

Technology Risk Checklist



May 2004
Version 7.3



Introduction

Digital technology enables the world to become increasingly interconnected as an entire economy becomes reliant upon a single, network infrastructure. While this offers tremendous opportunities to many industries, including financial, telecommunications, health, and transportation, it can also be a cause for concern if security issues are improperly addressed, or even neglected altogether. Heinous crimes such as theft, fraud and extortion can occur in great magnitude within a matter of seconds. The new network-mediated economy paradoxically presents unparalleled opportunities for the creation of good outcomes or the perpetuation of bad ones.

Trends in cyber crime reveal significant growth. Between 1999-2003 in the United States, attacks on computer servers increased by over 530% to 137,000 incidents.¹ This is partly attributable to vulnerabilities in software code, which have grown from a total of 500 in 1995 to over 9000 in 2002 (CERT). Developing countries are also being targeted, even as leapfrog technology is implemented. Brazil has seen hacker attacks increase by at least 100% yearly since 2000². These growing numbers bear particular importance on the financial sector. The International Data Corporation (www.idc.com) reported that more than 57% of all hack attacks last year were initiated in the financial sector (source and year). The FBI has corroborated this statistic. Equally troubling, FINCEN's Suspicious Activity Reports for Computer Intrusions have shot up more than 500% over the past year.³ With the growing amount of financial data stored and transmitted online, the ease of computer intrusions add to the severity of traditional crimes such as identity theft; to put this in perspective for the digital age, over USD\$222 billion in losses were sustained to the global economy as a result of identity theft.⁴

In an effort to mitigate these types of threat, the World Bank publication "Electronic Security: Risk Mitigation in the Financial Transactions" describes e-security processes and procedures. This is not just confined to the financial industry. As the network infrastructure spans across industry borders, so too, does the critical need for electronic security. As far back as 1995, the ISO/IEC 13335, better known as the Guidelines for the Management of IT Security (GMITS), recognized that the Internet was a hostile environment that would require the use of proper e-security. ISO 17799 is the most widely utilized security standard for information systems. ISO 17799 was written with the 90's cyber-space environment in mind, it has become outdated and deficient given the growth

¹ http://www.cert.org/stats/cert_stats.html#incidents for 2003.

² NBSO Brazilian Computer Emergency Response Team. <http://www.nbso.nic.br/index-en.html>

² Suspicious Activity Reports (SAR) for computer intrusions have grown from 419 in 2001 to over 1,293 in 2002. Over 3,600 incidents have been reported as of May 2003. <http://www.fincen.gov/sarreviewissue5.pdf>

² Aberdeen Group June 2003 Report on the Economic Impact of ID Theft

³ Suspicious Activity Reports (SAR) for computer intrusions have grown from 419 in 2001 to over 1,293 in 2002. Over 3,600 incidents have been reported as of May 2003. <http://www.fincen.gov/sarreviewissue5.pdf>

⁴ Aberdeen Group June 2003 Report on the Economic Impact of ID Theft

in outsourcing, wireless usage, applications, blended threats and the organized and dynamic approach to hacking that various criminal syndicates have taken in recent years. This checklist aims to ask those questions that all too often have been ignored.

The rising trends in cyber crime are a direct result of three phenomena. First, organized crime has made a business model out of hacking. Second, criminal laws tend to overemphasize the risks in funds transfers rather than to address the current cyber-criminal modus operandi of identity theft, including salami slicing and extortion. Finally, there has been an overemphasis on protecting data in transit rather than in storage. Hackers attack data where it sits for 99.9% of the time, in “clients” e.g. desktops/PDAs and servers. Hackers target servers, remote users, and hosting companies, all of which assume they are secure because of their usage of robust end-to-end encryption. Over-reliance on silver-bullet solutions has created a panacea for online fraud. Business continuity is a key goal of e-security, and both this and business credibility depend upon data integrity and authentication. Thus, defense in depth, specifically through an implementation of Layered Security, is essential to achieving these goals.

The thirteen layers of e-security described in The World Bank publication covers both the hardware and software pertaining to network infrastructures. These 13 layers comprise a matrix, which manages the externalities associated with open architecture environments.

1. **Risk Management**—A broad based framework for managing assets and relevant risks to those assets.
2. **Policy Management**- A program should control Bank policy and procedural guidelines vis-à-vis employee computer usage.
3. **Cyber-Intelligence**- Experienced threat and technical intelligence analysis regarding threats, vulnerabilities, incidents, and countermeasure should provide timely and customized reporting to prevent a security incident before it occurs.
4. **Access Controls/Authentication**—Establish the legitimacy of a node or user before allowing access to requested information. The first line of defense is access controls; these can be divided into passwords, tokens, biometrics, and public key infrastructure (PKI).
5. **Firewalls**—Create a system or combination of systems that enforces a boundary between two or more networks.
6. **Active content filtering**—At the browser level, it is prudent to filter all material that is not appropriate for the workplace or that is contrary to established workplace policies.
7. **Intrusion detection system (IDS)**—This is a system dedicated to the detection of break-ins or break-in attempts, either manually or via software expert systems that operate on logs or other information available on the network. Approaches to monitoring vary widely, depending on the types of attacks that the system is expected to defend against, the origins of the attacks, the types of assets, and the level of concern for various types of threats.
8. **Virus scanners** —Worms, Trojans, and viruses are methods for deploying an attack. Virus scanners hunt malicious codes, but require frequent updating and monitoring.

