Global Information Assurance Certification Paper

STARTING AN INFORMATION SECURITY PROGRAM AND OVERCOMING BUSINESS PRESSURES

Tommy Tinner

Overview

Today's headlines about computer security break-ins and system vulnerabilities provide plenty of impetus for launching information security (infosec) programs. When starting one, it is not far-fetched to imagine that an organization's inherent security needs are readily apparent to all and apt to fall easily into place. Program organizers might also believe that upper management and others involved will eagerly embrace the program's goals simply for the sake of preserving their interests and those of the stakeholders. This sentiment may not hold up in practice because other factors may arise that complicate or impede their efforts.

Some experts believe "it is important to develop your security program within the context of your business objectives and culture" in order to "understand where the risk comes from and why."[1] Thus, an infosec program needs to uncover and respond to the business risks present in the organization. This process begins by critically assessing aspects of the practices and procedures from the standpoint of security. This can reveal unalterable aspects of the corporate culture, initiatives with a higher priority than security, staff and operational limitations, retention and recruitment difficulties, budget constraints, etc. Thus, infosec programs must now confront much more than basic security subjects.

Program developers may then discover other pressures, e.g., anxiety over potential of litigation or negative news media coverage in the event of a security incident, unresolved security issues pertaining to regulatory and certification requirements, fragmented existing security policies and procedures, reluctance to perform independent security assessments for what they might reveal, auditors' inexperience about security, a concentration of technical knowledge about system security in a few individuals minds, companies with many separate business units or technical concentrations, etc. These can be very sensitive, high-risk issues and management may be reluctant to cede control of them to an infosec program in spite of the security issues involved.

The program developers and business managers must strike a balance on these matters in order to establish the necessary security safeguards. A common mechanism to accomplish this goal is to create an infosec program. An early temptation is to limit the program's scope. However, restricting the program's powers may lead to trouble in resolving complex problems that are not easily compartmentalized or that cross several lines of business. Doing so can also build in operational inefficiencies and reinforce organizational barriers that already exist. Given the opportunity to make an informed

[1] Steve Hunt, *Guidelines for Security Investments,* Giga Information Group (June 19, 2000), p. 1.

choice, management may ultimately favor a less limited infosec program but developers will have to work hard to win this type of concession for the program.

The following narrative focuses on the importance of having adequate authority for incident handling. It describes some common business pressures and outside influences that make it hard for infosec program developers to get the power the job demands. It then offers summary conclusions for the benefit of others pursuing similar goals in like environments.

Background

The subject of this report is a governmental entity with two main operating divisions and several smaller ones. The major divisions are separated geographically and operate independently but report to a single executive management team. Each main division has their own information systems (IS) group and some technical interdependencies exist between them. Division A is the largest and the focus of this report. Its operations include system support of a mainframe, geographically distributed local-area-networks, client-server technologies, application development as well as a large number of Windows-based client PCs. Division A is also integrating new functionality to make select information accessible from the Internet thereby creating more new security and business risks.

An attempt was made in the past to appoint a Chief Information Security Officer (CISO) for the entire organization in response to an audit but the position failed to materialize after many months of discussions. Later audits continued to recommend having a central point of contact in the organization responsible for all security matters. Since then, new reporting requirements went into effect requiring the organization to report security incidents. The organization also participated in its first ever third-party vulnerability assessment. New legislation was also passed requiring the organization to report its security incidents as a single entity even though the divisions operate separately. Plus, outside entities have set more stringent security regulations for Division A to follow. The lack of a CISO and the mounting security-related pressures succeeded in making each division begin developing their own procedures for handling security matters. Division A chose to develop an infosec program and is the focus of this analysis.

Groundwork

An early audit reported a potential weakness in mainframe security and the lack of a single point of contact for all of Division A's security matters. This prompted management to create a new Information Security Officer (ISO) position to investigate the mainframe security issue and work on other IS-related security matters. Management filled the position after first researching the function's basic roles and responsibilities.

Interestingly, the finding that led to the creation of the ISO position proved to be inaccurate. In addition, the response of creating an ISO position did not satisfy auditors because the scope of the new position was confined to IS. Thus, the audit finding

continued to be reported as a deficiency and led auditors to schedule more security reviews in Division A.

