Global Information Assurance Certification Paper

Information Security in a Small Rural City
Staffing, Training and Executing

David Simmonds
20 November 2004

GIAC GSEC Practical Assignment V.1.4b - Option 2 - Case Study

Abstract

This is a case study of a small city government's information security evolution, starting from profound vulnerability, no IT staff, no budget and no strategy. The discussion is not intended to be pointedly technical; rather it presents the perspective of a one-person, generalist IT department for which security is a major concern, but not an exclusive one. It takes a fairly long (four year) look at the organization, and treats four subject areas:

- What was done - recognizing and solving specific security problems
- A critique of cultivating, versus hiring, IT security staff
- Economic considerations in security training and certification
- Teaching non-IT employees to be part of the solution.

Before: Out-of-Control

A rural city government (under 75 employees), without IT staff, had installed four physically separate LANs. The first two LANs were each 26-bit routed public subnets via a T1 which we shared with a local ISP. Those subnets served city hall offices and the public library, respectively. The third LAN served only the finance department and had no gateway whatever. The fourth LAN served the police department with a dialup gateway. Employees from various city departments had apparently installed and overseen their LANs, as well as an in-house SMTP/POP server. After the departure of many of these employees, problems rapidly escalated. The cost and effectiveness of using third-party contractors for support proved to be impractical due to the small size and remoteness of the city. The baseline conditions included:

- No firewalls or proxies of any kind were in place on the public-subnet LANs to which senior staff and library workstations were connected.
- Users managed their own antivirus, software and data.
- Financial backup data was kept in the open, on office desks.
- Users without access to the T1 gateways had unregulated dial-up internet.
- The desktop "freeware" mail server was an exploited spam open-relay.
- The separate networks had no interconnection; they could not communicate.

During: Mistakes Were Made

In response to their pressing needs, City management hired a local, entry-level, part-time employee (myself) to serve as the entire IT department. Although my background had been in personal and business computer services, it did not include formal training or certification in security or network administration. Frankly, if I'd been the person faced with such a hiring decision, I wouldn't have hired me, based on my qualifications at the time. Certainly no one consciously chose the wrong course, but the choice to hire staff untrained in information security under such circumstances was simply a mistake.

To be fair, it should be stated that the small size of the organization, the physical remoteness of the area (over 100 mountainous miles from a larger town), and the far higher cost of trained, qualified IT staff probably limited management's knowledge and options on how best to proceed. They knew they needed help, but not much more.

At the time I was hired, I insisted that just one condition be met by the city - a security and network training budget. Management agreed to provide a small annual sum for training, and I accepted the job. Sadly, I overlooked another fairly major item. I failed to ask what my operating budget would be. As it happened, poor communication between departments had the unfortunate result that the first-year operations budget for the new IT department was exactly zero. Nothing but my salary had been appropriated. Upon learning this, I met with my supervisor and told him that under these conditions, I would have little choice but to resign. I was assured that we would find a way to move forward through this first year, and was persuaded to stay.

While I was glad to get the job, and looked forward to the challenges, I found that (not surprisingly) I was unprepared for many of the tasks ahead, particularly security-related problems. Months of late-evening research, trial and error solutions, and cold sweats were to come. An assessment of the existing condition, as outlined above, and of the resources available, was truly frightening. By confronting management with the sobering conditions, a tiny first-year budget was extracted from other departments for security-oriented hardware and software.

It will be clear to a technically oriented reader that many of the security solutions adopted over the course of this project may have represented an incremental improvement, but were not at all ideal. Given my limited knowledge, I doubt that I could have understood or implemented more ideal solutions. Rather, I relied on widely adopted and well-supported products that I thought I could learn to manage on the fly.

As the project was begun prior to the wide acceptance and adoption of Windows Server 2000, it was decided to implement a Windows NT 4 domain controller, MS Exchange 5.5, and MS Proxy 2.0 on a single server in city hall. Password security was improved from Windows NT's non-existent policy, to a complex password policy implemented with Microsoft's "passflt.dll"[1] and Arne Vidstrom's freeware "strongpass.dll"[2] add-ons for NT Server.

Another NT server had recently been obtained by the police department through a grant, but it was effectively off-limits to me. Like city hall, the police had neither dedicated staff nor contract support to administer their IT environment. Because of constraints on access to evidence and confidential data, I was allowed only a limited role, and limited access, to the police department network. In other words, I wasn't able to deal with their information security environment, because of information security constraints. It was a difficult situation, but there really wasn't much I could do other than point out the dichotomy and wait for the situation to change. After an extended period of building trust with the police department and undergoing a thorough background

investigation, I was finally able to operate more freely within their environment and create a more consistent security framework across the organization.

