• having proper DNS firewall to stop known threats
• requiring ISP's to drop malicious botnet traffic before it gets to American homes and businesses.
• There are known databases of automated attacks have those blocked in USA.
• fine companies who harbor malicious network traffic.
• fine corporations who are not protecting american's data 10% of profits to effectively punish violators.
• work with analysts who can help guide and stop the automated attacks.

Jon Little
Security Analyst
[phone number redacted--NTIA]