1337 TECHNOLOGY SOLUTIONS

	Response (Yes/No)	Planned/ Partially Iniated/ Fully Implement	Security Risk (High/Medium/Low)
Network Security - Human Resources			
Are controls in place to restrict ability to transmit customer data to outside sources?			
Do your employees know know how to detect and avoid 'social engineering' attacks as well as competitive intelligence probes?			
Do your employees get regular bulletins alerting them to the newest risks and vulnerabilities in the technology field?			
Are controls in place to restrict nonwork-related downloads and internet surfing?			
Are employees educated on what constitutes a strong password? Or are controls in place to ensure that strong passwords are always used?			
Network Security - Firewall/Router			
Has, at a minimum, stateful firewalls been deployed at all external connections?			
Is the firewall configured with a policy that all services are denied unless expressly permitted?			
Do you have a process/critera to evaluate the risk of protocols and ports before implementing them on firewalls?			
Are firewall logs viewed regularly?			
Is access to all firewalls and routers restricted to only those people that need to manage these devices?			
Do users remotely access terminals? If so are they using secure passwords and encrypted login sessions?			
Is there a process in place to ensure that all routers and firewalls have the latest software and are patched regularly with the latest security updates?			
Network Security - VPN			
For computers used for VPN remote access, have you implemented a personal firewall?			
Do you only allow computers the implement antivirus software and personal firewall protection VPN access?			
Do you have a process in place to cancel anyone's VPN access when their project is completed or their reason for having the VPN is invalidated?			
Data Security			
Are backups of business critical data run regularly?			
Do you have a way of verifying that the backups are completing successfully?			
Are backups kept in a physically and virtually secure area?			
System Security			
Do you have a process to identify network, application, and OS based system vulnerabilities?			
Do you have tools to assess system vulnerabilities?			
Are user priviledges restricted to contain only rights that are needed to that specific user?			
Do you have antivirus software running on all platforms?			
Are your email servers configured to check all incoming and outgoing emails for viruses, spam, trojan horses, and other threats?			
Do you have a procedure to ensure all servers and workstations are configured to automatically install the latest virus definitions?			
Do you have a procedure in place to ensure that the patches are correctly installed?			
Do you have a mechanism in place to ensure all servers			
Do you have a policy on priviledged accounts?			
Do you have a list of personnel with root or admin privileges			
Are all default accounts disabled and all default passwords changed throughout your organization?			
Password Management			
Are users forced to change their passwords afer a certain amount of time has passed?			
Are users prohibited from frequently reusing passwords?			
Do you periodically run password cracking software to identify weak passwords?			
Intrusion Protection			
Do you have a process to review security audit logs in a timely and consistent manner and act upon any threats detected?			
Is there an automated notification process that is initiated when defined security thresholds are exceeded?			
Are you using network based intrusion detection on interconnections? (e.g. internet, 3rd party connections, etc)			
Are your business critical networks configured with switches so that sniffer software is ineffective?			
Software Management			
Is license documentation physically available for review?			
Are procedures in place to manage software license compliance?			
Are employees prohibited from installing unauthorized and pirated software on their workstations?			