Global Information Assurance Certification Paper

Theoretic Case Study:

Synergistic Security: Aligning Security with Business Goals

Scott A Smith

November 2003

GIAC Security Essentials Certification (GSEC) Practical Assignment

Version 1.4b (Option 1)

ABSTRACT

This paper will list four (4) different processes that can be added to any information security program, regardless of size or structure, to align the needs of the business with the requirements of information security. To achieve this new security alignment will require a fundamental change in corporate culture. Security requirements need to be proactively addressed during the development stage of the lifecycle, and revisited at each stage of the lifecycle to prevent the deployment of a non-secure application. Business units need to be the ones driving network security because the information infrastructure must be built in a manner that allows the corporation to conduct business securely and efficiently.

There are two fundamental assumptions made for the purpose of this paper: (1) The organization has well-defined, current, clear, and supported corporate security policies covering topics from server, workstation, and database configuration, firewall configuration and deployment, as well as having policies related to the confidentiality, integrity, and availability of data. (2) There are existing, working relationships between the information systems areas and the business unit managers. These areas need to work together to bring the security needs of the organization in alignment with the business needs of the organization. The "defense-in-depth" principle goes beyond firewalls, routers, antivirus solutions, and secure operating system images. The processes presented in this paper will demonstrate that if security is in alignment with the goals of the business, it will provide an advantage over the competition.

INTRODUCTION

Before we begin a discourse on how to improve an information security program by adding new processes to the program, we should first define what a process is and how a process becomes a part of an organization's mission. "An organization's processes are a series of successive activities, and when they are executed in the aggregate, they constitute the foundation of the organization's mission. These processes are intertwined throughout the organization's infrastructure (individual business units, divisions, plants, etc.) and are tied to the organization's supporting structures (data processing, communications networks, physical facilities, people, etc.)." [1] In short, processes are what drive an organization toward achieving its objectives.

Those involved in information security have come to embrace a cold, hard fact in attempting to secure an organization: We can't do it alone and we are being told to do more with less. Just as you catch your breath from deploying updated anti-virus definitions to all the servers, desktops, and laptops in your organization, you read about seven new vulnerabilities being reported in the news (and three of the seven are high risk issues) and all seven apply to your organization – meaning that your company

[1] Tipton, Harold F., Krause, Micki. Information Security Management Handbook, 4th Edition. New York: Auerbach Pubications, 2000, 564.

could be impacted by any, or all of, the reported vulnerabilities. What do you do? How do you go about determining what area of your company gets patched first? The answer comes in the form of the business unit managers. They tell you when it's okay to secure their environment; deploy the patches after operations have closed for the day or at a time when the level of activity is at a minimum.

Process 1: "Network Outages" Guided by Business Needs & Requirements

Let's face a simple truth when it comes to information security: there is no such thing as a 100% secure computing environment. A "hack proof" security stance no longer exists nor is it feasible. It is no longer a matter of "*if* we get hacked," it is a matter of "*when* we get hacked." Some statistics from CERT.org point out that more and more companies are indeed getting hacked *and* are reporting the incident. The number of incidents reported to CERT.org starting in 2000 and continuing through the 3rd quarter of 2003 show an alarming trend[2]:

Year	2000	2001	2002	1Q-3Q 2003
Number of Incidents Reported	21,756	52,658	82,094	114,855

While this is an alarming number, please keep in mind that many organizations are extremely reluctant to notify anyone (FBI, local police, CERT, etc.) that an incident has taken place. Consider this bit of information, as reported in the "2003 CSI/FBI Computer Crime and Security Study" released by CSI (Computer Security Institute): "The percentage of those who reported suffering incidents in the prior year who said they reported those incidents to law enforcement remained low (30 percent)."[3] You can look at the information in this fashion – 114,855 incidents reported to CERT reflect less than 1/3 of the actual number of incidents that are occurring.

You can make the case to the business managers that there needs to be an agreed upon time to protect the company from becoming the next organization to contact CERT.org for assistance. At the same time, you don't wish to interrupt daily operations because the company will cease to exist if the business can't make money.

