Security While On the Move

CrossTalk would like to thank DHS for sponsoring this issue.

The increasing convenience and ubiquity of mobile computing and smart personal communication devices presents an irresistible target for malicious actors. The rush to provide applications means few are tested to detect, analyze, and remediate weaknesses. Public Wi-Fi networks can also provide a vulnerable entry point to our mobile device information systems. As a result, hackers are able to quickly exploit software on smartphones.

The challenge of securing the mobile world is complex and therefore requires multi-disciplinary solutions. The security models currently provided by major mobile providers are not sufficient to meet the information protection needs of civilian and defense agencies. Application developers, network administrators, and incident responders need to collaborate to address mobile computing risk. To be effective, this collaboration requires rapid sharing of standardized threat and vulnerability information so public and private stakeholders can act quickly to mitigate risks to their operations and activities.

Fortunately, much of what we already know and do in cybersecurity applies to the mobile world and the challenge of securing it. Consistency in the identification and interpretation of software weaknesses, attack patterns, and malware data is essential for quick and efficient information sharing. DHS sponsors programs that help standardize such data, thus allowing companies and organizations to collect, store, and define it in compatible formats. By promoting common data taxonomies and methodologies for storing, indexing, and interpreting malware samples, DHS is driving towards seamless diagnosis and remediation of exploitable software across the various mobile platforms. These are necessary conditions for near real-time situational awareness of vulnerabilities and malware. However, collaboration should not end with remediation of malware. DHS envisions an environment that grants public and private sector owners and operators of information technology systems access to an entire range of security automation tools and capabilities, including software assurance education materials and security-content authoring services.

The public and private sectors occupy equally important—and equally informed—roles within their particular area of cybersecurity expertise. Rapid, bidirectional information sharing ensures that both sectors are able to bridge the critical information gap between what they know and do not know. Cutting through these knowledge gaps ultimately facilitates the real-time situational awareness necessary to defend cyberspace. Together, we can develop a trustworthy, sustainable, and flexible information-sharing environment that effectively secures our Nation's cyberspace—including the ever-growing mobile domain.

Roberta "Bobbie" Stempfley
Deputy Assistant Secretary
Office of Cybersecurity and Communications
Department of Homeland Security