making these concepts vector, by adding a context dimension. An individual may be highly tolerant, for example, to the risk of loss of ERP data, yet highly averse to the risk of impairment of a patent. A good understanding of both intolerance and tolerance to risk will therefore be an essential component of any successful Information Security policy.

Sources of information security risk are usually documented in taxonomies of risks. They tend to list broad categories of risk sources (Backhouse and Dhillon, 1996) that can be used to ensure that all sources of potential risks have been surveyed. For instance Loch et al. (1992) classify sources of information security risks as internal versus external, human versus non-human and accidental versus intentional. Similar classifications exist in the ISO 27001 control objectives (ISO, 2005) and in most text relating to Information Security (see for instance Whitman and Mattord, 2003).

Such taxonomies and classifications have been criticized by Dhillon and Backhouse (2001). They remark that checklists and taxonomies of threat tend to leave out the social nature of information security problems. This makes it difficult to get a clear picture of management's appetite for risk as an input to the Information Security strategy, and subsequently to ensure that the expectations and actions of various stakeholders are aligned. Yet, recent research suggests that understanding an organization's appetite for risk (and subsequently ensuring a good alignment between the stakeholders' attitudes to risk, and actual risk management practice) is perhaps as important to the success of an Information Security policy as is understanding risks clearly (Ashenden and Ezingeard 2005, Ezingeard et al., 2004). This is now understood in professional standards. COBIT 4.0 (ITGI, 2005) for instance firmly reinforces the need to understand an enterprise's appetite for risk as part of the information technology (IT) risk management process.

How then, can we measure (or estimate) the appetite for risk of an organization and use this estimate as an input to an Information Security strategy? Further, how can we ensure a good degree of alignment of attitudes to risk across an organization? Through a study of the risk appetite at a manufacturer of electronic testing equipment, this paper investigates the underlying dimensions of risk appetite pertaining to Information Security, and business continuity in general.

We begin with a review of the literature around risk management and alignment and linkages to social processes and risk perceptions and culture. We then present our case protocol and framework, and research methodology. This lays the groundwork for our case findings, after which we present a summary of what we believe this work has contributed, and suggest possible lines for further inquiry. This is followed by our conclusions.

Conceptual Basis: Risk Management and Alignment

Alignment

The notion of alignment is crucial in many areas of business. It has its origins in the concept of strategic fit, popularised by Tom Peters in the 1980s, who argued that congruence among seven elements strategy, structure, systems, style, staff, shared values and skills is necessary for success (Peters and Waterman, 1982). Alignment (also described as strategic fit) is important, because it leads to superior performance (Gietzmann and Selby, 1994, p19).

Defining “fit” is, however, difficult as fit goes beyond knowing what needs to be aligned, to include how alignment should be achieved. This led Venkatraman and Camillus (1984) to define fit as process (how to achieve fit) and content (what fit looks like). The importance of process is also highlighted by Reich and Bensabat (1996) who argue that two aspects need to be considered. As Venkatraman and Camillus, they highlight the importance of understanding how the planning process itself can help achieve alignment (in the case of Enterprise Risk Management, this would involve an examination of

the Enterprise Risk Strategy). They however take this further by suggesting the importance of looking at social relationships in the organisation.

The idea behind the argument that social relationships need to be looked at is that alignment is not only a strategic, logical process but also a social process. Therefore, communication between executive management and each function to be aligned (for instance IT executives) is often quoted as necessary for alignment (Reich and Benbasat, 1996, Reich and Benbasat, 2000). Alignment is also thought to be easier to achieve if business executives have a good knowledge of the functional areas where alignment is sought (Hussin et al., 2002).

The first link between strategic processes and social processes: risk perceptions

For almost two decades now, Information Security has been implemented as a process in many organizations. It follows a sequence of risk identification, risk classification (for instance in terms of impact and probability) and risk mitigation or avoidance. The approach has been at the basis of some of the most common Information Security best practice approaches such as the ISO 27000 series (ISO, 2005) at a management system level, as well as the Common Criteria Evaluation and Validation Scheme (CCEVS, 2005) at a lower technical level, since their inceptions. Whilst treating Information Security as a process is now seen as good practice, there have been many calls to ensure that the process should not be treated solely as a mechanistic one and should be capable of continuously adapting to its context. This approach is very "functionalist" (McFadzean et al., 2004) and can easily be seen as lacking completeness because its comprehension of the context of risk is limited. For instance both Beck (1992) and Baskerville (1991) argue that much work on risk analysis for Information Security is too functionalist. They suggest that practitioners have become over-reliant on predictive models for developing a secure information system thus ignoring important issues such as employee understanding, motivation and behaviour.

