2010

# Integrating modern business methodologies and behavior factors to better apply information technology security practices within the organization

Brian Matthew Edwards
*Iowa State University*

# Integrating modern business methodologies and behavior factors to better apply information technology security practices within the organization

by

**Brian Matthew Edwards**

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTERS OF SCIENCE

Major: Information Assurance

Program of Study Committee:
Doug W. Jacobson, Major Professor
Yong Guan
Sreevastal Nilakanta

Iowa State University

Ames, Iowa

2010

# TABLE OF CONTENTS

# ABSTRACT

Often in today's business environments, data collected through great care and effort never transforms into actionable information and intelligence because organizations lack the tools or skills to apply modern practices. Too many well developed tools exist but are overlooked. Too many projects fail to account for their organization's social and cultural attributes. The result is information being discarded because it cannot be effectively leveraged.

This work examines a collection of business tools and technologies, goals, and behaviors in the context of how they affect information security policy and programs within the business.

# CHAPTER 1. INTRODUCTION

***Scenario 1***

Consulting an organization to decide on appropriate level of contingency planning

ACME Corporation's 1300 employees hardly consider themselves a large business. Their culture still carries many tendencies of their founding team despite three years of rapid growth and a recent merger which then doubled their size. As a growing company, ACME executives have focused on controlling costs and meeting the most basic demands of developing their core services and providing them to their customers. However, an internal outage last week left the company without email for two days. Customers are also becoming more savvy in their sales questions and want to know how ACME is protecting their records and assuring availability. These issues highlight the need for the company to review their critical data processing infrastructure and align it with the needs of a bigger enterprise.

***Scenario 2***

Developing a security policy for internal / COTS application

At B&L Company, an effort is underway to improve the security of applications which are used company wide. This includes many internally developed tools and off-the-shelf software suites - some of which are quite complex. Under this program senior management aims to better control the quality of custom applications and understand the security position of their purchased software. With luck, the improved

visibility and depth of coverage in these security policies will lead to performance improvements and opportunities for more efficient infrastructure investment.

### *An Unlevel Playing Field*

Security vulnerabilities in software systems could be viewed in economic terms as negative externalities. Whether introduced during coding, from insecure architectures, or through some other vector, bugs that challenge intended functionality or enable attackers typically are not part of the original statement of work. In this context, the software vendors consumed labor and operational resources to create their software products with an expected set of features. Eventually unintended functionality which could compromises the system's confidentiality, integrity, or availability comes to light. In this situation not only is an unplanned cost introduced, but the problem needs to be mitigated at the most effort intensive phase of its lifecycle. It also damages the developers' credibility hurting future revenue. Such issues are pervasive in the software industry and represent a systemic problem.

No single factor is responsible for the present state of information technology security. Indeed, it is a very complex ecosystem. Over the past decade an unprecedented number of organizations have begun taking information security very seriously. For too many others it is still an enigma, a luxury that only big companies can afford, or a distant threat that seems as though it could never happen to them.

Although some facets of this domain are very new, many are as old as the information age itself. On a daily basis research uncovers better methods, more

efficient or robust algorithms, and alternative ways to apply technology to protect information assets. Meanwhile we still struggle with decades' old problems of managing the availability, accuracy, access to the data that drives the organizations efforts. Social forces such as politics, greed, entertainment, and curiosity play a significant role in the equation and are not even based in technical realms. The disparity of organizations adopting security practices and contributing forces is further compounded by the pace of change within information technology.

Even with industry wide improvements in software development practices, today's data security problems aren't going to disappear on their own. If the present state of data security was able to efficiently realize the costs of poor security, organizations would be on a natural path to fixing bugs early and design in sound security principles from the start. More often it follows a pattern of near term benefit with a delayed penalty. Much like an addictive drug, this model provides a poor incentive structure towards solution.

Interestingly, a concept borrowed from the world of public policy analysis shares some core correlations. Bardach summarizes key properties of market failure for a good or service as:

- Making it hard to collect payment from all the potential beneficiaries
- Making it hard to collect from the beneficiaries of consumption the true economic cost of making use for the good or service
- Making it hard for consumers to know the true qualities of the goods or service they are acquiring (Bardach 2009, p3)

Often times, market failure is used to rationalize a governing regulation, incentive, or policy to try to offset difficult to manage condition. These market failure properties apply well to the economics of software security vulnerabilities. Because damages of poor security occur throughout a system's use and can vary widely in value, the true economic impact is infeasible to calculate. Individuals whose data are being handled are rarely in the position to fund security efforts directly. Relatively simple software products are too complex for consumers to truly understand. Even when applications make their source code available, their workings are far from transparent without substantial analysis effort.

***Problem Statement***

Problems that arise from overlooking modern business tools and methodologies affect the quality and soundness of organizational data security decisions. This frequently leads to unrecognized or under-appreciated risks to information assets and costs which are unplanned or fail to deliver on their intended benefit. It can allow an organization to believe that it is in a dramatically different strategic posture than it truly is. Organizations may also be hurt through missed opportunities to deliver better goods or services and to mitigate information vulnerabilities early.

A solution would better equip decision makers with the right data and methods to manage data security consistently and efficiently in the unique context of their own organization.

