Global Information Assurance Certification Paper

GISO – Basic Practical Assignment

Information Security Officer Training

Version 1.0 (October 30, 2001)

Prepared by:

Rich Richenberg
SANS Network Security 2001
San Diego, California

04 Feb 2002

Description of GIAC Enterprises

- GIAC Enterprises is a San Diego, California-based consulting company with operations, sales and information technology support offices dispersed across the United States. Its revenues are derived solely from consulting engagements. GIAC Enterprises' primary services facilitate corporate asset management, IT support delivery and employee self-service functionality implementations.

IT Infrastructure

- GIAC Enterprises' IT infrastructure (figure 1) is centralized at its corporate campus in San Diego, California. The WAN incorporates a hub and spoke TCP/IP topology. There are four additional North American regional IT hubs servicing outlying offices. Virtual private network (VPN) technology is used to provide access to network resources for remote and mobile users. Each hub has its own T1 Internet connection, VPN concentrator, router, fire wall and switch fabric. Each hub site also has a DMZ. Intrusion detection and Network Address Translation is in use. This architecture supports GIAC's "defense in depth" strategy that incorporates access control lists, conduit statements, intrusion detection tools, internal network obfuscation and encrypted remote access.

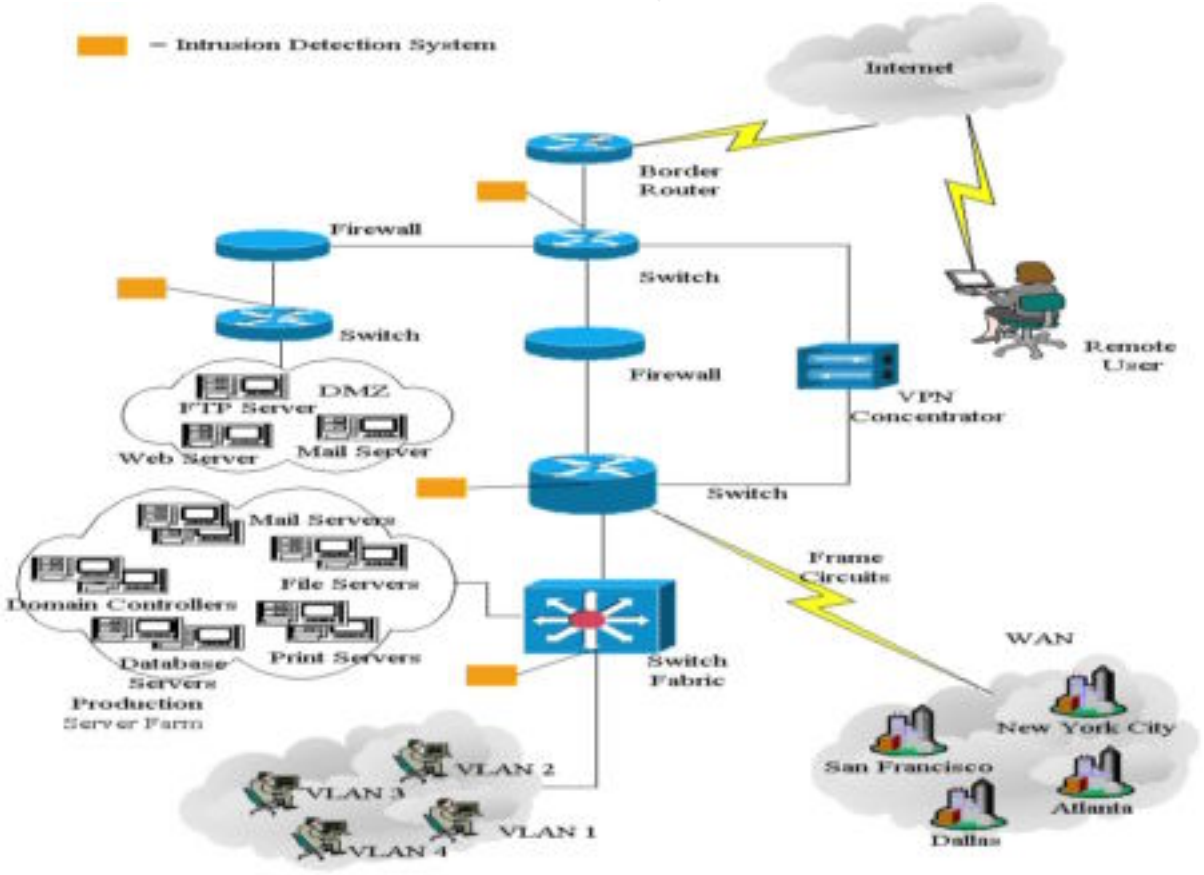

Figure 1

- The production servers are comprised of Compaq Proliant DL 580s with Smart Array Cluster Storage running Microsoft's Windows 2000 Server software. Service Pack (SP) 2 and the pre-SP 3 security rollup patch have been applied.
- Employee's computer systems are comprised of Intel-based Toshiba Tecra 8200 laptops and clone systems. All systems are procured, imaged and distributed via the San Diego site.

