Cyber Security Questionnaire

The following questionnaire is necessary to guarantee the accuracy of the time estimates as well as the thoroughness of the assessment. Please fill out as much of the information as possible.

Basic Information

Name:	
Title:	
Organization:	
Telephone:	
Cell phone:	
Email address:	
All machines: • IP Addresses • OS • All machine names (DNS, WINS, Virtual Hosts, etc.)	
Is your organization subject to any specific regulatory requirements? (Examples – PCI-DSS-ISO, COBIT, ITIL, etc)	

Audit Information

Would you like the Information Security Office to perform a network-based assessment? (A&P)	
How many Internet-facing hosts do you want the Information Security Office to assess?	
Would you like the Information Security Office to perform a host-based assessment?	
Which hosts?	
Would you like the Information Security Office to perform compliance, physical or enterprise assessment?	
If compliance, which regulations? (PCI-DSS-ISO, COBIT, ITIL, etc.)	
Would you like the Information Security Office to perform an application security assessment?	
Which specific applications? (URL, Application name, Installer, etc.)	
Would you like this tested with or without credentials?	
Would you like this tested with or without administrative credentials?	

Network Security Information

Has your organization ever been compromised (internally or externally)?	
List all IP address blocks registered to your organization. (Example – 12.34.56.x/24)	
List all the domain names registered to your organization. (Examples – acme.com; acmesales.com)	
Does your organization use a local Firewall(s)? If so, please list quantity and manufacturer(s) of firewall(s).	
Does your organization use a local Intrusion Detection System(s) (IDS)?	
Does your organization use a local Intrusion Prevention System(s) (IPS)?	
If your organization uses local IDS, do you use "host-based" IDS (HIDS) or "network-based" IDS (NIDS) or a combination of both? List the quantity of IDS (both HIDS and NIDS) and IPS devices, as well as the manufacturer(s).	
Do you use DMZ networks?	
Does your organization have any dedicated connections to other organization's networks (vendors, business partners)? If so, please list all dedicated connections to other networks.	
Does your organization use any Remote Access services? Specifically, what type of remote access services does your organization use (VPN or Dial-Up RAS)?	
How many employees use remote access services?	
Does your organization use site-to-site Virtual Private Network (VPN) tunnels? If so, how many site-to-site VPN tunnels are in use?	
Does your organization have any systems that use modems?	

System Information

How many Microsoft Windows NT/2000/2003 servers does your organization use?	
How many Unix servers (AIX, HPUX, Linux, Solaris, etc.) does your organization use? Please list specific distributions.	
List any servers with operating systems other than what is listed above. Please include quantities and list specific operating system versions/distributions.	
How many Microsoft Windows 2000/XP Professional clients does your organization use?	
List any clients with operating systems other than what is listed above. Please include quantities and list specific operating system versions/distributions.	
What Enterprise Resource Planning (ERP) application(s) does your organization use? (Examples – SAP, Peoplesoft, Oracle, JD Edwards) Please include a brief description of each.	
What E-commerce application(s) does your organization use? Please include a brief description of each.	
What database technologies does your organization use? (Examples – Oracle, Microsoft SQL, IBM DB2, MySQL) Please include a brief description of the purpose for each.	

Service Information

What services do you expose to the internet? (Examples: Web, Database, FTP, SSH, etc.)	
What services do you expose to the campus?	
What type of authentication do you use for your web services? (Examples: PubCookie, Windows Integrated, htaccess, etc.)	
What languages do you use for your web services? (Examples: PHP, Perl, Ruby, ASP, etc.)	
What antivirus application(s) do you use?	
Is your antivirus application implemented using a “managed” client/server architecture, or in a stand-alone configuration?	

Log Management

How many of your IT systems generate logs with relevant security-oriented data today?	
What percentage of these logs are you actively collecting and monitoring today?	
Is your process for collecting and storing all of those logs manual or automated?	
Do you have a single place to correlate, report and real-time monitor across all of these relevant logs today?	

Security Information & Event Management

Do you routinely manage, monitor and/or analyze the collection of logs of user activity, network activity, performance data, application activity, and/or flow data in your infrastructure?	
What is your process to proactively detect/analyze invalid user access or any anomalies in applications or network traffic in your organization?	
Is your process for this detection/analysis manual or automated?	
What kind of response and remediation procedures do you have in place to handle any incidents identified through this analysis?	
What kind of response and remediation procedures do you have in place to handle any incidents identified through this analysis?	
Is the output from this process automatically fed into a single security intelligence console?	

Anomaly Detection

Do you have a unified collection and analysis technology and process for event, network, vulnerability, asset, and intelligence data?	
Is this approach capable of contextual and in-depth analysis and correlation across these diverse data sets?	
Is this process automated, and does it provide response and remediation capabilities?	

Directory Management

How many definitive sources of identities does your infrastructure have today?	
Have you standardized on a primary enterprise directory platform?	
What percentage of those identity sources are actively synchronized to ensure currency?	
When you are audited, how do you prove what identities are actively defined within your infrastructure?	

Strong Authentication

How many userid/password combinations does your average user have to use daily within their jobs today?	
What percentage of your help desk calls are for password resets?	
Is your process for authenticating and resetting passwords manually performed within each system, or automated across the infrastructure?	
Do you have requirements for multi-factor authentication today, and if so, do you have this capability already deployed?	

Privileged user account management

Do you have a concise understanding of all shared service accounts being used in your infrastructure?	
Do you have a regular process to validate that all shared service accounts, and all users with access to them, are necessary?	
Are you able to automatically manage the check-out and check-in of shared service account usage, so you're able to audit exactly who was using a shared account at any given point in time?	

Encryption

Do you have self encrypting storage?	
Do you have requirement for encrypting all data at rest?	
Is your certificate management a manual or automated process	
Do you use encryption for data leakage protection?	

Network Protection

How many successful intrusions have you had in the last year?	
With your existing technologies, would you know if you had a successful attempt?	
What technologies do you use, that could detect such an attack and intrusion?	
What are you doing to block attacks against Web applications?	
Are you using your technology to passively detect or actively block attacks?	
What technology do you use to mitigate SQL Injection attacks?	

E-mail Protection

Does your organization offer end-users functionality to control the email coming into their inbox?	
What is your process to recover a single e-mail?	
Is your organization concerned about loss of confidential or proprietary information over email?	
Does your organization have filters in place to deal with unwanted email such as newsletters, inappropriate content such as pornographic emails or malicious content?	
Does your organization offer end-users seamless end-to-end email encryption to anyone on the Internet?	

Endpoint Management

Are you able to quickly identify all of your distributed endpoints (servers, desktops, laptops, smartphones and tablets, plus specialized equipment such as point-of-sale devices, ATMs and self-service kiosks) and check for rogue assets on the network?	
Do you have real-time visibility of endpoint status and automated compliance reporting?	
Does your solution provide a closed-loop integrated assessment and automated remediation for patch, configuration, vulnerability, anti-malware, and data loss prevention?	
Does your solution continually assess the status of the endpoint and ensure the endpoint remains in compliance with organizational policies?	