***Literature Review***

This work focuses on the convergence of business processes and tools, information technology management, and data security. Each of which is a very active field with ongoing research and its own overwhelming volume of publications. A brief search limited to just this year's publications indexed in the EBSCO Academic Search Elite database returns over a thousand hits for "business process" and "business tool" as of October 2010. The phrase "information technology management" found 994 articles. Together, "data security" and "information security" matched nearly another two thousand hits. Industry wide, each of these domains is more heavily published than an individual could possibly keep up with.

Other research in the disciplines of project management, policy administration, risk analysis, management information systems, and others has explored many facets of these topics extensively. However my contribution aims to bridge some of their best practices into applied organizational data security cases. It would be infeasible to try to cover the full spectrum of modern business tools and methodologies, much less enumerate them within a security context. So the following will focus on a narrow selection of decision making, risk, and performance management tools. This selective review will include many recently formalized models, as well as some well established methods.

***Methodology***

This paper's framework starts with an introduction to some key organizational goals, information security challenges, and technologies which affect any business operating in the digital age. From there, a number of business tools are described and discussed in comparison and how they can be applied to data security topics. It covers basic decision making methods ranging from simple and cost based methods to more dynamic and subjective analysis. With risk management it addresses challenges of identifying what to manage and how to assure the right amount of effort is applied to this phase. Performance measurement is addressed for tangible criteria and 'non-measurable' abstract aspects. Finally, some aspects of how human and organizational behavior impact rational methodologies are highlighted.

In bridging business and information security challenges and tools, this work is unique in its scope and applied approach. Key objectives are to raise awareness of the range of business management tools currently available and demonstrate their applicability within the security domain. The outcome of which is to enable security professionals to more optimally and comprehensively address the operational needs of businesses.

***Business Goals***

At the most basic dimension, businesses are formed as tools designed for generating profit. However, this simplified model falls short of recognizing the goals which will determine a business's success. Though start-ups and established

corporations are driven by individuals or boards in pursuit of wealth or prestige - real motivation is more abstract. In addition to the quest for an ideal profit margin, and sometimes even independent of profit, real world businesses exist as tools for solving real world problems.

Just as individual motivation thrives on factors other than money, organizations become energized through chasing common dreams, achievement, and institutional growth. For businesses that operates using any meaningful form of information, information security plays a number of enabling roles. No matter what the company produces as goods or services, staying in business means having access to an array of information artifacts.

Some artifacts, such as publications and information based products, have value outside the company. Others, like trade secrets, may need to be kept hidden for the company to remain viable. A loss or compromise of integrity to records of internal value, like customer contacts and transaction histories, would certainly hurt the organization's productivity as it expends effort to recover. By taking steps to protect these information assets from loss and having a plan in place for managing information security events, companies can better protect their core purpose.

Information security mechanisms may even offer opportunities to enhance the company's goods and / or services. In software development, undiscovered bugs are a frequent cause of both functional defects and security vulnerabilities. Developers may end up with more reliable software by improving code review standards for security. Designing an enterprise IT infrastructure with security principles in mind should lead to reduced downtime. Implementing an information system with robust

capabilities for handling different levels of access based on roles could even allow customers or business partners to have access to limited internal information. In these ways, information security could be used to improve or create new marketable competencies.

Similarly, internal operational procedures can benefit by adopting common and unified practices. Risk assessment emerges in many different efforts throughout an organization. If the assessment methods are kept fundamentally the same for managing project, financial, staffing, data security, and other business risks, the employee training and applied risk assessment exercises in separate efforts will strengthen practices throughout the company. Finally, developing a corporate culture that recognizes common practices and well defined policies which support core business goals will reflect the organization and ethical focus of the company.

# CHAPTER 2. ORGANIZATIONAL INFORMATION SECURITY CHALLENGES

Struggling with even the fundamentals of data security is common for organizations of all sizes. In small companies or independent business units, trained expertise is typically absent and efforts are ad-hoc, when they emerge at all. Larger organizations face many of the same difficulties plus the complications of unequally distributed talent and more complex data processing systems. This section will focus on challenges specific to classifying operational data, monitoring information systems, and aligning requirements to business goals.

The basis for data classification could be regulatory or voluntarily driven. Customer oriented data privacy laws are becoming more commonplace. Financial, government, and health industries, as well as anyone who handles credit card processing, are subject to ever growing sets of legal mandates. Non-public data may need to be restricted internally to prevent insider trading, limit its circulation, manage legitimate access, or any number of reasons. Yet classifying data poses some fundamental problems.

### *Data Classification*

Some types of organizations, particularly in financial industries, are expected to enforce separation of duties. In a software development setting, this principle could emerge through developers, testers, and system administrators each having non-overlapping staff roles and reporting to different managers. More often though, the same individuals are responsible for developing, validating, implementing, and

supporting data management systems. Even if multiple roles are involved, quality assurance or peer reviewers would likely not have the resources to really understand many details of a system's data, users, and potential for unintended exposure. In-depth expertise of any given system is typically limited to fewer than a handful of individuals, distributed throughout one or more teams, or only available through third party support channels. When is comes to finding out if an information system contains sensitive data, there may not be a credible separate or independent party available.

Classifying data is subject to two different dimensions of consistency. The same data, when viewed by two different people, could be identified as meeting or not meeting the category's requirements. A common example of this is personally identifiable information - while a report keyed from customer numbers may not directly map to individuals, if the customer number mapping is available through another channel the customer data becomes transparent. Secondly the data itself may cover similar content, but inconsistent business rules could lead to inconsistent classification. For instance in a human resources department it may be common practice to post names and employee numbers together freely on internal reports. In another operational department the employee number could serve as a private login credential which is not to be shared. Here, the different classification of employee numbers could enable someone passing through HR to improperly use someone else's account to access internal systems.

