GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Making Information Security Project Engagements a Business Process

© SANS

© SANS Institute 2000 - 2005 Author retains full rights.

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Jessica Thomas
Location: SANS@Home Local Mentor Program

© SANS Institute 2000 - 2005, Author

Abstract

Information Security as an industry has faced many challenges with strategically aligning themselves with the business, and integrating security into the design and construction phases of business critical projects. For an Information Security program to be successful, alignment must occur between information security needs and business objectives. Information Security must be viewed as a significant business partner, and included in the very early stages of business projects.

This research study will document lessons learned from a previous enterprise level project engagement, steps we took to properly align and integrate information security with business initiatives, and additional areas for improvement based upon the research study. Specific topics include information security governance, defining scope of services, injecting security into business cases, value of using an SDLC process, properly aligning reporting structures, identifying and building necessary partnerships, making information security a business decision, becoming a business enabler, customer service, communication with business unit leaders, and the importance of reducing costs.

© SANS Institute 2000 - 2005

Author retains full rights.

Table of Contents

Introduction 2
My Role 2
The ERP Project 2
Recap of the Mistakes 4
Steps we Took / Lessons Learned 4
- Build an Effective Information Security Governance Framework 4
- Inject Security into the Business Case 6
- Scope of Services 6
- SDLC – "You Can't Bolt On What's Not Built In" 8
- Align Reporting Structures 9
- Make Information Security a Business Decision 10
- Identify your Partners and Build Strong Relationships 12
- Conduct Regular Meetings 12
- Find Out What's Important to Them and Do a Good Job of Securing It! 13
- Become a Business Enabler 13
- Reduce Costs 14
- Last but not Least, Provide Excellent Customer Service! 14

Conclusion 14
References 16

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Introduction

The CIO of our organization has throughout the year given presentations on what it means to be operationally excellent. To be operationally excellent, all business units within an organization must understand the roles and services of each unit, and all units should be working together to achieve organizational goals. Operational excellence includes people, processes, and technology working in conjunction with one another focused on the same goals. During each presentation, I reflect upon all of the difficulties and lessons learned our information security organization has seen with integrating security into the goals of the all of the organizational units. This research study will document lessons learned from a previous enterprise level project engagement, steps we took to properly align and integrate information security with business initiatives, and additional areas for improvement based upon the research study. It is my sincere desire that this research study will give some hope to those who are currently experiencing similar scenarios, and provide some helpful insight into ways they can integrate and become more align with their business units.

My Role

To give some insight as to why this topic is important to me, I have been working directly with business owners and our production development organization over the last two years focused on integrating security into a new ERP (enterprise resource planning) system. It has been an extremely difficult and challenging to integrate system, application, and operational security requirements. I came onboard the ERP project as an Information Security consultant, and later promoted to manager responsible for our ERP security team. The ERP team consists of four security engineers that are responsible for all aspects of security including server hardening, solution development, assessment and remediation, monitoring and alerting, auditing, control validation, facility conversions, application security, user administration, and so forth. During a recent change in our organizational restructure, my new role is to lead a team that is responsible for engaging information security into the appropriate business driven projects and following the projects throughout the project life cycle.

The ERP Project

In August 2002, I was drafted from my position to be dedicated to the ERP project co-responsible for security. The project comprised of implementing a new HR and Payroll system across our 250+ facilities. The project was scheduled to go-live in June, however the project underwent a major reset due to poor communications between IT&S and the business teams. The IT&S teams were restructured under new leadership, and one IT&S team was formed that included developers, system administrators, database administrators, business analysts, QA testers, project managers, and now security. The IT&S

© SANS Institute 2000 - 2005

Author retains full rights.