⁵ http://www.cert.org/stats/cert_stats.html#incidents for 2002.

⁶ Suspicious Activity Reports (SAR) for computer intrusions have grown from 419 in 2001 to over 1,293 in 2002. Over 5,600 incidents have been reported as of July, 2003. <http://www.fincen.gov/sarreviewissue5.pdf>

⁷ Aberdeen Group June 2003 Report on the Economic Impact of ID Theft

9. **Encryption**—Encryption algorithms are used to protect information while it is in transit or whenever it is exposed to theft of the storage device (e.g. removable backup media or notebook computer).
10. **Vulnerability testing**—Vulnerability testing entails obtaining knowledge of vulnerabilities that exist on a computer system or network and using that knowledge to gain access to resources on the computer or network while bypassing normal authentication barriers.
11. **Systems administration**—This should be complete with a list of administrative failures that typically exist within financial institutions and corporations and a list of best practices.
12. **Incident response plan (IRP)**—This is the primary document used by a corporation to define how it will identify, respond to, correct, and recover from a computer security incident. The main necessity is to have an IRP and to test it periodically.
13. **Wireless Security**— This section covers the risks associated with GSM, GPS and the 802.11 standards.

The World Bank Technology Risk Checklist is designed to provide Chief Information Security Officers (CISO), Chief Technology Officers (CTO), Chief Financial Officers (CFO), Directors, Risk Managers and Systems Administrators with a way of measuring and validating the level of security within a particular organization. The CISO plays a key role in this initiative by overseeing the entire gamut of processes, procedures, and technologies pertaining to an institution's IT infrastructure.

Senior managers should pay special attention to sections 1 and 2 (indicated in red text), and note that technical data can be found in the Appendix.

Cyber crime statistics rise annually, as do the monetary losses to financial institutions on account of these crimes. In order to reduce the severity of these damages, it is absolutely critical to implement risk-management processes that can be monitored by bank examiners, and that impose a minimum standard for dealing with electronic security. We trust that this checklist will establish a methodology to assess the level of security within a particular organization, and create a benchmark by which to gauge the level of need for e-security.

1. *The findings, interpretations, and conclusions expressed in this paper are entirely those of the authors and should not be attributed in any manner to the World Bank, its affiliated organizations, members of its Board of Executive Directors, or the countries they represent.*

Acknowledgements

We would like to thank the following people for their invaluable knowledge and input: Julia Allen, Chris Bateman, Ken Brancik, Tony Chew, Chris Camacho, Charles Conn, Jerry Dixon, John Frazzini, Ed Gilbride, Thomas Glaessner, Erik Johnson, Christopher Keegan, Tom Kellermann, Hugh Kelly, Tom Lamm, Warren Lotzbire, Valerie McNevin, Shane Miller, Jim Nelms, Yumi Nishiyama, Bryan Palma, Troy Schumaker, Dave Thomas, and Shrimant Tripathy.

Layers of Electronic Security	Security Objectives	Checklist				
		Status		Target Date	Comments	
		Y	N			
Cyber-Risk Mitigation Processes						
I. Risk Management	1. Does management view e-security as an overhead expense or essential to business survivability? Is this reflected in documented policies and day-to-day procedures?					
	2. Does cyber-risk play in the corporate governance, mission and philosophy of the organization?					
	3. Does your organization educate and train the Board on cyber risk? How often? What percentage of your budget is dedicated to education and training of the Board?				___%	
	4. How does security and business interact in determining cyber risk and security? What are the roles and responsibilities of business towards security?					
	5. Has your company determined acceptable levels of cyber-risk as part of its overall strategic plan and ongoing operational risk and forecasted losses? If so, who approves this level of risk?					
	Organizational Management					
	6. What is the authority of the CISO to enforce corporate policy and procedure regarding cyber risk and security? Who does that person report to?					
	7. Does your organization have a CISO? Does the CISO report directly to the CEO? If you do have a CISO, what are their roles and responsibilities? If you do not have a CISO who is responsible for cyber-security and what role does that person play?					
	8. Is the security program aligned with overall business objectives? Is it part of organizations long term and short term plans?					
	9. Are security considerations a routine part of normal business processes? How is this reflected?					
10. Are security considerations included as a routine part of systems design and implementation?						

	11. Have you developed a protection strategy and risk mitigation plan to support the organization's mission and priorities?				
	12. A risk management framework requires both an identification and a prioritization of information assets for the purpose of determining the level of security and systems recoverability appropriate for each asset classification. Has such an identification and prioritization of information assets been performed? What is included in your company's definition of information assets?				
	13. Does the organization have a framework in place where they can adequately measure the success of security objectives? Has this benchmark been adequately communicated throughout the organization, including partners, vendors and employees?				
	14. How do business units identify, measure, monitor and control electronic ("cyber") security risks through their technology risk assessment process and ensure that adequate safeguarding controls exist over networks and customer data? Who monitors this?				
	15. Who is responsible for keeping records of cyber intrusions, costs of remediation, response time, and documenting procedures and processes?				
Asset Management					
	16. Have you taken an inventory of each access point to your network (e.g. every connected device, wireless, remote, etc.), both inside and outside of the firewall, in order to identify potential points of vulnerability?				
	17. Do you have an asset based threat profile?				
	18. What is included in your inventory of access points?				
	19. How often are risk assessments performed? Does an action plan result from each assessment? Is progress against the plan tracked and managed?				
	20. Does a network topology diagram exist, and if so, is it kept up-to-date? What is the update process, and how often, is it kept current? What trigger event must occur for it to be updated?				