Adams (2005) outlines three types of risk: those that are perceived directly, those that are perceived through science, and virtual risk. He suggests that risks that are perceived directly are dealt with using judgement (this refers to risks such as crossing the road, for example). Virtual risks are culturally constructed because science is inconclusive which means that "whom we believe depends on whom we trust". Those risks that are perceived through science are relatively objective in nature. Information security risk assessment has come from a scientific background and has worked on the assumption that information security risks can be perceived through hard science. It now seems the case that many of the facets of Information Security fall into the category of virtual risk and if we are to address them from this perspective then we need a better understanding of how they are culturally constructed. There is therefore a need to "understand the relationships between human factors and

risk and trust if a relatively secure cyberspace is to develop in the future" (OST, 2004).

A third reason why understanding how risk is perceived is important is the social complexity of risk itself. Willcocks and Margetts (1994) point out that recent research, "supports generally the finding that the major risks and reasons for failure tend to be through organizational, social and political, rather than technical factors". Although this is referring to risk in the broad information system environment rather than Information Security specifically, the same assertion still applies. They go on to recommend that risk should be assessed as "a result of distinctive human and organizational practices and patterns of belief and action".

The second link between strategic processes and social processes: risk culture

Information Security risk is only one category of risks organizations are exposed to and many organizations find it difficult to align their IT risk management efforts with those of the rest of the organization in other areas such as financial or business continuity risks (Birchall et al., 2004). Often this is because risk management strategies, and more specifically Information Security strategies, are not grounded in organizational values (Dhillon and Torkzadeh, 2006). Yet, legislative and regulatory requirements for instance in the corporate governance arena, requiring organizations to think of Information Security within their overall risk management frameworks (ITGI, 2003) make this a requirement. This means that not only do risk management processes need to be aligned across functional areas in the organization, but also that attitudes towards risk need to be aligned.

In order to address this need for alignment, Jahner and Kcrmar (2005) propose a model of risk culture. The model has three dimensions, namely Identify, Communicate and Act. Whilst the "Identify" and "Act" dimensions are often clearly embedded in many Information Security processes, Jahner and Kcrmar argue that an organization's Information Security efforts can only be successful if a shared understanding of possible threats is achieved and if a shared understanding of how to act consistently is reached. How people act in Risk Management is, according to Ciborra (2004)"intertwined in social processes and networks of relationships".

Whilst Jahner and Kcrmar's model of risk culture is useful as a basis for understanding the social processes around risk in an organization, it does not discuss the importance of a shared understanding of the risk/reward equation in any of its three phases. Yet, this is likely to be crucial to the success of any risk management process. Whilst the information systems (IS) risk management literature is often coy about making this explicit, the purpose of risk management is not solely the avoidance of risk to minimise losses, but in fact the need to take risks to reap rewards. The financial risk management community is of course more explicit about this since the risk/reward equation is one of the fundamental rules of business. As pointed out in the Turnbull report

"Since profits are, in part, the reward for successful risk-taking in business, the purpose of internal control is to help manage and control risk appropriately rather than to eliminate it" (Turnbull, 1999).

There is a growing body of literature that suggests that this risk-reward equation is an integral part of an organization's risk culture. For instance, according to Adams and Thompson (2002), the assessment of reward is a key aspect of the "risk thermostat" that is at play both at an institutional and individual level during Risk Assessment. In Adams' model, the "risk thermostat" includes perceptual filters (Adams, 1999) whose influence depends on the attitude of people to risk. Similarly, attitude to risks have been found to have a significant impact of the way Boards of Directors address information security in their organisation (Ezingeard et al., 2003). We therefore need to augment Jahner and Kcrmar's model of risk culture by adding assessment of reward and assessment of the risk/reward equation in the "identify" and "communicate" dimensions of risk culture.

Case protocol

The method we used for the case study presented below is based on the three aspects of alignment we have explored so far: Context, Content and Process. This gave us one dimension of the exploration framework. In order to help us explain context we chose to look at the competitive environment in which the organisation operates in detail. This was done at a high level of detail in so far as the business area is a niche one, characterised by complex products and few competitors. More specifically we looked at the influence of three key stakeholders on the Enterprise risk strategy: Customers, Employees and Investors.

The second dimension was provided by looking at the make up of Enterprise Risk Management (ERM), starting with plans and actions as well as the two conceptual links we discussed earlier, namely the need to understand how risk perceptions and risk culture influence the alignment between ERM and business strategy. The resulting case study framework is shown in Table 1.

	ERM Plans and Actions	Risk Perception	Risk Culture
Context	How the business context influences ERM.	How the business context influences risk perceptions in the organisation.	How the business context influences risk culture in the organisation.
Content	What are the ERM mechanisms in place?	How risk perceptions influence the ERM mechanisms in place (and vice versa).	How the risk culture influences ERM mechanisms (and vice versa).
Process	What are the processes in place to achieve and maintain alignment between business strategy and ERM?	How risk perceptions impact on the alignment process.	How risk culture impacts on the alignment process.