This perpetuation of audits set the tone for what was to follow. Soon there was a backlog of action items from audits requiring attention of management and the ISO. Division A's perceived need for a single point of contact for all security matters reporting high in Division A's management structure was at the top of the list. The ISO's reporting structure was important to auditors because they believed the security role needed greater independence and more authority over related internal processes to improve Division A's security practices. By bringing a proposal documenting the issue to management, the ISO sought to resolve it or drop it and move on to other matters.

Incident Handling Considerations

The concerns over the infosec program's access to top management and independence relate to the goal of establishing a new policy for incident handling. SANS' advice is to "recognize that incidents require changing the way we operate."[2] In the situation just described, the ISO's proposal attempted to formalize new practices for better addressing Division A's security concerns. The recommendation was to establish a direct communications channel between the ISO and the Division A's head and by giving the ISO more power over the execution of security work performed in the division. These were significant departures from current practices.

According to SANS, step two in the process of developing an incident handling policy is to "identify the various roles and responsibilities."[3] This is all about getting the authority to act on important work matters. In the situation described above, there was disagreement between auditors and Division A's management about the role and structure of the ISO position. In this instance it was necessary to approach Division A's authorities to resolve the matter. This conforms to step three of SANS' process in which you "identify the process for notification and escalation."[4] The final step is "to ensure that you learn something from every incident."[5] Approaching decision makers in this manner helped answer key questions about the managerial nature of the infosec program as well as how incidents were to be reported in the future. Management then made a separate counterproposal setting forth the basic operational guidelines that never existed before. This resulted in a better definition of various roles involved in implementing new security policies and practices.

Good News

[2] Fred Kerby and others, *GIAC Basic Security Policy, Version 1.35 September 5, 2000*, SANS Security Essentials, Part 1, January 31, 2001, The SANS Institute, p 5-18.
[3] Kerby, p 5-19.
[4] Kerby, p 5-19.
[5] Kerby, p 5-19.

Management's counterproposal was a rehash of the ISO's proposal and kept much it intact. However, it eliminated a direct communications channel with the CEO and the assignment of a staff attorney in a co-leadership role. The counterproposal showed sensitivity to the organization's need for high-level attention to security matters by naming two executive sponsors for the security program and council.

The counterproposal had other positive outcomes. It created a security council that would be composed of several subject-matter experts and be responsible for resolving day-to-day security matters. It also takes current industry thinking into account by proposing IS and non-IS individuals serve on the security council.[6] Management also authorized the security council to develop other security policies and procedures as required.

Management avoided making the security council an autonomous group similar to the audit group. This decision requires the security council members to take ownership of problems but does not grant them exhaustive powers. It succeeds in putting to rest the issue about the security council's lack of independence since management still receives outside opinions about security as long as regular audits continue. Thus, future audits cannot claim that upper-management is not receiving the unvarnished truth about security because they will be partly responsible for providing it.

Bad News

The counterproposal did not address the amount of time the security council members will commit to security work. In effect, serving on the security council is an additional duty each person must assume. Will these individuals share the same commitment to security work as they do to their other duties? Without the power to control the performance of security-related work done elsewhere, it becomes more difficult to produce measurable results.

The counterproposal does not address the security needs of the entire organization or facilitate the coordination of security tasks with the other major division. The chair of the security council was not named. This raises questions about whether it will be filled from existing staff, by whom and what the desired skill set is for the position.

Future Concerns

The outcome just described provides the infosec program with a greater sense of purpose than originally existed. It established a multi-person security council as the means for developing Division A's security policies. It settled difficult organizational issues so that other security work might begin. The vacant positions on the security council will need to be filled as well as a list made of the current security issues. No doubt, the list will be a combination of issue-specific, division-wide, local and possibly organization-wide policy matters.

---

[6] Philip Rosch, *Best Practices in Security: Enterprise Accountability for Security*, Giga Information Group (February 20, 2001), p. 1.