	21. Are your systems properly configured according to your architecture? Who determines this? How often are configurations reviewed?				
	22. Is someone on the Board of Directors responsible for overseeing technology risk?				
	23. If a department is found to be non-compliant, do you have a policy for disciplinary action? What types of disciplinary actions do you impose? Who is responsible for their enforcement?				
	24. Are executive level e-risk summaries produced for the CEO, CTO, CFO and Board? Are they produced on at least a monthly basis? If not, how frequently? Does any action result on account of these summaries, and if so, what kind?				
	25. Do external partners implement the 13 layer security model?				
	26. Are there procedures and controls for purchasing and eliminating software and hardware?				
	27. Does the information technology management authorize all hardware and software acquisitions?				
II. Policy Management	1. Are the Board and Officers aware of their liabilities? Are personnel?				
	2. Has senior management, including the corporate or organizational Board of Directors, established a comprehensive information policy and auditing process? If so, what areas are covered? How, and how often are these policies reviewed, and how are they created?				
	3. Does your information security organization report to the IT organization, or is it a separate organization that maintains its independence and freedom from conflicts of interest?				
	4. Has senior management established a security auditing process? Do you use third party auditors?				
	5. Is someone responsible for each security policy and procedure? How does each policy “owner” stay current? Do they attend security conferences? What are the qualifications for being in this position? What mechanisms, etc. are in place to keep policies up-to-date?				

6.	Are new users trained on security policies and procedures				
7.	Do current employees/users receive periodic security awareness training?				
8.	Are all users educated/trained as to the policies and procedures? Do all users have a copy of the policies and procedures? How do they demonstrate their acceptance of these as a part of their employment?				
9.	Are all business associations, partners, contractors or customers that have access to the company's computer systems made aware of the company's policies and procedures?				
10.	Must they agree to abide by the company's protocols in order to retain access? What occurs if business partners or customers are found to be non-compliant?				
11.	Do managers at each level of the organization understand their roles and responsibilities with respect to information security? How often does management receive security awareness training? How is that verified?				
12.	Do your security policies address both internal and external access to the network for each technological device?				
13.	What is each user's role in backing up the user data on their desktops, laptops, and mobile devices?				
14.	Do you have a process for retrieving a backup file that you inadvertently deleted? How long does this take?				
15.	Do users, including business associates and customers, know who to contact when they have problems with operating systems, laptops, access to new project data, passwords, security applications, or proprietary software?				
16.	Is policy management software (PMS) utilized?				
17.	Does your PMS manage the identified threats and vulnerabilities?				
18.	Does it map the threat intelligence to the protected assets of your organization?				
19.	Does it provide a policy management component related to policy and regulatory compliance?				

	20. Does it enable an organization to establish and manage a customized risk profile?				
Remote System Access Policy					
	21. Do system administrators note unusual access or instances of remote users?				
	22. Do administrators regularly review all VPN log files, system log files, firewall logs, IDS logs, etc?				
	23. Are laptops updated with critical patches and virus definitions? If so how- manually or through SMS push?				
	24. Do users employ standardized equipment?				
	25. Is each user only assigned one remote computer?				
	26. Is each user held accountable for the actions of their computer?				
	27. Do remote users have access to sensitive or confidential information?				
	28. Do you utilize at least at a two-factor authentication system?				
	29. Are remote users required to utilize VPN and firewall software?				
	30. Do you utilize internal server software that checks for VPN firewall settings? Are users allowed to log on if a firewall is not in place?				
Personnel Policy					
	31. Are your CISO's roles and responsibilities clearly stated?				
	32. Do you conduct background checks on all personnel, including full and part-time employees, temps, outsourced vendors, and contractors?				
	33. Have you established proper use policies concerning employee E-mail, Internet, Instant Messaging, laptops, cellular phones, and remote access?				
	34. Who establishes and enforces these proper use policies?				
	35. Are all employees trained on network security basics?				
	36. Are employees held accountable for Internet activity associated with their accounts?				

37. Are employees certified or verified after reviewing company policies?				
38. Do employees have an available and reliable mechanism to promptly report security incidents, weaknesses, and software malfunctions?				
Outsourcing Policy				
36. Have you established policies to restrict, control, or monitor systems access by vendors, contractors, and other outsourced personnel?				
37. Do outsourced personnel sign non-disclosure agreements?				
38. Are all employees required to receive information security awareness training? Is there a testing component to verify and validate such training?				
39. If outsourcing/contracting certain services, are the security controls under direct authority of your CISO within the contract?				
40. Do procedures exist to determine the security impact of linking new/external systems to the organization's infrastructure?				
41. Do outsourced companies implement a physical access policy? Are physical parameters and security measures implemented?				