Business Operations

- GIAC Enterprises employees must be provided with reliable telephone, fax, email, Internet, file and data base access whether accessing these resources locally from the GIAC internal network or remotely via the Internet. Furthermore, specific protections must be afforded employee and company private data. The company utilizes industry standard office productivity software (word processing, spreadsheet, data base, email and Internet browser, etc.) that is fully and solely supported by IT. Customers, business partners and suppliers must be able to freely access and exchange relevant information electronically with the company. To the extent that corporate network assets are directly accessed by non-company personnel, those assets must be located in the network DMZ and properly secured. For those employees in outlying hub and spoke offices, access to the corporate network is via frame relay circuits. Given the dispersed nature of the corporate sales force, remote access for employees not directly connected to the WAN is provided via dual-authentication VPN.

- File exchanges between customers and the company are conducted via ftp. The company's sole supported and authorized email is via Microsoft Outlook and Exchange. The Company has recently completed an enterprise-wide migration to the Windows 2000 operating system. As such, all current Service Packs, patches and hot fixes are applied. Necessary office productivity functions are enabled via Microsoft Office XP. The VPN client in use is Cisco's version 3.11 and dial up access is provided via a UUNet PAL dialer.

Areas of Risk

- Insufficient security awareness/training for users (initial/recurring).
    - This is an area of concern for GIAC Enterprises for the same reason it is a concern to all companies: employees are both the single largest security liability, from an exposure standpoint, and the single greatest asset, from a return on investment standpoint, a company has.
    - The particular threat risk falls into several categories
        - Employees may become victims of social engineering, unwittingly divulging sensitive information to people who do not meet both the appropriate clearance and need to know criteria established by the company (e.g. assuming a caller is from "IT Support" or is the CEO's secretary without verifying their identity)

        - Employees may increase the potential for a breach because their individual work behavior does not factor in security considerations (e.g. opening email attachments from unknown senders)
        - Employees who are "security aware" may not know what to do in the event of a breach or suspected breach (e.g. "coat-tailing")
    - The possible consequences are myriad. Some examples are
        - Passwords may be compromised
        - Malicious code may be spread
        - Unauthorized physical access may be gained
    - The recommended steps to mitigate the risk are
        - Raise employee awareness of the risks
        - Arm employees with the knowledge they need to participate in reducing risk exposure
        - Let employees know what their appropriate course of action is if the become aware of or suspect a breach
        - Update/reeducate employees regularly. This can be accomplished via regularly distributed newsletters. Since GIAC is not in the news letter business, services such as those offered by the Computer Security Institute could be enlisted:

          "Motivate your end-users to better security practices with FrontLine. This quarterly 4-page newsletter is designed to increase awareness in every employee in the organization. Written in an easy-to-understand format, it covers a wide variety of security topics of critical importance to the end-user. Customize with your own company logo, and include your own message in space provided. Saves hours of your time! PDF format for Intranet distribution also available."[1]

    - Relative to other security measures, costs for employee security awareness programs are extremely modest. Videos and customizable newsletters are widely available which means GIAC doesn't necessarily need to hire additional staff to provide regular security training for its employees. For about $700, the company can distribute a quarterly newsletter for one year or purchase one video. Additionally, there are security screen savers and interactive programs available, some of which can be launched at logon. These solutions cost from $2,000 to $3,000, depending on the size of the organization.
- Securing corporate information (internal/external)
    - This is an area of concern because GAIC Enterprises, like many companies, has information it needs to keep private in order to be both competitive within its industry and responsible within its own organization. GIAC's software code, its crown jewels, must be protected with the same vigor as the CEO's medical history and other employees' personal data. Furthermore, prying eyes are as likely to be inside the company as outside.
    - The particular threat or risk could be any one of a number of malicious code attacks that, if successful, would lay GIAC's network or computers bare. An

[1]Computer Security Institute, https://wow.mfi.com/csi/order/frontline.html

example would be Backdoor programs. These programs allow unauthorized access to computers. They can be used to steal passwords, log keystrokes crash systems and enable access to all manner of sensitive information. Some of the more common backdoor programs are Back Orifice, Sub7, Netbus and Deep Throat. Additionally, the increasing availability and use of peer-to-peer (P2P) and instant messaging (IM) applications in the workplace present special challenges of their own. TheP2P applications are agile enough to use varying ports and the IM providers can add and delete IP addresses practically at will, making these applications extremely difficult to control. Even if the P2P activity can be sufficiently monitored, a crafty employee or contractor with access to proprietary information, like source code, could use any of a number of utilities to disguise a file full of code as a music, graphic or similar file. Once that's done, source code could be transferred out of the organization and appear to be "usual" P2P activity.

  - The possible consequences stem from both legal and economic liabilities. In the legal context, GIAC, as a publicly traded corporation, has a fiduciary obligation to its stockholders to exercise due diligence in protecting corporate assets. Similarly, GIAC bears responsibility for protecting employee and customer information. Though the legal ramifications can get somewhat fuzzy, the economic consequences stemming from a loss of confidence in a company's ability to conduct business responsibly are well known. A plummeting stock price, the scorn of analysts, falling employee morale, fleeing customers, etc. are outcomes no company enjoys.
  - Recommended steps that can be taken to mitigate the risk reflect GIAC's strategy of "Defense in Depth." There must be layers of access controls and each layer must reflect prudent security practices.
  - The costs of enabling these protections runs in the hundreds of thousands of dollars and require dedicated security staff whether a managed security provider is contracted with or not. Depending on the assets being protected, initial implementation can take the better part of a year if the corporation is starting from scratch.