Table 1: Case framework

Data was collected in three ways. The second author of this paper is a member of the executive team of the organisation and this enabled us to base most of the observations in this paper on his experience. Secondly the case was informed by documentary evidence, relying on the examination of:

- Policies
- Risk Management Spreadsheets
- Audit reports and audit recommendations

Lastly, we collected quantitative questionnaire data from a yearly risk profiling survey of employees and the executive team of the company. This data helped us gain an understanding of risk perceptions in vector, quantified form. Examples of questionnaire results are presented later.

Case study

Company background

LeCroy Corp. (Nasdaq LCRY, FY2005 Sales $US165M) was founded by Walter O. LeCroy in 1964 in Irvington, New York, USA. It operates in the Test and Measurement business, with the tag line “Innovators in Instrumentation”. This illustrates a dilemma in so far as the business area the company works in is one where products must be trustworthy, and innovation must therefore not get in the way of an equally important reputation for stability and robustness. Consequently, whilst innovations are required and can be significant source of competitive advantage, they cannot be allowed to be synonymous with surprises for the customer. Thus instrumentation makers tend to test innovations heavily before introducing them into production. They are generally willing to spend heavily to avoid surprises. We can therefore, from the outset, categorise the organisation's strategic environment as “risk intolerant”.

LeCroy's products are software intensive. Most are designed to be used connected to local area networks. It is therefore important that they should be patchable and upgradeable easily. When LeCroy's products began to be designed with embedded x86 architecture processors running Windows™ operating systems, a rigorous information security regimen became a requirement (Hirsch, 2005), in order to prevent malware contagion incidents that could affect the company, and possibly thereafter its customers (Oshri et al., 2005). At that time, the CEO chartered a new change initiative to elevate the information security culture. Two years later, when the Security Team had taken solid hold and the information security culture had clearly moved solidly in the desired direction, the CEO further chartered a new supplemental change initiative to institute Enterprise Risk Management at LeCroy. This is viewed as a completing element of the information security project.

LeCroy's main competitors are two, much larger, public companies. Instrumentation design and production is a high fixed cost business, hence there is a substantial advantage conferred by size. LeCroy must compete with these larger companies for relationships with customers, employees and

investors. LeCroy therefore has a strategy of fostering longer than average relationships with its partners in each of the above three communities. “No Surprises” is an element of the strategy.

Context

The first aspect we investigated of LeCroy's information security and risk management programme is how it is influenced by its environment and business area. In particular we investigated how its policies and procedures are designed to enable enterprise management of risk, such that customers, employees and owners experience a coherent risk profile. The key influences we uncovered are represented in Table 2.

Influence of context on perceptions of risk (and risk tolerance)

The context LeCroy operates in recognizes “controllable risks” as those for which the probability of occurrence can be viably decreased or increased based on management's decisions to invest or withhold investment in mitigation strategies. Examples of such risk could be data loss or data corruption risk. Conversely, “uncontrollable risks” are those for which the probability of occurrence cannot be changed by management action. Examples of such risk would be the arrival of an Avian Flu pandemic.

It is clear that most managers at LeCroy are intolerant of controllable risks. On the other hand, most managers seem very comfortable to operate in a business environment and context where they know many risks are uncontrollable and only their consequences can be mitigated. For example, instrumentation makers must be (at least) one step ahead of their customers in terms of technology. If an oscilloscope is going to help a designer working on a 10 Gbit design, the oscilloscope itself must be significantly faster internally. Design activities therefore carry significant risk. Which technologies to “bet on”? Which vendors can supply the needed components within the tight specifications required? One chipset (processor, memory) may offer a longer period of stability while another may introduce the latest feature … which chipsets should be selected? Which development project is likely to succeed, and which is likely to fail?

Influence of context on risk culture

LeCroy's early years were spent in the high-energy physics instrumentation market. This market had two main participant segments: academia and military. From an information security and risk management perspective, these segments presented a dichotomy. The bias for information sharing, typical of the “un-caged information” culture of the University, stood in stark contrast to the “need-to-know” information culture of the military and national research labs. For this reason, the information security culture at LeCroy is nuanced and complex. Traditionally the collegial atmosphere at LeCroy had been characteristic of a relaxed information security culture with a bias toward knowledge management benefits obtained through easy and widespread access to information.

	Customers	Employees	Owners
Context	o Long warranties and product support; o Easy and cheap software upgrades; o Minimized risk of malware contagion.	o Employee benefits offerings are designed to reduce risks for employees; o Relatively comprehensive insurance coverage and support packages; o Facilities investments and procedures designed to help employees manage risk; o Health and safety policy based on halving exposure every year.	Expanding number of institutional shareholders.
Implications	Low tolerance of risks that could influence customer relationships; Decision to implement ISO9000, receiving the first certification issued under the ISO9000:2000 program; Information security policy is significantly influenced by the high software content of products.	Low tolerance of risks that could influence employee relationships; Risks to health and safety on the job are managed in a different paradigm than information security risks.	High tolerance of t marke risks; Management's strategy is to aggressively mitigate controllable risks, while managing the consequences of unavoidable risk.
Key Performance Indicators	Higher than typical values for customer retention and repurchase.	Average length of service at LeCroy is 8 years, double peer group average.	8.2% of total shares outstanding are held by institutional holders with at least 4 quarters of ownership.