<p>42. Who is responsible for the adequacy of policies, procedures and standards that govern security requirements for outsourced service providers, customers, and business associates? How often are these reviewed?</p> <p>At a minimum, policies, procedures and standards should address:</p> <ul style="list-style-type: none"> a. Due diligence requirements b. Security service level and operational readiness requirements; c. The general security scope and timing of third-party assurance reviews (e.g., SAS70 Level II, SysTrust, WebTrust certifications); d. Existence & adequacy of insurance to protect against financial losses due to third-party negligence and/or unauthorized access to service provider systems . e. Privacy policy. f. Disaster recovery and business continuity plan. g. Process of change management. 				
<p>43. Who reviews internal audits performed on service providers. These should specifically assess:</p> <ul style="list-style-type: none"> a. The adequacy of the scope and frequency of review, sufficiency of supporting work papers; significance of audit findings; and b. Conduct a gap analysis of audit coverage to identify areas that are not covered, or inadequately covered, by the internal audit function. c. Is there a follow-up with whom to remediate? 				
<p>44. What legal requirements are your hosting companies, data warehouse, software developers or application service providers contractually obligated to fulfill regarding security, e.g. duties, layers of security, notification of security breaches, and timeliness of responses?</p>				
<p>45. Does the outsourced entity have a formal and documented security procedure? Is this available for review?</p>				
<p>46. Are written job descriptions available to all outsourced personnel who have access to sensitive information? Are background checks conducted?</p>				

47. Do agreements with your outsourced, network service providers contain proper incentives and financial repercussions for instances of service outages?				
48. Are outsourced security policies constantly updated?				
49. Are consequences for non-compliance with policies clearly documented and enforced?				
50. Are outsourced entities required to report security incidents to you and depict their response and remediation of such incidents?				
51. Do your outsourced providers have adequate backup facilities?				
52. Are outsourced entities required to be insured?				
53. Does the outsourced company maintain an asset control and security policy?				
Physical Security Policy				
54. Do your security policies restrict physical access to networked systems facilities?				
55. Are your physical facilities access-controlled through biometrics or smart cards, in order to prevent unauthorized access?				
56. Does someone regularly check the audit trails of key card access systems? Does this note how many failed logs have occurred?				
57. Are backup copies of software stored in safe containers?				
58. Are your facilities securely locked at all times?				
59. Do your network facilities have monitoring or surveillance systems to track abnormal activity?				
60. Are all unused “ports” turned off?				
61. Are your facilities equipped with alarms to notify of suspicious intrusions into systems rooms and facilities?				
62. Are cameras placed near all sensitive areas?				
63. Do you have a fully automatic fire suppression system that activates automatically when it detects heat, smoke, or particles?				

	64. Do you have automatic humidity controls to prevent potentially harmful levels of humidity from ruining equipment?					
	65. Do you utilize automatic voltage control to protect IT assets?					
	66. Are ceilings reinforced in sensitive areas e.g. server room?					
III. Cyber Intelligence	1. Does your organization conduct cyber intelligence gathering?					
	2. Are intelligence reports disseminated to your information systems group?					
	3. Does cyber intelligence reporting include malicious code? Geopolitical threats? Both known and unknown vulnerabilities? Predictive analysis related to emerging cyber threats?					
	4. How does the cyber threat intelligence provider measure performance?					
	5. Do you conduct 24x7 monitoring and intrusion detection as a part of your cyber intelligence gathering?					
	Patch Management					
	6. When applying a patch to any system vulnerability, do you have a process for verifying the integrity, and testing the proper functioning of the patch?					
	7. Have you verified that the patch will not negatively affect or alter other system configurations?					
	8. Are patches tested on test beds before being released into the network?					
	9. Do you make a backup of your system before applying patches?					
	10. Do you conduct another vulnerability test after you apply a patch?					
	11. Do you keep a log file of any system changes and updates?					
	12. Are patches prioritized?					
	13. Do you disseminate patch update information throughout organization's local systems administrators?					
	14. Do you add timetables to patch potential vulnerabilities?					
	15. Are external partners required to patch all non-critical patches within 30 days?					
16. Are external partners required to patch critical patches ⁸ to servers and clients within 48 hours?						

⁸ As defined by the DHS, CERT or Vendor.

IV. Access Controls/ Authentication	1. Is two-factor authentication utilized for large value payments and system administrators?				
	2. Are policies and procedures documented that are used for both establishing and termination of access for consultants and employees?				
	3. Are users required to use robust passwords (long in length; mix of letters, numbers, and symbols)?				
	4. Do you provide automated enforcement for changing passwords? How often?				
	5. Are user ID's and passwords unique to each individual network user?				
	6. Do you prevent the use of shared, or group, user ID's?				
	7. If biometrics are employed, are "live-scans" conducted to verify the presence of the user?				
	8. Does your biometric system have a secure and reliable enrollment process?				
	9. Once a user's biometric information is recorded, is security in place to protect that information against theft, alteration, or forgery?				
	10. Do decision processes and supporting procedures exist to permit third party access (e.g. contract employees, customers, etc.)?				
	11. Do third parties retire or update accounts when partnerships terminate?				
	12. How do users access the organization's network and systems when working from home or when traveling? Who authorizes generic employee access?				
	13. Compared to what a user can do when physically working in the office, is remote access restricted? If so, how is this achieved?				
	14. Is access restricted to the minimum amount of access necessary for any particular job?				
	15. Are root-level, and other privileged access, given only on an as-needed basis? Upon what criteria is this based?				

