Optimizing Your IT Strategy for Risk Management
2 Is Your IT Strategy Optimized for Risk Management?

4 Use Risk Management to Make Security Proactive

5 The Six Most Common Misconceptions of Enterprise Security

7 The Five Best Practices of IT Risk Management
Is Your IT Strategy Optimized for Risk Management?

By Faisal Hoque

No investments can be effective in the long term without consideration of risk. Business risks can be both internal to the firm, such as rolling out an inadequately tested system, as well as environmental, in the form of an unanticipated natural disaster.

This creates a challenge for business and technology executives in that while the former type of risk is somewhat more recurring, predictable, and perhaps controllable and, therefore, the business case for investment in risk management is often easier to justify, the latter type of risk is unanticipated and episodic, and the typical firm questions the outlay of resources to protect against such rare occurrences. Yet, the consequences of not doing adequate business continuity planning can be potentially disastrous.

The outcomes of inadequate risk management span the gamut from financial losses, which can potentially be overcome, to a loss of customer goodwill that may well threaten the long-term viability and survival of a firm. Today, with an increasingly unforgiving regulatory environment and legislation such as the Sarbanes-Oxley Act that requires business technology systems to function without error, executives need to be concerned about risk management more than ever before.

At its essence, risk management involves three steps:

1. Identifying the nature of risks inherent in the situation
2. Assessing the likelihood of the risks manifesting themselves
3. Taking preventive and corrective action to reduce the firm’s level of exposure to the risk

The past three decades of business computing have contributed much to our understanding of risk in the technology context. Unfortunately, a dominant focus of this work has been on controlling and managing projects, rather than on the broader risks that executives face in firms where technology is deeply and fundamentally embedded within the business. Indeed, the turn of the century ushered in significant changes in the business-technology milieu that creates a compelling need to expand the focus of risk management from the micro project view to a broader enterprise perspective.

These changes include an increasing emphasis on:

- Buying and customizing packaged solutions rather than building systems in-house (i.e., solutions integration rather than software development)
- Partnering with a wide array of providers to acquire needed technical competencies and skills, including taking advantage of offshore resources
- Using business technology for systems that span
organizational boundaries and help link customers, suppliers, and other business partners together

- Deploying business technology as the platform upon which the entire business is run

**The Faces of Risk**

In this environment where business technology is pervasive, what is the nature of risk? Based on where they originate, risks are classified into three broad categories: systems, sourcing, and strategy. Some risks are predominantly intra-enterprise in nature, such as systems and strategy, while others, notably sourcing, reflect the challenges that arise in inter-organizational settings. Note that although these categories are somewhat overlapping and not mutually exclusive, they nonetheless provide a conceptually simple framework that can be populated through conversations and interactions among executives from both technology and business.

Risks originating from systems are typically intra-organizational, although in some instances when external partners are used for system development and integration, they may be inter-organizational in nature. The risks emanate from all aspects of systems deployment, including project planning and control; human capital and staffing; inadequate user requirements; changes in technology; the complexity, scope, and structure of systems; and inadequate support from senior management.

When these risks are not managed, the firm leaves itself open to dissatisfied users and failed implementations, cost and budget overruns, and the inability to achieve the strategic objectives. In addition to these immediate negative consequences, a longer-term undesirable outcome of inadequate attention to systems risks is an increasing lack of credibility for the IT function and growing distrust between IT staff and users.

Sourcing risks, which are inter-organizational in nature, are inherent in the partnerships and relationships that firms develop with outsourcers and span the gamut from deciding what to outsource, to selecting the right partner, to crafting and negotiating the right contract. Further, as the vendor marketplace matures in offshore locations that offer relative cost advantages, senior executives have the additional option of using partners that are not located within the same country. Although the value proposition of offshoring can be quite compelling, managing offshore relationships escalates the level of sourcing risk.