- Protecting remote users' systems (physical/technical)
  - Because security and convenience are diametrically opposed, remote systems are of special concern to GIAC Enterprises. This is true because these systems, more so than the desktop systems, spend less time under GIAC's direct supervision and require the greatest degree of flexibility in configuration. The users are often granted local administrative rights and may be more prone to being lackadaisical when it comes to security issues. So, these systems, unlike desktop systems, require special consideration for their protection. On the road, users enjoy the convenience of being able to surf the Internet, check email and provide sales demonstrations free, largely, of the security protections afforded the corporate network. Ultimately, these systems can all too easily be used to circumvent standard security protections in place, whether accidentally or intentionally, once reconnected to the corporate network. If stolen, sensitive data may be exposed on the local hard drive. If compromised, the system could become an unwitting back door to the corporate network.
  - A particular physical threat is that the laptop can be stolen.

> "Laptop theft is a huge problem, according to security industry and insurance company statistics. Safeware (www.safeware.com), an Ohio-based insurance firm specializing in PC policies, reports that nearly 320,000 laptops valued at $800 million were stolen in 1999, a 5 percent increase over the previous year. The trend is mirrored by the expansion of the laptop security market, with some manufacturers reporting 40 to 50 percent annual growth rates. "Criminals are definitely targeting laptop systems, especially systems that cost more than $3,000," says Brian Haase, a commercial marketing manager for Safeware. Haase says that in 1999, notebook computers accounted for 88 percent of all of Safeware's total computer theft claims, compared to 53 percent in 1997."[2]

    - Also, since users work both on and off line, there is increased risk of sensitive information being exposed either by someone looking over their shoulder as they work on the plane or at the airport terminal or by their connecting to the network at a client's site, etc. Additionally, there is increased risk because these users are also more likely to access the Internet through unprotected connections from their hotel rooms or airport payphones, etc. There is ample opportunity for backdoor programs to be installed, which ultimately, could circumvent protections in place on the corporate network once a remote user reconnects. Sessions, unless encrypted, can also be sniffed, with the intent to facilitate further compromise.
    - The possible consequences are the same as for other points of exposure: information compromises that could lead to public embarrassment (e.g. the Qualcomm CEO whose laptop was stolen practically from under his nose), loss of credibility with customers and/or share holders, loss of competitive advantage, depressed stock price, etc.
    - Recommended steps that can be taken to mitigate the risk fall into two categories:
        - Anti-theft: the installation of physical security devices (e.g. "screamers", cables, etc.)
        - Access controls: the installation of personal firewall software (e.g. ISS BlackIce), password protecting the hard drive, remote access encryption (e.g. Cisco's VPN solution) and dual-authentication requirements (e.g. RSA's SecureID solution).
    - Initial costs for providing dual-authentication VPN access start at around $70 per client plus an additional $3,000 to $10,000 for backend hardware. Personal firewall protection adds about another $50 per client. Security cables run about $25 per client and the audible theft alert devices run about $45 per client.
- Adequately addressing legal liability issues (copyrights, harassment, etc.)
    - Much the same as for other areas of concern, this issue can have a direct and disastrous impact on a company's bottom line.
    - Specific risks can be enumerated in the context of lawsuits brought against a company that doesn't take proper measures to
        - reign in the illegal downloading and/or sharing of copyrighted materials using corporate assets

[2] Korzeniowski, p69

        - prevent the viewing and/or distribution of offensive materials using corporate assets (pornography, discrimination, stigmatization, etc.)
    - Add to that potentially nullifying much of the investment in security infrastructure that accompanies peer-to-peer networking schemes and it's easy to see why this is of concern to GIAC Enterprises.
    - Consequences range from financial penalties to morale problems to negative publicity
    - The recommended steps to mitigate these risks must include clear acceptable use policies for corporate assets as well as appropriate consequences for anyone running afoul of the policies. The policies and consequences must be well publicized. In addition, the company must have mechanisms in place to monitor use of corporate assets and provide for non-repudiation when necessary.
- Integrating acquired companies and/or personnel
    - As mentioned in Hacking Exposed, Second Edition, organizations will often "scramble to connect the acquired entities to their corporate network with little regard for security."[3] Inasmuch as GIAC Enterprises is an acquisitive company, this behavior and the ensuing vulnerabilities it creates is of grave concern. Hackers or other malcontents can use the acquired company's security weaknesses to circumvent protections in place at GIAC. As an example, even though GIAC Enterprises may have multiple layers of anti virus protection in place, if the acquired company has no anti virus protection, it is ripe for being infected by NIMDA or similar code and passing it on to GIAC through file shares.
    - Backdoors that either exist in a company about to be acquired or find easy entry because of a lack of security protections could also create significant problems for GIAC. Absent the acquisition, the company being acquired may have gone unnoticed by hackers. Once made public knowledge though, an unprotected company can quickly be compromised with the ultimate goal of creating an entry point to GIAC Enterprises. An analogy would be attacking a global corporation's tertiary web sites because they may be easier to compromise than the main site as has happened to Microsoft.
    - Here again, the possible consequences are staggering stemming from both legal and economic liabilities. Did GIAC exercise due diligence in planning and executing the integration? Was customer or employee data compromised? What does this say about GIAC's ability to be a responsible corporate citizen? How were GIAC's profits/stock price affected? What resources will GIAC have to siphon away from product development, marketing, etc. to clean up the fall out? Did GIAC's compromise expose partners, customers, etc. to compromise?
    - Fortunately, the questions raised above can be easily avoided by laying some groundwork ahead of time. Steps must be taken to assess the new acquisition's security posture. Have they ever been compromised? What's the network topology? What are the critical assets? What are the critical applications? What security protections are currently in place (anti virus, intrusion detection, etc.)? What procedures are in place? Are employees educated on security issues? Once this information has been gathered, GIAC can take steps to apply their corporate