ERP team was relocated so they could work in the same building with the business owners, and the new go-live date was set. Previously one developer had been elected to implement security within the application, and the O/S security was left up to the system administration staff. Production servers were built and three facilities were scheduled for the new go-live date before our information security team was engaged. Our team began by developing an assessment tool that would be used to identify the security issues in the applications that comprise the ERP system, and the many data interfaces. We then gave this tool to the business owners and various IT staff who had been declared as system owners for them to complete. Needless to say, this wasn't well received. We then added an additional team member whose role was to work with the system owners to complete the assessments. It became very apparent that no one knew who the system owner was or should be. After receiving what information we could back from the various teams, we prepared a presentation for the business and IT&S leadership team. We were now only three months away from the new go-live dates. The presentation revealed that security policies and procedures had not been taken into account during the design phase of the project, and explained at a high level what remediation steps needed to be taken. The leadership team wanted a clear distinction between the new issues that were created with the introduction of the ERP system versus the issues that were present prior to entering the system into the mix, one of which we could not answer. The business owners felt that it was an IT&S responsibility to ensure that their data was secure, and was alarmed at the overall assessment. At the same time, the security team felt that the most difficult part of performing the assessments was trying to understand the business processes that would trigger actions that would transmit confidential information. The IT&S project team members were solely focused on meeting the new implementation deadline of the system, and were not open to making additional changes or adding more work. They were frustrated that security was now requesting changes to this new system this late in the game, and the staff that had been on the project for a while argued that "this was the way things had always been done on the older system and security didn't have a problem with it before." While the project teams may have understood the reasoning behind security policies and procedures, to them the risks did not justify delaying the project or making all the required changes. In addition to the manual assessments, an initial Nessus scan of the production servers revealed 256 security holes and 135 warnings. In summary, security was not seen being a critical business function, but rather one that the risk could be taken on. The issues that were raised by our team were seen as low risk threats even though many of them were exploits listed on SANS top 20 vulnerability list. There was a serious communication and education gap between our security team and the rest of the project team and business owners. As a last resort, the only option at the time was to involve our internal audit team and report to them our findings. That created a "we" versus "them" environment, however, it did get our issues escalated and into project plans.

© SANS Institute 2000 - 2005

Author retains full rights.

Two years later we have had many accomplishments, conflicts, disappointments, and many lessons learned. The project spans across four years, thus we have had to resolve and work through our differences. We have carefully reviewed our engagement process to ensure we have learned from the experience, and we have already seen the value that that learning process has had on other projects we have engaged in.

Recap of the Mistakes

The ERP project was a well-known, business driven project across the IT&S organization, however Information Security personnel did not engage until the project was scheduled for go-live implementation. Our Security Governance committee only included the developer that was responsible for the application security, and did not include anyone from the business teams. So, the first big mistake was that we were not aligned with the business initiatives, and thus did not engage during the design phase of the project. The second mistake was the change in reporting structures. Once the new IT&S ERP team was formed, Information Security personnel reported directly to the Infrastructure Director. This by nature created a conflict of interest. The next mistake was that once the security team was engaged, the first reaction was to assess and remediate everything, and we assumed that everything should be remediated. Instead we should have developed a scope document that would outline our activities in a phased approach, and focused on building our relationships. We gave the business teams and IT&S project members a lot extra work during a time-crunched period. They did not feel that they should be the ones completing the assessments, nor did they even understand what a lot of the questions meant. Since Information Security did not engage in the design phase, security requirements were not taken into consideration, nor was anyone designated as being responsible for the security of the systems. In short, security was not part of the SDLC process.

Steps we Took / Lessons Learned

Build an Effective Information Security Governance Framework

In the Ernst & Young Global Information Security Survey 2003, “security governance focuses on strategic alignment, delivering value while managing risk, and measuring overall performance”. The article goes on to quote John Cieslak, CIO of Toronto Stock Exchange in which he states “the alignment of information security spending with an organization’s business objectives is only possible when information security is viewed as an organizational issue, not just an IT issue”. The survey quotes that “fifty-one percent of respondents said their information security spending was either completely or closely aligned with business objectives”. However, the article goes on to state that “perhaps this percentage is over-optimistic due to the fifty-five percent of respondents that stated that they conduct meetings with their business unit leaders less than once per quarter or do not meet at all”. (pg. 3) A comprehensive security