Although the organization has a basic information security policy, Division A has more immediate concerns regarding security than the rest of the organization. This will make reconciling new policies against the organization's existing ones more difficult. The other division needs to at least designate a security policy contact to promote greater awareness of issues effecting both divisions. The rest of the security council will need also to be trained in the basic process of developing and evaluating security policy. This can be accomplished thorough formal training or reviewing materials published by SANS.

This discourse leads back to a major infosec program goal of "using security policy to manage risk".[7] The new security council needs to formalize an on-going process to accomplish this goal. According to SANS, the basic steps involved are to "identify risk, communicate your findings, update the security policy as needed and develop and refine methods to measure compliance with the policy."[8]

Since the members of the security council have never formally worked together before, they may need some coaxing to obtain their active participation. Thus, management needs to attend the first few security council meetings to assist in getting it started. The chair of the security council will need to have a grasp of the current security issues as well as a familiarity with security policy development. It will be the council's shared responsibility to perform the work required to both identify and evaluate security policy from then on.

Summary

Wanting to solve all security-related problems that exist in an organization is admirable but may simply not be achievable in the short term because of other business considerations. Accepting this premise may be difficult but it may help program developers concentrate their efforts on more easily resolvable problems while postponing the bigger ones for a while longer.

It is also critical for developers to recognize the sometimes-contradictory nature of what it takes to start infosec programs. Infosec program developers have a basic decision to make. They can either attempt to shape the infosec program to their wishes regardless of management's resistance or wait for management to define the program in line with their expectations. A decision about this also dictates one's tactics.

Advocates of the first option risk alienating management to the goals of the infosec program if discussions turn into contentious debates on the relative merits of specific items. Also, presenting plans that management perceives as too ambitious to be workable can doom the program from the start. If proposals tread on organizational taboos, one risks further alienating management to the extent that fighting for certain changes could lead management to look for less radical security consultants. Proponents of the other

[7] Kerby, p. 5-5.
[8] Kerby, p. 5-5.

option may have an easier time establishing an infosec program but they have to endure it shortcomings once it is implemented.

Knowing the boundaries of what is organizationally acceptable is a key determinant of an infosec program's scope. Prodding management to do what is required is often necessary to build a solid program. Accomplishing this requires the developer to pay attention to business and technical details, present ideas diplomatically and be flexible. Even so, management may reject the developer's ideas and adopt a program along different lines. In the end however, knowing the strengths and limitations of any infosec program that management does finally endorse is liberating, if only to know what the consequences might be.

It is necessary to know the fundamentals of security to be able to apply them to a business situation. Developers then need to know the business and technical practices well enough to establish risk factors to them. It then takes keen communication skills to overcome various obstacles facing the infosec program. Finally, it takes a commitment from the entire organization to make it all work.

Research List

Marc Cecere, February 20, 2000, *Multiple Leaders Can Run IT - Sometimes*, Giga Information Group.
http://www.gigaweb.com/Content/GigaCritiques/RGC-022000-00009.html.

Tom Field, October 1, 2000, *Protection Money*, CIO Magazine.
http://www2.cio.com/archive/100100_money_content.html.

Steve Hunt, June 19, 2000, Guidelines for Security Investments, Giga Information Group,
http://www.gigaweb.com/content/gib/out/rib-062000-00178.pdf.

Kazim Isfahani, October 17, 2000, *Data Security Function Job Description*. Giga Information Group, http://www.gigaweb.com/Content/GIB/rib-102000-00152.html.

Fred Kerby, January 31, 2001, Security Essentials, Part 1, The SANS Institute.

Meridith Levinson, February 15, 2000, *Zen and the Art of IT Governance*, CIO Magazine.
http://www2.cio.com/archive/021500_harley_content.html.

Basil H Pflumm, January, 2001, *CIP: What Auditing Can Add Information Security from an Internal Auditor's Perspective*, Pages: 30-32.
http://www.contingencyplanning.com/article_index.cfm?article=343.

Philip Rosch, February 20, 2001, *Best Practices in Security: Enterprise Accountability for Security*, Giga Information Group.
http://www.gigaweb.com/Content/GIB/RIB-022001-00162.html.

Jan Sundgren, March 17, 2000, *Qualifications and Duties of a Chief Security Officer*, Giga Information Group.
http://www.gigaweb.com/Content/GIB/RIB-032000-00218.html.