The city hall offices are mostly public space, so physical security was a particular challenge. Tightly focused permissions for data, users and services, and short-timed screensaver lockout of workstations, helped improve both network and physical security. Users were taught to “lock” their screens when leaving their desks. Servers were relocated to a locked rack, remote from the public areas. A nightly backup routine was designed, automated and centralized, and backup media kept in locked cabinets.

Workstation and server OS vulnerability announcements were checked daily, with attention given to timely application of patches and service packs. For the most part, I followed a manual security patch process which was not efficient or fully effective. As the project progressed, Windows XP was adopted - very early after its release - as a standardized desktop OS, based on its major selling points of improved stability, security, and manageability. Its native automatic update process drastically reduced desktop patch management labor.

Internet email was initially secured from its open-relay condition by moving from the freeware, open-relay mail server to MS Exchange 5.5 with IMC (internet mail) using the recommended anti-open-relay configuration[3]. Periodic follow-up testing showed that the open-relay condition was, and remained, resolved. It should be noted that there are organizations that offer free resources to test mail systems for open-relay conditions, including the Network Abuse Clearinghouse (http://www.abuse.net/relay.html), and the Open Relay Database (http://www.ordb.org/submit/).

In our case, it was decided that no webmail, remote Exchange or other external services - except for an SMTP gateway - would be provided in order to prioritize resources and minimize the risk environment. While those services were desired by staff and could technically have been implemented, the vulnerabilities and complications that would have arisen were not acceptable at the time, particularly with the limited resources and knowledge available. (As discussed later in this document, some of the most desired remote services have now become practical for us to implement.)

Internet access from the private networks was initially firewalled, proxied and filtered with multihomed MS Proxy servers in both city hall and the police department. The gateway security of this arrangement was limited, however, and the performance was poor for a variety of reasons, including their enormous, slow browser caches. A hardware firewall had been provided for the public library early in the project. As soon as funding was available, hardware firewalls for the other networks were added, and the less satisfactory, aging proxy servers were removed.

When initial measures to secure and scrub the city hall LAN were complete, the finance department LAN was integrated with it to provide a single private city hall network with domain security, email, software updates, data backup and network printing for all staff. An additional server dedicated to financial data and applications was added at the time

of a major software upgrade to segregate physical access, database management, file systems and backup media. The police department LAN was provided with a separately firewalled gateway address via the T1, and access to dialup internet was removed.

During this remediation and modernization phase, management provided a great deal of flexibility for what were often hours of research and continuing education on a daily basis. This was a major cost of hiring unqualified staff. The high level of on-the-job training nonetheless became the foundation of my own security skills and knowledge, which were desperately needed for problem solving. The steep learning curve, and the time needed to overcome it, was exacerbated by the part-time nature of the job. In subsequent budget years, as management grew to understand the importance and complexity of security issues and the broad scope of the job they had created, my position was upgraded from part-time to full-time.

A system of multi-layered antivirus defense was implemented. Centrally managed desktop and mailserver definition updating, and education of staff in both good email practices and emerging threats, helped manage virus risks. The result was that only a single computer was infected with one zero-day virus over the entire project timeframe. While this may indicate a measure of success, it should be noted that the cost of this single virus incident was calculated to be $432.00. Over the project period, incoming email-borne viruses grew to an average 2,000 per month, or a total of about 42,000 live, user-targeted viruses, worms and trojans.

Managing gateway virus defenses intensively to minimize our exposure to emerging threats has been a very productive use of time and money for us. Some gateway antivirus products have the capability to customize the type and frequency of definition updates to meet special needs, such as SMTP scanning, either routinely or during an outbreak. We have taken full advantage of those capabilities. As an example, Symantec Antivirus Enterprise Edition can utilize provisional, “rapid release” virus data (http://securityresponse.symantec.com/avcenter/beta.download.html) which is released hourly. It can be applied quickly as required, or through a scheduled script[4]. Although this approach certainly doesn’t counter all zero-day threats, it does convey a dramatically better level of detection than the best “out-of-the-box” antivirus software configurations.

