



INFORMATICA SECURITY WHITE PAPER

Six Critical Management Mistakes

Mismanaging Security Can Kill Your Business

By Claudiu Popa, President and Chief Security Advisor, Informatica Corporation

Information security is a universal business challenge. The security threat exists in all businesses, regardless of location because we live in an information-dependent society. That means information has value: a high value.

This important attribute makes information a critical business asset. It wasn't until spreadsheets and databases began to be regarded as essential business tools that businesses began to place dollar figures on what information represents for their business. Computers make it easy to collect, store and crunch unimaginable amounts of data, most of which takes effort to collect. The fact that this data is so easily stored is the beginning of the disconnect that puts businesses at risk on a daily basis.

Data storage together with information management represent contrasting perspectives on the effort required to simply 'have' the information. The ease of storing terabytes of data is deceptive. The difficulty of manipulating meaningless data into valuable information is surprisingly resource-intensive. It is easy to see that a focus on 'what you want' can entirely sideline any thoughts of risk and threat to these valuable resources. Once the 'standard' measures are in place, security is 'taken care of' in the minds of so many managers.

Not to be confused with apathy, this apparently superfluous effort with no clear indication of success is often overlooked and minimized in favour of things we simply know more about. Like making money. This makes sense, but security is the one area where businesses simply can not afford to drop their guard.

For various reasons, information security often falls into the category of business distractions. Perhaps the main reason is that business schools do not teach information security at any level as a part of the critical aspects of running a business, despite indications that over \$22 billion are lost on a yearly basis to such attacks. That means management has no way to evaluate information security expenditures with any hope of generating any return on investment. It is automatically classified as an expense and shelved. Few people in the organization can put a figure on the value of integrating information security directly into core business processes. Although making security a part of business makes logical sense, management has no frame of reference and even those who have an interest in it see a huge can of worms waiting to be opened. With serious business challenges ranging from budgeting to productivity losses, it is easy to understand why.

1. Mistake #1: Failure To Understand The Value Of Information

Without a savvy CFO who understands precisely what information means to the business, no company has a chance of adequately protecting itself. It is one thing to understand that the costs of acquiring, managing and protecting information are actual expenses. Placing a dollar figure on the repercussions of any security breach, loss of information or even the result of a rumour about lack of business asset protection can be a serious challenge. But this is one challenge that must be faced by any organization that is serious about protecting its reputation, client data and business assets.

The effort of putting ball-park figures on the effect of loss, theft or unauthorized disclosure of business information is the beginning of a corporate security strategy. Unfortunately, without a way to classify this business information there is no foundation to this strategy and a realistic budget can not be put into place. The often-quoted issue of throwing two dollars' worth of protection at one dollar's worth of data can only be solved by using a classification scheme. These matrix-like simplifications of information assets are used to create a map of value, risk and sensitivity. Once this is done, the data classification model is put to the test.

Mistake #2: Underestimating Information Sensitivity and Risk

The data classification model needs to be developed together with policies and procedures that correspond to each data 'class'. The more sensitive the data, the more serious the degree of protection. Most organizations can't imagine the multifaceted risk facing sensitive information on a daily basis until put through this test and until a professional security assessment is conducted.. Unfortunately, according to an Informatica survey, only 20% of companies have any understanding of data classification while even fewer actually document it. The data viewed and manipulated by different departments places the business at risk from loss of business to litigation so the concepts of confidentiality and integrity need to be well understood. Without this understanding, policies, procedures and the overall security strategy has no chance of succeeding, leading only to ineffective processes and loss of productivity. Not to mention increased risk.

Mistake #3: Delegating Security To The IT Department

Perhaps the most common error made by today's executives is to put security on the IT department's plate and treat it as a checkbox on their list of responsibilities. According to a recent study, 71% of all organizations delegate security to the IT department. This is both ineffective and unfair. The role of the IT department is to facilitate the management of the technology that manages all the information assets. IT managers understand security and the need for asset protection, but it isn't their responsibility to make their own job harder by evaluating security strategies, testing and implementing solutions that may or may not be fit for the organization. Security is a business problem. IT should be involved in all security management initiatives. However, anytime a manager completely delegates security to a sometimes overzealous IT manager they end up with an incomplete plan for information protection and a potpourri of security products designed to solve a specific problem while making the job easier to manage. Technology doesn't become a security issue until people start mis-using and mis-managing it.

The train of thought is simple. IT will not come to management recommending sweeping, multifaceted changes that will close all information security threats. It would be unfair to expect them to do so and it represents an incredible business challenge to have such a strategy approved even aside from the tremendous additions to the department's workload. What typically happens is when management enquires about a specific type of risk, IT produces a solution that is easily priced and managed. This is all fine for a business that doesn't consider the overall security to its assets. Closing one security hole, even if the effort is successful, has nothing to do with implementing security. A mature approach to security management and the creation of a security strategy involves a company-wide risk assessment, the adoption of manageable protection methods, regular reporting mechanisms and consideration for regulatory compliance. Most companies delegate security concerns to IT and suddenly lose visibility simply because it was an unfair thing to do in the first place. Even more unfair is to blame IT for lapses in the implementation of a security strategy. Remember: security management starts at the top.