© SANS Institute 2000 - 2005

Author retains full rights.

governance comprises of stakeholders that play a vested role in the information security posture of the organization, defines roles and responsibilities for information security across the organization, and develops a forum for the governance committee to meet regularly to appropriately align business initiatives with information security services. It is critical to ensure that each business unit is appropriately represented on the committee. In an ISACA article entitled "Information Security Governance", the purpose of Information Security Governance is to "establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations." (par 1) The article goes on to specify the below key tasks required to build the framework:

- Develop the information security strategy in support of business strategy and direction.
- Obtain senior management commitment and support for information security throughout the enterprise.
- Ensure that definitions of roles and responsibilities throughout the enterprise include information security governance activities.
- Identify current and potential legal and regulatory issues affecting information security and assess their impact on the enterprise.
- Establish and maintain information security policies that support business goals and objectives.
- Ensure the development of procedures and guidelines that support information security policies.
- Develop business case and enterprise value analysis that support information security program investments. (par. 2)

One crucial mistake that was made on the ERP project was that our security governance committee only included representation from our product development organization and did not include the business owner. Hence, we were not aligned with the business initiative and did not engage into the project until the project was scheduled for implementation. In large organizations, an effective security governance committee will be the key source for ensuring that information security resources are focused on delivering information security services to the most business critical projects and operations.

In addition to our security governance committee, we now have two separate groups that focus on ensuring that we are engaging on the most business critical projects and operations, as well as ensuring that we are building the right relationships. My new department is called organizational management. Our mission is to properly align information security resources with the priorities of the business, including both projects and operations. To do this, we are to be heavily engaged in understanding all of the projects in our organizations project portfolio and the associated priority of each project. We are also to focus on understanding all of the services that our information security organization offers along with their associated priority. Together we are able to allocate resources

© SANS Institute 2000 - 2005

Author retains full rights.

intelligently to ensure that our resources are focused on supporting organizational goals. We depend heavily upon our customer solutions department whose goal is to build effective relationships across our organization to ensure that we are meeting the needs of the business.

Based upon the research and learning from the ERP project experience, I would have to conclude that we still need a lot of work in identifying roles and responsibilities of information security across our IT&S organization. Far too often, security requirements are left behind and not included in product delivery. Our organization needs to sit down with all of the organizational leaders and map out specific roles and responsibilities within each business unit.

Inject Security into the Business Case

Once the business strategy is set, information security resources should be included in business cases during the initial phases of project inception. In the Ernst & Young Global Information Security Survey 2003, "insufficient budget is the number one cited obstacle to implementing effective security. The survey goes on to state that Information Security managers are harder pressed than ever to formulate and present a good business case because of their inability to explain the relevance of information security to the broad, overall business strategy." (pg. 1) The ERP project began in 1999 and is scheduled to be complete with HR and Payroll implementations by the 4th quarter of 2006. Needless to say the business case is reviewed and adjusted annually for the following year spending. Business cases have also been completed for additional ERP modules. In the beginning, information security was not included as part of the business case. However, each year I now review the existing as well as the proposed business cases and adjust security headcount and any other resources needed based upon the business need. For example, a business case has just been completed for replacing our corporate financial system with our new ERP software. I met with the project teams to discuss the changes in infrastructure, approximate number of security roles and users, number of packaged and customized programs, etc. I also took in consideration the regulatory compliance requirements such as Sarbanes Oxley, and any additional business requirements. It is difficult to get the exact amount of security resources and funding required into a business case when the detailed business requirements is still missing. Through discussions though with the business teams, one should be able to give a good estimation, and most importantly, ensure security is included in the business case.