It should be noted that the cost associated with even a small security incident, like the one described above, is important information. Estimating the cost of real and potential security incidents is a key component in measuring the return on investment (ROI) for training[5], certification, and technologies to mitigate or prevent those incidents. Some workable approaches to incident costs, such as those outlined by David Dittrich[6], should be easy to adopt for small organizations with limited staff, time and expertise. The process of calculating and defending the ROI of security training and project proposals can be daunting, especially for small IT departments - but according to Debra Young of TechRepublic[7], “Due diligence is key,” when you need to convince management that your proposal is worth the effort and expense. She presents a helpful introduction and framework for the rationale, criteria and methods needed to get started in ROI analysis.

From an economic perspective, security training and certification have value to management, who can use training as a major component to improve their risk management position[8]; and to IT staff, whose earning power goes up significantly in proportion to their security qualifications[9]. While the economic flux of the last several years has created some inconsistency in IT compensation overall, a September, 2003 report by Information Security magazine concluded[10] that information security compensation continued an upward trend, and possession of a security certification increased base pay by an average of nearly nine percent over non-certified placements. The ROI of security training and certification should, therefore, be a commonly attractive incentive for both management and labor.

Throughout the project timeframe - and much like the rest of the world - both prudence and budget limits on technology expenses have led us toward considerable improvising, scrounging and reliance on homegrown solutions and freeware. For example, our firewall and network logs have been aggregated and continuously monitored using the freeware "Kiwi Syslog Daemon" (http://www.kiwisyslog.com/software_downloads.htm). Batch language and command-line utilities can be off-putting to the less technically inclined and Windows-oriented among us, but they typically have provided us with no-cost alternatives to premium, packaged software that we couldn't afford, and that may not have done a better job. A prime example would be our use of plain, old "ntbackup" instead of expensive, third-party server backup solutions which we have tried and abandoned. Ntbackup is harder to configure with its endless command-line syntax called from batch files, and in turn called from schedules, but it has done a far better (perfect, actually) job for us in reliable Exchange Server backup and disaster recovery than any of the expensive products we've tried. (During this period, simple disaster recovery planning and secure offsite backup rotation were implemented and tested.) In a security context, most of the tools needed to monitor and analyze network traffic are both freely available, and command-line driven.

In order to reinforce good employee practices and reduce social engineering risks, Information Security and Acceptable Use policies were drafted from readily available sources, including sample policies from the SANS Institute[11]. These were vetted and adapted by our legal staff and added to the City's personnel policy. Employees clearly understand that personnel policies aren't suggestions, and straying from them can be cause for termination.

Three employee-oriented tactics have been productive for us in helping manage human security risks. They are:

1. Enlisting the support of employees by boosting their basic security knowledge,
2. Keeping them briefed on developing threats, and
3. Setting high standards and expectations with regard to security practices.

Succeeding with this approach has required placing a high value on interpersonal relationships, communication skills, and team building. Whenever the security situation has gotten interesting, it has been beneficial to work with non-technical staff who can

sense that they are in some measure on the front line with me. A fairly high degree of interdepartmental teamwork is almost a necessity for an organization with a one-person IT department. That sense of teamwork has had tangible benefits. Especially during zero-day events, other employees have sometimes been the first to notice a suspicious email, request or other activity. When non-technical staff know that you rely on them for help, as well as vice versa, they're likely to be more motivated to raise an issue or ask a question when something doesn't seem quite normal.

Providing information to help employees with their home-computer security issues also has helped build good will and a team spirit. Beyond providing all staff with virus, scam, hoax and vulnerability alerts oriented to both the business and home environments, informative resources such as US-CERT's primer on home computer security[12] have been made available. Licenses for enterprise antivirus have been distributed for use on some employees' personal computers in those cases where they have had a need to work at home. It is no stretch that helping employees, within reason, to secure their home computers has been in our interest, and is, to the extent that it is practical, likely in the interest of most organizations.

After: A Maturing, but not Mature Organization

While the local security environment has dramatically improved, potentially serious vulnerabilities still exist or continue to come to light, and continue to be addressed as resources permit. Have I become qualified along the way to match the needs of the organization? That's an open question in some sense, but I've made the effort to learn, have gotten pretty good results, and at a minimum I feel I now have the resources and momentum to keep moving forward.

On the down side, there is a real threat embodied in the constant distractions and diversions from security issues. One of these distractions, spam management, eats up substantial and increasing resources[13] for every person in the organization. Being the network engineer, webmaster, help desk, purchasing manager, hardware technician and more, doesn't do much for my prospects as a successful security manager. At some point the dilution of effort overcomes forward progress, and that point appears closer today, not further away, than at the outset.

