

[WP-015]

## Whitepaper: Why do Organizations Need a 'Modem Policy'?

Another Reason to Mitigate Risks of Legacy Systems Utilizing Modems

**Version 041102**

November 2004

Author: Bob Radvanovsky, [rsradvan@unixworks.com](mailto:rsradvan@unixworks.com)

*(A special thanks goes to those listed for being my "sounding board" on this project.)*

Copyright © 2004 Bob Radvanovsky. All rights reserved.



## **Limited Liability Statement**

---

In no event shall the author(s) be liable for any found errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained within this document may be subject to change without any notice. No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this whitepaper.

Documentation pertaining to any security-related technical or proprietary information, its data and all information provided and contained within this document is considered proprietary in nature and subject to copyright protection and is intended solely for use by its owner. Additionally, this documentation is solely for discussing a possible, and/or proposed IT security issue, and is not dependent upon any specified infrastructure, architectural condition or its issue(s). Source information is through observation from previous employers, and discussions with colleagues within the IT security field.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners. NOTE: Any names not outlined or mentioned above are fictional in nature; as such, any relation to any name or trademark (if any) is purely coincidental.

## **Why does any organization need a good ‘modem policy’?**

---

For most users, company policies are management’s instructions indicating how an organization is (or would like) to be run. Having a modem usage or modem availability policy is designed (mostly) as an addition to an existing corporate security policy (if any exist). Logically, having a modem usage policy may be piggybacked or incorporated with an existing policy, such as the enterprise-wide remote access policy, or if none exist, to make one as modem usage or access policy.

Similar to a wireless access point, but from older technology, modems pose a serious threat to the integrity of the company and its infrastructure. Having either/or modem or access policies in place, and having wide acceptance with management, is the first step in eliminating unauthorized and/or poorly installed modems within and throughout the enterprise. Near the end of this policy might contain a section entitled “Steps for Deployment of the Modem Policy” which may outline some of the necessary steps within the organization for ensuring that modem use and its deployment (or replacement) and have been secured.

Having any kind of modem policy (usage or access) displays due diligence in regards to securing the enterprise at an organizational level. Thus, organizational-wide acceptance of this policy at a management level will assist in auditing functions by assessing the security posture of the organization. As with anything related to the organization's security management, a thorough risk analysis and/or assessment is recommend, and should be made for each modem or remote access device found. In today’s corporate environment,



there may be a plethora of business reasons or needs for modems to exist, and each one of those reasons needs to be weighed against the potential vulnerability of a poorly configured modem, which widely opens up (and potentially exposes internally) any company. The modem policy outlines these potential areas of conflict between the security management aspect and business operations aspect of the organization. Thus, the modem policy attempts to resolve any conflicts (which may arise from their detection and identification) in a clear manner that might enable an organization to have a firm understanding of all issues relating to modems within the organization.

Many organizations rely heavily on their internal automated resources (networks, computers, telephones, etc) to meet operational, financial and information requirements. Any and all information that passes through a given workflow process is stored on, through and within these resources, and are considered important assets to the organization. This information, having or not having it readily and securely available, can make or break a company. A system of internal controls and policies should exist to safeguard and control any misuse of these assets (as information is today considered an “asset” or “resource”, signifying a unspecified value placed upon it by the company). Information should be processed securely, such that all employees share the responsibility for ensuring the information’s confidentiality, integrity and its availability. The modem policy should cover both accidental and intentional disclosure of, or damage to, any organizational information lost or stolen due to improperly installed remote access devices, more specifically, modems.

The scope of the modem policy applies to the confidentiality, integrity and availability of the organization’s information with regards to remote access via telephone and/or broadband connections, and (perhaps) more specifically, modems. The primary function of a modem policy is to outline the extent of which devices should allow access, to whom, and for what reason, are to be deployed within the organization, and should demonstrate how the enforcement of this policy will be carried out.

Any information processed within the organization must have an identified owner, and this assignment must be formally documented. The owner may delegate ownership responsibilities to whoever is (ultimately) responsible for safeguarding and processing the data/information. Within the scope of modem policy, the owner of the data/information has the authority and (more importantly) the responsibility to:

- authorize access methods and assign custody of assets to (one or more) custodian(s);
- determine requirements regarding how access is enabled, and communicate any information towards the custodian(s) of the data/information;
- specify any (or all) methods for access control and communicate the control requirements towards the custodian(s), as well as the users, of the data/information;
- support responsibility and authority of the custodian(s) to perform any actions necessary in keeping the data/information secure.