	16. Do you deactivate the access controls of an employee to both the building and computer networks prior to the employee's termination? What other precautions are taken before or after an employee's termination?				
	17. Are all your access controls and authentication mechanisms monitored to correct instances of false positive/negatives? Explain.				
	18. Do you check for modems attached to PCs, routers or printers?				
	19. Do you periodically war-dial your telephone number range to check for new devices?				
	20. Do you utilize a private branch exchange (PBX) firewall, PBX log or other such control to keep track of any attempts to hack into systems using war dialing techniques?				
	21. Do you have controls in place to detect modem scanning attempts on your systems?				
V. Firewalls	1. Do you use nationally certified firewalls? If there is no national certification, what criteria do you use to purchase firewalls?				
	2. Do you have a comprehensive list of what should be allowed/disallowed through the firewall? Is this document kept up-to-date?				
	3. Where do you place firewalls? How do you secure them against unauthorized access from Internet, Extranet and Intranet users? E.g., are inner firewalls placed around all critical, financial and transactional systems?				
	4. Do you place firewalls at all sub-network boundaries where policies differ between the connecting sub-networks?				
	5. Is the firewall placed in between the network router and the network or given application?				
	6. Do you prevent entry or exit through any network port that is not required by your organization?				
	7. Do you prevent use of any network protocol not in use by your organization?				
	8. Are your routers properly configured for your system requirements? How has this been verified?				

	9.	Are default router configurations used, and are they set to Default/Deny?				
	10.	Are rule sets backed up and tested regularly?				
	11.	Are your firewalls configured such that servers that should accept only inbound connections (e.g. Web servers) are prohibited from making outbound connections?				
	12.	Are your firewalls updated at regular intervals? How often? Is it updated when a patch is available? What initiates a review?				
	13.	Do you use ingress and egress filtering? Do you follow the following filtering rules listed in the Appendix? If so, which ones do you follow?				
	14.	Do you employ rate-limiting filters?				
	15.	If users are allowed to connect from the Internet to the internal network, is access restricted to either a virtual private network (VPN) or an encrypted software session? How is it restricted?				
	16.	Is access to the management interfaces of routers, firewalls and other network appliances adequately secured? For example, are these devices also subject to appropriate password policy enforcement, or is two factor authentication employed?				
	17.	Do you explicitly configure your network to restrict access for everything that does not need to enter your firewall? Please see Appendix for technical examples.				
VI. Active Content Filtering	18.	Is firewall administration limited to authorized staff?				
	1.	Is your system configured to filter hostile Active X?				
	2.	Is your system configured to filter JavaScript?				
	3.	Is your system configured to filter Remote Procedure Calls (RPCs)?				
	4.	Is your system configured to filter Perimeter-Based Security (PBS)?				

5.	Is your system configured to filter Berkeley Internet Name Domain (BIND)? ⁹				
6.	Is your system configured to filter Simple Network Management Protocol (SNMP)? Please see Appendix for details.				
7.	Is your system configured to filter the Java Virtual Machine (JVM)vulnerability?				
8.	Have you upgraded to the latest version of Sendmail and/or implemented patches for Sendmail ?				
9.	Do you prevent Sendmail to run in daemon mode (turn off the -bd switch) on machines that are neither mail servers nor mail relays?				
10.	Is your system configured to filter Internet Message Access Protocol (IMAP) and Post Office Protocol (POP)?				
11.	Is your system configured to filter Sadmin and mountd? Please see Appendix for details.				
12.	Does your organization have a standard desktop configuration and software standards?				
13.	Do you employ enterprise level desktop configuration management?				
14.	Is your system configured to filter E-mail?				
15.	Do you filter all .exe attachments?				
16.	Do you filter all .doc attachments?				
17.	Have you considered filtering all arriving and departing e-mail by a spam threshold (greater than 40 identical messages blocked and source traced, if inside the network)?				
Web Application Security					
18.	Do you check the lengths of all input? If greater than the maximum length, do you stop processing and return as failure?				
19.	Do you allow source packets coming from outside to have internal IP addresses. Conversely, do not allow inside packets to go out that do not have valid internal IP source addresses.				

⁹For more details refer to the Appendix.

	20. Are user names and passwords sent in plaintext over an insecure channel?				
	21. Do you restrict user access to system-level resources.				
	22. Do you limit session lifetimes?				
	23. Do you encrypt sensitive cookie states?				
VII. Intrusion Detection	1. What types of intrusion detection systems (IDS) are used? How is their placement/location determined?				
	2. Is your IDS outsourced? If so, what is your criteria for choosing an outsourced vehicle?				
	3. Do you use host-based and network-based intrusion detection systems? How often is this updated?				
	4. Who maintains and configures rule sets and routing controls, and what is their process for doing so?				
	5. Are IDS systems appropriately configured for system anomalies, file and data problems, and aberrant usage?				
	6. Are your IDS programs updated on a regular and frequent schedule? If so, how often? Upon what criteria is it updated?				
	7. Are all system logins and intrusions being tracked? If so how often? If logs are kept, how frequently are they reviewed? Do metrics exist where the intrusions are tracked?				
	8. Are log files kept in a secure location, and are they protected against malicious access, including any alteration or deletion? Who has access to them? Does management review these on a regular basis?				
	9. Do you conduct frequent vulnerability testing against your IDS systems?				
	10. Who conducts your vulnerability testing?				
	11. What is the criterion for choosing a vulnerability tester?				