I can still say with honesty that in some areas, "I don't know what I don't know," and that is both a constant worry and a motivation for more training. The drudgery of managing Microsoft desktop and server vulnerabilities never seems to end. Critical third-party software vendors fail to test or certify their applications for changing OS or service pack environments, such as Windows XP SP2, causing train wrecks, slowing implementation and extending risk. The worm-and-virus-of-the-moment threat environment has vastly deteriorated and takes a chunk out of most workdays. Staff demands and infrastructure have grown like Topsy, but the IT department still consists of just the author. Peer support and interaction in such a geographically remote area is quite minimal and

unsatisfying, so the internet has been - and remains - my lifeline for security information and help.

On the positive side, we've achieved a long-term, consistent operational uptime of about 99.98% and have, with the one exception previously mentioned, entirely avoided virus infection across the whole organization. Our employees know more, and are most often part of the security solution rather than part of the problem. An open-ended strategic program of security improvements has evolved. It includes continuous evaluation of technologies and a three-year planning horizon which are captured in structured reports to management as part of every budget development process. A realistic budget for annual security training and certification is in place. Management has been attentive and accommodating as the IT "department" has evolved from crisis and struggle, to a stable, managed state. Their confidence has taken the form of a rising budget, a hands-off management style, and a sense of trust in my ability to get results.

The organization is now in mid-transition to a Windows Server 2003/ Exchange 2003 environment, and phasing out the last of its Windows NT / Exchange 5.5 servers. Improvements in security, manageability (such as MS "Software Update Services" and the upcoming "Windows Update Services"[14] , for small-network patch management), standards-based services (like DNS) and feature sets (i.e., email filtering and more secure Outlook remote access) in the 2003 products, not to mention NT's soon-to-be unsupported status, have prompted the transitions. We also have had a multi-domain NT environment, but can now consolidate to one domain, using organizational units instead. This should vastly simplify the management of domain trusts and user accounts. Why such total reliance on Microsoft? Open-source server solutions have been evaluated, but are not a good fit for us now because of MS-dependent software that the City has adopted. It has been our experience that practical choices in non-Windows financial and law enforcement packages for small cities like ours, sadly, range from slim to none.

Segregation of our outward-facing services in a stand-alone hardware DMZ is underway, and this, coupled with security and feature improvements in Exchange 2003, should finally provide the ability to add secure webmail and Exchange services for traveling staff. Hardware is in place to provide fixed-IP ADSL global-tunnel VPN connections with our three remote department offices, and implementation testing has begun. Bringing the remote departments under the managed LAN / domain umbrella in this way will simplify antivirus, filtering and patch management tasks, will complete the migration of data storage from desktop to server, and provide direct Exchange server and document management services to the remote users. The risks of implementing the VPNs seem to be pretty evenly balanced against the risks and extra work of having unmanaged remote offices. Our ADSL network provider has managed to keep VPN traffic locally routed, which reduces its exposure to sniffers.

Improved border security through IDS (intrusion detection) and IPS (intrusion prevention) hardware and software is being budgeted for each of the coming two years. Without the benefit of security and network training, however, the information gleaned

from such systems would probably mean little to me. Open-source border routers and hardened external mail relays are being explored as additional, affordable security improvements. A basic third-party network security audit has been planned and budgeted for the upcoming fiscal year, which will undoubtedly put all of my previous efforts into a new and interesting perspective - and create a new punch list of issues to fix.

Despite the shortcomings of this city's experience with information security, I'm honestly convinced that we've come a long way, and are in a far better place today. Good luck has helped, which is another way of saying that luck sometimes did substitute for skill. While we still have quite a distance to go, there's more skill and less luck involved these days, and it seems we're headed in a good direction.

Conclusions

1. Security staffing is serious business. If you're a small organization just tackling the question of whether to hire IT staff, *please* don't do what we did. Even small organizations with information security issues should find, and be willing to pay for, security-qualified staff or contractors. Information security is a dauntingly complex moving target, and failure can have a very high cost. In retrospect, the profound level of insecurity which existed at the beginning of the project was a real emergency, and needed immediate resolution. Assessing problems and providing solutions with untrained staff prolonged the vulnerabilities and risk, and did not help to insure thorough, positive results. Retaining fully qualified staff or contractors even at a much higher cost would have been the appropriate choice for the city.