Social or political pressures can also work against the proper classification of data because there is typically a measure of cost and effort associated with more

restrictive levels. When faced with an effort to figure out if a system is storing any sensitive customer data, management might be initially biased towards confirming that is does not. Or knowing that other projects would need to be cut to enable remedial security efforts, they may review the system less thoroughly or even act unethically and report that it has no sensitive information. In some situations a decision maker might mistakenly or naively assert incorrect system attributes. Imagine a sales consultant working to close a deal with an important client - when asked whether their solution has the security mechanisms in place to handle payment card sales transactions, the consultant's answer may differ from the developers.

***Monitoring***

Monitoring information processing systems is another key facet of managing data security which is notoriously error prone. Similar to data classification, it is prone to political pressures. It also falls victim to difficulties stemming from funding, assumptions, configuration, and constantly shifting targets.

Human nature doesn't tend to favor bad news. It spreads virally throughout an organization leaving a trail of half true permutations and assumed causes and consequences. Often the social fallout takes longer to return to normal than the original issue itself. It is no wonder that data security incidents face a natural tendency to be addressed quietly and swept under the rug. Internally, raising the awareness of a data breach or ongoing critical vulnerability can be career limiting if it results in individuals getting blamed. A best-case response would be for

management to realize the incident as an opportunity to improve internal processes. External customers and business partners also tend to hold a negative stigma against organizations associated with reported data security incidents. Acting ethically and responsibly disclosing findings or incidents publicly can lead to significant costs and losses.

The first phase of many incident response plans involves identifying or detecting that an incident may have occurred. Effective monitoring is necessary trigger the well designed workflows that aim to keep operations running. Unfortunately it involves the continued effort of staff with very specialized knowledge. Manually reviewing logs is time consuming, tedious, and with luck, unlikely to turn up any problems. As such, this task tends to get offloaded to junior team members or overlooked entirely as budgets look for efficiency and people get busy. Monitoring logs, configurations, access rights, and functional parameters is prime territory for automation. Automation, however, can only evaluate known cases and it is impossible to account for all situations that will show up in real use. This can leave an organization placing too much reliance on automated monitoring facilities and not realizing the system's limitations for detection.

Modern information technology infrastructures frequently involve the services of multiple third party companies and complex tool sets. Ideally, these relationships would bring economy of scale for highly specialized business needs. In practice they also introduce opportunities for miscommunacation and lax accountability. If maintenance activities are managed by an outside group, the maintainers won't necessary have accounted for important details of data processing systems. With

incomplete information, automated monitoring could be set up for a system's web server and database, but miss a separate application log although thinking that the system is fully managed.

Relying on outside providers can also introduce maintenance support incompatibilities that impact efficient or comprehensive monitoring and detection. Third party maintainers may be relying on out of date tools, or tools which only work with a subset of the technologies deployed. Configuration and log monitoring tools require substantial customization to be optimized for a given environment. If the tools are deployed without the appropriate planning, expertise, or level of detail applied, they will not be able to deliver a suitable level of assurance to alert support staff to important issues. Furthermore, as data processing systems are upgraded, extended, and replaced, systems designed to monitor them also need modified to address their changing behavior. Without regular effort to keep synchronized, monitoring systems may discover that their target profile is no longer accurate.

***Requirements***

The last class of organizational challenges covered here focuses on divining, dissimulating, or dealing with information security requirements. In one recent article the author highlights how the differences of perceived and actual risks plays into cloud based information services. (Gardner 2010) An organization's blindness to application vulnerabilities becomes especially problematic when they can no longer apply traditional mechanisms to secure their virtual parameters.

Many information systems that support business operations are the result of years of organic growth. Even major commercial systems commonly are composed of bits and pieces of applications which have been assembled over time to deliver certain functionality. Security principles and their effective implementation vary widely among applications and systems - the organization may expect a much higher level of security capability than a tool was designed for. Another variation of this same challenge pertains to internally grown databases and applications. Well intended and technically savvy staff often develop tools to improve departmental productivity without understanding or addressing the security implications.

Even full time developers face challenges applying security principles. Security design and configuration items can be extremely detail oriented. Tying the detailed elements to high level requirements is necessary for coherent traceability. But if high level requirements do not address security designed in from the beginning, effort may never get allocated for flushing out security details. Alternately, a design may have high level security requirements defined but suffer from inconsistently implemented or interpreted detailed design specifications. A development framework helps to assure that requirements are reviewed and common standards get applied. But even in organizations with rigorous development lifecycle management it is common for some software to be created outside of that framework - typically just for one-off use, prototypes, or developer tools. Of course, if these applications work well, they get widely used and soon become mission critical.

Legacy systems can be the most cost prohibitive to retool to meet modern data security needs. With small organizations or highly competitive industries this can be

particularly problematic as investing in a secure solution puts the company in an uncompetitive position. For a company that has transitioned to mandating high assurance for data security, making even minor modifications to legacy systems can uncover preexisting security problems which suddenly become high-priority findings.

One final way that information security requirements can affect organizations is in the selection of mitigation mechanisms. Specifically, if the company doesn't know what their data security needs are they may invest in tools, technology, and infrastructure that does nothing to improve their security posture. In this manner, the risk is unnecessary expending resources. Perhaps even leaving important vulnerabilities unmitigated.

