Economics of Information Security

Ian Burke

Regis University

MSIA676

August 6, 2011

Abstract

The adage is that it is not a question of if but rather when your data will be breached. Perhaps this is so true that security is a bit irrelevant. But if that was true then why do we have all of the regulation and the millions spent each year in security? The answer is in the economics. A business with a secure web sales portal on its web site is more apt to make a sale then a business that asks for your credit card in clear text. A business that can say, “yes we were breached but no we did not lose any confidential information.” Will suffer less damage to its reputation than the company that loses millions of credit card numbers.

But in the days of Fraud insurance and cyber insurance how do you convince a company to adequately invest in security? Again the answer is economics. The best built security solutions are integrated into the fundamental business frameworks and product designs. This is also the most cost effective way to implement security as well.

This paper will look at some of the economic motivators to security. It will explore how security has traditionally been seen as a financial drain and how a more effective model to implement security is to turn it around into a business motivator.

Discussion

Some will argue that the profession of information security started with the early code breakers. Others will argue that the profession started with the introduction of the first firewalls. This is an important distinction as the prior served as an enabler for business and the later served and an inhibitor. These distinct models have a dramatic difference on the perspective of how you look at information security. Is a firewall a tool to enable secure communication or an inhibitor to open communication? This debate can make the difference between getting the budget dollars to implement new security technology.

Businesses, whether public or private, for profit or non-profit, all are in the business of making money. Ultimately they all need to end with a balanced budget. They all have a limit to the dollars they spend. Innovation, advancement in the business objectives, motivators that improve competitiveness, these are all things that land a project onto the budget sheet for an institution. Security initiatives have had a hard time showing these selling points.

Changing the approach to security may improve the effectiveness of the security initiative. Many organizations secure to compliance. If security is approached as a business process and is built into the business life cycle, the integration of of security in to business processes and solution development becomes smoother. Looking at business to client solutions, as an example, integration of information assurance methodologies into the development of the solution will help to improve the marketability of the solution.

There are two approaches to this integration of information assurance. Security can be added after the launch of a product or it can be integrated into the development process. As a component of the business life-cycle it will be a natural component of the system development life-cycle. This will help to reduce cost and improve quality. Some key components of this will

be through change control, testing and mitigation, and design and implementation. At each of these stages, with security integrated, risk is reduced and future risk is mitigated. This method of risk management builds into the process life-cycle as when systems come back for review, upgrades, or future process management, the security components are a natural process. When risk management, change control, and other security functions are ancillary to the business life-cycle or to the system and process life-cycle than their work flow becomes additional work and becomes an inhibitor to the development process.

Looking at patch management as a case example. In many environments systems are built and deployed as part of a project development cycle. This process is independent of the system management process across the organization and the scoping of the systems is often unique to that project. When it comes to patching those systems patches are applied just before it is deployed and then it becomes the responsibility of the systems administrators to ensure that the system stays patched along with all other systems in the data center. In this scenario the issue is that the system administrators have no way of knowing all of the applications that reside on every server and therefore no way of knowing what needs to be patched or what impact different patches may have.

When integrating patch management and the system management into the development process the patch management solution integrates application owners along with system designers and system managers. As these core individuals work together to ensure that a base system platform is deployed so that there is uniformity across the data center and that a base level of patches can be safely deployed, a standard is set for the organization mitigating cost overrun and risk. Beyond that, working security and patch management into the process life-

cycle allows for ownership of the applications and patch management of those applications to either transfer to the system managers or to become more informed and enabled to mitigate risk during management and maintenance of the applications on the systems. This detail is critical in the maintenance and security of any application. Often the risk is not in core operating systems but rather in ancillary application on the server. Ensuring that these applications are maintained is important. Embedding security into their life-cycle lowers cost and mitigates risk.

This model goes to show a method of how security works as a businesses model. It also shows how integrating security into the business life-cycle is more cost effective than integrating it after the fact. But, many organizations may still argue that it is cheaper to by-pass security completely. Patching systems is one thing but investing in hundreds to millions in architecture and appliances that limit network visibility and functionality may seem extreme to an organization with a limited budget. As a CFO or CEO I also would skip an expense such as this as well. In contrast a project that would facilitate the integrity and confidentiality of new research data on a critical new business process that could make the company move from a hundred million a year market to a billion a year market would be an easier sell. Making these distinctions of security in its traditional roles and security as a component of business is essential. These two views above were both looking at segmentation with IPS and firewall implementations. One was an old sales pitch one was a new sales pitch.