Finally, risks and threats emanating from strategy represent the dangers a firm faces when its management of business technology is poorly executed. Such systemic risks are manifest, for example, when business technology strategy is developed without the involvement of key business stakeholders; when project portfolios are constructed with a short-term orientation with little or no consideration of strategic goals and priorities; and when sourcing decisions are made in a vacuum without sufficient understanding of the hazards of a lean in-house capability.

The net negative result of not managing strategy risks is twofold. One, the firm is unable to extract the maximum value from its IT assets and business technology capabilities, and over time the ability of the firm to deploy business technology effectively declines. Two, there is a potential for business sub-optimization due to either insufficient or inappropriate investment in business technology management.

Although technology investments can be strategic and rational, very often they succumb to normal human tendencies. Many companies go from one extreme to the other. When things are good, the CIO promotes the idea of technology being a strategic enabler. When the business is in a downturn, the CIO is back to running technology as a cost center and trying to outsource as much as possible. Two years down the road, these organizations realize they’ve lost many capabilities and need to regroup.

In today’s economy, the days of reward outweighing risk are a thing of the past.
Optimizing Your IT Strategy for Risk Management

Use Risk Management to Make Security Proactive

By Alex Goldman

IT departments know that they need to modernize, but a fundamental cultural change requires leadership from the top of the org chart, according to one consultant and author.

“This is not just information security,” said John Pironti, president of IP Architects. “This is true business alignment.” Pironti speaks on the subject at events like the ISACA International Conference.

“Security has to start at the top,” he said. The board of directors of the company decides where the risks lie. The IT manager becomes the Chief Information Security Officer (CISO), reporting to the CIO and also to the board.

“Most security people don’t understand risk — they understand threats,” Pironti said. “Threats are just one input into the risk equation. Others come from operations, strategy, and marketing.

“Where does the business find value? Most executives are more worried about availability than security,” he added. “Organizations will sometimes leave systems up if they’re compromised because availability wins. You don’t need security if you can’t have availability.”

Pironti explained that he’s not arguing for less security. In some cases, less security may make sense. “If it’s marketing data that I give away at trade shows and I want people to have it, then go ahead and sniff away on the network.” Instead, he argues for more appropriate and effective security. “I’m arguing for a meaningful analysis of security needs based on conversations, deployed in areas with a high threat likelihood and a high impact to the business if a threat occurred. The many controls now in place may not make sense.”

For example, Pironti said that many datacenters have bulletproof glass even in non-military environments where a frontal assault on the datacenter is not expected.

“If we have other filters, do we still need a stateful inspection firewall? It’s still required by standards. Heartland is doing end-to-end encryption. Ironically, it can take away the ability to do network protection by disabling the ability to inspect traffic. So when you implement security, you need to think about what threat you are worrying about.”

Pironti said that compliance standards are threat-based, not risk-based, and can be an obstacle to changing the IT mindset. “My biggest fear is security by compliance. It’s spending all your time thinking about an audit and none thinking about what’s important to you. The PCI conversation is outdated in my mind. PCI is a baseline and I think we need to move beyond it.”

He added that the FTC’s Red Flags Rule was manipulated by lobbyists so that the banks could meet the standard immediately.

Even Heartland, which suffered a real breach, should think about costs as it implements stronger security. “Heartland was off the PCI lists for two months. It was fined $7 million to $12 million. Senior business leaders know that they can mitigate that risk with insurance. Why buy $14 million of controls when instead you can buy less and also buy insurance?”
Stay informed about IBM products, services, and other offerings!