[3] Scambray, et al, p. 12.

security standard for protection and make it a prerequisite to connecting the two companies' infrastructures. GIAC's Acquisition Integration Security Questionnaire (Appendix A) provides a good start on assessing posture

- The incremental costs involved in bringing the company about to be acquired into compliance with GIAC security standards is small and provides an attractive return on investment. This is because GIAC already has established relations with vendors and receives preferential pricing based on the licenses, maintenance and consulting services previously purchased. Add to that the accounting benefits of being able to charge the expenditures to the mergers and acquisitions budget, and you remove a disincentive from the CIO's department: no budget for unforeseen security expenditures.

Security Policy

- The following GIAC security policies are set forth by the CIO and shall remain in effect indefinitely. Exceptions to said policies require express, written approval by the CIO
  - Acquisitions Integration
    - **Purpose:** This policy is being established to ensure acquired companies are protected in accordance with GIAC's security protection standards prior to being connected to GIAC's infrastructure.
    - **Background:** GIAC has made a substantial investment in security protection procedures, tools, personnel and policies to safeguard corporate assets. Since merging corporate infrastructures can create opportunity for unauthorized access if not properly planned and executed, it is imperative that no such merging take place absent appropriate pre-merger considerations. Considerations will include but not be limited to applying the GIAC security standard to the acquired company's LAN/WAN, server, laptop and desktop infrastructure.
    - **Scope:** This policy will apply to all merger and/or acquisition activity undertaken by GIAC Enterprises.
    - **Policy Statement:** An acquired company's network shall not be connected to GIAC Enterprise's network nor shall any assets of the acquired company be authorized to access GIAC Enterprise's network without the express written consent of the CIO. The CIO's consent will be predicated on successful implementation of the standard GIAC security protections within the acquired company as certified by the Director of Corporate Security.
    - **Responsibility:** The CIO is responsible for ensuring this policy is fully enforced. The Director of Corporate Security is responsible for certifying GIAC security standards have been successfully implemented. The Directors of IT Operations and Network Communications are responsible for implementing the GIAC security standards, documenting the actions taken and certifying completion to the Director of Corporate Security.
    - **Action:** Upon formal notification that a company is to be acquired the Director of Corporate Security will initiate GIAC's Mergers and Acquisitions Integration IT Plan (Appendix B). All documentation will be

thoroughly reviewed by Security, Operations and Network staff. The current state of the acquired company's infrastructure will be assessed against GIAC's standards and the plan will be used to address any changes necessary. This process will be fully integrated into planning and implementing the actual network integration. In no case will the acquired company be authorized to connect to the GIAC network prior to all protection actions being completed without the express, written authorization of the CIO.

- Protecting remote user's systems
  - **Purpose:** This policy is established to ensure adequate security protection is afforded to GIAC's mobile and remote user systems.
  - **Background:** Mobile and remote users will be accessing the GIAC network and the Internet via non-GIAC controlled venues. GIAC cannot be assured these connection transports provide the same level of protection from intrusion afforded GIAC systems based in corporate facilities. Further, GIAC cannot assume the traffic between the mobile systems and the corporate LAN is safe from compromise. Additionally, GIAC's current Internet content filtering architecture cannot be easily extended to mobile or remote users since they will not be obtaining Internet access via the corporate LAN. Absent appropriate protections, these systems would be easy prey and could provide unauthorized entry points (backdoors) to the corporate network.
  - **Scope:** This policy applies to all mobile and/or remote systems issued by GIAC. For the purposes of this policy, "mobile" and "remote" systems are defined as any GIAC systems not connecting to the corporate LAN or the Internet via venues not governed by GIAC security standards.
  - **Policy Statement:** All GIAC issued mobile or remote systems must be configured with the corporate standard anti virus, personal firewall and VPN (if applicable) software. Further, no configuration modifications are authorized without the express, written consent of the CIO. For those systems requiring VPN access, a dual-authentication mechanism will be required.
  - **Responsibility:** The Corporate Security department is responsible for certifying the anti virus, personal firewall and VPN software configurations adequately reflect GIAC's security concerns within the constraints set forth by the CIO. Corporate Security is also responsible for conducting random audits of system builds to verify compliance with this policy. The IT Operations department is responsible for installing, configuring, maintaining and supporting the anti virus and personal firewall software in accordance with the certified configuration. The Network Communications department is responsible for installing, configuring, maintaining and supporting the VPN software in accordance with the certified configuration. The IT Operations and Network Communication departments are also responsible for providing and administering the backend servers necessary to support the client software.