Scope of Services

Defining a scope document along with the services that you will provide is a critical element in ensuring and measuring project success. Again, one of the mistakes we made when we first engaged was that we tried to assess and remediate everything, and we did not define our scope of work. This caused us to be extremely ineffective in implementing security. It also gave the perception

© SANS Institute 2000 - 2005

Author retains full rights.

that we were completely responsible for all aspects of security, and no ownership fell on outside groups.

In chapter three of "An Introduction to Computer Security – The NIST Handbook", the roles and responsibilities of various company officials can be categorized in the following groups:

- senior management,
- program/functional managers/application owners,
- computer security management,
- technology providers,
- supporting organizations, and
- users.

More detailed information on the responsibilities of each role can be found by visiting http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter3.html. Having a documented list of roles and responsibilities across the organization is valuable when it comes time to gain buy-in on who is responsible for security during the different phases of projects.

For future application project engagements, we have developed a scope process that is summarized below:

Introduction – Defines the purpose of the scope document. Sets the stage that the scope will include defining the roles and responsibilities that the Information Security group views as part of the introduction of a new application platform.

Overview – Defines the different domains of security including system, application, and operational security. Defines the security guiding principles.

Scope – Defines the engagement level for each of the security domains. This section details the specific security controls that will be included as part of the engagement. For example, under application security it includes areas such as roles and permissions, client and data access methods, change management and change control process, database table permissions, etc.

Areas of Responsibilities – This section documents the roles and responsibilities for each of the security domains and includes system, application, and operational security. This is documented in the form of a matrix and includes the roles for each phase of the project. The matrix has columns for the following: Identify, Assess, Advise, Implement, and Monitor. A responsible group is documented for each area for each of the security controls. For example, our Unix Services team is responsible for the identification and

© SANS Institute 2000 - 2005 Author retains full rights.

implementation of the O/S build and configuration, while our Information Security team is responsible for the assessment, advisement, and monitoring of the security controls implemented. This section documents all of the roles and responsibilities within the SDLC process as well as documents operational roles and responsibilities for when the project is complete.

Once complete, signatures will be obtained by the business owners, information security leadership, and all responsible parties that were designated as having a role to play. This scope document should aid in setting clear objectives and expectations up front, and will prevent confusion over who is accountable for each of the security domains.

SDLC – "You Can't Bolt On What's Not Built In"

Once production systems are live and in use, it's typically impossible to integrate security requirements due to fear that the changes may break a piece of functionality or adversely affect a business process. Thus integrating security into the system development life cycle is crucial. In the NIST Special Publication 800-64 Executive Summary, entitled "Security Considerations in the Information System Development Life Cycle", NIST (National Institute of Standards and Technology) has developed SDLC models that integrate security into the process. According to NIST, "a general SDLC includes five phases: initiation, acquisition/development, implementation/assessment, operations/maintenance, and sunset (disposition). Each of the five phases includes a minimum set of security tasks needed to effectively incorporate security in the system development process. Including security early in the information SDLC will usually result in less expensive and more effective security than adding it to an operational system." (par. 3). Details on the five phases can be found in the report:

http://www.iwar.org.uk/comsec/resources/security-life-cycle/

Our opportunity to integrate security into the O/S on the ERP project came when it was necessary to upgrade the system. We decided this time to attempt to do things the right way and follow an SDLC process. To summarize the SDLC process we used, our security team was engaged in four phases of the project: inception, elaboration, construction, and operational. The first phase was the inception phase where the team identified business requirements, reviewed all pertinent security policies and procedures, and began a project plan. The next phase was the elaboration phase. During this phase the team translated all pertinent security policies and procedures into detailed security requirements, and documented the specific system configurations. In other words, the team stated specifically what needed to be secured and how it needed to be configured in regards to the project. A risk assessment would have been conducted during this phase if one hadn't already been done before the project began. Also included in this phase was the development of a security test and evaluation plan, and that plan was communicated to the project team members.

© SANS Institute 2000 - 2005

Author retains full rights.