Enhance and secure critical business operations with end-to-end business driven security solutions
Securing IT assets — servers, networks, applications, data and the processes supported by them — is a top priority for organizations of all sizes, across all industries. Learn how to help mitigate enterprise security risks by leveraging IBM solutions to drive business innovation and success, while reducing complexity and costs along the way.
Click Here to Download

Develop effective user management to demonstrate compliance efforts and achieve business value
With IBM, organizations can develop comprehensive solutions to help gain visibility into business continuity risks, achieve control over utilization of sensitive business assets and automate a variety of processes for managing access to critical assets and data. Read this white paper to learn more.
Click Here to Download

Take a Holistic approach to business-driven security
Take a business-level view of security and risk management, so you can prioritize security activities and focus on those that make the most strategic sense. With this white paper, learn to direct resources to mitigate risk and costs, and see how IBM enterprise security can optimize business results.
Click Here to Download

Escaping PCI purgatory
PCI compliance is a challenge for midsize and large companies alike, as there are four phases to meeting the PCI DSS requirements: assessment, remediation, compliance and maintenance. Read this white paper as IBM reveals five key ‘sticking points’ organizations have been facing on the path to PCI DSS compliance.
Click Here to Download

Secure and compliant collaboration and access
This white paper discusses how the need for faster access to resources can enable more effective collaboration but can also create significant security and compliance challenges. The paper then describes how IBM offers an adaptable, business-driven, holistic approach to security that addresses the different risk domains across organizations.
Click Here to Download
The Six Most Common Misconceptions of Enterprise Security

By Ed Adams

My thoughts on common misconceptions about enterprise IT security focus on five core issues, the top three of which are the biggest offenders.

Over-Relying on Network Defenses

The problem isn’t our networks (which are pretty well protected), it’s the software. There is no discipline or rigor to software engineering like there is in other engineering disciplines.

I’m a mechanical engineer by trade so this is a very serious problem to me and one that I’m intimately familiar with. But examples in other industries are just as stark by comparison, e.g., doctors have residencies; civil engineers have to be certified and train under another certified engineer (they’re called EIT, engineer-in-training, and can’t lead any projects).

Believing the Hype of Technology/Tools

I love tools. I worked for a vendor that sold software testing tools for more than five years. But I also recognize that tools don’t make people better. They simply make people more efficient in jobs they are trained to do.

Tools don’t teach a surgeon how to operate. I wasn’t a better engineer because I learned AutoCAD, it just made me more efficient in the job I was trained to do. That’s the problem — no training in the discipline; not tools. They aren’t the panacea people want them to be.

Too Many “People” Assumptions

Causal hackers aren’t the real threat. Hackers actually help trip land mines that are waiting to be exploited. The real threats are organized hackers (think terrorist cells or enemy states) who could cripple our infrastructure, utilities, and communication systems.

Real threats are insiders who already have access and know where the crown jewels are. Companies focus on hackers but that is the wrong assumption. And they always forget that it’s their poorly designed software that allows the hackers to exploit them in the first place.

Fix the problem — software — and you mitigate the threats.

Using ROI as a Leading Indicator/Metric

Organizations look at software and security as an investment. They are liabilities that need to be mitigated, not exploited for ROI. If companies thought about their applications as threats instead of assets they’d treat them a lot differently from conception through development and deployment.
Assuming Secure Software is Costly

Though it may add time to the up-front software development cycle (SDLC), defining requirements properly and designing systems well by integrating security into each phase of the SDLC saves tons of time and money in later phases; especially testing and deployment, when security holes take a long time to troubleshoot, re-code, and patch.

Microsoft has some good case studies on this utilizing its SDL (secure development lifecycle) internally on SQL Server. I realize they have a bias interest in promoting it, but the numbers don’t lie — SQL Server 2005 (which was built using SDL) had substantially fewer security bugs than either Oracle or MySQL.

Falling into the “Recency” Trap

I love this one. It’s a psychological problem more than anything. People react to the most recent scare. An epidemic of lost laptops led to net data encryption, while netbots led to investment in intrusion prevention systems.

This is a trend that is well-documented and it’s a shame. It happens not just in IT of course. In 1967 Sweden changed from driving on the left side of the road to driving on the right. What happened? In the 12 months following, auto fatalities dropped by 35 percent. Not because the right side of the road is safer, but because there was a change and people felt more at risk.