	12. Understanding that applications such as VPNs conceal malicious code from IDS programs, do you use additional layers of defense to protect these programs?				
	13. Is the use of open source IDS software investigated?				
	14. Do you subscribe to alerts on the latest threats and vulnerabilities?				
	15. Who is responsible for keeping records of cyber-intrusions, cost of remediation, etc?				
	16. Are you certain your IDSes are seeing all of the data? Of 100 "test" attacks you inject on your network, how many does the IDS see? How many packets/sec. are being processed by your IDS?				
	17. Is your IDS set up in a redundant and/or load sharing fashion?				
	18. Do you use span ports on switches, hubs, or passive fiber taps to accomplish IDS? If hubs are used, how do you ensure that someone can not plug another device into the hub, and thereby view all of your networks data?				
	19. Does the IDS page or email security personnel? Of 5 injected attacks, how many times did security personnel respond?				
	20. Are your IDS rule-sets protected (i.e.: what does your IDS look for, what are the time deltas that it uses to detect network scanning)? E.g. If someone can find the rule set they know what you are/not looking for.				
	21. Are all system clocks set to the exact same time?				
	22. Do you keep a profile of general characteristics for each server? These can great aid in incident analyses.				
	23. Are Honey pots utilized? If so, where are the placed?				
	24. Do you keep logs of any honey pot activity?				
	25. Do you check for signs of rogue tunnels (see appendix)?				
	VIII. Virus Scanners	1. Are anti-virus signatures updated on a daily basis?			
		2. Are all executable attachments filtered in email?			

	3. What actions do you take if you discover a virus? Are these procedures documented?				
	4. How do you recover compromised files? Do you document these actions?				
	5. How do you contain the damage caused by a virus? Do you document instances of viruses?				
	6. Do you document the actions taken to eradicate and prevent future instances of these viruses?				
	7. How do you avoid propagating a virus to others? Do you document these procedures?				
	8. Do you minimize the risks of virus propagation by limiting the use of disk drives, and by limiting or restricting software downloads/uploads?				
	9. How do you verify that a recently created file has not been infected?				
	10. Do computer systems run automatic and routine virus scans?				
	1. Is the level of SSL encryption 128 BIT or higher?				
	2. Is there an established policy regarding the sharing of your public key with others and how they share theirs with you?				
3. When utilizing RSA, is the level of encryption at least 1024 bits?					
4. Are keys stored in a secure location? Is there adequate protection against theft, disclosure, and alteration?					
5. Do you have a secure means by which to issue keys?					
6. Are secret keys unlocked securely?					
7. Is use of root keys tightly controlled? ¹⁰					
8. How are encryption keys managed, including key retirement/replacement when someone who has access leaves the organization?					

¹⁰ Refer to Appendix

	9.	Do encrypted keys contain expiration dates?				
	10.	Is there a secure means for replacing keys?				
	11.	Is there a secure way of destroying keys?				
	12.	Are the CRL (Certificate Revocation Lists) maintained on a real-time basis?				
	13.	Are certificates properly validated against the hostnames/users for whom they are meant for?				
	14.	Do you have a policy for cross-certification with external parties?				
	15.	Do you have a contingency plan that can recover data in the event of an encrypted key being lost?				
X. Vulnerability and Penetration Testing	16.	Do you archive private keys? Is there a policy in place to retrieve archived keys if needed in future?				
	1.	Is vulnerability testing conducted on a quarterly basis?				
	2.	Are the results acted upon?				
	3.	Are penetration tests conducted on a bi-annual basis? If they are conducted do they address the following: <ul style="list-style-type: none"> a. Describing threats in terms of who, how and when b. Establishing into which threat class a threat falls c. Determining the consequences on the business operations should a threat be successful d. Assessing the impact of the consequences as less serious, serious or exceptionally grave injury e. Assigning an exposure rating to each threat, in terms of the relative severity to the business prioritization of the impacts according to the exposure rating 				
	4.	Is there a timetable for acting upon the above results?				
	5.	Do penetration tests assess both the external and insider threat?				
	6.	Do your tests include performing a network survey, port scan, application and code review, router, firewall, IDS, trusted system and password cracking?				

