Global Information Assurance Certification Paper

GIAC – Level One Internet Research Project

Developing a Computer Security Proposal for Small Businesses – How to Start

by Greg Bassett **August, 8th 2000**

Introduction

It has been widely reported that computerization has played a significant role in the current economic expansion.[1] It is also understood that small businesses are the backbone of the economy: small businesses "represent 99% of all employers, employ 52% of all private workers, and provide 51% of the private sector output."[2] By extension, small business computer automation is playing a vital role in the economic expansion. However, when it comes to systems management in general, and systems security in particular, small businesses are ill prepared to deal with the challenges that increased automation and increased connectivity bring.[3]

The Problem

Our computer systems are under siege. Systems managers are under increasing pressure to secure their systems from outside attack. The attacks reach into the business via electronic mail messages, malicious web sites, and exploits of newly found holes in standard business software.[4] Large and mid-sized companies are hiring all the available, qualified security professionals at an increasing rate. Further, the salaries that security professionals command are increasing at a rate higher than the rest of the IT industry.[5]

The problems are magnified in smaller companies. Systems managers employed at smaller companies are often not as well trained and are less experienced than their counterparts in larger organizations. Often, in very small organizations, systems management tasks are assigned to non-technical staff. The typical systems manager at a small business also may be responsible for duties other than systems management.

How can a systems manager at a small business IT shop convince management that the business is at risk, and the business systems need to be secured – all without blowing the entire corporate budget? This paper will help systems managers with limited business experience focus their requests for security funding.

Step 1. Identifying the Risks

Part of any good security assessment is an *overall* assessment of the systems in use at a business. First, the systems manager should list the different applications that are available to the business, then begin to rank them in order of importance to the business. For example, if the company in question is a

small e-commerce shop, then the company's web site and, possibly, its product database should rank higher on the priority list than the companies word processing system. However, if the company's internal office automation suite is used to generate consulting revenues, then it may rank higher than the static, display only, web server.

Step 1 also helps reinforce the concept that the computer systems in place at the company are a *means to an end, not an end in themselves*. In the proposal, it is important to emphasize this phase of the process. It forces the systems manager to speak in business terms that senior management understands. The focus should be on the highest risk items, namely, the most mission critical applications.

Determining what constitutes a mission critical application is not as easy as it sounds. The complexity of systems and the interconnectedness between these systems increases geometrically with the overall size of the organization. In this case, the small business systems manager has an advantage in that his or her span of systems tends to be much smaller. There are several tools available to help systems managers determine what constitutes a mission critical system. One of these is the *Critical Infrastructure Assurance Office's (CIAO) Infrastructure Asset Evaluation Survey*.[6] While this document is written for large federal government agencies, the methodology can be scaled down to the small business.

Step 2. Identifying the Platforms

Once the mission critical applications are identified, the systems manager should identify the various hardware and software platforms that need to be secured. This may sound simple, but it forces the systems manager to enumerate the various component pieces of each vulnerable application. Some systems managers at small companies may *not* know that the mission critical XYZ application is built around a particular type of database. This is a constant dilemma with systems managers at smaller organizations. More technical knowledge may be required to understand and enumerate the various components of a given application than is required for the systems manager's normal job duties. This is a particular problem when system management duties are assigned to other individuals in the business. All that the systems manager may know about a particular application is that when application XYZ has problems, he or she is supposed to call in the consultant or vendor that deployed the application for the company.

Step 2 forces the systems manager to become more familiar with the inner workings of each mission critical application. Frequently, this requires lengthy telephone sessions with various software vendors or applications consultants. This step helps the systems manager build skills and contacts in dealing with vendors and their support staff.

Step 3. Identifying the Current Vulnerabilities
In this step the systems manager uses various resources to check for known vulnerabilities in the component pieces of each mission critical application. Step 3 serves two purposes: It helps the systems manager find fixes or patches for the known vulnerabilities, and it opens up a community of like-minded users to the systems manager. The systems manager can draw on this community to find current best practices, recommended tools, and other resources. A major component of this step includes a risk management analysis. During the investigation, systems managers need to ask themselves several questions for each of the vulnerabilities. A good starting point for this can be found in *Critical Infrastructure Assurance Office's (CIAO) Practice for Securing Critical Information Assets*.[7] In this document, the risk analysis includes the following questions:

- Can a known vulnerability be better minimized through physical or IT measures?
- How much would it cost to minimize the risk posed by the vulnerability?
- Are the security enhancement costs commensurate with the asset's overall importance?
- Do projected plans or anticipated developments suggest that the vulnerability is likely to become irrelevant in the near- to mid-term?
- How long will it take to implement fully the proposed security enhancement?
- Is it likely that advances in IT will allow the proposed security enhancement to be defeated in the near future?[8]

Step 4. Identifying the Best Practices to Cover the Vulnerabilities
Through the research in Step 3, systems managers should develop a list of best practices that are specific to their application mix and the components of each of the applications. These best practices can include specific products, such as anti-virus software, recommended patches for operating system vulnerabilities, or specific checklists in securing specific types of systems.

During this step, systems managers should work backward to apply what they find in Step 4 to the vulnerabilities found in Step 2. Further, these best practices should be prioritized based on the risk analysis and the relative weight given to each mission critical application identified in Step 1.

The number of resources available to help systems managers with this step is increasing at a rapid pace. There are web site clearing houses for newly discovered systems vulnerabilities as well as Internet mailing lists and

newsgroups that can help the systems manager with this step. Two of the most notable sites follow:

- *Carnegie Mellon's Software Engineering Institute CERT Coordination Center* http://www.cert.org

- *SANS Institute Global Incident Analysis Center* http://www.sans.org/giac.htm

Step 5. Identifying the Costs for Each of the Best Practices

Some of the best practices will not have an apparent cost. It is important for systems managers to understand that their time is a high-cost component. Systems managers must remember that the cost of performing a particular task also has an opportunity cost for *not doing something else.* For example, if a systems manager needs to choose between purchasing an automated tool that performs a security task that the manager could do manually, the manager must also include the actual labor cost and the *lost opportunity cost* into the equation. There are no hard and fast rules for this, particularly in the small-business realm where systems managers may play multiple roles. It is important for systems managers to ask two questions: Is what I'm doing *right now* adding value to the company? If *not,* is there some tool or utility that can do this job for me, so I can focus my efforts on value-added tasks? Sometimes spending a few dollars can pay back big dividends in timesavings for the systems manager. This type of cost justification can really help when writing the funding proposal.

Step 6. Make the Case.

Now that the systems managers are armed with the facts, they can go forward and begin the request process. A few gentle reminders:

- The funding request is going to be evaluated based on the *cost/benefit* criteria that is put forward. The systems manager should make sure that the claims are based in solid facts, and external validations of the claims are cited. Systems managers should not take vendors words for truth; they should find satisfied users to help back up the claims.

- Systems managers should be sure to include the why, what, how, when, where, and who[9] elements that are involved in the proposal.

- Systems managers should make sure that the proposal includes everything needed to complete the security project, such as maintenance contracts, consulting, subscriptions, etc. There is nothing a business manager hates more than to be bombarded with a never-ending series or funding requests for various problems that occur. Savvy systems managers identify as many of the problems as possible, *up front*.

- Systems managers should show that there is a plan of action to implement the proposal. In the request, they should explain how to deploy the products or services listed in the proposal. This tells the business manager that he or she is reviewing a well-crafted and complete proposal.

- Systems managers should ask themselves several questions: Does the proposal make sense? For example, does the proposal request a complete $100,000 security system for a company that has less than $1 million in annual revenue?

Final Considerations

These steps can be modified to work with almost any information technology purchase that the small business systems manager may need. The key concept to remember is that the systems manager is developing a *business* case for the purchase.

References:

[1] Business Technology Association, JBMA/BTA Annual Meeting, July 13, 1999 http://www.bta.org/main/pressRelease/releases/archive/1999/economic_situation.htm (07 Aug 2000)

[2] United States Small Business Association, Small Business Week 2000 (25 February 2000) http://smallbusinesssuccess.sba.gov/sbw2000didyouknow.html (07 Aug 2000)

[3] Lohr, Steve, "Computer Age Gains Respect of Economists," New York Times on the Web, April 14, 2000 http://search1.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+102685+0+wAAA+Computer%7EAge%7EGains%7ERespect%7Eof%7EEconomists (07 Aug 2000)

[4] Berkowitz, Steven, "The Accountant's Role in Enhancing Computer Security," January 31, 2000 http://accounting.pro2net.com/x12248.xml, (03 Aug 2000)

[5] SANS, "1999 SANS System, Network and Security Administration Salary Survey," December 1999 http://www.sans.org/sal99.htm (03 Aug 2000)

[6] Critical Infrastructure Assurance Office, "Practices for Securing Critical Information Assets," January 2000 http://www.ciao.gov/CIAO_Document_Library/Practices_For_Securing_Critical_Information_Assets.pdf (08 Aug 2000)

[7] Ibid

[8] Ibid

[9] Turisco, Fran, "Valuing IT Investments Justify the Purchase… Realize the Value, " November 1999 http://www.fcg.com/webfiles/WhitePaper/white_paper_files/wpValueIT.asp (09 Aug 2000)

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event