# CHAPTER 3. BUSINESS TOOLS AND TECHNOLOGY

## *Business Technology*

Human cultures have developed any number of techniques to facilitate barter and commerce over the past ten thousand years or so. From the invention of the wheel and continuing discoveries through sail, steam, electric, and combustion powered transportation, improvements have extended the range, speed, capacity, safety, and efficiency of of moving goods. Our spoken and written languages grew, in part, to support property ownership, contracts, and enable transactions.

More advanced principles emerged over time leading to progressively more robust standards for accounting and dispute resolution. Through economics, we have learned ways to more accurately model how resources are valued, exchanged, and consumed. Investment is understood to have more than a zero sum potential. When two or more parties contribute jointly to an effort, they can achieve better results than if any single party had tried alone. With industrialization, society has found far greater capacity at producing goods and services through specialization.

The modern business technology landscape pulls every possible domain of knowledge in complex and interrelated ways. After thousands of years of refinements we can now perform incredibly precise calculations quickly and communicate practically anywhere at near instant speeds. Complex projects ranging from coding to construction can be effectively analyzed for feasibility and successfully coordinate among many independent groups, often spread across the globe. Financial and transactional records can be retained perpetually and accessed from from many places at once. Many barriers to conducting business that were

substantial even a generation ago have been made insignificant, or at least possible through technologies applied to business.

### *Business Tools*

Techniques and tools which are particularly applicable to information security are the focus of the next few sections. These are pulled from diverse bodies of knowledge and represent only a subset of the tools available. Here, several facets of performance measurement, risk management, and decision making concepts are described and analyzed as applied in an information security context.

### *Performance Measurement*

Information processing systems can be very difficult to describe in terms of organizational performance. They tend to have an abundance of functional metrics such as processing or storage capacity, number of transactions handled, and uptime. But these attributes do not directly translate to operational or strategic business value. Devices and practices intended to introduce or enhance information security mechanisms often suffer from a similar deficiency of meaningful measures.

In "Measuring the Value of Metrics" (Thurman, 2006), an IT security manager recounts his team's efforts in selecting just a handful of metrics for senior management. After discarding the previous manager's reporting methodology, his team choose to focus on the percentage of corporate workstations that meet the current Trend Micro and Microsoft SMS managed policies. Reporting from their IDS

was also provided - with the caveat that only an estimated 40% of their network was being monitored. This information, along with the more concrete measures like the number of tickets closed, was selected to support their overall security posture. It also expresses results in a manner that can be tracked over time and compared for further trend analysis.

Two general classes of measurements exist - a metric can be either tangible or abstract. As Thruman's experience illustrates, there are many potentially valid ways to describe an organization's effort and progress. Here, we will cover several specific methods of tangible and abstract measures that may apply to evaluating the performance of information security mechanisms and policies.

The most easily compared metrics tend to have precise and quantitative results. While there are certain applications which warrant advanced statistics or complex mathematical modeling, simple metrics are almost always a better choice. By applying the least complicated method of describing an attribute, the method and its result will be more transparently understood by a wider audience. Their is also less potential for human error in calculating or interpreting these results.

Counting is just about the simplest metric and it is very tangible. Alone or combined with a unit of time, it can be applied in a wide variety of security related measurements. How often does Alice log in to the reporting system? How many alarm conditions are being detected per hour? Which workstation has the most MP3 files? It applies meaningfully to the number of transactions that succeed or fail, or the number of issues reported and closed. As long as the context is well defined, simple counting is very repeatable.

Coverage is a natural extension of counting - by having a list of expected results and a list of observed results, the amount of overlapping elements are counted and expressed as a percentage of the ideal list. This class of metrics is discussed in in depth in Elizabeth Nichols's Beautiful Security Metrics chapter in Beautiful Security (Oram & Viega, 2009). There, she cites four coverage examples as they could have been used to detect an insider's abuse of information systems. She lists:

- Percentage of applications or basic services ... whose access is managed by an authoritative system
- Percentage of login accounts that are explicitly linked to a valid employee
- Percentage of accounts or of employees whose access and entitlements are formally reviewed at least once a year
- Percentage of group overlap (Oram & Viega, 2009, p46)

By phrasing the target of coverage as a topic based in business rules and policy, these examples are well suited to highlight visible cases where the potential for abuse is high.

Time related metrics can be especially useful for tracking availability, incident detection, response, and resolution efforts. Uptime, both as perceived by an information system and by those using the system is an important part of user satisfaction and service level agreements. By regularly tracking the timing attributes of systems, support staff can get insight in to impending capacity limitations or more readily detect that something has changed and investigate the cause of an otherwise unknown event.

In contrast to tangible metrics, abstract ones are imprecise and assume a degree of uncertainty. However, they are no less significant than more concrete measures. With the right questions, abstract metrics can improve the manageability of unmeasurable systems and policies.

Starting with a simple question such as, "How good is your organization's data security?" any nominal response (poor, excellent, even 'I don't know') produces some amount of information that can be applied towards an objective assessment. In a variety of domains, customer service is typically evaluated through targeted surveys. Customer service is a concept that is about as unmeasurable as they come - the same interaction could be perceived very differently by different customers and many external factors influence the experience. Yet through the lens of a large number of independent surveys, a reasonably accurate depiction can be found.