Table 2: Key stakeholder influences

Content of the risk management framework

The company bases its enterprise risk management methodology on a cycle of measurement and education. A significant element of the risk management framework is data driven with the overarching philosophy that employees and managers are responsible, and empowered, to align their risk management decisions to the company risk management strategy, and only require data and understanding in order to carry this out.

A risk management team comprising executives, managers and employees has been formed and charged with developing and implementing an enterprise risk management program. The program differentiates between those risks for which a return on investment (ROI) figure can be calculated should the company decide to mitigate the risk, and those risks for an ROI basis for investment decision making would be inappropriate (for instance employee discomfort, health and safety).

For those risks where a mitigation ROI can be calculated, LeCroy uses a spreadsheet with key columns labelled as shown in Table 3. Each of these factors figures into an algebraic expression, whose value indicates an estimated ROI on mitigation, and a confidence level in the estimate. The spreadsheet gives management a first indication of which mitigation decisions to consider, based on expectation of financial return. This is well aligned to the company's "willingness to spend to reduce uncertainty" model of risk management.

Estimated Probability FY08 Event in %, as of May 1 2007	Estimated Severity of Consequences of Event in $	Estimated Seriousness of Threat (B*C)	Confidence level in Estimate (0 low; 1 high)	CommentsExternal Cost to Mitigate ($)	Extent of Mitigation in %	Expected ROI	Action Plan	Estimated Seriousness of Threat following Action Plan

Table 4: Headings of the non-quantifiable risks spreadsheet

Influence of risk perceptions on the risk management framework

As explained earlier, the basis of the risk management framework is numerical. This means that perceptions of probability, severity, and seriousness of threat as well as costs to mitigate inevitably influence the robustness of the framework and its ability to deliver strategic objectives. For instance, we asked members of the Company's executive team how much they would be prepared to spend to halve the probability of:

- 2 day building closure
- The loss of 2 days of BaaN (ERP) data
- Bodily injury to 2 employees
- The 2 most important LeCroy patents become invalidated
- A large bin of confidential documents intended for shredding is accidentally released into the insecure dumpster
- The website being attacked and defaced for 2 days
- A malware infestation of the network and 200 infected products are shipped to customers

The responses we got varied significantly. Interestingly no significant pattern seemed to emerge based on the function of the respondent. When pressed for an explanation it became apparent that the perceived severity, rather than the perceived likelihood, of such events was the cause of the variation. The loss of two days of ERP data, for example, implied vastly different levels of pain to various respondents.

Influence of the risk culture on the risk management framework

We have so far characterised the company's risk culture as one that prefers to give priority to knowledge sharing and collegiality, and one that historically had a “relaxed” attitude towards Information Security. Yet, we have also described how the “risk thermostats” are set fairly low for controllable risks, and higher for uncontrollable risks. The need to resolve this apparent tension influences the risk management framework at two levels:

- Risk management structures: A high profile is given to risk management, with two committees (the Information Security Team and the Risk Management Team) dealing with risk company-wide. These teams meet regularly. The Chief Information Officer sits on both teams. The teams regularly seek (and get) input from members of the Company's executive team and annually from the Board.
- A strong sense that the company's efforts towards risk avoidance were made necessary by the market, and are appropriate. This is illustrated for instance by the views of the sales force about whether LeCroy should be more risk tolerant than it is. Out of 7 senior sales employees we questioned, only 1 thought LeCroy should be more risk tolerant, yet 3 described the company's culture as risk intolerant. Similarly, only one member of the executive team thought that LeCroy should be more risk tolerant.

Formal Alignment process

It is assumed that each manager or employee, who was hired for their job expertise, is the most capable person to estimate the probability and consequences of unexpected outcomes in their area of activity (first two columns of the spreadsheet tool). However, attention is paid to the alignment

between the risk-management actions of individual managers and the company's desired risk profile. For information risks, generally viewed as not employee health or safety related, assessments are made of likelihood of an unexpected outcome during the coming fiscal year, and of the expected cost should such an event occur. Whenever possible this is done based on LeCroy or peer company data. Then alternative mitigation actions/strategies are listed, as are the extent of estimated mitigation for each. Costs are listed as well, and from these factors an estimated ROI can be computed. In general, for information related risks, mitigation strategies are selected using this method, and applied to the current year's hurdle rate. The first alignment mechanism is therefore project finance.

The second routine alignment process in place in the Company is the participation of the Chief Information Officer in three key forums with a significant stake in the Company's ERM: The Information Security Team, the Risk Management Team and the Executive Team. This is seen to be an effective alignment mechanism in so far as both the Information Security Team and the Risk Management team are responsible for overseeing all planning related to ERM.