Twelve months later, auto fatalities were exactly where they were pre-1967. People “forgot” they were at risk and adjusted behavior. It’s a classic example.
Earlier I wrote about common information security misconceptions and mistakes organizations make. As valuable and occasionally humorous as those mistakes can be to learn about, the real payoff comes when you understand what proactive steps to take to prevent your organization from making those same mistakes.

Below I provide five practical tips to get you on your way. Of course, every organization’s mitigating controls are highly contextual, so adopting all six may not be right for you. But if you follow these, even just a little bit, you will be much more informed about information security and better equipped to make decisions on time and resource investment.

This short, five-step plan will help you to integrate risk management into your information management and application lifecycle. Each step is a short-term investment for a long-term gain; the best of both worlds as risk management is fast becoming a non-negotiable business requirement that your customers are demanding.

1. Make a Self Assessment

This is quick and inexpensive. It means going through a checklist to see if you have incorporated application and information security into your risk management framework and determine whether you have integrated security into each phase of the software development lifecycle.

It is a very simple meeting with your VP of Application Development to have him or her list the different phases of their specific software development process. Then ask how they handle security at each phase and determine whether or not the outputs of those activities are usable in your risk management process.

If the outputs aren’t useful, perhaps you should be measuring something different. In most cases, the answers you get will be something like, “Well, we’ve just started thinking about how to integrate security into our application development, so we don’t really have anything tangible for you at this time.”

That’s OK because that would be an ideal time to discuss your needs with that team. Bridging the gap between application development and risk management is a highly valuable activity and it can be jump-started by this simple self-assessment.

It’s a simple checklist that will give you a quick gap analysis as to where you stand on the information and application security maturity model.

Threat modeling is also an important and valuable step in a self-assessment. It is a more mature and sophisticated approach than the checklist mentioned in the previous paragraph, but the payoffs are substantially greater. Threat modeling, at the business level and the application level, is part of risk analysis and risk management that allows you to identify where the biggest threats are to
your business. This is the Sun Tzu approach of “To know your Enemy, you must become your Enemy.” The basic idea is to define a set of attacks or negative scenarios and assess the probability, potential harm, priority, and business impact of each threat. This can be done at any stage — design through deployment — and yields more valuable results the earlier it is applied. You may need help on your first couple of threat modeling exercises, but there are plenty of good information security consultancies that can provide this.

When you develop a threat model it becomes a tangible, persistent asset for your organization as well. If a new vulnerability or a threat is detected, you can reuse your threat model to determine whether or not you are at a risk increase, decrease, or static. The threat model can help you avoid falling into the Recency Trap mentioned in the previous article and will tell you whether or not a newly identified threat is already mitigated in your system.

2. Believe the Application Security Hype

This is an unfortunately necessary action as there is a lot of hype and fear out there that vendors and media are spreading unnecessarily. However, the application security hype is very real and we have seen it from recent and past headlines: the Lexus-Nexus breach, the problems at TJX, and even the incidents at T-Mobile and CardSystems were all information security incidents caused by application security holes.

How do you filter through the chaff to determine what is real and what isn’t? One thing that can help is to focus on the application layer. The network and systems layers represent less than 30 percent of all security vulnerabilities (according to Gartner); this number is less than 10 percent according to NIST.

Also, consider that network security is much more mature than application security and the investments you have already made here are probably orders of magnitude higher than those you’ve made in application security.

Don’t ignore network security, but try this practical tip: Make a list of the investments and compensating controls you have in place on the network, e.g., anti-virus, IPS, firewalls, etc. Then list their costs (initial/purchase cost is fine). Now do the same for your information and application security investments and compare them.

If the application security investments aren’t at least two to three times that of network security you have an imbalance in the number of vulnerabilities you’re mitigating.