Spending can also tell a lot about performance in certain cases. Even if no other measurements are being tracked, following the money can help detect what is working, or what isn't being invested in. For instance, if their is a sudden increase in spending to maintain system patches or handle workstation security incidents, the situation probably warrants deeper investigation. Alternately, if no dollars are being allocated to security projects or training, there is a better than average chance that those activities are not occurring.

Another method described in Beautiful Security Metrics deals with inferring whether introducing some treatment to a process causes a statistically significant change to some measurable attribute (Oram & Viega, 2009). For instance, assume that a new password policy is to be published with a goal of reducing support calls to

reset login credentials. First a baseline of support call metrics would be collected. The policy would be published, advertised, and given an opportunity to show some effect. Then another set of support call metrics would be evaluated to determine if it has changed significantly from the baseline. If other environmental influences are accounted for and their is still a change, the data supports that it may be due to the policy change.

Other inferential sources which may offer alternate indications of performance include written policies, procedures, other internal documentation, and system logs. The organization's adopted policies and procedures are a reflection of their values as well as issues which are of high concern or may have come up before. Well planned and operated groups tend to demonstrate good organization throughout their companies. If policies are incoherent, missing, outdated, or not specifically tailored to the organization that is using them, it may indicate that they do not put much effort into the business's upkeep. Such good or poor organization can show up in project and design documents, or even in system log review and management efforts.

When considering the merit of abstract of tangible measurement criteria, it is important to choose attributes that can be matched up with business interests. For any measurement to be valuable it should be reliable repeatable to get results within an acceptable variance. The method of collecting data or performing the measurements tasks should also follow a consistent process for the results to be comparable over time. Often, a member of the same group is responsible for collecting and publishing the performance metrics. As they may not be able or willing

to represent unbiased data, independent audits should be considered depending on the criticality of information. Finally, any metric that is used for making business decisions should be used with a good background of the origin and limits of the data set. If the metrics do not provide a logical foundation for the decision that they support, different data might need to be explored.

### *Risk Management*

Risk is central to many aspects of an organization's operation, but it holds an inseparable relationship with security. For our purposes, risk can be generally defined as a potential for loss. In contrast, information security aims to regulate potential losses related to information and data processing assets. Managing risk is a process which is often highly individualized to the needs of an organization. Even when adopting a generic risk management framework, the company's tacit interpretations, internal culture, and unique operating environment affect their process.

In risk-informed Decision Making, the authors trace the origin of risk to ancient maritime challenges. They discuss the nature of risk as an effort to answer the questions of, "What can go wrong? How likely is it? What are the outcomes or consequences if it occurs?" (Ayyub, Prassinos, & Etherton, 2010) Their work presents a model for evaluating probability and impact of consequences as dimensions to reduce failures in mechanical systems.

Another study touts the benefits of their new framework in managing risk for records management settings. By their method, risks are first categorized as natural

events, human activities, or technical risks. Probability and impact are assigned through the use of a survey to determine weights and priorities for each identified risk. Interestingly, this study noted in closing that their participants were aware of general risk management methods but often did not have any resources budgeted for risk management activities (Soon-Jae & Hye-Kyung, 2008).

Whether the measure of frequency is once in 100 years or one in 100,000 units and the likely outcome is rated in hours of effort or fatalities and long-term environmental impact, these two approaches to risk management targeting very different audiences are fundamentally the same. Variations of these same risk models abound for information security problems ranging from small projects to elements of enterprise wide development lifecycle methodologies. Even so, organizations generally have a hard time doing risk analysis exercises well. These next few paragraphs address specific topics which often undermine effectively managing risk.

How can you keep something safe if you don't know what it is? Identifying what to protect seems like a first logical step in developing a protection strategy. However this basic activity often overlooked entirely or only fully realized late in the effort. Accurately describing the nature of digital assets can be challenging because many different roles need to reach a common understanding of it. Business analysts may know the value of certain data, but not its technical attributes or the capabilities of the systems that use it. Operational staff might be the best to define who needs access to what data to keep customers happy. Developers have the best insight of what is really in any given data set. Sometimes extensive and focused discussion is

needed to realize sensitive data which could expose the company to financial loss is being published to operators who don't even want to see it.

While failing to accurately describing assets is a sin of omission, identifying threats is challenging in different ways. Threats can be misidentified through ineffective templates, irrational bias or optimism, or simply by being evaluated by the wrong group. Fires, floods, earthquakes, and power outages are all well documented events, but many data security threats change over time. If a business is well enough organized to have a standard reference of common data security threats, they could easily end up missing threats that are not on their common list or spend time unnecessarily evaluating threats which truly don't apply. Going online and adopting the first threat template that shows up in a search may also lead to a poor threat analysis. Often individuals will intuitively perceive the potential of threats without any real basis. While this may be well intentioned, it could result in designing robust protection against data leakage but leaving data backups untested and unrecoverable. In other cases, real and valid threats may end up being dismissed as improbable. Finally, not all professionals have the appropriate background for evaluating information threats. A Corporate Finance Officer would probably do a poor job of accurately assessing threats to information processing systems because his or her expertise is biased differently.

***Decision Making***

Ultimately, after taking the effort to collect data and analyze performance and risk considerations, an organization's goal is to apply that information towards making better decisions. Often times the accumulated information doesn't get effectively managed to enable optimal choices. This section discusses several methods of modeling the available information and using it to form a sound basis for decisions.