This is supplemented by two other mechanisms, which whilst not designed with the sole purpose of alignment in mind are widely seen in the organisation as important vehicles for validating the alignment of the ERM strategy. The first such mechanism consists of formal and regular Board agenda items where the ERM strategy and its Information Security components are discussed. The second such mechanism is company-wide (driven by IS and Finance) participation in debates and preparations for risk related audits (ISO, Sarbanes-Oxley).

The company does not generally screen recruitment candidates using risk-tolerance filters. The company therefore expects its employees and managers, in the absence of an enterprise risk management program, would represent a spectrum of individual risk cultures similar to the general population at large from which these groups are drawn. Therefore the company seeks to define actively and communicate vocabulary, concepts, and methods in its risk management program, which will allow functions as diverse as Sales, Facilities, Marketing, Production, Logistics, Finance, and Engineering, to achieve alignment in their approach to their diverse risk management tasks. These functions also need to be able to adjust risk-management calibrations quickly when company circumstances require an adjustment. In order to ensure that this is done in a fashion that accounts for the varying spectrums of risk perceptions, these are discussed regularly. This is explained below.

Managing the inter-dependence between risk perceptions and ERM alignment

Each year managers and selected employees fill in a risk profiling survey. Those individuals reflect a range of working groups, including the

Executive team, the Security team, the Risk Management team, Sales teams, the Board of Directors, and others. An example of a question asked in the survey is:

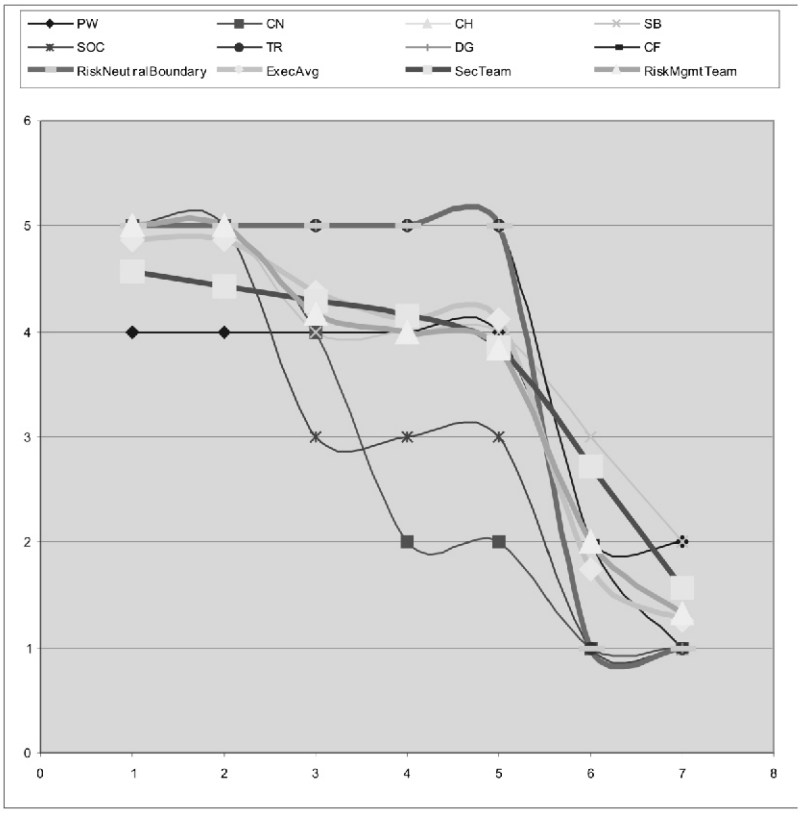

Figure 1: Example results of risk tolerance survey (Initials represent members of the executive team)

"I would accept a business proposition that has n% chance of doubling LeCroy's size, enterprise value, and EPS over a one year period, however it also carries a y% chance of bankrupting the company..", with sets of [n,y] as follows:

[5%;95%], [25%;75%], [45%;55%], [50%;50%], [55%;45%], [75%;25], [95%;5%]

The results for the Executive Team members only are shown in Figure 1, on a 1-5 vertical scale (reflecting responses of strongly agree =1 ; strongly disagree = 5 on the questionnaire). The lighter font traces are individual responses, with the firstname/lastname initials of the respondent. Bolder

traces reflect the locus of key groups of managers and employees, including the security team and risk management team. The arithmetically neutral risk agnostic trace is in orange, and the relative locus of this trace versus the others carries important insight into risk tolerance.

Whilst at first sight the exercise may look like an academic one, results are presented to various stakeholders (Executive Team, Board, Information Security Team and Risk Management Team) the resulting discussions are seen as an important and valuable mechanism to achieve a common understanding, and convergence. Each participant is given insight into their risk perception and tolerance characteristics as well as those of the other members of their work group, and of work groups adjacent in the value chain. Providing this annual reminder of company vocabulary and methodology, is expected to drive enterprise risk management behaviour to converge over time toward alignment. That has been the case each year between the first and second, and second and third, cycles.