The critical difference is how the two would integrate into a business process. Trying to introduce segmentation after a network and business processes are in place would be very disruptive and difficult. Introducing it as the project was under design and development would be less expensive and would ultimately lead to a more secure environment.

A much less complex model where we can see security integrate into business processes is with the use of passwords. We all have passwords, pins, credentials of all sorts that we have to remember both in our personal lives and in our professional lives. Our capacity to remember this information is finite. As our environments become more complex we have more credentials to remember. One solution that we can introduce is single sign-on. These are nice for users but can create large security holes in critical systems. But failure to offer some solution results in users simply bypassing policy and security measures. We have seen the short cuts with credentials written down or standardized across systems. Integrating this solution into the business process so that it works with the objectives of the organization will ultimately lead to a successful solution. You may deploy a single sign-on solution for some applications and a password vault for other applications. Whatever the solution is that works, it must be in line with business objectives.

Ultimately security is about mitigating risk. Businesses are adverse to risk but subject to lots of risk. If these two statements are true than security should be a critical component of business. It is not all about setting up a perimeter and preventing the attacker from getting in. Often the breach starts inside and often it is easier to let them in and prevent the data from getting out. Security may be simply about knowing what assets a business has and where they are. Most importantly, be it through education or policy, making security a part of the business culture is critical.

Looking at the user as a case in point. In many organizations the typical user may get a brief conversation from the IT department about passwords and email during orientation. If it is a regulated organization such a a healthcare company their will be HIPAA training as well. Beyond

this there is little training on information security. In their daily practice users seldom think about plugging in the thumb drive of pictures from home or syncing their personal iPod with their company laptop. Yet these employees are your database administrators and your application owners. They have your administrative credentials and many, if not all, are local administrators on their corporate computers.

When security is integrated into the business life-cycle, these users receive security training on an on-going basis. It is a part of the culture across the organization and a part of the regular dialog. Users understand and respect the risk of connecting personal assets to corporate assets. They recognize the how data flows through the organization and understand that they access critical data. This recognition may not prevent all risk but it will reduce many threats and will also help when a risk turns into a exploit.

Whether it is the inside threat or the external threat the objective is to mitigate the risk. Illustrating that information security is the tool that when leveraged properly as a component of the business life-cycle can do this most effectively it becomes not a matter of selling the security project to management but rather an issue of integrating security into the business processes that are already in place. This argument fits whether for a new security initiative of some other nature.

Lets look at the introduction of an intrusion prevention solution into an existing network. With every network there are maintenance cycles. The intrusion prevention system could be introduced as a security solution intended as a way to monitor for bad guys. Or it could be introduced as a part of the business objectives: maintaining integrity of PII, or confidentiality of health records, etc. the solution could then be integrated into the network as a part of the routine

network maintenance. When introduced it is important to ensure that the solution works well with the business objectives. You could choose a solution that stands alone or choose a solution that integrates with other network equipment and security solutions.

Conclusion

It all boils down to economics. As we work to integrate our security solutions into our business processes we have a choice of how we do this. We have worked for some time now under the fear factor regime. This has resulted in the secure to compliance stance that we have reached. Businesses, whether for profit or not for profit, ultimately work from a budget. Information security needs to justify being a line item on that budget. Becoming a critical part of the business life-cycle helps to reduce the cost of security as well as mitigate risk. It helps to integrate security into the culture of the organization while increasing the quality of both business processes and products produced.

In the end we are looking for the economic motivators for business to invest in security. If businesses are risk adverse and security mitigates risk it should be a natural match.

References

Cranor, Garfinkel. (2005). *Security and Usability*. O'Reilly Media. CA.

Erbschloe, (2009). *computer and Information Security Handbook*. Morgan Kaufmann Publishers.

MA.

Kim, Sivasailam, Rao. (2004). *Information Assurance in B2C Websites for Information Goods/Services.* Electronic Markets. Retrieved from:http://www.som.buffalo.edu/isinterface/papers/Information%20Assurance%20in%20B2%20Websites.pdf

The Hidden Risks (and Opportunities) of Information Assurance.(2011). Martin Yale Group. Germany. Retrieved from: http://www.intimus.eu/data/media/40/4050_0x0_White_Paper_090710.pdf