Cost Benefit analysis can be used to determine if a process change is worth implementing or a risk mitigation effort will likely save money. In its simplest form, an project evaluator adds up the expected costs for one total and the anticipated benefits for a second total. If the project costs more than the benefit that it is planned to deliver, the data does not support pursuing that solution.

Often times, a project's benefit is only realized over time - a Cost Benefit analysis can be revised to take periods of time into account. In figuring the Payback Period, both benefits and costs may be expressed in terms of dollars per year, quarter, month, or other relevant time frame. As an illustration, consider a company looking in to spending $50,000 on a centralized enterprise authentication system when they anticipates that it will save $10,000 a month in improved productivity and reduced support calls. Payback Period is calculated simply by dividing the total cost by the total benefit per period. For this case, at five months the monthly savings will have broken even with the initial expense of the system.

When comparing several potential systems, tools, or mitigation activities to direct resources to, their relative values can often be expressed in terms of a Return on Investment. This value is calculated by starting with a project's expected total benefit

and subtracting its total cost. This result is then divided by the total cost to get a percentage return on the investment. From this metric, the option with the greatest return can be easily identified. However, note that the largest percentage return may not necessarily reflect the biggest cost return.

Cost benefit, payback period, and return on investment valuations get more complicated if the time involved increases. For short term calculations, cases where the time involved is one year or less, changes in the value of money over time can usually be ignored. With longer time ranges and large dollar amounts, calculations should account for the time-value of money too. Typically this involves adjusting future dollar values to present value estimates.

To calculate the present value of a monetary amount, you will need to make an assumption about an interest rate to use for comparison. The actual factors to consider in picking an interest rate depend heavily on specific situations and will not be covered in depth here. The following example follows the same notation as in the MindTools.com "Net Present Value (NPV) & Internal Rate of Return (IRR)" reference (mindtools.com). Starting with a future dollar amount and an interest rate, the present value is calculated as follows.

$$\text{Present Value (PV)} = C_t / (1+r)^t$$

Where $C_t$ is a dollar amount in t future periods, r is the interest rate, and t is the number of future periods.

Applied to an example, a system that costs $45,000 now and will result in saving $10,000 a year for five years could be valued as follows.

| | |
|---|---|
| Initial Cost | ($45,000) |
| Present value of first year savings: | $9,708.74 |
| Present value of second year savings: | $9,425.96 |
| Present value of third year savings: | $9,151.42 |
| Present value of fourth year savings: | $8,884.87 |
| Present value of fifth year savings: | $8,626.09 |
| Total Present Value Savings | $45,797.07 |

Here, a decision which may have intuitively appeared favorable by $5000 at five years has a much smaller time adjusted benefit. With only a slight change in the assumed interest rate, this investment would perform at a loss.

More advanced decision making models can be applied to situations where uncertain outcomes or individual preference are important criteria. Diagramming a strategic question structured as a decision tree visually maps out the evaluated options. Starting with a root question, first level branches are drawn for each broad class of solution. Next, each first level node is considered and child branches are developed enumerating each variation. This process is repeated until the evaluator is comfortable with the depth of the decision tree. After the tree is created, likely outcomes for each branch are added and assigned a probability based on previous data or best guess. By calculating the relative value for each outcome node of the tree, the evaluator can choose the best valued solution based on the available information.

Grid analysis excels in cases where an ideal solution would meet several attributes. The evaluator's preferences are reflected in the weights assigned to each evaluation criteria - this method would correctly generate different outcomes for evaluators with different interests. A new column is placed for each factor being considered and each option is assigned a row. Next, the evaluator decides on how well each factor is satisfied by each solution - often the cell scores 0 if the factor is not satisfied and would range up to 5 for a very good match. By adding up the total scores for each solution row, the largest total identifies the best overall match for that set of factors.

Often, the choices of others have a very real impact on the outcomes of your own decisions. Game theory concepts can be applied to strategic business decisions in efforts to model the best course of action for others and understand how they may respond to your own choices. Two main game models are typically considered. In simultaneous move games, all players disclose their decisions at the same time. Otherwise players take turns considering and exercising their choices in sequential move games. To evaluate a simultaneous game scenario, a table is constructed depicting all possible options for each player. Then the likely payoffs are figured for each player at each outcome. Analyzing the results of this table can provide insight into what choices do or do not make sense for both players. Outcomes for sequential games are better mapped to trees identifying the possible choices for each player at each turn. Due to the complexity of applying this method to real life situations, the goal is often just to evaluate the next three or four likely moves. Most often, this is already a deeper strategic foresight than the other player is considering.

Borrowing another formalized method from financial domains, real options analysis offers a framework for assigning present value to future potential choices. As described on Wikipedia, "A real option itself, is the right - but not the obligation - to undertake some business decision; typically the option to make, abandon, expand, or contract a capital investment." (Real options valuation)

One common thread through these diverse decision models is that the perceived benefits of security policies, controls, and risk mitigations have a large effect on the decision model outcome. Even a small change in assumptions can lead to substantially different results. There continues to be a growing body of documented security incidents, but the data is still too sparse and unreliable to draw meaningful projections from. Applying historical data to current information security systems faces challenges from changing technological and legal environments too. With more regulations going into effect and constantly evolving software and threats, data from an incident only months ago may not be a valid source for predicting potential losses.

