



# Corporate Information Security

*Vulnerability Management & Incident Response Team (VMIRT)*

## **Executive Summary:**

The FCC is soliciting the public and businesses for thoughts and opinions for its CyberSecurity Roadmap being created. The purpose of this document is to provide a response, from the viewpoint of KeyBank, of the specific questions asked in the request, which may be found at [http://www.fcc.gov/Daily\\_Releases/Daily\\_Business/2010/db0809/DA-10-1354A1.pdf](http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db0809/DA-10-1354A1.pdf). Additionally, the questions are listed below.

1. What are the most vital cybersecurity vulnerabilities for communications networks or users?
2. How can those vulnerabilities be addressed?
3. What role should the Commission play in addressing them?
4. What steps should the Commission take, if any, to remediate them?
5. If the FCC does play a role in addressing these vulnerabilities and problems, what agency or entity would fulfill that role?

How should the Commission coordinate its efforts with other agencies of government?

## **Response to FCC Request:**

### ***What are the most vital cybersecurity vulnerabilities for communications networks or users?***

- End user understanding of information security best practices.
- Resiliency/Redundancy/Bandwidth requirements in core communication infrastructure.
- Security of mobile devices connecting to corporate networks and web applications.
- Applications being able to dynamically choose a port to communicate over based on firewall settings.
- ISP awareness of the internet traffic flowing through their network.
- Free Wireless access points.

### ***How can those vulnerabilities be addressed?***

- End user understanding of information security best practices
  - This needs to be addressed on at least two fronts.
    - A public security awareness campaign needs to be created and distributed through something such as a public service announcement via radio, television, internet ads, etc.
    - Corporations need to build upon the public security program to address company specific security vulnerabilities.
- Resiliency, Redundancy, and Bandwidth requirements in communication infrastructure
  - Add additional/redundant infrastructure to communication networks
  - Place primary and redundant infrastructure in locations secure from disasters
    - Core network systems should not be in a high risk areas (ie, upper floor of a skyscraper).
    - Place more core infrastructure underground rather than overhead



# Corporate Information Security

*Vulnerability Management & Incident Response Team (VMIRT)*

- Security of mobile devices connecting to corporate networks and web applications
  - Security needs to be a top concern for the manufacturers of mobile devices such as iPhones™ and Android™ devices so that they can not, or are difficult to become, part of a Bot network or a wireless hot spot for hackers.
- Dynamic port usage from applications
  - Software companies should standardize what TCP ports applications communicate over the internet on and not allow dynamic port usage. For example, AOL Instant Messenger defaults to ports 5190-5193 upon installation, but if those ports are blocked outbound by a firewall, AOL IM dynamically changes the port used until it can communicate with the AOL IM server. This is usually port 80, since this is the most common port used for internet traffic.
- ISP awareness of the internet traffic flowing through their network.
  - ISPs should have policies, standards, and best practices in place to protect their customer's networks from "bad" internet traffic. It is these policies, standards, and best practices that a respectable ISP would follow.
- Free Wireless access points that are used to VPN into corporate networks
  - This can be addressed with security awareness education on the risks of connecting to such networks and what can/should be done to have a secure connection.

## ***What role should the Commission play in addressing them?***

The FCC should be the governing body that develops the standards that secures all public communication infrastructures. However, this standard should be realistic for all entities from the consumer to large corporations to implement and maintain without causing an unacceptable expense.

## ***What steps should the Commission take, if any, to remediate them?***

The FCC should not take any steps to remediate the vulnerabilities that require a technology implementation. However, the FCC should create standards and policies for corporations to follow as well as be the governing body over these policies and standards.

## ***If the FCC does play a role in addressing these vulnerabilities and problems, what agency or entity would fulfill that role?***

No specific recommendations.

## ***How should the Commission coordinate its efforts with other agencies of government?***

The members of the Commission should include those that are from other government agencies and act as the central authority of the program. In turn, those members from the other agencies of government can be the line of communication between the Commission and their respective agency.