ISSUE PAPER

Not an End In Itself: Information Protection and Return on Risk

Andreas M Antonopoulos, SVP and Founding Partner,
Nemertes Research

Executive Summary

Information protection, a core discipline of information stewardship, must balance rick mitigation with business utility. Balancing risk against return turns information security into a primary enabler of technology innovation. By shifting the focus from asking "is this technology secure enough" to saying "we can enhance our security in order to adopt this technology" security can make the enterprise more confident in reaping the greater rewards—and assuming the greater risk—of deploying new technologies.

The Issue: Information Protection and Information Stewardship

Information protection is one of the core disciplines of Information Stewardship, alongside business continuity, information lifecycle management, data quality management, and compliance. The purpose of Information Stewardship is to enhance the value of information and reduce the risk to information within the context of the business value. In other words, Information Protection is only relevant in the context of the broader value of information.

©Nemertes Research 2008

Maximizing information protection must always be balanced against maximizing the business value of information. The business value of information is derived from the processing, transformation, sharing and dissemination of information – the very activities that create risk! It is crucial to look at information protection as one axis in a broader picture of investment and innovation decisions: you cannot focus only on maximizing information protection (maximizing security). After all, the best way to maximize the protection of information is to lock it up and throw away the key – which of course means that the information is then no longer available to the business. Being a good steward of the information requires using security to enable business functions but to minimize the risk of them as far as necessary.

The Regrettable Veto

No CSO has "veto power" explicitly stated in his job description, but , security is one of the few things other than money that can bring a project to a screeching halt. Do circumstances exist when a security veto should be wielded? What are the hidden costs of a security veto?

Clearly there are circumstances where security overrides business utility: "No, you cannot load 200,000 of our customers' credit card numbers onto your son's iPod for testing purposes," for example. Such situations are usually just a matter of policy and compliance. A real veto is where there is a strong business case for the use of a technology, strategy or application and it is blocked because of an overwhelming risk. Very rarely is there no technology, process or control to mitigate the risk.

Perhaps then, the use of a security veto is an indication of either an insufficient "return on risk" or an insufficient security investment. In the former situation, we are making a wise business decision. In the latter, we are merely hiding a bad decision behind the unassailable excuse of "lack of security". To determine which it is, we have to assess not only the risk and the cost to secure it, but also the opportunity cost — the potential upside of taking the risk.

This evaluation becomes very relevant when we are looking at new, innovative and untested technologies or applications. With new technologies it is hard to evaluate potential risks, and there may not be any well-established controls or countermeasures. It is even harder to foresee the potential upside of new technologies. Technology will be applied in unanticipated ways, yielding unanticipated benefits. It is precisely these risks that have the potential for the biggest competitive advantage and return. It seems it is precisely these risks that are subject to veto.

Nemertes 2007 *Security and Information Protection* benchmark demonstrates this type of regrettable veto. Fully two-thirds of the responding companies had decided against using a technology or service because of security concerns. Many were forgoing investments in collaborative tools (instant messaging, wikis and so forth). Our research shows these tools can have a direct impact on top-line performance, for example, when used by sales. Insufficient investment in security can therefore lead to competitive disadvantage, while more robust investment can help create competitive advantage. When we wield

©Nemertes Research 2008

the security veto, we must consider the cost of a missed opportunity. With sensible, controlled risk comes reward.

The CSO: Risk Controller?

The chief security officer is a fairly new position. We first saw it emerge in larger corporations in the late 1990s; these days, it's standard in most organizations. The CSO's role varies, but typically it combines risk management, policy development and investment in security technologies.

Fundamentally, the CSO is responsible for evaluating the risk of different business choices, and then directing the mitigation strategy. In other words, the CSO is tantamount to a strategic-information risk manager.

Every business has to balance risk and reward continuously, to find a way to achieve the best returns and the least risk. For security professionals, this is the most difficult part of the job: objectively analyzing risk in the context of business goals and possible ROI. It may seem counterintuitive, but the goal for the business as a whole is not to minimize risk — shutting down would be the best way to achieve that. Rather, the goal is to maximize the business's risk to just below an acceptable level (its risk tolerance).

This means the CSO is not looking at ROI but at return on risk (ROR). In a way, the CSO is the counterpart of the CIO on the risk side. If the CIO is looking to maximize ROI, the CSO is looking to maximize ROR. The board of directors or CEO then is responsible for finding the right balance between ROI and ROR.

That brings us to an interesting conundrum: the potential for the CIO and CSO to have conflicting interests. In many organizations the CSO reports to the CIO, which is like having the fox guarding the henhouse. The CIO's job is to maximize ROI — in other words, to invest in technologies that deliver the maximum bang for the buck. The CSO's job is to control risk — in other words, to say no to practices (including, but not limited to, technology investments) that increase risk beyond an acceptable level. If the CIO can override the CSO's decisions, the CSO's ability to mitigate risk is compromised

Ideally, the CSO should report to the CEO or board of directors. If that is not possible, the CSO should report to the head of auditing or risk management. That way, the CSO's goals at least are directly in line with his boss.

If that is not possible, then the best solution is to have the CSO report to the head of audit or risk management. At least that way, the CSO's goals are directly in line with those of the person he reports to.