Unfortunately, even the cost of a solution is not likely to be known accurately. One author prominently identifies a common software sales trend of offering a low initial price tag for a solution but having high support and maintenance costs (Pendergraft & Blakely, 2010). A total cost for a security device or management system may need to include licensing, training, implementation, and ongoing support.

# CHAPTER 4 INDIVIDUAL & ORGANIZATIONAL BEHAVIOR

## *Individual and Organizational Behavior*

One of the most fascinating works reviewed while creating this paper is a case study dealing with implementing a performance measurement methodology at a bank. That paper, published in 1988, discusses efforts at the bank over a period of five years. Many of their technical challenges are still applicable today - some even more so as the expectations for service level agreements have become stricter. But the article is more remarkable in the frequency of times that it alludes to changes in the organizational culture. Their framework for service level agreements was created so that for the services to be provided, responsible individuals from the departments providing and consuming the service needed to be identified and work out the agreement details together. This provided increased responsibility for the resource consumer and promoted communication. Then upon realizing the benefit of the business relationship, users gained confidence in the process and measurement efforts. One of the study's key observations was that for the process to be successful, not only does it need strong senior management buy-in, but the organization needs to go through the effort of learning the process on their own (Singleton, Mclean, & Altman, 1988).

Not all business tools are appropriate for any given situation, similarly, not all business tools may be a good fit for a specific organization, or even an individual. For decisions which are strongly influenced by political pressures, adopting an analytical decision model could be ineffective. If the CEO has decided that the company needs to have more firewalls, or a high profile customer only wants to get

their reports over a certain vendor's VPN client and encrypted with a specific program, other requirements and processes may need to yield. Even determining an acceptable level of risk can be difficult. One study aimed to quantify an organization's general risk tolerance through a set of mock scenarios provided to company managers. Their results illustrated wide differences in how managers rated the scenarios, and frequently even identified that the same managers were inconsistent with their risk ratings (Walls, 2005).

Often times, people do not behave rationally at all. Escalation of commitment is a phenomenon where individuals continue to drive effort and resources into a project that is not reasonably likely to succeed. Instead of cutting their losses or looking to salvage parts of the project, this response makes the loss more costly. Status quo bias refers to a tendency to avoid change. Decision making tends to become more difficult as more options are presented. In a 2009 study, these three factors were brought together to help identify their impact on complex decision making. Here, participants generally tended to make good choices when a project was clearly failing and only one or two alternatives were available. As the number of alternatives increased though, participants were more likely to continue on the original less favorable project investment path (Fox, Bizman, & Huberman, 2009). This tendency is especially dangerous in the context of data security projects where there may be very many evaluation methodologies, services, and mitigation options to consider.

# CHAPTER 5. CLOSING DISCUSSIONS

## *Scenarios Revisited*

There is no best solution for either of the opening scenarios. However the real and complex issues faced with ACME Corporation and the B&L Company can apply the techniques and considerations here to approach their challenges with a better understanding. By focusing on the goals and needs of their respective businesses, they can construct a coherent plan for identifying and prioritizing their information security needs and help others apply better business tools too.

## *Conclusions*

Even though information assurance is still an emerging field, many information security challenges resemble those of other domains or can be approached through common techniques. This work reviewed research, case studies, business tools, and methodologies originating from other fields but which can be applied to information assurance objectives to better enable organizations. It began with an introduction to some key organizational goals, information security challenges, and technologies which affect any business operating in the digital age and describes a number of business tools and how they can be applied to data security topics.

It covers basic decision making methods ranging from simple and cost based methods to more dynamic and subjective analysis. With risk management it addresses challenges of identifying what to manage and how to assure the right amount of effort is applied to this phase. Performance measurement is addressed for tangible criteria and 'non-measurable' abstract aspects. Finally, some aspects of

how human and organizational behavior impact rational methodologies are highlighted.

While no operational performance measurement is universally ideal, designing a portfolio of measurements which are closely related to business interests can identify real threats. They can also set the baseline for improvement if similar data can be consistently tracked over time. Risk management is an art which continues to be practiced irregularly, however its penalty is that discovering risks, flaws, and vulnerabilities after the fact is very costly. Decision making methods can be tailored to a variety of needs and are closely interrelated with the other concepts here. Every method has limitations though, and the tendency for small changes in assumptions to have a disproportionate affect on the outcomes is amplified by the complexity and uncertainty of information assurance scenarios.

In bridging business and information security challenges and tools, this work raises awareness of the range of business management tools currently available and demonstrate their applicability within the security domain. Through improved awareness, decision makers can view their needs, challenges, and available solutions differently. The outcome of which is to enable security professionals to more optimally and comprehensively address the operational needs of businesses.

## REFERENCES

Angelou, Georgios N., Economides, Anastasios A. (2009, August 14). A multi-criteria game theory and real-options model for irreversible ICT investment decisions, Telecommunications Policy, Volume 33, Issues 10-11, November-December 2009, Pages 686-705, ISSN 0308-5961, DOI: 10.1016/j.telpol.2009.07.005. Retrieved October 31, 2010, from http://www.sciencedirect.com/science/article/B6VCC-4X0MPGX-1/2/372a3fd723678507d742196dc5d3555c

AURUM, A., WOHLIN, C., & PORTER, A. (2006). Aligning Software Project Decisions: A Case Study. International Journal of Software Engineering & Knowledge Engineering, 16(6), 795-818. Retrieved October 31, 2010from Academic Search Elite database.