	7. Do you employ network sniffers to evaluate network protocols along with the source and destination of various protocols for stealth port scanning and hacking activity?				
	8. Are penetration tests conducted upon hosting provider systems and existing partner systems before connecting them to the organization's network?				
	9. Are vulnerability/penetration testing results shared with all appropriate security and network administrators?				
	10. Do your penetration tests encompass social engineering?				
XI. Systems Administration	1. Before new technology is deployed, is a security peer review criteria published and subsequently reviewed?				
	2. Are short timetables mandated for the test and installation of software patches that fix security flaws?				
	3. Are daily audits of network logs conducted?				
	4. Are default software settings changed to ensue a secure configuration?				
	5. Is the use of SNMP, telnetd, ftpd, mail, rpc, rservices, or other unencrypted protocols for managing systems prohibited?				
	6. If Instant Messaging is employed, is it necessary for business? And is it properly encrypted?				
	7. Do you prohibit passwords assignments over the telephone, IM, or other unsecured transmission mechanisms?				
	8. Are passwords encrypted during both transmission and storage?				
	9. Are administrative accounts and passwords shared over multiple systems?				
	10. Are administrative accounts changed quarterly with very strong passwords?				
	11. When resetting passwords, can users utilize a password they entered in the past?				

XII. Incident Response Plan (IRP)	1. Does the IRP provide guidance on what to do if there is an attack?				
	2. At what point do you report an incident? To whom do you report this incident?				
	3. What is your escalation procedure? Do incident responders determine what systems were attacked? Do incident responders determine how attacked systems were affected?				
	4. At what point do you determine if this is a crime scene?				
	5. Is there an attempt to trace the source of the attack?				
	6. Can you determine the servers from which intruder data was sent?				
	7. Can you determine downstream victim sites? How is this determined?				
	8. For the purpose of forensics are the logs secure and images of the compromised server taken? Do your policies and procedures for IRP address: <ul style="list-style-type: none"> a. Evidence collection and technical & investigative guidelines; b. Documentation & preservation processes; c. Data & information analysis; d. Requirements for completing SARs and other law enforcement documentation (e.g., USSS Network Incident Report); e. Legal guidelines and constraints (e.g., journaling criteria, including legal review); f. Computer forensics tool selection process. 				

	9. Does the IRP provide you with a description of the authority and discretion you have when responding? E.g. Key points of contact and communication channels (e.g., law enforcement, regulatory agencies, public relations, internal communications)				
	10. If the incident resulted from an unpatched vulnerability, is the patch acquired, tested, and installed in a timely manner?				
	11. Are searches conducted for backdoors and other unexpected violations of integrity?				
	12. Are compromised systems repaired? If so, are the repaired in a timely fashion?				
	13. Is a disaster recovery plan in place?				
	14. Do you have cyber-insurance coverage for cyber-risks or fraud due to the internal and/or external hackers?				
	15. Are system back-ups and redundant servers in place in the event of a system failure or attack? What is the distance between the primary and backup servers?				
	16. Is the backup facility on a different power grid than the primary facility?				
	17. Are the facilities served by the same or different telecommunications exchanges?				
	18. Are the disaster recovery facilities sufficient to allow continued operations in the event of a regional disaster?				
	20. Do secondary systems undergo thorough security maintenance, including abiding by all security policies and procedures?				
	21. Have you identified authorized personnel to manage contingency plans?				
	22. Are authorized personnel responsible for evidentiary data workflow management (e.g., journaling, audit trails, etc.) and completion of internal and external network incident reports (U.S. Secret Service), SARs, regulatory and other reports?				

23. Do you have procedures and processes for securely switching to and from back-up systems, including expiring or short-term access privileges?				
--	--	--	--	--

Forensics

24. Do you employ a digital forensic policy?				
--	--	--	--	--

25. Do you have evidentiary data guidelines and preservation practices?				
---	--	--	--	--

26. Do you provide or utilize comprehensive digital forensics training?				
---	--	--	--	--

27. Do you provide a post-mortem “lesson’s learned” analysis?				
---	--	--	--	--

XIII. Wireless

802.11

1. Is there an institution-wide wireless policy? Is this clearly exhibited to all employees?				
--	--	--	--	--

2. Are all wireless connections mandated to register?				
---	--	--	--	--

3. Is someone responsible for tracking the number of employees with WLANs at home?				
--	--	--	--	--

4. Have all unnecessary services and applications on each client and server been disabled?				
--	--	--	--	--

5. Have all default settings, including passwords, been changed?				
--	--	--	--	--

6. Have you limited radius coverage to the windows, and not beyond?				
---	--	--	--	--

7. Have bi-directional antennas been provided for all wireless devices?				
---	--	--	--	--

8. Do you have a VPN endpoint inside a wireless DMZ?				
--	--	--	--	--

9. Have you deployed VPN tunneling between the network firewall and the wireless devices?				
---	--	--	--	--

10. Have you installed enterprise-wide antiviral software on all wireless clients?				
--	--	--	--	--

11. Has two-factor authentication been employed? Where? Why?				
--	--	--	--	--

12. Have you disabled DHCP and the use of static IP addresses for wireless network interface cards (NICs)?				
13. Have you disabled all Simple Network Management Protocol (SNMP) community passwords on all access points?				
14. Do access points contain “flashable” firmware only?				
15. Are wireless firewall gateways used? Where? Why?				
16. Are Access Points (AP) placed in secure areas, and are Layer 2 switches employed in lieu of hubs?				
17. Do you employ a network-based intrusion detection system on the wireless network?				
18. Do you perform routine checks to find rogue access points?				
19. Do you monitor all wireless logs at least once a week? Do you scan critical host logs daily?				
20. Do you employ two-factor authentication on all wireless devices?				
21. Have you moved or encrypted the SSID password and the WEP key?				
22. Have you disabled SNMP community passwords on all access points?				
23. Have you enabled 128-bit WEP encryption?				
GSM				
24. Is a power-on password required?				
25. Do PDAs have anti-virus and VPN software installed?				
26. Is robust encryption utilized?				
27. Are users required to store devices securely				
28. Do you ensure that desktop mirroring software is password protected?				