Managing the influence of culture on alignment

In discussing risk culture, we have so far highlighted the potential tensions between the low tolerance of customer and employee related risks and the collegiate, knowledge sharing culture. We have also highlighted the high tolerance for market related risks. Further culture-related complexity arises out of the confluence of all these daily risk management activities. Does each actor know what the overall enterprise risk objectives are at the time? Does each actor know the risk management practices of the other actors up and down the value chain to whom they hand off, or from whom they receive workflow?

One supporting action is an annual reminder to all members of the Security and Risk Management teams. An extract is shown in Figure 2.

2.0 Purpose

The purpose of this policy is to foster well-aligned decision-making throughout LeCroy, so that the levels of business risk embodied in the LeCroy information and physical infrastructure are managed to within tolerable limits at the lowest commensurate cost.

...

4.0 Approach

4.1 General

Material risks should be:

o Anticipated: To the greatest extent possible. Responsible teams should periodically brainstorm 'what might go wrong', listing these areas out in writing.

o Evaluated: An estimate, based on the best available data, of the probability of each type of event occurring, and of the likely consequences of that event should it occur, in $$ and where appropriate in injury terms, should be made.

o Considered: Possible mitigations and their costs should be explored, including an analysis of how much risk would remain after mitigation, and what the ROI of the potential mitigation would be.

o Addressed: Risk areas that are above tolerable levels should be continuously addressed to bring overall risk continuously lower. Mitigation actions that offer the highest ROI should be considered most attractive. Each quarter a substantial number of risk mitigation actions must be completed (for FY05 H1 the required minimum number is 20 per quarter).

In general, risk areas with financial consequences are largely in the domain of LeCroy Information Systems Dept., while risk areas with safety consequences are in Facilities.

In general, the criteria for approving a proposed mitigation action, in an area where the risk is expressed in financial terms, is an ROI > 1.

In general, the criteria for approving sets of mitigation action plans, where risks are expressed in safety terms, is the target of continuously reducing the total aggregated seriousness of threat to within acceptable levels, and by at least half each year.

4.2 Tolerable Risk

LeCroy's executive management team offers the following guidance to help you calibrate your risk-related decisions:

- LeCroy wishes to actively anticipate and mitigate risks where such actions are sound business management behaviour (ie ROI >1).
- LeCroy sees itself as lowering pooled risks (ie insurance companies would view us as an attractive customer) due to proactive risk management. LeCroy usually experiences lower than average insurance claims in a variety of areas, and has adjusted its insurance choices accordingly.
- Restating the two bullets above, LeCroy has a low tolerance for controllable risks (ie risks that could be profitably and proactively mitigated).
- LeCroy participates confidently in highly dynamic markets, and as such has a high tolerance for uncontrollable risks. The executive staff rates LeCroy's uncontrollable risk tolerance at 7.5 on a scale where 1 represents a staid organization such as a utility, and 10 represents a high-tech start up. The staff also rates LeCroy's ideal tolerance for uncontrollable risk at 7.5.

Figure 2: Extract from the ERM Annual Reminder

Each year the company conducts a Security Fair for all employees, up to and including the Board of Directors. The fair is comprised of 5 8 booths, including at least one staffed by outside experts in the field. Each employee must take a test and/or sign a declaration at the end, establishing metrics for the company as to the state of “education” of its “human firewall”. The human firewall is a stated part of the overall defence-in-depth strategy, summarized in the Security Mission Statement (see Figure 3) that is posted prominently at the company.

> LeCroy's most important assets are its employees and their knowledge. Protecting our assets preserves a competitive advantage and helps us achieve our goals. Security risks introduced by individuals' decisions affects the entire LeCroy community, including visitors, vendors and customers.
>
> It is the responsibility of everyone at LeCroy to use good judgment to continuously manage security risks in a manner consistent with our business mission and culture. Alongside our security hardware, software and systems, the employees of LeCroy act as a human firewall to reduce the likelihood and extent of loss or harm.

Figure 3: Security Mission Statement

Top management further expresses its commitment to security by sponsoring an annual facilities survey that captures employee concerns about physical safety and security. Investments such as upgraded outdoor lighting, traffic calming schemes, and security cameras have arisen from this process.

Contributions of this research

One reason organizations shy away from attempting to align risk perceptions, is their belief that such perceptions cannot be quantified and compared. The approach presented here, quantifying magnitude of perceived risk in terms of “how much would you spend to halve the risk”, overcomes this obstacle and enables organizations to take the first steps.

The understanding that “survival bets” present a different, non-arithmetic, risk perception profile than “run of the mill bets” to executives, enables alignment in organizations. Without this understanding, adjacent players in the execution chain might apply the usual arithmetic lens to risk management decisions in situations that require special treatment.

The paper has presented a specific and detailed methodology which readers could adapt and apply to a wide variety of organizations in order to elevate enterprise risk management practices.