Ayyub, B., Prassinos, P., & Etherton, J. (2010). Risk Informed Decision Making. Mechanical Engineering, 132(1), 28-33. Retrieved October 31, 2010 from Academic Search Elite database.

Bardach, E. (2009). A practical guide for policy analysis: the eightfold path to more effective problem solving (3rd ed.). Washington, D.C.: CQ Press.

Brown, P. (1992). The failure of market failures. Journal of Socio-Economics, 21(1), 1. Retrieved October 31, 2010 from Academic Search Elite database.

Decision Tree Analysis - Decision Trees from Mind Tools. (n.d.). Mind Tools - Management Training, Leadership Training and Career Training. Retrieved October 31, 2010, from http://www.mindtools.com/dectree.html

Dixit, A., & Nalebuff, B. (2009). The Art of Strategy. New York: W. W. Norton & Company.

Fox, S. (2009, December 20). ROI and the InfoSec Value Statement : Information Security Resources. Information Security Resources. Retrieved October 31, 2010, from http://information-security-resources.com/2009/12/20/roi-and-the-infosec-value-statement/

Fox, S., Bizman, A., & Huberman, O. (2009). Escalation of Commitment: The Effect of Number and Attractiveness of Available Investment Alternatives. Journal of Business and Psychology, 24(4), 431-439. Retrieved October 31, 2010, from http://dx.doi.org/10.1007/s10869-009-9124-2

Gardner, D. (2010, June 12). Juggling Risk in the Cloud Security Circus. Technology News. Retrieved October 31, 2010, from www.technewsworld.com/story/70195.html

Grid Analysis - Decision-Making Skills Training from MindTools.com. (n.d.). Mind Tools - Management Training, Leadership Training and Career Training. Retrieved October 31, 2010, from http://www.mindtools.com/pages/article/newTED_03.htm

Juliusson, E., Karlsson, N., & Gärling, T. (2005). Weighing the past and the future in decision making. European Journal of Cognitive Psychology, 17(4), 561-575. doi:10.1080/09541440440000159.

Kraigsman, M. (2010, June 24). Behavorial economics: The IT failure domino effect. IT Project Failures. Retrieved October 31, 2010, from www.zdnet.com/blog/projectfailures/behavioral-economics-the-it-failure-domino-effect/10065

Losi, S., & Allen, J. (2006, October 17). CERT's Podcast Series: Notes - The ROI of Security. CERT. Retrieved October 31, 2010, from http://www.cert.org/podcast/notes/2roi.html

McClure, B. (n.d.). Modern Portfolio Theory: Why It's Still Hip. Investopedia. Retrieved October 31, 2010, from www.investopedia.com/articles/06/MPT.asp#12856987137092&close

Modern Portfolio Theory criticisms. (n.d.). Australian Independent Financial Advisers Pty Ltd: Independent fee for service financial planners. Retrieved October 31, 2010, from http://www.travismorien.com/FAQ/portfolios/mptcriticism.htm

Net Present Value (NPV) & Internal Rate of Return (IRR) - MindTools.com. (n.d.). Mind Tools - Management Training, Leadership Training and Career Training. Retrieved October 31, 2010, from http://www.mindtools.com/pages/article/newTED_74.htm

Oram, A., & Viega, J. (2009). Beautiful security . Sebastopol, Calif., O'Reilly.

Pendergraft, L., & Blakely, A. (2010). Ten Steps for Evaluating and Selecting Software and Service Providers. Information Management (15352897), 44(1), 40-44. Retrieved October 31, 2010 from Academic Search Elite database.

Quinn, K. (n.d.). 2007 Information Builders. Worst Practices in Business Intelligence. Retrieved October 31, 2010, from www.b-eye-network.com/files/2007%20Information%20Builders%20Worst%20Practices%20in%20BI%20WP.pdf

Real options valuation - Wikipedia, the free encyclopedia. (n.d.). Wikipedia, the free encyclopedia. Retrieved October 31, 2010, from http://en.wikipedia.org/wiki/Real_options_valuation

Rice, D., & Rothke, B. (2009, December 10). Audio Podcast - Geekonomics: The Real Cost of Insecure Software Parts 1,2,3 . OnSecurity. Retrieved October 31, 2010, from onsecurityvid.pearson.libsynpro.com/rss

Schneier, B. (2008, September 2). Schneier on Security: Security ROI. Schneier on Security. Retrieved October 31, 2010, from http://www.schneier.com/blog/archives/2008/09/security_roi_1.html

Singleton, J., Mclean, E., & Altman, E. (1988). Measuring Information Systems Performance: Experience With the Management By Results System at Security Pacific Bank. MIS Quarterly, 12(2), 325-337. Retrieved October 31, 2010 from Academic Search Elite database.

Soon-Jae, L., & Hye-Kyung, C. (2008). Building a Framework to Measure and Minimize Information Risks. Information Management Journal, 42(3), 39-44. Retrieved October 31, 2010 from Academic Search Elite database.

Thurman, M. (2006). Measuring the Value of Metrics. Computerworld, 40(40), 34. Retrieved October 31, 2010 from Academic Search Elite database.

Walls, M. (2005). Measuring and Utilizing Corporate Risk Tolerance to Improve Investment Decision Making. Engineering Economist, 50(4), 361-376. doi:10.1080/00137910500348434.