Satellite Security “GPS”

	29. Have you implemented adequate security around your GPS receivers? Please see Appendix for details.				
--	--	--	--	--	--

Appendix

Firewalls	<p>If you restrict network entry and exit, which restrictions do you place?</p> <ul style="list-style-type: none"> ○ Any packet coming into your network must not have a source address of your internal network. ○ Any packet coming into your network must have a destination address of your internal network. ○ Any packet leaving your network must have a source address of your internal network. ○ Any packet leaving your network must not have a destination address of your internal network. ○ Any packet coming into your network or leaving your network must not have a source or destination address of a private address or an address listed in RFC1918 reserved space. These include 10.x.x.x/8, 172.16.x.x/12, or 192.168.x.x/16, and the loopback network 127.0.0.0/8. ○ Block any source-routed packets or any packets with the IP options field set. ○ Reserved, DHCP auto-configuration, and Multicast addresses should also be blocked: <ul style="list-style-type: none"> ▪ 0.0.0.0/8 ▪ 169.254.0.0/16 ▪ 192.0.2.0/24 ▪ 224.0.0.0/4 ▪ 240.0.0.0/4
	<p>Do you block the following ports:</p> <ul style="list-style-type: none"> ○ Login services—telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al. (512/tcp through 514/tcp) ○ RPC and NFS—Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp) ○ NetBIOS in Windows NT—135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000—earlier ports plus 445(tcp and udp) ○ X Windows—6000/tcp through 6255/tcp ○ Naming services—DNS (53/udp) to all machines that are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp) ○ Mail—SMTP (25/tcp) to all machines that are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp) ○ Web—HTTP (80/tcp) and SSL (443/tcp) except to external Web servers; may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.) ○ "Small Services"—ports below 20/tcp and 20/udp, time (37/tcp and 37/udp) ○ Miscellaneous—TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/udp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp) ○ ICMP—block incoming echo request (ping and Windows traceroute); block outgoing echo replies ○ Have you considered port camouflaging (i.e. change the default SSH port of 22 to say 500)

Active Content Filtering	<p>Does your system filter the following Simple Network Management Protocol (SNMP)?</p> <p>III. If you do not absolutely require SNMP, have you disabled it?</p> <p>IV. If you must use SNMP, do you use the same stringent policy for community names as used for passwords (hard to crack, changed periodically)?</p> <p>V. Do you validate and check community names using snmpwalk</p> <p>VI. Unless it is absolutely necessary to poll or manage devices from outside of the local network, do you filter SNMP (Port 161/UDP) at the border-router or firewall?</p> <p>VII. Where possible, do you make MIBs read-only?</p>
	<p>Is your system configured to filter Berkeley Internet Name Domain (BIND)?</p> <ol style="list-style-type: none"> a. Have you disabled the BIND name daemon (called "named") on all systems that are not authorized to be DNS servers? b. On machines that are authorized DNS servers, have you updated to the latest version and patch level? c. Do you run BIND as a non-privileged user for protection? Is BIND configured to change the user ID after binding to the port? d. Do you hide your version string? e. Do you run BIND in a root directory structure? f. Do you disable zone transfers except from authorized hosts? g. Do you disable recursion and glue fetching to defend against DNS cache poisoning?
	<p>In addition to Sadmin and mountd, is your system configured to filter the following?</p> <ul style="list-style-type: none"> ▪ Wherever possible, do you turn off and/or remove sadmin and mountd on machines directly accessible from the Internet? ▪ Do you install the latest patches? ▪ Do you use host/IP-based export lists? ▪ Do you set up export file systems for read-only where possible? ▪ Do you nfsbug to scan for vulnerabilities? <p>Do you employ MAC address filtering on a per-port basis?</p>
Intrusion Detection	<p>What are the longest sessions running on port 80? HTTP sessions are usually short lived and initiated per-page (or per graphic). A session to port 80 that lasts more than 60 seconds is a red flag.</p>

	<p>Also look for: - Large time spacing between small packets from client to server. - Lack of browser identification to the server. - Connection attempts at even time intervals from internal systems to the same external system that are reset with no data exchange.</p> <p>Implement an application level proxy and block HTTP CONNECT Require outbound authentication on the firewall for http, https and SSL</p>
Encryption	Is an HSM(Hardware Security Module) being used to secure the Root CA Private Key?
802.11	Are AP Channels at least 5 channels different from other nearby wireless networks in order to prevent interference?
	Have you changed the default settings of the SSID to a complex password?
	Have you at least moved or encrypted the SSID and Wired Equivalent Privacy (WEP)? These files should not be stored in the default Windows registry folder.
GPS	Is your monitor carrier to noise density c/n (o) within the range of 48-50 bbhrtz?
	Are your internal clock backups concurrent with real time?