The managers know their business better than anyone else. Therefore, they should be informing you when defense measures can be updated – and not affect daily business operations. These "network outage times" are decided by the business unit managers to minimize the impact to their respective daily operations. Please keep in mind that multiple business units can agree to an outage at the same time, provided two conditions are met:

[2] http://www.cert.org/stats/cert_stats.html
[3] http://www.gocsi.com/forms/fbi/pdf.jhtml (Need to complete request form in order to view report)

1. Resources are available to implement the measures within the agreed upon outage window.
2. The measures can be completed on time so normal daily operations are not impacted.

By having the business managers determine when it's acceptable to be taken briefly offline, the groundwork has been set for defining an overall business unit driven approach for more closely aligning business needs with security needs. Additionally, this process is sustainable, repeatable, and capable of being measured for overall effectiveness. In cases where emergency patch deployments are needed, the reason for deploying emergency patches is that the risk to the business is far too great to wait and must be deployed during the course of normal business hours.

The business driven outage times can be viewed in another perspective in how to protect the business without affecting the business. In a recent cioinsight.com article by Marcia Stepanek titled "Re-Engineering Security," she states the need to shift the security focus in this manner: "The ultimate goal, of course, is not to slow down the business of business but to create new ways to think about security and control in the context of the corporation, as long as it doesn't interfere too much with the process of making money."[4] That is what is at the core of having the business determine the times for legitimate network outages – not interfering with the process of making money.

Process 2: Logical Network Segmentation

A key information security principle will serve as background here – identify your assets and then protect them. You need to know what you have on your network before you can protect it, but it doesn't end with simply identifying network assets.

You should also know what the "name" of this asset is and what function this asset performs. For example, does "Server X" act as the production server for the ERP application? Or, does "Server Y" house all of the development Oracle database instances? Which desktop computers belong to the production application support teams? Before too long, you will have identified all network assets, what functions they perform, as well as classifying the environment of the asset itself (production, test, general, etc.). Performing an inventory of network assets can pay off in other ways. "Obtaining listings of information system assets (e.g, data, software, and hardware) inventories on a device-by-device basis can be helpful in risk assessment as well as risk mitigation." [5]

By logically dividing these assets into certain environments, the business units can take the "defense in depth" approach one layer deeper by "insulating" itself from widespread harm in the event of a virus or worm or Trojan horse slipping through your perimeter

[4] http://www.cioinsight.com/article2/0,3959,1213561,00.asp
[5] http://www.ffiec.gov/ffiecinfobase/booklets/information_secruity/02_info_security_%20risk_asst.htm

defenses. How? Imagine if the network was segmented into areas such as production, test, and general computing. A virus infects the desktop of a user who performs general office type functions. If the virus response team follows documented plans and procedures, they instruct the network security team to shut down the general computing segment to contain, isolate, and remove the virus. In this case, the overall level of impact is much less compared to a network that is not segmented – and the entire network needed to be shut down to perform virus eradication efforts. With this strategy, you act in the best interests of the business. You shut down the affected area of the network, yet allow the main business functions to continue without impact. You still allow the business to conduct business. By adding an extra bit of information or two in the documentation (documentation is always essential), you can go an extra step in protecting the business and its information by documenting the information processed by each network asset. The network segmentation team is tasked to "describe and document the information handled by the system and identify the overall system security level as low, moderate, or high. This element includes a general description of the information, the information sensitivity, and system criticality; which includes requirements for confidentiality, integrity and availability, auditability and accountability…" [6] You now have a thorough network asset reference that you can use to accurately segment the network into four different zones.

An example of network segmentation zones could be as follows:

1. External Zone – The network assets that connect to business partners, vendors, or any other entry point that is beyond your network perimeter.
2. Production Zone – The network assets that allow the business to conduct business. This includes the workstations of those employees who support the production applications (database administrators, system administrators, application support teams, etc.).
3. Test and Development Zone – The network assets serving in non-critical, non-production capacities. This zone can also include QA (Quality Assurance) environments.
4. General Computing Zone – This is where most of the network assets will be located. This zone will contain desktop workstations for those employees not providing "front line" support for production applications. Network file servers can also be located in this zone, depending on the level of sensitivity of information related to the files stored on the server.

