

1. Please describe your network/security architecture diagram?

Please include:

- The physical topologies
- Logical topologies (Ethernet, ATM, 802.11, VoIP, etc.)
- Types of operating systems
- Perimeter protection measures (firewall and IDS placement, etc.)
- Types of devices used (routers, switches, etc.)
- Location of DMZs
- IP address ranges and subnets
- Use of NAT
- Diagram retaining/change management

2. Please define what resources are located on your DMZ?

3. Please define what resources are located on your internal network?

(e.g. internal web, mail, and DNS servers, databases, application servers, and test and development servers)

4. Please identify where your organization's security policy is posted? Please provide a copy, or thoroughly detail what these policies cover?

(e.g. policy(ies) that establishes the direction of the organization and its security mission as well as roles and responsibilities; system-specific; appropriate use of computing resources; security controls around passwords, backups, proprietary information)

5. Please describe your organization's password policy? (e.g. number of characters, type of characters, method of change, use, lock attempts)

6. Please identify what applications and services are specifically denied (prohibited) by your organization's security policy?

(e.g. inappropriate material, spam, file sharing, messaging, devices, encryption)

7. Please identify what type(s) of IDSs your organization uses?

8. Please describe what activities are actively monitored by your IDSs, other than default rule sets. (e.g. customization, configuration, rules,)

9. Please describe the type of remote access allowed, and how it is controlled, monitored and audited?

10. Please describe your wireless infrastructure?

11. Please describe how your wireless infrastructure is secured?

12. Please describe what desktop protections are used, how they are deployed and how they are controlled? (e.g. anti-virus software, personal firewall, host-based intrusion detection)

13. Please describe where, when, and what type of encryption is used? (e.g. VPNs, IPSEC, 3DES, AES, 128-bit SSL and SSH)

14. Please describe your backup policy? Include: timeframe, storage, access, local/offsite

15. Please describe how sensitive information is disposed of? (e.g. pulping, shredding, incinerating, erased)

16. Please describe your disaster recovery plan?

17. Please identify how often your disaster recovery plan is tested? And what is covered in the testing.

18. Please identify what types of attacks you are seeing?

19. Please identify how often logs are reviewed? (e.g. timeframe, type of logs)

20. Please identify how often you are performing vulnerability scanning?

21. Please describe the physical security controls in place in your organization, and at any of your storage centers? (e.g. physical access controls, CCTV, motion detectors, smoke and water detectors, and backup power generators)

22. Please describe your critical business systems and processes? (Critical business systems and processes may include an e-commerce site, customer database information, employee database information, the ability to answer phone calls, the ability to respond to Internet queries, etc.)

23. Please describe what the specific threats are to your organization?

24. Please identify what the tolerable levels of impact are to your systems? (e.g. system downtime, impact on cash flow, service level agreements, and the key resources)

25. Please identify how often your systems are patched?

26. Please describe how you are protecting against social engineering and phishing attacks?

27. Please describe what security measures are in place for in-house developed applications?

28. Please describe what type of traffic you are denying at the firewall?

29. Please describe how you monitor for Trojans and backdoors?

30. Please identify where the data is stored both physically and logically?