A market view of information security

The concept of Return-on-Risk is of course borrowed from financial markets and specifically Modern Portfolio Theory. There are big differences between running a business and managing a portfolio, just as there are some revealing similarities. But since the balance between risk and innovation is so often misunderstood in Information Security, it is worth examining portfolio management to see how risk should inform decisions about IT.

©Nemertes Research 2008

When managing a portfolio the ultimate goal is, of course, to maximize the return on investment for the portfolio as a whole, without taking *unnecessary* risk. Modern Portfolio Theory assumes that investors are risk averse and that, given two portfolios of equal return, they will select the less risky one. Equally, an investor seeking higher returns *must* accept more risk. If the risk appetite is assumed to be constant, then the investor will attempt to maximize the return within the constraints of the maximum acceptable risk. In fact, the goal of the investor is not to minimize risk, but to minimize the risk, within the context of a given return, or conversely, to maximize the return in the context of a given risk.

In IT portfolio management, the CIO is attempting to maximize the return-on-investment by investing in technology innovation. Each such investment carries a non-zero risk component. To maximize the return-on-investment, the CIO would have to invest in the most innovative and aggressive technologies, which are also the riskiest. Then the ROI has to be tempered by the need to keep risk within an acceptable range. The acceptable range, in turn, is a strategic determination that is made by the board of directors or CEO and characterizes a business's risk appetite for technology. Just like financial investing, it makes no sense to try to minimize risk – the minimum risk in investing is either government short-term bonds or a mattress stuffed full of cash[1] and will guarantee a minimal ROI, even though risk is still not zero.

A striking similarity with financial investing is how the risk appetite changes with maturity of the investor. A conservative blue-chip business will operate much like a person approaching retirement. Investments will be concentrated in the low-volatility and low-return markets of bonds and blue-chips, just like IT buying in conservative companies is focused in well established technologies and blue-chip vendors. A startup company's IT then behaves similarly to a young professional investor: using innovative, cutting-edge, riskier technologies, like investing in all growth stocks with high-risk and high-return.

Finally, another similarity between financial investing and IT decision making is that over-estimation or under-estimation of risk carries significant costs. The recent sub-prime problems show how risk uncertainty can cause widespread volatility and panic. In information security, CSOs are prone to both under-estimating certain risks and over-estimating others.

But while a lot of information security analysis is focused on the under-estimated risk, there is little focus on over-estimated risk. There is an unstated assumption that over-estimated risk carries no cost – in common terms "you can't be too careful"—but you *can* be too careful. The hidden cost of risk underestimation is unfortunately borne by the rest of the business. Taking on less risk necessarily means less return on investment. In IT, this opportunity cost is most visible in the scenario of the "regrettable security veto" outlined above. Essentially, companies are slow to adopt certain, very promising technologies because of uncertainty or over-estimation of risk. This leads to competitive disadvantage and therefore an impact on top-line revenue.

[1] A minimum-risk portfolio of cash or T-bills is still not a zero-risk portfolio. There is inflation risk and government default risk, however small. Similarly, there is no zero-risk business or IT decision.

©Nemertes Research 2008

While much of the focus of information security is on making sure that risk is minimized, that attitude serves to bias decisions towards over-estimation of risk. Worse, since the cost of delayed innovation is borne by the business units and not by the security team (even perhaps reducing the security cost!) there is a serious misalignment between the business interests and those of a well-meaning but ultimately costly security veto. If such a misalignment of interest persists, most CSOs will find it irresistible to over-estimate risk at the cost of the business: the failure of security falls on their shoulders, the failure of innovation does not.

Most importantly, the mistaken view of the CSO's role as a minimizer of risk makes information security a barrier to investment in technology. The CSO becomes the grand inquisitor of technology whose most overused tool is the word "NO". A balanced view of risk and return means that information security is not a barrier to technology, but instead the primary *enabler* of technology innovation

Information Security as an enabler

In financial markets it is well understood that the ability to accurately evaluate risk, enables a portfolio manager to *maximize* the return on investment by maximizing the ability of the portfolio to absorb risk in some areas while mitigating it through hedging or diversification in other areas. In IT, the ability to accurately ascertain risk and mitigate it enables IT investments to proceed and innovation to accelerate. Security, then, is the enabler of business by allowing the business to finely control the level of risk it assumes while aggressively pushing the competitive envelope. Those competitors, who have a less accurate risk assessment, must necessarily take less risk and absorb less technology and innovation for fear of too much risk. A great business leader is always worried not just about risking too much, but also about risking too little.

For information security to be seen as an enabler in the business the primary question of risk vs. innovation should not be "is this technology secure enough for us to adopt" but "can we enhance our security enough to *enable* us to adopt this technology?"

Conclusion

By inverting the traditional understanding of the role of the IT security professional, from minimizing risk to maximizing the return on risk, security becomes not an impediment to innovation but an enabler of it. By shifting its role from throwing up roadblocks to putting up guardrails, security can make the rest of IT and the enterprise more confident in assuming the greater risks and reaping the greater rewards that can come only with the new.

About Nemertes Research: Founded in 2002, Nemertes Research specializes in analyzing the business value of emerging technologies for IT executives, vendors, and venture capitalists. Recent and upcoming research includes Web services, security, IP telephony, collaboration technologies, and bandwidth optimization. For more information about the analyst, please contact Nemertes at research@nemertes.com.

©Nemertes Research 2008