Okay, you have identified all network assets and placed them into one of the four categories above. But how do you go about implementing this strategy? First and foremost, there must be an on-going working relationship between the information security areas and the business areas. Both areas work for the same company, and have one common goal – to keep the company in business. Please keep in mind that the purpose of the segmentation strategy is to protect the business so the company can conduct business in the first place. Several key steps need to be followed in order for

[6] http://csrc.nist.gov/fasp/FASPDocs/risk-mgmt/RA_meth.pdf

the project to come to fruition. These steps have been greatly oversimplified to show the general purpose of each checkpoint.

First, identify the resources within the organization that will be needed to complete the project. As always, assemble the project team first before moving forward. Second, identify which applications used by the business are critical for the very existence of the organization and continue listing each and every application in terms of "criticality" to the organization. Or, in other words, which applications can you live without and which applications are a must have? Based on previous efforts, you already have your network assets identified by the applications they support – so it only makes sense to determine which applications are more crucial than others so you can determine which assets to bring back online after an incident has occurred. Third, place the applications (and its related components) into one of the network zones you have defined according to your segmentation categories. Next, publish this information to the project team (including the business unit managers) to verify the accuracy of the information. If the information is correct, develop timeframes to implement the actual segmentation – taking into account the outage windows so normal business operations are not impacted. Communication to all project team members is vital to the success of the program. Lastly, implement the segmentation strategy through the use of VLANs at the switches and routers located throughout the environment using the agreed upon outage times (which again, were determined by the business unit managers).

Process 3: Change Control Procedures

Not knowing the proper procedures of how to move from development to test to production is no longer acceptable from an operations and risk management perspective. Performing any type of work without notifying anyone else is bad for business. Instead of attempting to update or improve something, you can actually break it and take the business offline until the issue is resolved. All one has to do is take a look at the recent patch history of Microsoft. Microsoft releases a patch one day, then two days later – has to release a patch for the patch because the first patch actually ended up breaking something instead of fixing the issue. Would you want that to happen to your organization? Would you want to implement a patch or fix to your mission-critical ERP system without conducting extensive testing on the test system first? One of the ways to prevent this is through change control procedures.

Everyone involved in the information systems area, from developers to system administrators to database administrators to contingency planners to application support managers – and even business unit managers – need to know how the operations environment changes. If you don't know something has been added to your network, how will you know how to monitor and protect the device? This reinforces the principle of "protect what you know is yours."

How do you go about adding this procedure to your existing framework but yet avoid making the change control process a "rubber stamp" part of the overall framework? No one ever said this was going to be easy to implement, enforce, and maintain.

Obviously, the first step in building this procedure is to identify personnel in both business and technical systems areas that can, or will, be affected by a change in the environment. Areas such as application support, system support, database administration, risk management, infrastructure engineers (those in charge of routers and switches), business unit managers, and project managers should be represented at these proceedings. The overall purpose of these meetings is to bring both the systems areas and the business areas into closer alignment in achieving the goals of the overall organization.

Once the change control board has been assembled, it is time to develop a framework in which to operate. This framework includes documenting the changes to be made, the test plans that were executed, the proper way to open "tickets" (which serve as a request notifying the change control board of a modification to the environment), rollback and removal plans (in case things don't go as well as planned), escalation procedures, and meeting times – just to name a few of the components of the overall framework. One key restriction to put in place is to not allow those who open tickets to approve their own requests. The components of the framework should be built around protecting and improving the business, including which application will be affected and the business areas that will be impacted by the changes being made. By incorporating this into the requirements, managers are made aware of what applications are being affected when, as well as how these changes will impact operations.

But, how does this change control process work? Perhaps an example will work best. Suppose there is a need to add a new feature to the payroll application used by the HR and Finance departments. The manager of this project would need to open a "ticket" requesting approval from the Change Control Board to begin developing the new feature. As part of this initial request process, information such as which network assets are being impacted in the development environment (where all new project start), as well as the date and time of the initial installation (which should coincide with the outage times for either the HR Department or the Finance Department). If the ticket is approved by the Board, the work can proceed as planned. If the ticket is not approved by the Board, then discussions need to be held to clear up any issues or questions that prevented the ticket from being approved. This process is repeated as work is completed in development and the project is ready to be moved into the test environment. The same "request for approval" process is followed as the project successfully completes its user acceptance testing as is ready to be moved into production. Since the Board is composed of a cross-section of company representatives, no one group bears more power than any other group; any one party has the authority and ability to reject any request of any nature if questions or concerns arise that put the business, and its operations, at risk. No project, regardless of time constraints or importance to the company, moves into production unless there is complete and unanimous approval from the Change Control Board. By making the business units responsible for the entire lifecycle of the project, the expectation is that managers will pay more attention to the security controls and safeguards being built into the project at the outset – which is where these items need to be addressed.