Probably the most important role of the data/information exchange is the custodian. The custodian is responsible for the (possible establishment and) administration of controls and requirements as specified by the owner of the data/information. This includes having the authority and responsibility to:

- provide physical and technical safeguards for the data/information;
- provide procedural guidelines for the users of the data/information;
- maintain listings of all authorized modems, with their settings (i.e. "auto answer mode off") that will facilitate future examinations of telephone auditing logs;
- administration access to the data/information;
- evaluation of cost-effective controls.

To correctly perform the activities outlined above (and these activities are crucial to maintenance of the data/information), the custodian must define and keep current listings of ALL call-in and call-out modems deployed within and throughout the enterprise of the organization. Also, keep any and all records (or keep active records of any) activities of each modem, and what is provided by the modem that adds value to the organization. That is, why is the modem necessary?

The custodian will also, several times per year (referred to as the "modem testing period"), update the list of all telephone numbers available to the organization, and regularly perform security audit tests against the modems. The testing should be performed at regular intervals (on a monthly or quarterly basis,) and will ensure that:

- all modems deployed within/throughout the organization are configured properly;
- no additional, unregistered modems have been deployed without proper authorization for any telephone within and throughout the enterprise of the organization;
- any modem decommissioned is recorded as being removed from service, and if a replacement exists, what alternative to the modem has been implemented.

Results of this testing will be regularly reported to the owner (and/or management) of the asset, as well to the principals of the organization (i.e. a vice president, or higher, within the executive chain, as appropriate within the organization).



Lastly are the users of the data/information (and why this is important – as in “who” will utilize the information and why it is important to them). Each user has the responsibility to:

- comply with controls/policies with regards to modem usage as outlined by the owner and custodian. This includes relaying information about this policy to any external parties, employees, vendors or other members of the organization;
- acquire appropriate authorization from the owner/custodian of any network a newly placed modem will be connected to BEFORE attaching and activating the modem;
- supply the custodian with the telephone number, proper settings of the modem, and physical and logical location of all authorized modems the user deploys (this will assist the custodian significantly, esp. when the custodian performs the routine/regular telephone audits);
- report any known violations of this policy to the custodian or owner immediately upon discovery.

As with any policy document, the policy is worthless unless it is enforceable or managed by the owners and/or custodians of the data/information process flow. If a violation of the modem policy is uncovered as a result of the custodian’s normal audit process, the custodian has the authorization to stop, cease, and shut down the offending modem immediately after determining the modem is not listed on the custodian’s list of authorized modems.

Second, any violation of standards, procedures or guidelines established pursuant to this policy shall be presented to the management of the organization for appropriate action. This could result in disciplinary action, including dismissal and/or legal prosecution. Last, are the steps necessary of ensuring deployment of the modem policy, which are:

1. Ensure that the policy is approved by appropriate management within the company.
2. Obtain and acquire permission and authority to perform a telephone line scan on the company’s internal telephone system. The time of the scan (during business hours, outside of business hours, etc.) needs to be defined during this stage.
3. The custodian needs to gather an initial listing of all telephone numbers, including internal extensions that the company owns or can potentially own (whether or not the telephone number is currently known to be "in use" or not). This includes the "block of numbers" the telephone company has reserved for use for the company.
4. A telephone line-scanning product should be chosen and purchased.
5. The telephone line-scanning product should be used on all potential telephone numbers (both external AND internal) for the company.
6. Examination of all results of the scan will be undertaken. With the assistance of the telephony department, all items will be addressed, and the initial list of authorized modems/configurations/locale will be created.

All said and done, this is how a modem usage and deployment policy should be implemented within an organization. Alternatively, many companies are referring back to VPN tunneling technologies, such as Cisco’s VPN Client for Workstations. Products such as this, offer an alternative method of remote access in lieu of modem provisioning, thus reducing the amount of threat to the organization. A comparative threat matrix might look something similar to what is shown below:

