Bickford Consulting
Making Security a Business Advantage

The politics of Security

This is the first in a series of articles discussing the practical issues related to enterprise security.

Overview

The mere mention of the word “security” in most enterprises today is sure to raise a number of guaranteed responses: eye rolling, weary resignation, silent fuming, and even outspoken resistance. Despite the very real possibility that millions or billions of dollars might be at risk, that critical business functionality could be crippled, or that intellectual property or strategic information could find its way into the wrong hands, IT departments typically face a steep uphill battle in funding, implementing, deploying, and maintaining the integrity of security solutions.

Whether it is the federal or local government, Fortune 500 companies, universities, or small businesses, the complexity and difficulty around security are more often found in selling the concepts, gaining buy-in (funding), and managing expectations, than the specific technologies required.

For that reason, this series is focused on the “politics”, with a lower case “p”, of security. It should be noted that there are also significant “Politics”, with a capital “P” in certain sectors, notably the government. The issues there are often similar but played out on a much larger, public stage. This series focuses on the commonalities found in most enterprises today.

Security Awareness

No one would argue that security isn't critically important in today's climate.
There isn't a single CIO or CEO who is not acutely aware of the genuine internal and external threats that could seriously impact their business. In addition, technically trained personnel have typically all had reasonable grounding in the basic principles and understand the issues. Increasingly, a large percentage of non-technical users are now aware of security and privacy risks both at work and with their home environments.

If that is the case, then why is security such a thorny knot? Looking at the typical enterprise today reveals a number of reasons for increased threats and the difficulties in pro-actively addressing them.

◆ Selling security

Unfortunately, security experts can sometimes be their own worst enemies, even when they have the best of intentions in protecting the company.

Security is a fascinating, concept-rich area of specialization. It attracts brilliant and

opinionated individuals, and the technologies are rapidly evolving but true solutions that present clear ROI tend to lag in the market.

Within the enterprise, security experts are often regarded as didactic and technology-centered. Selling security solutions internally to executive management is critical, but project proposals often fail when the underlying complexity and benefits cannot be explained in simple, clear business language. The result is that many proposals may seem to advocate boiling the ocean without a quantifiable benefit, possibly disrupting many users, plus adding impediments for deploying critical services, including meeting the needs of the customer community

- **Technologies Vs business processes**

While it is true that technologies and standards in the area of security continue to evolve, the biggest challenges with security deployments today is rarely the technology.

The primary challenge is a business one. Funding is required and for that a significant, executive-level internal selling effort is needed. Even more importantly, the business processes are often effected and without true buyin on the part of those segments, a technology solution may never be successful.

Another challenge exacerbating situation is this that solutions, as opposed to the underlying technologies, tend to lag in the market. This means that an enterprise may need to consider how to develop the solution internally.

As any experienced IT manager knows, this can be a recipe for longer term disasters. Internally developed solutions are invariably based on a snapshot in time of the enterprise, its business models, and the technologies available. Scalability, extensibility, upgrades, maintainability, are typically outside the scope of the design center and what can be afforded.

In addition, for very pragmatic reasons, security is often not staffed as a core competency, or minimally so. Expensive consultants may be brought in who will soon disappear, and internal security experts will move on to other roles.

Eventually, there will be a commercial product that will meet the needs, but by then the homegrown solution may be so embedded that it cannot be safely or cleanly removed with very little internal knowledge of the service itself.

- **IT seen as unresponsive**

One distinguishing characteristic of today's business climate is that strategic agility has become critical and the ability to address that nimbly with technology solutions is often the lynchpin. For example, it is not merely sufficient to establish a web presence. It is just as important to be able to pro-actively reach out to customers, book orders, integrate suppliers, enable services provided by outside vendors. Content and functionality may emerge, evolve, and change significantly over a period of months or

weeks.

Since most IT budgets and project plans are set at the start of each fiscal year, this means that turning on a dime becomes problematic, even when processes are in place to review and refine those plans. Simply put, it is not easy to defund an existing project that is undoubtedly viewed as mission-critical to one part of the business in order to spin up a hot new, flashy solution in another.

Adding to this chronic conundrum, is that IT is an overhead item. Despite the fact that IT may be providing the infrastructure for pulling in revenue, in and of itself IT does not generate income. Even in the best of times, gaining additional funding is difficult, but in recent years with tough economic challenges including layoffs, outsourcing, and reductions on all fronts, it has become one of the toughest management challenges in IT.

As a result, IT is often seen as unresponsive, unable to deliver on its current commitments by one set of the business users, and unable to adapt and commit by others.

Adding to this perception is that, security processes and policies, if they do exist, are typically regarded as a significant part of the problem, introducing restrictions, review time, and complexity. In short, security is seen as a roadblock or, at best, a large speedbump.

- **Loss of IT control**

Although not a new concern, there is a steady increase in the tendency or temptation to move projects and control away from IT.

Not only is IT often perceived, rightly or wrongly, as a barrier, the fact is that business conditions are evolving and lines cannot always be drawn as cleanly between what used to be products, marketing, sales, distribution, and the operational facets of those activities.

Pointing to a very simple example, these days disks for most software products are prepared and shipped only to customers as a backup solutions for customers who cannot download directly over the internet. The pages offered by the company portals are increasingly rich in content and customer knowledge as well as offering access to multiple levels based on support agreements and so forth. The line between release engineering, content creation, access control, and the infrastructure has become very blurry.

Business users are often very sophisticated in their knowledge of the technologies required to accomplish setting up their own sites, but the chances that they not consulting IT policies, particularly in regard to security.

In addition, many technology products are simple to install and very low in cost. The

case of wireless routers being plugged into the company Ethernet is a classic case in point. Users are usually not aware of the vulnerabilities this introduces and even if they are, may not fully comprehend the business risk. They are definitely not motivated to consult the IT bottleneck for approval.

When adding in the threats generated by users downloading software on their own, clicking on websites, most enterprise IT environments have become a very risky places to do business.

While the forces that drive users to do these things are understandable and to some degree inevitable, it is critical that this situation not be ignored. It is well known that companies cannot manage what they do not measure.

- **New technologies, new business models, new risks**

It should be no surprise that as technologies and products evolve, new risks are introduced to the enterprise.

VOIP is currently an excellent example of a technology that many government agencies and companies have on their roadmaps, but one that also opens up new challenges for avoiding the common performance, latency, and virus issues seen in the WAN/LAN environments. For most businesses, the telephone is the critical life line, even when the network fails. Simple denial of service attacks, including inadvertent ones created internally, present new challenges.

In this category, it is also important to include changes in the ways in which systems and services are deployed and managed. Although utilizing consultants and contractors has always been the norm and hosting service are common, outsourcing large segments of a business that was previously a core competency means coping with identity management and access control on a much larger scale. In addition, with more in-sourced and out-sourced workers based world-wide, the ability to do background checks and the laws regarding security and privacy may vary significantly, country-to-country.

As many know, using obsolete or dormant user IDs is one of the reliable ways to gain unauthorized access to applications, data, and services. Since most enterprises have multiple systems for entering user information and providing access, keeping all those so-called stove pipes in synch has become a bigger hurdle.

The good news is that new compliance requirements such as Sarbanes Oxley and HIPAA in the United States and similar standards in other countries has made it impossible to ignore this situation for many companies and institutions. Although painful to implement and retrofit legacy systems, particularly given time constraints, IT departments have to deal concretely with the issue of identity management.

- **Remedies**

Despite the challenges, security is not an area that can be ignored. Proactive security management becomes a business enabler when tackled successfully. Although security is a somewhat specialized area, basic management models still apply for tackling the challenges faced by businesses today.

Although it has become something of a cliché, it is a true one: security must be a process, not a collection of one-off projects. So-called self-sustaining solutions do not happen by magic. Given the agility of internal and external hackers to exploit new vulnerabilities, the inadvertent risks introduced by critical business drivers, and the increasing requirement around audibility and compliance, a sustained focus is required.

There are many aspects to setting up a robust security practice. Briefly, a few key points to consider:

- Carrots don't usually work. “Sticks”, aka pain points such as SOX and HIPAA, are usually the strongest drivers.
- Strong executive support is required. Make sure that executives have the information they need to back up and enforce commitments.
- Develop and publish security policies, including those that impact users as well as architectural and operational facets of the business. Review and update them regularly and make them easy to find on the corporate website.
- Education of the user base is critical. Many vulnerabilities are introduced inadvertently. Make sure that users know where to find information and ask for assistance, clarification, and reporting security breaches.
- Acknowledge the business hurdles, not just the technical ones. Enlist individuals who have good end-user and internal selling skills and also those with proven program management experience. These may often be just as or more effective than domain expertise.
- Develop a clear set of review processes and engage projects early on in their planning and development stages. Most significant security defects can be remedied if they are identified early enough in the cycle. One week before deployment is not sufficient.
- Plan to review system and service updates as well as initial deployments.
- Design for reporting and audibility.

Planning for and managing security is a large topic with encompassing many different technologies and business challenges. Future whitepapers will be addressing a number of these in more detail.

For further information contact:

Susan Bickford
Bickford Consulting
650.210.9958
susan@bickfordonline.com