Limitations of this research and potential for extensions

The case organization chosen had recently completed two acquisitions (Oct. 2004 and Oct. 2006), and integration of acquisitions, each with its own risk

culture, may have introduced effects not typical in a stable continuing organization.

The case organization has an unusually long average length of employee service (LOS). Furthermore, within the span of that average LOS, the case organization was engaged in the high-energy physics research market, one which is highly unusual in that it is centered in military and university settings. These two settings traditionally have highly dissimilar information risk management cultures. Therefore today's LeCroy organization may contain echoes of this earlier atypical confluence of risk cultures.

The case organization is unusual in other aspects that impact information security risk, including:

- a high proportion of revenue derived from non-domestic market sales for a SME
- high intellectual property content (ASICs for data acquisition and oscilloscope operating system)
- Windows-based embedded OS
- remote production (Tokyo and Penang) networks

Further investigation along these lines could be carried out in a larger and more complex organization, where the likelihood of larger discontinuities in risk perception alignment are greater. Such an organization would provide fertile ground for investigating alignment methods which support a greater level of indirection, i.e. more links in the alignment chain.

Investigation over a greater period of time would certainly be more likely to capture effects of special circumstances. For example, how external stresses such as those introduced by the business and economic cycle may impact risk perceptions. Related longer term influences might be detected from sources such as election cycles, currency fluctuations, interest rate changes, and others.

Conclusion

In conclusion, the case study of LeCroy offers an illustration of the effective use of mixed formal and informal ERM culture alignment mechanisms, ranging from committee structures to security fairs, surveys, to spreadsheet tools. The methodology is partly data-driven, partly a qualitative cycle of education and training. An interesting aspect of the methodology is that it encourages discussion to bring about a shared understanding of the appetite for risk of the organization. Recent work on aligning Information Assurance with business strategy (Birchall et al., 2004) has shown that an essential element of alignment is communication between the stakeholders and managers accountable for Information Assurance in the organisation. The case presented here suggests that this communication around risk and risk perceptions can be an important component of ensuring that alignment is achieved. This need for communication is implemented through a variety of mechanisms that encourage alignment (rather than prescribe it).

The case also raises interesting questions about the link between Enterprise Risk Management and other forms of risk management in the company. At LeCroy, three committees have an important risk management function: the Executive Team, the Risk Management Committee and the Information Security Committee. Because the Risk Management Committee and the Information Security Committee are at the same level this raises possibilities of duplication of business between the two committees and accountability. Furthermore, the recommendations of the two committees may potentially overlap. There is therefore the need for coordination between them, as well as appropriate overseeing by the Executive Team. At LeCroy this is achieved by the role of the CIO (who is also a member of the Executive team).

References

Adams, J. (1999), Risk-Benefit Analysis: Who Wants It? Who Needs It? Cost-Benefit Analysis Conference. Yale University.

Adams, J. (2005), "Risk management, it's not rocket science: it's more complicated" (draft paper available from http://www.geog.ucl.ac.uk /~jadams/publish.htm)." (Accessed on 20 January 2005).

Adams, J. and Thompson, M. (2002), Taking account of societal concerns about risk. Framing the problem. London, Health and Safety Executive, Research Report 035.

Ashenden, D. and Ezingeard, J.-N. (2005), The Need for a Sociological Approach to Information Security Risk Management. 4th Annual Security Conference. Las Vegas, Nevada, USA.

Backhouse, J. and Dhillon, G. (1996), "Structures of responsibility and security of information systems." European Journal of Information Systems, 5(1): 2-9.

Baskerville, R. (1991), "Risk analysis: An interpretive feasibility tool in justifying information systems security." European Journal of Information Systems, 1(2): 121-130.

Beck, U. (1992), Risk Society, Sage Publishers, London.

Birchall, D., Ezingeard, J.-N., McFadzean, E., Howlin, N. and Yoxall, D. (2004), Information Assurance: Strategic alignment and competitive advantage, GRIST, London.

CCEVS (2005), Common Criteria - Part 1: Introduction and general model (Draft v3.0, Rev 2), Common Criteria Evaluation and Validation Scheme.

Ciborra, C. (2004), "Digital Technologies and the Duality of Risk." Discussion Paper - Centre for Analysis of Risk and Regulation, London School of Economics, (27).

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: toward socio-organizational perspectives." Information Systems Journal, 11(2): 127-153.

Dhillon, G. and Torkzadeh, G. (2006), "Value-focused assessment of information system security in organizations." Information Systems Journal, 16: 293-314.

Ezingeard, J.-N., McFadzean, E. and Birchall, D. W. (2003), Board of Directors and Information Security: A perception grid. In Parkinson, S. and Stutt, J. (Eds.) British Academy of Management Conference. Harrogate, Paper 222.

Ezingeard, J.-N., McFadzean, E., Howlin, N., Ashenden, D. and Birchall, D. (2004), Mastering alignment: bringing information assurance and corporate strategy together. European and Mediterranean Conference on Information Systems. Carthage.