The next phase was the construction phase. During this phase, the dedicated security engineer worked hand in hand with project team members to secure the system throughout the certification process. Issues were documented and resolved, and all change requests to the security configuration were reviewed for approval. The test plan was executed, and a final gap analysis was performed. The results were documented in the security requirements document as either being achieved or not complete. The results were shared with the project team members, and outstanding items were documented into business issue decision forms for stakeholder decisions. Once decisions were made, outstanding requirements were either put into a new project plan for further development work, or an exception to security policy was submitted for approval. A security baseline was developed and documented. This led into the transition phase. During the transition phase, auditing and monitoring procedures as well as change control procedures were developed. Service Level Agreements (SLA's) and operational processes and responsibilities were agreed upon and documented. Now our team conducts weekly assessments through a script that compares the security baseline to the system settings. Now if something changes and we have a new security hole, the question is no longer, "is this really a threat and worth the change", but rather "what caused this change to occur and has this been corrected?" Most importantly, in the end, we participated in a program-wide update presentation and presented to everyone involved with the ERP project what had been achieved. We used statistics to illustrate the difference in the security of the system. Remember those 256 security holes on our application server? Well, once the upgrade was done, we had 10 security holes, which come out to a 93.4% improvement in the security posture of the system. We also implemented 86 of 102 detailed security requirements, which equates to 84%. Again, the outstanding requirements and security holes were documented into business issue decision forms, and the issues that we agreed upon by the business teams to resolve have been addressed. The numbers spoke for themselves. It was obvious that engaging in the design phase and following the project throughout all of the cycles did indeed make a significant difference in the security posture of the end product.

-
-

We have found that following an SDLC process does indeed create a lot of work for the information security engineer. However, the benefits greatly outweigh the time investment. In reviewing the NIST SDLC documentation, I have discovered several holes with the SDLC process we followed with the above upgrade, primarily with the operations/maintenance and the sunset phases. We will need to refine our process to ensure that we are bringing projects to complete

© SANS Institute 2000 - 2005

Author retains full rights.

closure.

Align Reporting Structures

In an online article entitled "Map Out an Organizational Structure for Security", author David Foote states that "ultimately and legally the board of directors is responsible for protecting the company's assets, but someone has to keep the board informed about the risks the company is facing from security threats. This should be the job of a chief security officer, however they are rare and almost always too low on the organizational chart to effectively interact with the board." (par. 3). Foote goes on to explain that organizational reporting issues come down to which C-level executive your top security person reports to. Foote differentiates the challenges with information security reporting to the CIO, COO, or CFO. Foote states that "chief information officers want to be seen as value-adders, focused on productivity and profits, and cannot afford to be branded as inhibitors. This mind-set can cause CIOs to delay reporting potential security problems upward." (par. 4). Foote continues and says, "chief operating officers are concerned about delivering products and services, resolving customer issues, and increasing sales. Instead of protecting the company's larger goals, the focus is too often on finding solutions for customer complaints, continuously monitoring satisfaction, and fighting for market share." (par. 5) With chief financial officers, Foote states that they "all too frequently act as if the best way to grow profits is to cut costs. When they oversee a security organization, they evaluate security budgetary issues by scrutinizing every capital expenditure or headcount increase." (par. 6). "An effective security organization hinges on collaboration among the CFO, auditors, legal staff, business-unit managers, corporate and physical security teams, IT senior managers, midlevel administrators, and the entire range of corporate stakeholders, whose awareness of and participation in a security program is essential. For information security, this means a structure where the security head's reporting relationship is an enabler, not a deterrent, to integrating the activities of primarily the IT, operations, and corporate auditing groups." (par. 8)

Our information security organization has changed over the last two years and has begun to overcome several of the above organizational structure obstacles. When we first started on the ERP project, information security personnel were move organizationally from an information security department into a dedicated IT&S ERP department. Also, our information security groups were divided into three separate departments with no leading CISO. Today, our information security organization is now headed by a CISO that has a direct reporting structure to our CIO, but also has a dotted-line reporting structure to the Board of Directors and to the SVP of Internal Audit. This gives him a responsibility to meet his commitments and the ability communicate effectively with the board of directors without having his communication clouded by a middle executive. This also gives him additional avenues if he feels that the company is not meeting their commitments to Information Security. With that same philosophy, my