With that first filter applied, you can now consider where and when it is most costly to address application security. IDC and IBM conducted a study a few years ago that mapped the cost of fixing a problem through the software development lifecycle. The results were roughly exponential with respect to time and phase.

Said another way, if a defect found at the design phase costs 1X to repair, the same defect costs 6.5X to fix if found during the coding phase, 15X if it were found in the pre-deployment testing phase, and 100X if it’s found by your customers in the field after it is deployed.

Keep in mind that this only accounts for the time and effort it takes to fix the problem (internal costs). It doesn’t even factor in things like reputation loss, cost of patching and deploying, and other losses that usually come along with security defects — things like loss of market share and stock price.

3. Ask Tough Questions

Tough questions are great because they make you think. The challenge is usually to determine what questions are the tough ones. I provide a short list here to get you started. You will see the pattern fairly quickly and can expand on them for your own environment.

These are questions that are useful to ask your vendors before making a software purchase. You should also ask the same questions of yourself as you build and maintain applications for your business to use.
Finally, use these questions to improve your service-level agreements with outsourced partners (especially software development partners). Since you are probably making a purchase or partner contract to automate or transfer some business function shouldn’t you also consider how to mitigate or transfer your risk when you’re doing this?

- What is your vulnerability response process?
- What is your patch release strategy?
- What methods do you use to inform customers of vulnerabilities?
- What guidance do you provide for secure deployment/maintenance of your product?
- What security training does your development team receive?
- Do you patch all versions of your applications at the same time?
- What are the terms and period of your security support agreement?
- Do you practice security reviews at each phase of your software development lifecycle (requirements, design, coding, testing, and deployment)?
- Do you employ independent third parties to conduct security assessments on your products?

4. Create an Internal “Red Team” of Ethical Hackers

This is a term borrowed from the military. The concept here is that you dedicate a small team (usually three people or less) to act as attackers. This can be a permanent role if you can afford the resources, or you can take some nasty-minded testers and make this part of their job at various phases in the development process.

Their job is to attack your application systems and your networks as if they were evil. I don’t recommend constraining them to act just as “outsiders.” The insider threat is often overlooked and you can learn a lot from creating attack scenarios from an insider’s perspective.

If you don’t have the resources or skill set to create Red Teams, there are many third-party consulting shops that can do this for you. Start with your most critical applications and work your way down the risk rank stack.

By the way, you also need to be certain that any third-party assessments company you use is capable. Ask those same tough questions of them, focusing on things like methodologies used, credentials, engineers they are going to use on your application, how/if they depend on the use of automated tools, etc.

5. Educate Your Teams

I cannot overstate the value and importance of this practice. Education is the first step toward awareness.

The challenge most organizations face here is two-fold: How to best educate their teams, who might be geographically disbursed and of different skill sets, and which team(s) to invest in for security training.

Deciding which team to train (or in what order) is a highly contextual decision that needs to be made based on your specific organization. However, having helped several companies successfully roll out security awareness programs recently, I have observed a few critical success factors that I will share here:

Management Buy-In: Security awareness will likely lead to behavior and policy changes at your organization. For that to happen effectively and efficiently, management must be on board. Even better make them part of the change by ensuring that your program has elements that appeal to management.
Ensure Policies Can Be Enforced: Write clear, understandable, current, and measurable policies. Naturally, the policies need to reflect the corporate, threat, and regulatory environments. Awareness and training programs should address the importance of adhering to policies, as well as the potential financial and reputation impact to the organization from security events.

Measure and Report: Use both qualitative and quantitative metrics to obtain feedback and then measure and benchmark the effectiveness of your security awareness and training program. Most importantly, communicate these metrics and results (good or bad) to your management team for their input, support, and insight.

If at all possible don’t limit education to only security awareness, but also provide technical security training for your engineers, auditors, and others. This training is more difficult to find, but you can locate some excellent security specialists that provide training in scalable formats, like e-learning for both management and technical staff.