Process 4: Adding Security Requirements in Project Development

Historically, talking about security requirements usually increases frustration and a reluctance to incorporate security into the design of the application. The best way to prevent this frustration and not impact deadlines is to get employees involved very early into the project. A quote from David Weldon provides a summary of this process: "A great way to head off employee frustration or protest is to get their involvement up front." [7] This process has the potential for the most profound change in an organization and how it views and incorporates information security. Senior management must support this process from the start or else the project will be doomed to fail. Senior management has the ability to effect changes in corporate culture, and this information security process is exactly the type of change many corporations need. Projects are required to incorporate corporate information security requirements into existing design specifications; add information security controls as a core requirement of the project – and add these controls in while the project is still in the development phase. By addressing these controls in development, the long-term effect is that security becomes part of the process, and not added on after the initial design and development of the project has been completed.

Information security professionals have heard it often enough from other areas of the organization – "How am I supposed to know what the security requirements are? No one ever told me what the requirements are or that I should talk to you about it." Companies are getting better at informing employees what information security standards are and where they can be found. In some cases, employees are required to read and sign a document that states you have read and understand the corporate security policies. But does that go far enough? Why can't the applications the company uses be held to the same level of responsibility and accountability as employees? How can a company be secure if its applications aren't?

This process, "Adding Security Requirements in Project Development," isn't strictly limited to just applications. This can easily be applied to servers, workstations, and databases as well. The center of this process comes from repackaging your current corporate information security standards in to a different package that may be more easily understood by developers, server and desktop administrators, and database administrators. If done correctly, this process has the ability to save a company a great deal of money in a short period of time. To help illustrate the point, take a look at the costs associated with patching servers.

In her article "Re-Engineering Security,"[8] Marcia Stepanek refers to an example provided by Christopher Klaus, CTO of Internet Security Systems Inc.:

"When you total how much it would cost to roll out security patches rigorously in a Fortune 1,000 environment, the result could easily by more than $20 million. Say, it

[7] Weldon, David. "@Work: Creating Awareness." Information Security. Volume 6 (2003): 20.

[8] http://www.cioinsight.com/article2/0,3959,1213561,00.asp

takes four hours to install a patch and make sure the applications still work. Say you're paying someone $80 an hour to do this and it costs $320 to patch that one machine and you have 1,000 servers in your environment. That's now $320,000. Multiply that by a conservative estimate of five as the number of Microsoft, and Linux and Cisco and Oracle patches each month, multiply that again by 12 months, and it's about $20 million."

Let's go back to the part about patching 1,000 servers at $320 each, and look at it from another perspective. What if all 1,000 servers came from operating system installations performed by different technicians? And each technician performed the installation differently? What if all 1,000 servers had the same identical operating system image and the patch installed on the "standard" image only took 1 hour to install and test? Now look at the cost savings: $80,000 compared to $320,000. Granted, this is an oversimplified example, but it illustrates the potential cost savings of doing something right the first time while a server or application is still in development – fix the problem on one machine or two machines instead of on 1,000 machines.

It is possible to save time, money, and effort if projects make security requirements a main focus point in the development phases. "Projects" as defined here refer to any new application, server, database, workstation, or an enhancement to an existing resource used by the company. As with any new corporate policy or procedure, senior management must support it from the very start. Senior management needs to be on your side for this effort because it will be a fundamental shift in overall business practices and processes, and you cannot affect this type of change by yourself.