© SANS Institute 2000 - 2005 Author retains full rights.

team now has a direct reporting structure to our Information Security organization and a dotted-line reporting structure to the IT&S ERP team. We also have a responsibility to the ERP team to deliver on our commitments, as well as an avenue to escalate security issues through our Information Security organization if the ERP team does not follow through on their commitments to us. Given the above research, however, perhaps we should review the different groups across the organization and determine who should have a dotted-line reporting structure to our CISO.

Make Information Security a Business Decision

Mary Ann Davidson, Chief Security Strategist with Oracle, presented an onsite seminar to our Information Security group on how to integrate security into business operations. Mary Ann is seen by the industry as a leader in Information Security, and is highly committed to serving customer needs. One quote that I had written down was "security professionals must evaluate the threats based upon business risk, and if the business owners are willing to accept the identified risks, then the business owners must be ready to accept the consequences. If security professionals did not educate the business regarding the risks, then they should be the ones held accountable." At the time of Mary Ann's seminar, we had not tied security threats back to real business risks in a language that the ERP leadership team could understand. Therefore, it was understandable as to why they just thought we were paranoid security engineers.

In an article entitled "Integrating Security into the Corporate Culture", author Steve Purser states that "one of the biggest paradigm shifts that has taken place in the area of Information Security in the last decade is the realization that security is a business issue. In other words, although much of the analysis, design, and implementation of security solutions will require highly-competent technical staff, the key decisions should be driven by business concerns and not technical ones." (par. 6). Purser goes on to say, "when viewed from an opportunity and risk perspective, this model makes a lot of sense – organizations take risks every day and the way in which they take risk can be considered to be a part of their business model." (par. 7) In the NIST Guide to Information Technology Security Services, there are innumerable factors that affect IT security service decisions, which can be grouped in the following categories:

- Strategic /Mission – related to the organization's mission and business function.
- Budgetary/Funding – related to cost, funding, and value of IT security.
- Technical/Architectural – related to the technical and architectural environment of the organization

© SANS Institute 2000 - 2005 Author retains full rights.

- Organizational/Cultural – related to the intangibles of the organization such as image, reputation, and resiliency
- Personnel – related to the organization's employees and contractors
- Policy/Process – related to the organization's business and IT security policies and procedures. (pg. E-2)

On the ERP project, there was a lot of security issues identified through our assessment process that needed business owner decisions. Our Risk Management team developed a form entitled "Business Issue Decision Form", and we customized it for our ERP project. It gave us a forum to document issues we found, document the associated business risks, document our recommendations as well as any other alternate solutions, document any discussion points or analysis relating to costs and benefits, and most importantly a place to document the agreed up decision with signatures from all involved business teams. We used this form for every security issue that required resources or changes to the system or to the way they conducted business. We would meet with everyone involved to educate them on the issue, discuss all the options along with our recommendation, and gain their buy-in on the final decision. As long as we had done our homework, in most cases the decision would be based off of our recommendation. We found that this process worked well from an education and documentation of business decisions standpoint. It also ensured that we were not being viewed as security renegades, and it started bridging the communication gap between the business teams and us. It established a forum to officially link security requirements to business needs, as well as a forum to educate the business and IT&S teams on security risks. Finally, it took the burden of accountability off of Information Security shoulders and placed it on the business teams' shoulders. Given the above research, however, we should ensure that we are including all of the different factors that go into the decision-making process as outlined by NIST.

Identify your Partners and Build Strong Relationships

Many times partnerships between teams are viewed as the relationships that exist on the peer-level of upper management. However, we found that our most valued partners were the personnel that had a direct impact to security risks. In the Ernst & Young 2003 Global Information Security Survey, it states "In order to have an effective information security posture, organizations need to align their information security with their business objectives. To do this, they must eliminate the hierarchical layers between the C-suite and the functional managers." (pg. 2) That is the approach we have taken on the ERP project. Partnerships in the Information Security Industry can be described as those individuals that either receive or provide an Information Security service. On the ERP project, our most valuable partnerships included developers, system administrators, business analysts, project management, and QA staff. In all of the partnerships, we took a vested interest to ensure that their needs were met, while at the same time working with them to implement security requirements.

© SANS Institute 2000 - 2005

Author retains full rights.

However, due to the fast pace of the project, this area continues to be one of our most difficult challenges. It's not an easy task to convince someone who already has a tremendous workload that they need to implement security controls in order to prevent what to them seems like a highly unlikable event. This area will continue to be a struggle for our security team on future deadline pressured projects.

Conduct Regular Meetings

Again, according to an Ernst & Young 2003 Global Information Security Survey, "fifty-one percent of respondents said their information security spending was either completely or closely aligned with business objectives". However, the article goes on to state that perhaps this percentage is "over-optimistic due to the fifty-five percent of respondents that stated that they conduct meetings with their business unit leaders less than once per quarter or do not meet at all." (pg. 3) This was one critical mistake that was made on the ERP project. As the manager of the security team, I meet with each business owner quarterly to discuss their current initiatives and address any concerns they may have. Information Security updates are presented quarterly to the ERP leadership teams, and a forum is opened to discuss any Information Security concerns. During times of go-live implementations, I check in with the various business teams daily to ensure that we are meeting their needs. Additionally, a security representative attends business related meetings such as planning sessions, change approvals, and program update meetings.

Find Out What's Important to Them and Do a Good Job of Securing It!

When it comes to security, the majority of business owners are mainly concerned with user access privileges and user administration within their application. This is understandable given the fact that their business will come to a halt if the employees cannot access the application or do not have proper permissions. To them, this is a much greater and real business risk than a hacker attacking the system. Business owners need to know that you are there to support them and that you care about their business. Again, one of the mistakes we had made when we first engaged in the ERP project is that we wanted to assess and remediate everything. To get things back on the right track, we hired a security business controls analyst. This position was responsible for developing an appropriate security approval process that included business owner approvals for all programs, user security class definitions, segregation of duties, and application access. A process was documented on how security defines, implements, migrates, validates, and monitors access controls. We followed the SDLC process as described below. A baseline was developed for all programs and user security class definitions, and a solution was developed to compare the baseline security to the system security. This gave us the ability to communicate back to the business owners that we are 100% confident that the production system is completely aligned with what they have approved. Our security business controls analyst conducts

© SANS Institute 2000 - 2005

Author retains full rights.

weekly assessments to monitor the integrity of the access controls, and periodic reviews are held with the business teams. A security awareness presentation was developed and presented to business owners that illustrated the security model. The business owners were impressed with our processes, and they thanked us for communicating and clarifying the model.

Become a Business Enabler

Again, to obtain true business alignment, you need to be concerned with the pain points and areas of concern that your business partners may have. For example, maintenance of user security in regards to employee turnover was a major pain for our HR business team. Our ERP system includes a manager self-service portal, and the turnover rate in the hospitals kept our HR business personnel busy with paperwork. Given the fact that our team was responsible for setting up new users and revoking user ID's, the security maintenance on our side was also painful. To reduce the pain, our security team worked with development and with the business teams to develop an automated user provisioning solution. This solution tied the user's position in HR to security access roles, and the program acted upon actions such as new hire, transfer, leave of absence, termination, etc. This solution also made security a business enabler by having the capability of setting up hundreds of users with the execution of the program during facility implementations.