Gietzmann, M. B. and Selby, M. J. P. (1994), "Assessment of Innovative Software Technology: Developing an End-User-Initiated Interface Design Strategy." Technology Analysis & Strategic Management, 6(4): 473-483.

Hirsch, C. (2005), Do not ship Trojan Horses. In Dowland, P., Furnell, S. and

Thuraisingham, B. (Eds.) Security Management, Integrity, and Internal Control in Information Systems. Fairfax, VA, Springer.

Hussin, H., King, M. and Cragg, P. (2002), "IT alignment in small firms." European Journal of Information Systems, 11(2): 108-127.

ISO (2005), ISO/IEC 27001:2005(E) Information technology - Security techniques - Information security management systems - Requirements. BSI, London.

ITGI (2003), IT Control Objectives for Sarbanes-Oxley. Rolling Meadows - IL, Information Technology Governance Institute.

ITGI (2005), COBIT 4.0: Control Objectives and Management Guidelines, Information Technology Governance Institute, Rolling Meadows - IL.

Jahner, S. and Krcmar, H. (2005), Beyond Technical Aspects of Information Security: Risk Culture as a Success Factor for IT Risk Management. Americas Conference on Information Systems.

Loch, K. D., Carr, H. H. and Warkentin, M. E. (1992), "Threats to Information Systems: Today's Reality, Yesterday's Understanding." MIS Quarterly, 16(2): 173-186.

McFadzean, E., Ezingeard, J.-N. and Birchall, D. (2004), Anchoring Information Security Governance Research. In Dhillon, G. and Furnell, S. (Eds.) Third Security Conference. Las Vegas, Nevada, USA.

Oshri, I., Kotlarsky, J. and Hirsch, C. (2005), Security in Networkable Windows-based Operating System Devices. In Dhillon, G., de Sá-Soares, F. and Hu, Q. (Eds.) Softwars 2005 - Issues in protecting intangible organizational assets. The Information Institute, Washington DC, USA.

OST (2004), Cyber Trust and Crime Prevention. London, Office of Science & Technology - UK Department of Trade and Industry.

Peters, T. J. and Waterman, R. H. (1982), In Search Of Excellence: Lessons From America's Best Run Companies, Harper and Row, New York.

Reich, B. H. and Benbasat, I. (1996), "Measuring the Linkage Between Business and Information Technology Objectives." MIS Quarterly, 20(1): 55-81.

Reich, B. H. and Benbasat, I. (2000), "Factors that Influence the Social Dimension of Alignment Between Business and Information Technology Objectives." MIS Quarterly, 24(1): 81-113.

Turnbull, N. (1999), Internal Control: Guidance for Directors on the Combined Code: The Turnbull Report. London, The Institute of Chartered Accountants in England & Wales.

Venkatraman, N. and Camillus, J. C. (1984), "Exploring the Concept of 'Fit' in Strategic Management." Academy of Management Review, 9(3): 513-525.

Whitman, M. E. and Mattord, H. J. (2003) Principles of information security, Thomson Course Technology, Boston, Mass.; London.

Willcocks, L., and Margetts, H. (1994), "Risk assessment and information systems." European Journal of Information Systems, 3(2): 127-138.

Author Biographies

Corey Hirsch is CIO of LeCroy Corporation, a leading supplier of oscilloscopes, protocol analyzers, and other test and measurement equipment, located in Chestnut Ridge, New York. He also serves as a Lecturer at Columbia University in New York City, and as a Visiting Executive Fellow at Henley Management College in Henley, UK, providing leadership in the areas of CRM and Competitor Intelligence. His research is focused on Information Security,

Enterprise Risk Management, and Global System deployment. His work has been recently published in book chapter form (Decoy Effect and Mobile Communications Technology Combine to Empower Underdog Sales Force, in *Inside the Minds: Aligning Technology with Business Objectives,* Aspatore Books, and Aligning IT Teams' Risk Management to Business Requirements, in *Social and Human Elements of Information Security : Emerging Trends and Countermeasures,* by Hirsch C. and Ezingeard J.N., Editors Manish Gupta and Raj Sharman) and in journals (IEEE Security & Privacy, September 2007 and October 2007; Computers and Security, Volume 26, 2007), and conference proceedings (Softwars 2005 and 2006).

Jean-Noël Ezingeard is Dean of the Faculty of Business and Law at Kingston University (London). His research is focused on Information Assurance, Information Security and Enterprise Risk Management, topics which he has researched, taught and consulted about in Europe, North America and South Africa. His work on Information Assurance has been used in publications by QinetiQ, Axa, and the Federation against Software Theft. He is a founding member of the British Computer Society's Information Assurance working group. He joined the Business School world 9 years ago. Prior to this he worked as a Chartered Manufacturing Engineer (Operations Management) and a Lecturer in Computer Integrated Manufacturing.