        - **Action:** Effective immediately, IT Operations will incorporate the inclusion of anti virus, personal firewall and VPN software (where appropriate) into all base images designed for mobile and remote systems. IT Network Communications will ensure necessary user accounts and user training are in place at time of system issuance.
    - Awareness training
        - **Purpose:** This policy is being established to ensure GIAC Enterprises adequately trains its employees in the context of security awareness.
        - **Background:** No amount of technology will ever replace the "ounce of prevention" afforded by properly training employees on security issues, policies and responsibilities. Despite the perceived high tech cloak and dagger image of the hacker world in some people's view, hackers often rely on low-tech social engineering to gain unauthorized access. A password, even a really strong password, is of little consequence if not jealously guarded. A physical access control system is of little value if a "helpful" employee holds the door open for a person unknown to them.
        - **Scope:** This policy applies to all GIAC employees and contract employees.
        - **Policy Statement:** As a condition of their employment, all GIAC employees and contract employees must receive initial and recurring security awareness training and sign the GIAC User Agreement. These actions must be accomplished within one week of their official start date, in the case of the initial briefing, or as part of their performance evaluation activities, in the case of the recurring briefing.
        - **Responsibility:** It is the responsibility of Corporate Security to develop, maintain and present the initial Security Awareness briefing, the recurring Security Awareness briefing and the GIAC User Agreement. It is the responsibility of Human Resources to arrange both the initial and recurring training, maintain file copies of the GIAC User Agreement and ensure employees complete the training.
        - **Action:** Effective immediately, Human Resources will incorporate the Security Awareness briefing into its New Hire Orientation and annual performance evaluation cycles. The signed User Agreement is the only acceptable confirmation that the training has been completed. Corporate Security will review the contents of the Initial and Recurring Security Awareness briefings with a designated Human Resources representative and an agreement will be reached on the amount of time slated for security in the New Hire Orientation and recurring training events. Corporate Security will review the content of the User Agreement with Human Resources and Legal department representatives before submitting to the CIO for approval. Corporate Security will also conduct random, spot audits to verify User Agreements are signed and on file as directed by this policy.

Security Policy Procedure

The following procedure will be used to implement and enforce GIAC's **Acquisitions Integration** security policy. Preparatory actions proscribed herein will be certified as accomplished in writing by the respective designees to the CIO within 30 business days.

- The CIO will brief the Mergers and Acquisitions (M&A) team on the necessity for integrating a security component into their decision-making process. Further, he will appoint the Director of Corporate Security to the M&A team. These actions are important to both establish the importance of security as a core integration consideration and to provide for accountability in the event security is not given proper consideration.
- The CIO will brief the current principal owners of the IT integration process (the Directors of IT Operations and Network Communications) on the necessity of including the security component into their integration process. Further, the CIO will formally establish completion of the Mergers and Acquisition IT Integration Plan and the Acquisition Integration Security Questionnaire as prerequisites to integrating an acquired company. The CIO will also formally establish the application of GIAC security standards to the acquired company as a prerequisite to network integration authorization. These actions are important to both establish the importance of security as a core integration consideration and to provide for accountability in the event security is not given proper consideration.
- The CIO will modify the composition of the IT acquisition team to include the Director of Corporate Security as one of its three principal owners. These actions are important to both establish the importance of security as a core integration consideration and to provide for accountability in the event security is not given proper consideration.
- The Director of Corporate Security will brief the M&A team on the current GIAC standards for protection and present the Mergers and Acquisition IT Integration Plan and the Acquisition Integration Security Questionnaire. Further, the Corporate Security Director will formally establish completion of the plan and questionnaire as part of the M&A process. These actions are important to ensure the M&A team understands both the current security posture at GIAC and the scope of the security concerns when integrating another company. Establishing completion of the plan and questionnaire as part of the formal M&A process ensures all members of the team are aware of their joint responsibility for these items.
- The M&A team will formalize the appropriate point in the process at which discovery of the target company's security posture will begin. This is important to ensure security considerations are brought in sufficiently early so as not to adversely impact the overall progress of the integration process.
- The Director of Corporate Security will, in cooperation with the IT Operations and Network Communications Directors, establish the appropriate time frame to audit completion of the plan and questionnaire and all security standards implementation actions. This time frame must reflect the possibility the audit will find some actions as yet incomplete. The time frame must also provide sufficient lead-time for the CIO to have any questions answered or details provided as a prerequisite to his approval for moving forward with the integration. These steps are necessary to ensure the integrity of the process that supports the policy.

- The Corporate Security Director will brief his IT Operations and Network Communications counterparts on GIAC's current security protection standards. He will also present the Mergers and Acquisitions IT Integration Plan and Acquisition Integration Security Questionnaire and establish completion of these as part of the formal IT integration process. This action ensures all members of the team are aware of their joint responsibility for these items.
- Upon notification of acquisition activity, the Corporate Security Director will determine who the security point of contact is for the target company. If there is no security point of contact, the Corporate Security Director will determine who the IT operations, network and facilities points of contact are. This step is important because it establishes who is responsible for initiating the process and communicates the importance of security considerations to the company being acquired.
- At the agreed upon time in the acquisition process, the Director of Corporate Security will initiate the Mergers and Acquisitions IT Integration Plan and formally introduce the plan and questionnaire to the point(s) of contact at the target.

