DEALER I.T. SECURITY & THE G.L.B.A.

DEALER LAN SECURITY & GLBA COMPLIANCE
The Gramm-Leach-Bliley Act Brief Overview
It is essential for Dealers to recognize that the application of the Act's provisions extends well beyond depository institutions. Under the Act, a financial institution is any business that engages in financial activities ranging from insurance brokerage to data processing to automobile financing/ leasing. The Act specifically references automobile dealers that provide financing to their customers are subject to the Act's Privacy and Safeguard Rules. The Privacy Rule is intended to raise customer awareness of the different ways their non-public, personal information may be used, and requires dealers to present certain paperwork on their information sharing policies, or information notices to the customer during the information-gathering process. The Safeguards Rule is intended to protect the financial institution's customers from identity theft and other harm by requiring financial institutions to assess their data and information from misappropriation, alteration, tampering, etc.

SAFEGUARDS RULE
The elements of the Safeguard Rule are:

1. Information Security Program Coordinator – The SPC is in charge of assessment, implementation, and updates to the physical and electronic security of the dealership. This person(s) is in charge of managing security policies, procedures, and FTC required paperwork.

2. Risk Assessment – Financial institutions are required under the Safeguards Rule to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information. This process of identification should be done by the SPC (With the assistance of a person trained in specifically threats, network security and government / industry regulations, rarely will this be able to be accomplished by a network engineer) through a process of Risk Assessment. Foreseeable risks include:
a. Attacks through the Internet via hackers or other malicious software applications.
b. Viruses downloaded by employees inadvertently.
c. Compromises to the physical aspects of security. Open PC's with no password

3. Risk Control – Financial institutions must design and implement safeguards to control the risks identified through the Risk Assessment. To protect from inside and outside threats, dealerships must take "reasonable measures" to implement a system for intrusion detection and prevention.
a. For electronic data, this is an up-to-date security device that continually monitors threats through intrusion detection system (IDS) and other mechanisms.
b. To control the risks from within the dealership, every dealer should at least protect each PC with anti-virus software and unique passwords. GMDIT recommends a corporate antivirus solution that is designed to protect the entire network as opposed to just individual PCs. GMDIT also recommends a password protection solution that limits the data each user is permitted to see. This would allow customer information to be viewed on a "need to know" basis only.

c. Reporting on the activity of data going into and out of the dealership is a key element to monitoring, detecting, and responding to threats. Only timely reports specific to a dealership can give the PSC a true sense of the threats they are faced with. Customized reporting is the only way to monitor the security program and its effectiveness.

4. Provider Control – Dealerships are required to take reasonable steps and oversee service providers, and retain those that are capable of protecting the dealer's customer information. The Safeguards Rule states that one method of overseeing the providers is to require them by contract to implement and maintain such safeguards.

5. Evaluate and Adjust – Financial institutions are required to evaluate the measures they have taken and continually adjust and reevaluate their information security program.

NIST Standards

The National Institute of Standards and Technology has published a paper on firewall recommendations. This paper, "Guidelines on Firewalls and Firewall Policy," can be downloaded from http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf. The choice of firewall, or in the case of a dealership, a Unified Threat Management ("UTM") device, should largely be driven by its feature set, rather than the type of firewall. Firewalls and UTMs are vulnerable themselves to misconfigurations and failures to apply needed patches or other security enhancements. Accordingly, UTM configuration and administration must be performed carefully and organizations should also stay current on new vulnerabilities and incidents. While a UTM is an organization's first line of defense, organizations should practice a defense in depth strategy, in which layers of UTMs and other security systems are used throughout the network. Most importantly, organizations should strive to maintain all systems in a secure manner and not depend solely on the UTM to stop security threats. (Executive Summary) Also, as stated in Appendix C – Section C.2 Organizations should examine carefully which UTM and security environment is best suited to their needs. Assistance is available from a number of commercial sites that deal with UTM selection and analysis.

A UTM environment should be employed to perform the following general functions:
• Filter packets and protocols
• Perform Stateful inspection of connections
• Perform proxy operations on selected applications
• Log traffic allowed and denied by the UTM
• Provide authentication to users using a form of authentication that does not rely on static, reusable passwords that can be sniffed
• The UTM should be able to filter packets based on the following characteristics:
o Protocol, e.g., IP, ICMP
o Source and destination IP addresses
o Source and destination ports (which identify the applications in use)
o Interface of the UTM that the packet entered
o The proxy operations should, at a minimum, be operable on the content of SMTP, FTP, and HTTP protocol traffic. Proxy applications should be used for out-bound HTTP connections and for inbound/outbound email that are capable of the following operations:
☐ Blocking Java applets and applications
☐ ActiveX® and JavaScript filtering
☐ Blocking specific MIME extensions
☐ Scanning for viruses
Organizations and agencies may find that they need several security appliances to accomplish

The GMDIT Unified Threat Management device versus the Cisco PIX device

The Cisco PIX IOS utilizes a Deep Packet Inspection process, otherwise known as Intrusion Prevention Scanning or IPS. Network threats have evolved from simple, connection-based attacks to more complex content-based attacks such as viruses, worms, and Trojans. Financial institutions are struggling to cope with content-based threats, such as email spam, inappropriate web content, spyware, and other malicious greyware." Deep Packet Inspection does not detect a substantial portion of active viruses, Trojans and worms, and is ineffective for dealing with inappropriate web content, email spam, and spyware. As long as an attack is contained within a few packets (i.e. buffer overflows, DoS, and a small percentage of worms), Deep Packet Inspection works. It cannot, however, detect threats that require many packets to transmit. For example, suppose a user wants to download a file from an FTP site or even a web mail message. A typical firewall will see that a user is trying to use an FTP or HTTP service and allow this to occur. A security device that is designed to protect against "Unified Threats" will actually analyze this traffic to make sure it is safe from viruses or other malicious application (i.e. greyware). While a client AV solution in most cases will protect the client, many AV solutions do not protect against applications such as key loggers, mail relay engines, or other malicious spyware applications. A better approach to network security is Complete Content Protection. The key aspect of CCP is the ability to reassemble packet payloads for scanning and analysis. Such solutions are capable of detecting a full range of threats – including viruses, worms, Trojans, inappropriate web content, spyware, and email spam. Cisco's IOS detects 59 threats through its IPS system by default. A device, such as GMDIT's, currently detects over 1300 intrusions; furthermore, GMDIT supports dynamic updates on a minimum monthly basis for new threats and vulnerabilities. As an added layer, the GMDIT device also supports Web Content Filtering to block inappropriate web content and sites. Finally, the Cisco IOS does not have antivirus filtering capabilities. To recap, while the Pix has a very good Stateful Packet inspection engine, and does has IPS (although it is very basic due to the limited amount of signatures it scans) it does NOT have antivirus scanning abilities or IDS. Also please realize that while the correct hardware itself is very important, the proper management, back end support and realtime monitoring using a SIEM (Security Information and Event Management) tool is also recommended for a full solution.