Mistake #4: Bottom-Up Security

This is typically why organizations, in particular small and mid-size businesses (SME) regard security as an IT problem. There are so many tools available to provide protection from a multitude of threats that this becomes a matter of having the money to buy the next 'elixir of security'... and there is always a new one.



By keeping security on the desk of C-level executives, businesses ensure that it remains a part of management meetings, in line with business goals and security management is a product of management policy, not the other way around. As most IT employees already know, security threats become reality because of users, not because of inadequate technology. For that reason, security awareness needs to pervade the entire organization, beginning precisely at the top. The concept of top-down security doesn't stop there. It is the only way to ensure that managers and employees at every level are accountable for the impact of their activities on the overall security of the organization. Furthermore, as we move down through the organizational chart, we observe degrees of specialization and process visibility that we simply don't have at the top. That means the people best suited to protecting business assets are the ones directly involved in managing them. Only when departmental and individual initiatives result in increased security do we see a gain from added security products. When employees are motivated to protect business assets and support the organization's goals, it makes sense to streamline these efforts by adding controls and technology. Only then does the overall security strategy have a chance of succeeding and delivering actual, tangible value.

Mistake #5: Failure To Leverage The Value Of Security Investments

Organizations that achieve a sustainable degree of effective security should be proud of their efforts, in particular those of their people, without whose trust, loyalty, accountability and dedication lasting security would be an impossible proposition. However, achieving security is only half the ROI picture.

Leveraging this accomplishment presents numerous benefits. Using security as a competitive advantage and *differentiator* is a powerful statement, indicating both pride in the business and a dedication to protecting business assets. These assets may belong to business partners and clients, all of which instinctively know the value of working with a company that exhibits both a rare degree of integrity and a dedication to go the extra mile. The implication of having absorbed the costs of security is a powerful positive statement. Even more convincing are the impact of regulatory compliance and the demonstrated emphasis placed on client data at every step. Managers that emphasize the privacy and security aspects of their business processes are effectively articulating a message of stability, integrity and quality.

Without making a particular effort to make these procedures overwhelming, organizations can make available detailed privacy policies, compliance seals, public security policies and discrete messages that strengthen the message of dependability and security. The full benefit of security investments can then be fully realized.

Mistake #6: Delayed Security

Managers and executives who delay security expenses exhibit a dangerous level of apathy towards business assets. In a world where connectivity and convergence have made availability the status quo, the risk to information doesn't stop at the end of the business day. Each day, night and hour, unprotected data is a sitting duck, waiting for someone to stumble upon a particular weakness or vulnerability.



Conducting a security assessment paints a picture of the risk to specific resources, the threat to the business and the implication of a successful attack. It also helps managers rapidly determine a course of action.

If the risk is not properly articulated, there is no way to create the necessary urgency, awareness or budget to initiate change. When the urgency is clear however, the need for that change is immediate and should never be underestimated. A system that has been compromised can be impossible to effectively secure or diagnose, so any delay can increase the chances of that resource being lost. Planning related to such resource losses needs to be made well ahead of the disaster and put through periodic testing. A delay of such practices will translate into significant losses when the need for

business continuity becomes urgent. The implications are infinitely complex. Suffice it to say that delaying information security initiatives is bad for business and fundamentally so.

In conclusion, we must underline the importance of painting a big picture of organizational security, assigning people and numbers to keep initiatives in check. Corporate awareness, strategy and planning remain the indispensable ingredients of effective security management. The alternative is a substantial loss of business, resources and the trust of clients, partners and employees.

Additional Resources:

Survey: From Deloitte Touche Tohmatsu

<http://www.deloitte.com/dtt/cda/doc/content/Global%20Security%20Survey%202003.pdf>

Key findings from the recently released 2003 Global Security Survey conducted by D&T, are:

- Respondents are recognizing the need for employee awareness and education.
- Reporting relationships play a key role in the perception of the importance of the information security function.
- IT security budgets appear to be a single digit percentage of the overall IT budget.
- There is an absence of Key Performance Indicators (KPI) for Information Security functions.
- Fragmented security products contribute to the lack of unified security programs.
- There is a lack of clarity on the impact of multiple governance initiatives on information security.
- Financial services companies are spending approximately 6% of their IT budgets on information security

SANS: Top 7 management errors that lead to security vulnerabilities.

<http://www.sans.org/resources/errors.php>

- Number Seven: Pretend the problem will go away if they ignore it.
- Number Six: Authorize reactive, short-term fixes so problems re-emerge rapidly
- Number Five: Fail to realize how much money their information and organizational reputations are worth.
- Number Four: Rely primarily on a firewall.
- Number Three: Fail to deal with the operational aspects of security: make a few fixes and then not allow the follow through necessary to ensure the problems stay fixed
- Number Two: Fail to understand the relationship of information security to the business problem -- they understand physical security but do not see the consequences of poor information security.
- Number One: Assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job.

Information Security Magazine survey of 518 senior security managers:

- Just over half (53%) of those surveyed said their information security budgets would **increase** in 2003
- 16% said their budgets would **increase** by over 20%
- 30% said their budgets would **remain flat** in 2003
- 17% said their budgets would **decrease**