Appendix A

GIAC ENTERPRISES
ACQUISITION INTEGRATION SECURITY QUESTIONNAIRE

PHYSICAL SECURITY

Security Administration

Who is the primary contact for all Physical Security systems?

1. Name
2. Email address
3. Phone number

Access Control Systems

1. Do you have access controls at all locations?
2. What type of system is it?
3. Who is the primary administrator?
4. Are Photo Badges issued to all employees?
5. Do you have a set lock down schedule for all outside doors?

Intrusion Detection System (physical)

1. Do you have Intrusion Detection systems installed at all locations?
2. What type of system is it?
3. Are PIN codes issued to all employees?
4. What is the process for arming and disarming the system?

Hard Keys

1. What type of hard key control is used at each office?
2. What key system is used?
3. Who is issued Master keys?
4. Are records kept regarding whom keys are issued to?
5. If so, by whom

Emergency Evacuation

1. Do all offices have posted emergency evacuation plans?

a. If yes, please include a copy of the plan

2. How often is the plan tested?
3. When was the last evacuation drill preformed?
4. Do all buildings have audible fire alarms? If no, what is the secondary plan?

Security Guard Services

1. Is a Security Guard Company employed to patrol the facilities?
2. If yes, what company?
3. What are the hours of the patrol?

TECHNICAL SECURITY

Security Administration

Who is the primary contact for all technical security issues?

1. Name
2. Email address
3. Phone number

Incident Response

Has your company ever been compromised? If so

1. Describe the nature of the compromise
2. Describe the corrective actions taken
3. Was it made public knowledge?

Do you have an Incident Response Procedure? If so, please attach to this questionnaire

Intrusion Detection Systems

Do you have Intrusion Detection systems installed? If so

4. At which locations?
5. What types of systems are in place (i.e. host and/or network based)?
6. What software/hardware is used?
7. Is licensing current?
8. When is renewal due?
9. What reports are run?
10. How often are reports run?
11. How and by whom are the systems monitored?
12. What process is in place to resolve actionable events (incident response/false alerts)?

Vulnerability Assessment Systems

Do you have vulnerability assessment systems installed? If so

1. At which locations?
2. What type of system is it (i.e. Host and/or Network based)?
3. What software/hardware is used?
4. Is licensing current?
5. When is renewal due?
6. What reports are run?
7. How often are reports run?
8. How and by whom are the systems monitored?
9. What process is in place to resolve actionable events (fix or accept risk)?

Internet-Filtering Systems

Do you have Internet-filtering software in place? If so

1. At which locations?
2. What type of system is it?
3. What software/hardware is used?
4. Is licensing current?
5. When is renewal due?

6. What reports are run?
7. How often are reports run?
8. How and by whom are the systems monitored/updated?
9. What process is in place to resolve actionable events (e.g. a user requesting access to a filtered site, creating specific blocks for unauthorized sites, etc.)?

Anti Virus\Malicious Code Protection
Do you have anti virus\malicious code defense systems installed? If so
1. At which locations?
2. What software/hardware is used?
3. Is licensing current?
4. When is renewal due?
5. What reports are run?
6. How often are reports run?
7. How and by whom are the systems monitored/updated?
8. What process is in place to resolve actionable events (incident response/false alerts)?

Security Policies
Do you have Security Policies in place? If so, please attach documentation to this questionnaire
1. Where are they published?
2. How are employees informed of new policies?
3. Is there an "Employee Agreement" in place?
4. How is policy compliance audited?

Security Patch Process
Do you have a process in place to discover and/or install OS/Application security patches? If so, please attach documentation to this questionnaire
1. Are they tested prior to installation? How?
2. Who determines if the patches are relevant?

Network
Describe your network topology
1. Is it documented? If so, please attach to this questionnaire
2. Where is network documentation archived?
3. What is your change control process?

Servers
Describe your server population
1. Is it documented? If so, please attach to this questionnaire
2. Where is server documentation archived?
3. What is your change control process?

Desktops
Describe your desktop population
1. Is it documented? If so, please attach to this questionnaire

2. Where is desktop documentation archived?
3. What is your change control process?

Remote Access
Describe your remote access architecture
1. Is it documented? If so, please attach to this questionnaire
2. Where is remote access documentation archived?
3. What is your change control process?

Other Access
Describe any access to the company network provided for assets and/or people not employed by the company
1. Is it documented? If so, please attach to this questionnaire
2. Where is this access documentation archived?
3. What is your change control process?

Other Access
Please describe any other issues relevant to security as it applies to your company.