2. Build on a solid conceptual foundation. Looking back, as the pieces of the security puzzle slowly fell into place, it seems that almost without exception they represented aspects of "defense-in-depth". While it may often be a hackneyed buzz phrase, in a deeper sense it is arguably both an intangible, philosophical construct and at the same time a shifting set of principles that is constantly tailored to a shifting context. My discovery of defense-in-depth principles early in this project gave me a touchstone by which to judge how we were doing, what was important, and what was missing.

3. Management should be your ally. Cultivating management's support of ongoing staff training and an adequate security budget is vital. Briefing them regularly on the threat environment in terms they can understand moves them closer to where you are standing, and helps them to be more successful managers. Knowing how to calculate incident and training costs, and thus the ROI of training and certification, is likely to be necessary to achieve management's support. And finally, IT staff must earn their employers' unqualified trust by getting positive, consistent results, so that they are not second-guessed into ineffectiveness.

4. Security staff needn't, and shouldn't, go it alone. For a small organization, a "team approach" to security awareness and defense can be decisive in good outcomes, such as achieving risk avoidance rather than incident remediation. Providing employees with security briefings, take-home information and how-to sessions on such topics as spyware, viruses, scams, phishing, social engineering and basic security practices is an investment that makes sense, builds good will, and leverages the limited resources of a small IT shop.

References

1. Microsoft Corp. "How to Enable Strong Password Functionality in Windows NT." Microsoft Knowledge Base Article – 161990. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q161990 (6 Sept. 2004.)
2. Vidstrom, Arne. "Strongpass." NTSecurity.nu. URL: http://ntsecurity.nu/toolbox/strongpass/ (6 Sept. 2004.)
3. Microsoft Corp. "Relaying and unsolicited commercial e-mail in Exchange Server 5.5." Microsoft Knowledge Base Article 836500. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;836500&Product=ech (8 Sept. 2004.)
4. Symantec Corp. "Updating Symantec AntiVirus Corporate Edition virus definitions without using LiveUpdate." Document ID 2004061116024848. 5 Aug. 2004. URL: http://service1.symantec.com/support/ent-security.nsf/pfdocs/2004061116024848?Open&dtype=corp (13 Sept. 2004.)
5. Salois, Gene. "Case Studies in the ROI of Training." Chief Learning Officer. March 2003. URL: http://www.clomedia.com/content/templates/clo_feature.asp?articleid=132&zoneid=31 (10 Sept. 2004.)
6. Dittrich, David A. "Developing an Effective Incident Cost Analysis Mechanism." Security Focus. 12 Jun. 2002. URL: http://www.securityfocus.com/infocus/1592 (13 Sept. 2004.)
7. Young, Debra. "Battling the Bean Counters -- and Winning." TechRepublic. 17 Nov. 2003. URL: http://techrepublic.com.com/5102-6298-5090897.html (14 Sept. 2004.)
8. Mullins, Michael. "Use risk management to balance functionality and security." TechRepublic. 4 Nov. 2003. URL: http://techrepublic.com.com/5100-6264-5094245.html (14 Sept. 2004.)
9. Schaadt, Nancy. "High-tech security full of opportunities." Seattle Times, Business & Technology (web edition). 14 March 2004. URL: http://seattletimes.nwsource.com/html/businesstechnology/2001878537_hottech14.html (14 Sept. 2004.)

10. Walsh, Lawrence M. “Infosecurity Salaries: Dollar Daze.” Information Security. Sept. 2003. URL: http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss81_art186,00.html (16 Sept. 2004.)
11. SANS Institute. “The SANS Security Policy Project.” URL: http://www.sans.org/resources/policies/#template 7 Sept. 2004.
12. Rogers, Lawrence R. “Home Computer Security.” US-CERT. 26 May 2004. URL: http://www.us-cert.gov/reading_room/HomeComputerSecurity/ (13 Sept. 2004.)
13. Pisello, Tom. “The ROI for antispam initiatives.” SearchSmallBizIT.com. 2 July 2004. URL: http://searchsmallbizit.techtarget.com/columnItem/0,294698,sid44_gci991440,00.html (14 Sept. 2004)
14. Microsoft Corp. “Windows Update Services Open Evaluation Version.” URL: http://www.microsoft.com/windowsserversystem/sus/wusbeta.mspx (14 Sept. 2004.)