For the purpose of this paper, suppose senior management supports your ideas for "proactive project-based security requirements," meaning corporate security standards will be addressed and incorporated into the project at the project development phase. The next step will be to identify the target audience. Here is where senior management can be of great assistance in helping you promote your ideas. Senior management can present this information in an all-employee meeting, or to the development managers, or to their direct staff. The key role of senior management in this case is to raise awareness of the new procedure to be followed and the business reasons why this new procedure is being introduced. At the same time, please realize that the first couple of times using this new procedure will be extremely difficult for those involved. A good way to describe how this will work for the first several iterations is "angst followed by ease." Granted, it will be tough and stressful at first, but as the process is repeated, it will become easier each time it is used.

At this point, awareness has been raised and expectations have been set. But what exactly are the "proactive project-based security requirements?" The requirements come from your corporate security standards – but presented in a different format. You repackage the standards into a checklist style format, instead of the traditional document style format. The checklist can be arranged in a manner shown here:

Security Requirement	Guideline	Included in Project Documentation	Confirmed in Non-Production	Confirmed in Production
Default account passwords shall be changed to meet password complexity requirements	Required	Yes / No	Yes / No	Yes / No
Rename the "Administrator" account with a complex password	Required	Yes / No	Yes / No	Yes / No
All privileged accounts shall have a complex password	Strongly Recommended	Yes / No	Yes / No	Yes / No
Blank passwords are not permitted under any circumstance	Required	Yes / No	Yes / No	Yes / No

The fields of the chart above are explained below:

- Security Requirement – The control measure stated in the corporate security policy.
- Guideline – Is the control "recommended," "strongly recommended," "prohibited," or a "best practice" and comes from your corporate security policy.
- Included in Project Documentation – As the project team begins to draft the requirements based on technical specifications, include security requirements into the specification documentation. Incorporate both the technical requirements and security requirements into one set of documents.
- Confirmed in Non-Production – This column states whether or not the security requirements were addressed and incorporated into the project, in a non-production environment, by the project team. Utilize available testing tools to determine whether or not the requirement were actually met; the additional effort spent at this point will save time and money in the long run after the project has been implemented into production.
- Confirmed in Production – This acts as an additional safeguard and checkpoint. Perform another round of tests during a pilot production phase to verify that all relevant security requirements have been successfully implemented. Again, be sure to fully document any and all exceptions to the requirements.

A key point to remember throughout this entire process relates to the acceptable level of risk to the business; the risk tolerance of your company. The project team needs to weigh the risk to the business against the level of technical risk in the project itself. For example, what are the business risks associated with having an e-commerce site?

What are the technical risks associated with having an e-commerce site? Is the potential of an extra $50 million in revenue from e-commerce worth more to your business than the technical risk associated with having customer credit card data stored in a weakly protected database (and the information ends up being posted all over hacker web sites)? Only the business managers can answer that question. The time has come to bring the security requirements of an organization in alignment with the business goals of the organization.

After several passes through this, one theme will keep repeating itself. As the needs of the business change, so to will the security requirements. Granted, you will always need to ensure the confidentiality, integrity, and availability of data – but the ways you achieve this will change over time. As the checklists are revised and improved, the entire process improves. Over a period of time, business unit managers will see that security is an enabler, and not a roadblock, to organizational success. When security is aligned with the goals of the organization, the entire company benefits in a variety of ways – customers know their data is safe, vendors can rest assured that they are conducting business with an organization that delivers on their promise of security, and senior management knows the company will not end up on the front page of the paper as a result of a publicized attack on their sensitive information.

Summary

Several processes have been discussed throughout the course of this paper, but each one has a common theme – security coming into alignment with the goals of the business.

A high level of corporate computer network security is possible, but it will take a fundamental change in how the organization views security and the overall value security brings to the organization. Is security regarded as an afterthought or a roadblock within the company? Or is security an active partner that works with the business in helping deliver better, more reliable, and more secure products and applications to the company and its customers? In the minds of most information security professionals, the former question is the overwhelming choice. For those who answered the latter, go ahead and pat yourself on the back for a job well done. You and your company have moved past your competition in realizing that security has become a cost of doing business. Many other organizations have yet to come to that conclusion.

If your company still does not believe that security is a cost of doing business, think of your employees. How many companies identify their employees as their most important asset? Are some of these employees working on the "next big thing" that could make your company millions of dollars? This proprietary information is worth millions to you and your company, and could cost you millions if the data ends up in the hands of your competitor. Consider the following recently released statistics from the October 2003 edition of CSO Magazine in a survey titled "The State of Information Security 2003":

- "Most security incidents lasted less than a day and cost less than $100,000. And most companies had 10 or fewer such events in the past year." [9]

For those interested in the loss of proprietary information, the losses are even more dramatic. According to the "2003 FBI/CSI Computer Crime and Security Survey," there is a cost figure associated with the loss of sensitive proprietary information:

- "As in prior years, theft of proprietary information caused the greatest financial loss ($70,195,900 was lost, with the average reported loss being approximately $2.7 million)."[10]

Here are two other interesting items found in the CSI/FBI Computer Crime and Security Survey:

- 70% of survey respondents said they did not report intrusions to law enforcement due to the possibility of receiving negative publicity.
- In 2003, 75% of survey respondents acknowledged financial losses, but only 47% could quantify the losses.[11]

Security is no longer just an information systems or an information technology issue. Security is a business issue. There are real costs associated with security, whether it is done correctly or incorrectly. The losses tied to doing security incorrectly have a direct impact on the profitability of a company – which is a business issue, not a technology issue. Senior management must begin to recognize this and the costs of security on the company profitability. "Until security matters as much to management as the bottom line, the rank-and-file users will not make security policies, guidelines, and procedures a priority…A company spends money to have security, because it is *not* willing to accept the risk associated with all of the vulnerabilities that put the business at risk. Security does not increase business profitability unless a company can show that its security provides an advantage over its competition." [12] Clearly, having an advantage over your competition does have an impact on company profitability.

This paper has identified four different processes or procedures that can be introduced into an organization, but with one major difference – these processes are designed to align security with business goals. Processes such as network outages determined by business needs, stringent change control procedures, logical network segmentation, and proactively incorporating corporate security standards into project development will contribute to the continued profitability of those companies who embrace security as a main part of doing business, and utilize these processes to provide a competitive advantage in an increasingly competitive marketplace.

---

[9] http://www.csoonline.com/read/100103/survey.html
[10] http://www.gocsi.com/forms/fbi/pdf.jhtml
[11] http://www.gocsi.com/forms/fbi/pdf.jhtml
[12] Tipton, Harold F., Krause, Micki. Information Security Management Handbook, 4th Edition, Volume 3. New York: Auerback Publications, 2002, 529.

REFERENCES

Books:

Tipton, Harold F., Krause, Micki. Information Security Management Handbook, 4th Edition. NewYork: Auerback Publications, 2000, 564.

Tipton, Harold F., Krause, Micki. Information Security Management Handbook, 4th Edition, Volume 3. New York: Auerback Publications, 2002, 529.

Magazine Articles:

Weldon, David. "@Work: Creating Awareness." Information Security Magazine. October 2003 / Volume 6 / Number 10 (2003): 20.

Internet Sources (URLs):

Carnegie Mellon Software Engineering Institute. CERT/CC Statistics 1988-2003. 17 Oct 2003 URL: http://www.cert.org/stats/cert_stats.html (24 Nov 2003)

Computer Security Institute. CSI/FBI Survey Request. URL: http://www.gocsi.com/forms/fbi/pdf.html (24 Nov 2003)

Stepanek, Marcia. "Re-Engineering Security." (12 Aug 2003). URL: http://www.cioinsight.com/article2/0,3959,1213561,00.asp (24 Nov 2003)

Infosec – Information Security Risk Assessment. URL: http://www.ffiec.gov/ffiecinfobase/booklets/information_secruity/02_info_security_%20risk_asst.htm (24 Nov 2003)

Department of Health & Human Services, Centers for Medicare & Medicaid Services (CMS). "CMS Information Security Risk Assessment (RA) Methodology Version 1.1" (12 Sept 2002) http://www.csrc.nist.gov/fasp/FASPDocs/risk-mgmt/RA_meth.pdf (24 Nov 2003)

CSO Magazine Online. "The State of Information Security 2003." (Oct 2003) URL: http://www.csoonline.com/read/100103/survey.html (24 Nov 2003)