Appendix B

GIAC ENTERPRISES
MERGERS AND ACQUISITIONS IT INTEGRATION PLAN

SECURITY	
PRE-PLANNING	
Notice Received	Corporate Security Director
Preliminary Information Gathered	Corporate Security, IT Operations and Network Directors
Due Diligence Support - As Required	Corporate Security
Await M&A Planning Approval	M & A
Discovery Planning	
Discovery Plan	Corporate Security, IT Operations and Network Directors
Identify Contacts	Corporate Security, IT Operations and Network Directors
Identify Locations/Sizes	Corporate Security, IT Operations and Network Directors
CONTACT AUTHORIZED	M & A
Launch Acquisition Security Questionnaire	Corporate Security Director
Initial Contact	Corporate Security Director
Determine Organization	Corporate Security Director, Corporate Security Information Specialist, Corporate Security Physical Security Manager
Identify Local Points of Contact	Corporate Security, IT Operations and Network Directors
Visit/Dialogue	Corporate Security, IT Operations and Network Directors
Collect Information	Corporate Security, IT Operations and Network Directors
Assess Policy	Corporate Security, IT Operations and Network Directors
Assess Standards	Corporate Security, IT Operations and Network Directors
Analyze Information	Corporate Security, IT Operations and Network Directors
Refine Integration Plan	Corporate Security, IT Operations and Network Directors
Await Acquisition Approval	M & A

DISCOVERY	
Physical Access Control	
Policy	Corporate Security Physical Security Manager
Processes	Corporate Security Physical Security Manager
Key Management	Corporate Security Physical Security Manager
Access Control Systems	Corporate Security Physical Security Manager
Access Categories/Privileges	Corporate Security Physical Security Manager
Intrusion Alarm Plans	Corporate Security Physical Security Manager
Surveillance System Plans	Corporate Security Physical Security Manager
Custodial Services Access	Corporate Security Physical Security Manager
Reception	Corporate Security Physical Security Manager
Guard Force	Corporate Security Physical Security Manager
Response Force	Corporate Security Physical Security Manager
Badge System(s)	Corporate Security Physical Security Manager
Physical Access Control Contracts	Corporate Security Physical Security Manager
Emergency Plans	
Assess Evacuation Plans	Corporate Security Physical Security Manager
Assess Duress Procedures	Corporate Security Physical Security Manager
Assess Threat Procedures	Corporate Security Physical Security Manager
Infrastructure Protection	
Discover the Network	Network Communications Director, Network Specialist
Identify Critical Servers	IT Operations Director, Sys Admin Specialist
Assess Vulnerability Identification	Corporate Security Information Specialist
Assess Perimeter Protection	Corporate Security Information Specialist
Assess Authentication Process	Corporate Security Information Specialist

Assess Intrusion Detection	Corporate Security Information Specialist
Assess Malicious Code Protection	Corporate Security Information Specialist
Assess Event Forensics Capability	Corporate Security Information Specialist
Assess Desktop Protection	Corporate Security Information Specialist, Desktop Specialist
Assess Configuration Management	Corporate Security, IT Ops and Network Directors
Document Infrastructure Protection	Corporate Security Information Specialist, Network Specialist and Sys Admin Specialist
Bandwidth Protection	
Assess Bandwidth Protection	Corporate Security Information Specialist
Assess Network Utilization	Network Specialist
Business Continuity Plans	
Request Current Plans	Corporate Security, IT Operations and Network Directors
Assess the BCP Program	Corporate Security, IT Operations and Network Directors
Identify Deficiencies	Corporate Security, IT Operations and Network Directors
Current Budgets	
Current Projects	Corporate Security, IT Operations and Network Directors
Planned Projects	Corporate Security, IT Operations and Network Directors
Get Actuals	Corporate Security, IT Operations and Network Directors
Awareness Programs	
Assess Plans	Corporate Security, IT Operations and Network Directors
Assess Current Program	Corporate Security, IT Operations and Network Directors
PHASE 1	
Plan Phase 1	Corporate Security, IT Operations and Network Directors
Policy Review	Corporate Security Director
Policy Determination	Corporate Security Director
Plan Technical Risk Assessment	Corporate Security Information Specialist
Plan Physical Risk Assessment	Corporate Security Physical Security

	Manager
Process Deficiency Mediation	Corporate Security, IT Operations and Network Directors
Deficiency Mediation Plans	
Access Control	Corporate Security Physical Security Manager
Key Management	Corporate Security Physical Security Manager
Access Control Systems	Corporate Security Physical Security Manager
Access Categories/Privileges	Corporate Security Physical Security Manager
Intrusion Alarms	Corporate Security Physical Security Manager
Surveillance Systems	Corporate Security Physical Security Manager
Reception	Corporate Security Physical Security Manager
Guard Force	Corporate Security Physical Security Manager
Response Force	Corporate Security Physical Security Manager
Badge System(s)	Corporate Security Physical Security Manager
Resources	
Physical Access Control Contracts	Corporate Security Physical Security Manager
Identify Budget Source	Corporate Security Physical Security Manager
Awareness Programs	
Formulate Awareness Initiative	Corporate Security, IT Operations and Network Directors
PHASE 2	
Physical Requirements Analysis	
Schedule vendor Visit	Corporate Security Physical Security Manager
Coordinate Site Visits	Corporate Security Physical Security Manager
Advise vendor and Sites of Standard	Corporate Security Physical Security Manager
Vendor Site Analysis	Corporate Security Physical Security