Reduce Costs

The cost of Information Security should be calculated upfront with the business case and ongoing as business owners are included in making business decisions. However, Information Security professionals should take every opportunity to reduce costs both for themselves and for the business. When we first engaged on ERP, the developer that was responsible for security had three very high-dollar business consultants designing and implementing application security. Immediately we began a plan to hire additional personnel and developing knowledge transfer plans. We also took advantage to reduce costs by automating as many aspects of security operations as possible. Through our user automation programs and implementation tools, our facility rollouts have drastically reduced the number of personnel required. This shows the importance that we took to not only reduce costs, but also to illustrate to the business that we were there to provide solutions that would support them during their implementation phases.

Last but not Least, Provide Excellent Customer Service!

In the book entitled, *Delivering Knock Your Socks off Service*, authors Anderson and Zemke state that how well you listen, understand, and respond to each customer, how you handle face-to-face contact, how you use the telephone, the words you put on paper, the way you anticipate a customer's needs, and whether you thank them for doing business with you all add up to the elements

© SANS Institute 2000 - 2005

Author retains full rights.

needed to delivering “knock your socks off service” (43). This type of service should be applied to all internal customers in an effort to build lasting relationships. On our ERP team, we have remained separated from our Information Security organization just so we can be together with our business owners and IT teams. The team knows that they are there to provide quality support to all of our internal customers. During facility implementations, a detailed checklist is communicated and followed to ensure that we deliver on our commitments to the business. Our security team took the initiative to setup a separate phone line that rings on everyone’s phone just so our internal customers would not have to spend time calling each one of us when they needed us most. Most importantly, being onsite has given us the opportunity to develop the necessary relationships that are needed in providing great customer service.

Conclusion

Successful Information Security project engagements are a business process. The framework begins with building an information security governance that maintains project portfolios, roles and responsibilities of security across the organization, and understands the business impacting projects. Once business strategy and alignment is set, security resources should be funded through business cases so the value of security is set up front. Developing a scope of services along with roles and responsibilities in the design phase of projects sets expectations that security is everyone’s responsibility. Following and integrating security requirements into the SDLC process has proven to be an effective methodology to integrate security within the system. Turning information security issues into business decisions builds a forum for non-technical decision makers to make educated decisions. Most importantly, focusing on business needs and building strong effective relationships that include two-way communications is key to aligning security resources and cost-effective solutions with business strategies.

© SANS Institute 2000 - 2005 Author retains full rights.

References

Anderson, Kristen and Ron Zemke. Delivering Knock Your Socks Off Service. New York AMACOM Books, 1998.

Davidson, Mary Ann. "Integrating Information Security into Company Operations." HCA Inc., Corporate Headquarters, Nashville TN. April 30, 2003.

Foote, David. "Map Out an Organizational Structure for Security." Information Week, July 12, 2004: pars 1-8. <http://www.informationweek.com/showArticle.jhtml?articleID=22103859>

"Global Information Security Survey 2003." Ernst & Young Global Report. pg. 3. <http://www.ey.nl/?pag=2027&publicatie_id=952>

The National Institute of Standards and Technology (NIST). Guide to Information Technology Security Services. The National Institute of Standards and Technology (NIST). Special Publication 800-35. Oct.2003. pg. E2 http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf

"Information Security Governance." Information Systems Audit and Control Association (ISACA). pars 1-2. <http://www.isaca.org/Content/NavigationMenu/Security/CISM_Certification/Exam_Information1/Content_Areas1/Information_Security_Governance.htm>

© SANS Institute 2000 - 2005, Author retains full rights.

The National Institute of Standards and Technology (NIST). An Introduction to Computer Security – The NIST Handbook. Special Publication 800-12. July 2004. Chapter 3, par. 2. <http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter3.html>

Purser, Steve. "Integrating Security into the Corporate Culture." SecurityDocs. October 2004. pars. 6 & 7. <http://www.securitydocs.com/library/2631>

The National Institute of Standards and Technology (NIST). Security Considerations in the Information System Development Life Cycle. NIST Special Publication 800-64 Executive Summary. pars 1-2. <http://www.iwar.org.uk/comsec/resources/security-life-cycle/>

© SANS Institute 2000 - 2005, Author retains full rights.