	Manager
Vendor Recommendation	Corporate Security Physical Security Manager
Formulate Physical Plan	Corporate Security Physical Security Manager
Access Control	
Access Control Systems	Corporate Security Physical Security Manager
Access Categories/Privileges	Corporate Security Physical Security Manager
Intrusion Alarms	Corporate Security Physical Security Manager
Badge System(s)	Corporate Security Physical Security Manager
Technical Requirements Analysis	
Determine Revised IT Configuration	Corporate Security, IT Operations and Network Directors
Apply GIAC Policy	Corporate Security Information Specialist
Assess Current Protection	Corporate Security Information Specialist
Identify Need for Technical Tools	Corporate Security Information Specialist
Formulate Technical Plan	Corporate Security Information Specialist
Implement Technical Plans	Corporate Security Information Specialist
DMZ	
Assess DMZ Configuration	Corporate Security Information Specialist
Establish Gateway Policy	Corporate Security, IT Operations and Network Directors
Establish Firewall Policy	Corporate Security, IT Operations and Network Directors
PHASE 3	
Physical Security Implementation	
Receive Authority to Implement	Corporate Security Physical Security Manager
Confirm Plans/Budgets	Corporate Security Physical Security Manager
Obtain Funding	Corporate Security Physical Security Manager
Vendor PR/PO Signed	Corporate Security Physical Security Manager
Access Control	Corporate Security Physical Security Manager
Access Control Systems	Corporate Security Physical Security

	Manager
Access Categories/Privileges	Corporate Security Physical Security Manager
Badge System(s)	Corporate Security Physical Security Manager
Procedures	Corporate Security Physical Security Manager
Training	Corporate Security Physical Security Manager
Test/Acceptance	Corporate Security Physical Security Manager
IDS Implementation	
Perform initial risk analysis	Corporate Security Information Specialist
Identify critical servers	IT Operations Director
Acquire appropriate licenses	Corporate Security Information Specialist
Server Protection	
Install vendor System Scanners	Corporate Security Information Specialist
Run Planned Scans	Corporate Security Information Specialist
Assess System Vulnerabilities	Corporate Security Information Specialist
Consult with IT/Ops	Corporate Security Information Specialist
Open Problem Tickets	Corporate Security Information Specialist
Validate Ticket Closure	Corporate Security Information Specialist
Install System Sensors	Corporate Security Information Specialist
Connect to Infrastructure	Corporate Security Information Specialist
Train Personnel	Corporate Security Information Specialist
Network Protection	
Install vendor Network Scanners	Corporate Security Information Specialist
Run Planned Scans	Corporate Security Information Specialist
Assess Network Vulnerabilities	Corporate Security Information Specialist
Consult with IT/Networks	Corporate Security Information Specialist
Open Problem Tickets	Corporate Security Information Specialist
Validate Ticket Closure	Corporate Security Information Specialist
Install Network Sensors	Corporate Security Information Specialist
Wire into Infrastructure	Corporate Security Information Specialist
Train Personnel	Corporate Security Information Specialist
Database Protection	
Install vendor Database Scanners	Corporate Security Information Specialist
Run Planned Scans	Corporate Security Information Specialist
Assess Database Vulnerabilities	Corporate Security Information Specialist
Consult with IT/Ops	Corporate Security Information Specialist
Open Problem Tickets	Corporate Security Information Specialist

Validate Ticket Closure	Corporate Security Information Specialist
Train Personnel	Corporate Security Information Specialist
Anti-Virus Protection	
Assess Antivirus Configuration	Corporate Security Information Specialist
Configure Mail Server Protection	Sys Admin Specialist
Deploy Desktop Anti virus Protection	Desktop Admin Specialist
Bandwidth Protection	
Order Internet content filtering Server	Corporate Security Information Specialist
Expand License Quantity	Corporate Security Information Specialist
Build Internet content filtering Server	Corporate Security Information Specialist
Install Internet content filtering Server	Corporate Security Information Specialist
Identify VPN Needs	
Order VPN Authentication Tokens	Corporate Security Information Specialist
Deploy VPN Solution	Network Specialist
BUSINESS CONTINUITY	
Assess Business Continuity Plan	Corporate Security Director
Integrate Into BCP Planning Process	Corporate Security Director
AWARENESS TRAINING	
Training Assessment	Corporate Security Director
New Employee Briefing	Corporate Security Director
Employee Awareness	Corporate Security Director
Security Point of Contact Training	
Contingency Planning	Corporate Security Director
Emergency Evacuation Planning	Corporate Security Physical Security Manager
Procedures	Corporate Security Physical Security Manager
Reporting	Corporate Security Director

REFERENCES

Berg, Al. "P2P, or Not P2P?" Information Security Magazine February 2001 (2001): 38 – 51.

CSI.com. URL: https://wow.mfi.com/csi/order/frontline.html (1 Feb. 2002)

Korzeniowski, Paul. "Locking Down the Laptop." Information Security Magazine February 2001 (2001): 68 – 72.

Scambray, Joel. McClure, Stuart. Kurtz, George. Hacking Exposed: Network Security Secrets & Solutions, Second Edition. Osborne/McGraw-Hill, 2001. 12.

Vnunet.com. "Microsoft's New Zealand Web Site Hacked." 23 January 2001. URL: http://www.vnunet.com/News/1116687 (1 Feb. 2002).

Last Updated: October 17th, 2017

Upcoming Training

SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
Community SANS Columbus MGT512	Columbus, OH	Jan 15, 2018 - Jan 19, 2018	Community SANS
Community SANS New York MGT512^	New York, NY	Jan 22, 2018 - Jan 26, 2018	Community SANS
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Boston Spring 2018	Boston, MA	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced