Today's Mobile Cybersecurity

Blueprint for the Future

CTIA
The Wireless Association®

Executive Summary:

The evolution of the connected society of the 21st century has mobility as its cornerstone. Indeed online security and privacy go hand-in-hand to protect consumer information and the corresponding digital assets and identity. The mobile communications industry has made and continues to make significant investments in cybersecurity solutions, and understands that partnership is the most effective mechanism to maintain security in a dynamic threat environment.

Increasing demand by consumers and enterprise users for more ways to stay connected on the go drives innovation and industry efforts through CTIA–The Wireless Association®. CTIA's Cybersecurity Working Group (CSWG) is committed to the exploration and research needed to develop future blueprints that build upon today's cybersecurity solutions.

In the first white paper, *Today's Mobile Cybersecurity: Protected, Secured and Unified,* the latest cybersecurity solutions were explored in the context of the complex wireless ecosystem. This white paper provides an overview of trends in mobile usage and threats, and shows how this analysis is reflected in the industry's blueprint for ongoing cybersecurity investigation and technical improvements under study. A number of important areas are covered:

1. Ongoing consumer education
2. Consumer and user credential protections via trusted identities/mobile cloud
3. Enhanced security features
4. Software update distributions
5. Multiple air-interface security
6. Side-loading
7. Login/password locks
8. Root-of-trust and policy enforcement engine
9. Machine-to-machine (M2M) and near-field communication (NFC)
10. Text messaging (SMS)
11. Device enhancements
12. Disrupt malware spread

The mobile industry monitors the threat landscape, analyzes trends and is guided by a blueprint for technical advances and enhancements to protect consumers and end users. This blueprint is continually updated and adjusted based on emerging threats and ongoing research.

However, consumers, as well as enterprise and government users, must be part of the solution. For cybersecurity to work, it must be an all-in commitment

Digital Information is the Currency of the Connected Society of the 21st Century

Categories of Information:

1. Digital Assets/Media: e.g., Video, Pictures, Recordings
2. Consumer/Enterprise Information: e.g., Passwords, Account Numbers, Confidential IP, Health Information
3. Real-Time Information: e.g., Location, Web Preferences, Surfing History, Social Nets

Introduction

Cybersecurity is more widely appreciated than ever as rising numbers of Americans depend on mobile communications to conduct tasks that involve their personal information. Highly publicized cyberattacks by terrorists and criminals around the world have raised awareness of the need for strong protections to ensure data security and privacy.[1]

Digital privacy **cannot** exist without cybersecurity. These two domains are the currency of protection in the digital era. Privacy covers **what** we protect, from mobile purchases to proprietary business and sensitive government data. Cybersecurity represents the technology and practices that determine **how** that protection is delivered throughout the mobile environment. The mobile communications industry invests significant resources in the ongoing safeguarding of the many elements that comprise the expanding mobile ecosystem. In addition to its 24/7 focus on securing today's mobile services, the industry is also working on solutions to serve consumers and enterprises in the future.

The blueprint that will help ensure tomorrow's cybersecurity and privacy solutions is a top priority for members of CTIA–The Wireless Association.

Cybersecurity & Privacy– Opposite Sides of the Same Coin Protect Digital Information

Privacy

"What" to Protect

Examples: Healthcare, HIPPA, Financial, Enterprise Proprietary, Personal, Government

Cybersecurity

"How" to Protect

Examples: Encryption, Policy Management, Root-of-trust, Countermeasures, Threat Assessments, VPNs

Through its Cybersecurity Working Group (CSWG), companies representing security expertise throughout the entire mobile ecosystem engage in ongoing research and dialogue with government entities such as the National Security Agency, Defense Information Systems Agency, National Institute of Standards and Technology and Department of Homeland Security. This cooperation was recently demonstrated by the agencies' officials who participated in a public sector cybersecurity panel at MobileCON™ in October 2012.

Thanks to the CSWG's commitment, the wireless industry has a good command of the path forward to stay ahead of the "bad guys."

However, no one underestimates the challenge. Growth in demand for mobile communications is accelerating at an almost unimaginable pace. Last year, industry estimates show smartphone purchases outstripped computers (desktops, laptops and tablets) for the first time. By 2015, it is estimated that more Americans will access the Internet via mobile devices than PCs or any other type of wireless device. CTIA data shows more than one connected wireless device per American today (322 million), a usage rate that is only expected to increase.

Preserving privacy and security for mobile data and communications requires everyone's best efforts to advance the nation's cybersecurity interests. Industry and government. Consumers and enterprises. Cybersecurity is everyone's shared goal. When it comes to dealing with today's cyberthreats, the solution requires everyone.

Preserving privacy and security for mobile data and communications requires everyone's best efforts to advance the nation's cybersecurity interests.

State of Industry Solutions

Mobile communications companies invest millions of dollars in cybersecurity solutions, resulting in a strong foundation for the future evolution of security across the ecosystem. Participants, including carriers, equipment makers, operating systems and applications providers, are constantly engaged in monitoring and introducing new approaches to stay ahead of criminals and hackers focused on compromising cybersecurity. In the CTIA white paper, *Today's Mobile Cybersecurity: Protected, Secured and Unified,* there is a detailed explanation of the mobile landscape and comprehensive solutions for end users. To provide context for the future, here is a brief summary.

...a strong security offense is an asset for every participant...

Effective delivery of cybersecurity protections is ongoing and requires solid defensive and offensive strategies to thwart cyberattacks in a constantly changing environment. Security is a defensive necessity to protect and maintain operations, and a strong security offense is an asset for every participant, providing a competitive differentiator and supporting a company's growth.

Important players in securing the wireless ecosystem are varied, and include:

- *Mobile Network Operators (MNOs) that are facilities-based and virtual*
- *Manufacturers of hardware, including mobile devices, chipsets and network equipment*
- *Applications developers and marketplaces*
- *Operating system vendors*
- *Network service providers*
- *Support software vendors*
- *Value-added service providers, such as aggregators, Wi-Fi hot spot providers, over-the-top (OTT) providers and other platform providers*

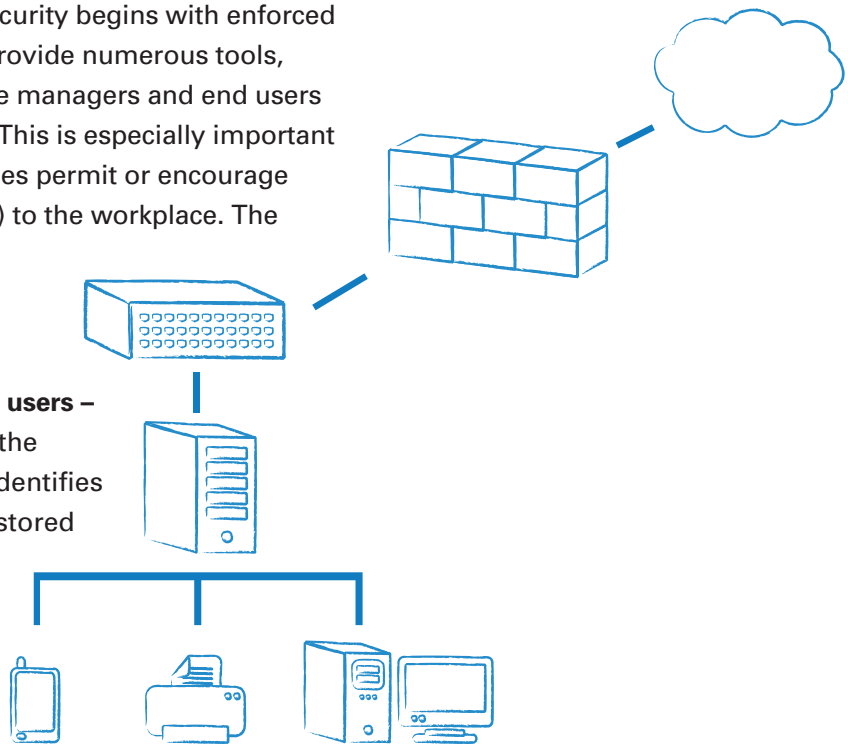
Cybersecurity involves all of these entities at many touch points in the integrated "system of systems" that enables the wireless environment so essential today for mobile voice, video and data communications. The five major cornerstone elements of the industry's security focus are comprised of a variety of solutions aimed at preventing intrusions and securing against data theft or loss of privacy:

1. **Consumers and end users –** The industry works hard to educate consumers by providing guides for best practices to protect personal data and avoid problems in the mobile environment. This advice covers security at every stage, from how to configure devices to be more secure to how to check permissions and understand the security (or lack of) found on different types of networks to how to protect personal data in the event a device is lost or stolen. In addition, the overall industry, including platform providers and application developers, continually works to make the loading of applications and software permissions more intuitive and easier to understand.

2. **Devices –** Today's mobile devices are miniature computers that need to be secured against all sources of intrusions. Some of the security features available for wireless devices include anti-malware and anti-spam settings, strong authentication and secure device connectivity.

3. **Network-based security policies –** Proper security begins with enforced good network policies. Network operators provide numerous tools, guides and support to consumers, enterprise managers and end users to enable them to protect their information. This is especially important as more business and government enterprises permit or encourage employees to bring your own device (BYOD) to the workplace. The result is more emphasis on mobile device management (MDM) systems designed to enforce network policies.

4. **Authentication and controls for devices and users –** Authentication is enormously important in the mobile environment. It is the process that identifies a user as authorized to access information stored on a mobile device or over a network connection from the device.



5. **Cloud, networks and services –** The complex security solutions the industry provides encompass multiple types of network connections: the cloud, the Internet backbone, core network and access network connections that represent methods of transmission, storage and processing data that support industry security solutions. Aspects of these security solutions include consumer and enterprise applications, features for secure storage and virtual solutions and backup and disaster recovery.

Mobile industry participants are committing significant assets to cybersecurity solutions to protect devices and networks and the data they store and carry.

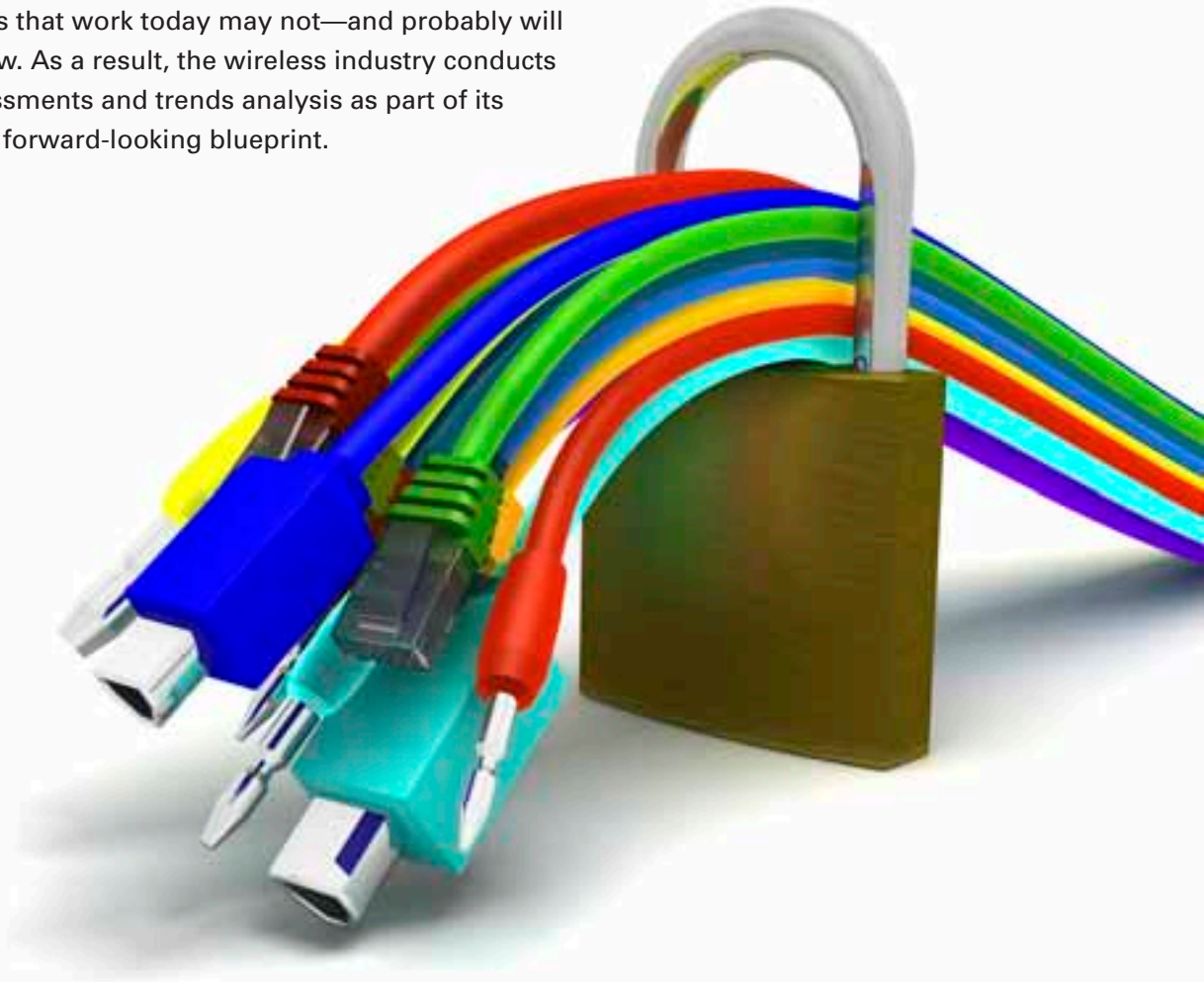
Mobile industry participants are committing significant assets to cybersecurity solutions to protect devices and networks and the data they store and carry. This list is not comprehensive, but provides a sample of current solutions in the mobile environment:

- **Security policies and risk management –** This field is so extensive today that it is nearly an industry unto itself. Among the safeguards are providing enhancements to security policies and risk management protocols; covering definitions and documentation; ongoing scans of the threat environment; and security assessments.
- **Security technology and standards –** From specific directives to general guidelines, the industry relies on a wide landscape of security standards that is continually evolving in response to the threat environment. Various industry standards-setting organizations, such as 3GPP, IETF, Committee T1 and IEEE demonstrate the ongoing commitment to advance the state of the art for mobile cybersecurity.
- **Monitoring and vulnerability scans –** The goal of these tools and processes is to assess threats in real time and stop problems before they happen.

- **Monitoring malware and cyberthreat profiles –** At the heart of effective multi-layered protection throughout the mobile environment is the capability to monitor, quickly assess and act using a robust cyberthreat profile, from the cloud to Internet gateways, network servers and devices.
- **Industry cooperation –** The CSWG is an example of the security-enhancing collaboration that takes place in the mobile communications industry. This CTIA group, comprised of experienced senior representatives from 29 leading companies, advances industry solutions and communications on mobile cybersecurity with government entities, promotes standards and best practices and conducts industry-wide research and analyses.

...mobile mini-computers are increasingly attractive targets for cybercriminals.

Monitoring trends, staying ahead of threats and providing advanced solutions in this dynamic environment demand continual efforts in technology innovation. The changing threat environment means the solutions that work today may not—and probably will not—work tomorrow. As a result, the wireless industry conducts regular threat assessments and trends analysis as part of its commitment to the forward-looking blueprint.



Projections in the Mobile Cyberthreat Landscape

Consumer and business adoption of wireless devices have migrated rapidly from feature phones to smartphones and tablets, and along with the wide range of personal and sensitive information they contain, these mobile mini-computers are increasingly attractive targets for cybercriminals.

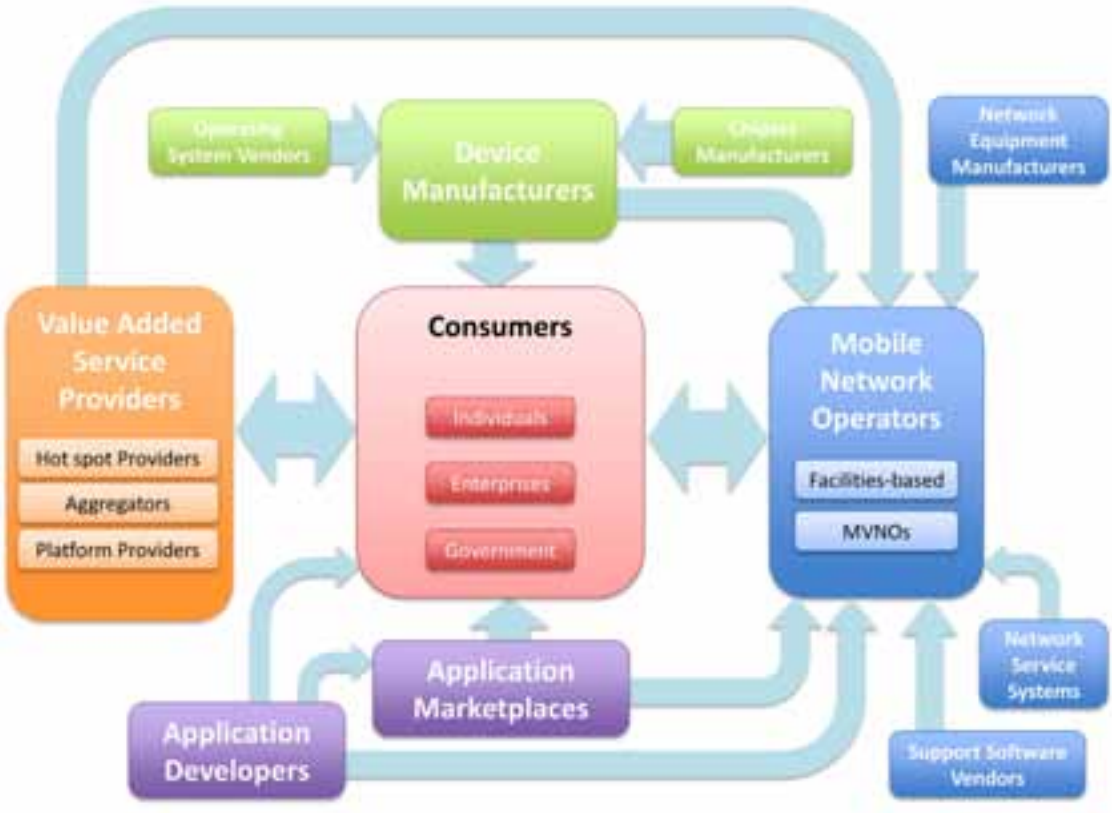
A recent analysis by Frost & Sullivan found malware infection rates of mobile devices in the United States range from a relatively conservative 0.5 percent to a moderate 2 percent. Their analysis projects growth in mobile malware with a fast-growth range (showing a sevenfold increase to 14.9 percent in 2013) for the worst-case scenario of commoditized malware spreading via the Internet.

Frost & Sullivan reports that installers, no matter how these applications are accessed, are the most commonly used "bait" on the Internet by criminals that usually leads back to already identified malware families. Expanding criminal use of installers is growing more rapidly than the major classifications of mobile malware.

The biggest risk and worst-case scenario, according to their analysis, is mobile malware becoming a commoditized product, a malware toolkit produced by a programmer and then sold to other cybercriminals to use in building their own malware attacks and for programming expertise.

A complex, fast-moving threat environment: This section examines trends, based on the Frost & Sullivan findings, which affect four important components of the mobile ecosystem: smartphones and tablets, mobile applications, mobile operating systems and mobile infrastructure/networks. The trends will be viewed from the perspective of how consumers and government and enterprise employees typically use mobile devices. In the context of Today's Mobile Ecosystem (see figure next page), the paper explores the implications of the trends and uses, including mobile wallet services, to highlight the risks overall along with three typical scenarios—going online from a carrier network (3G/4G) to the Internet; going online from a Wi-Fi location; and "side-loading," which is downloading from the Internet to a laptop and from there to a mobile device.

Today's Mobile Ecosystem



Frost & Sullivan forecasts that by 2017, more than 80 percent of all mobile phones in the United States will be smartphones, and that Americans will be using more than 200 million tablets. Both types of devices are making strong inroads in the consumer and enterprise market segments, in part based on the rapid growth of BYOD at work.

Cyberthreats to these devices are increasing, and include a range of malware and rogue programs, often disguised as seemingly legitimate updates, utility and productivity tools and downloadable applications.

Currently, the biggest difference between threats to smartphones and tablets is based on how the devices are principally used. For example, tablets appear to be used more for media consumption, including video, games, e-books and accessing the Web; whereas smartphones are used more for data communications activities such as SMS, email, mobile financial transactions and voice calls.

Example:
Mobile Wallet Services

Smartphones are used for a broad array of services from mobile banking to surfing the Internet and social networking. Today, the youth segment shows the fastest adoption of smartphone technology and services and will likely continue to be the largest users of new mobility services. As the youth segment matures, experts predict that consumers will increasingly rely on their smartphones as credit cards, to make routine retail purchases and to access personal bank accounts. Cyberattacks on mobile payment applications and firmware can occur whether the consumer is accessing the Internet from a carrier network, from a Wi-Fi hotspot or from a personal computer. As a result, the mobile wallet serves as a broad illustration of the mobile threat environment.

Mobile Banking Services: Example Use Cases

	Informational	Transactional	Value-Added Services
			
Examples	• Checking Account Balance • Checking Transaction History • Receiving Alerts (Balance, Transaction Limits)	• Transferring Money to Another Person • Paying for Goods and Services • Paying Utility Bills • Receiving Remittances	• Receiving Coupons Based on Device Location • Transaction Flagging for Fraud • Accessing Goods and Services of Cross-Industry Offerings (Retail, Health Services, Travel)

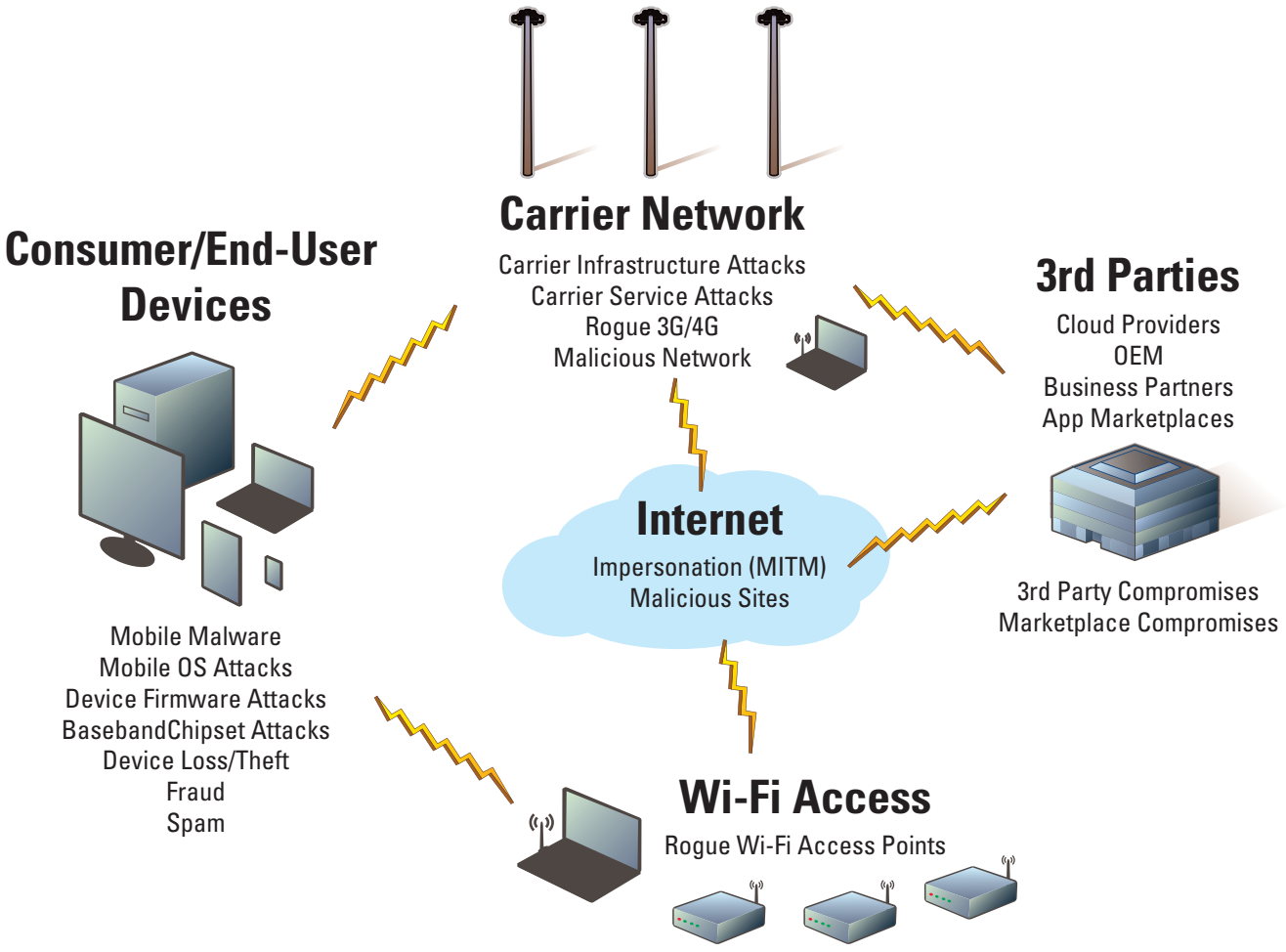
Consumers use mobile wallet services to get information, such as checking a bank balance; to conduct transactions, such as making a purchase or transferring funds; or to gain a value-added service, such as receiving alerts or coupons, as shown in the Mobile Banking Services: Example Use Cases (see figure above).

The cybercriminal, of course, is after the stored credit card or bank account information, and the key identifiers consumers use to access these accounts. On-the-go payment or banking services

can utilize storage in the smartphone itself or in the cloud on secure services. Currently, most providers anticipate using the secure element, or firmware, in the device itself, in combination with a PIN and password.

The next three scenarios go into more detail about the implications of mobile cyberthreats in the context of how consumers and end users typically connect to the Internet through their mobile devices and the corresponding threat landscape.

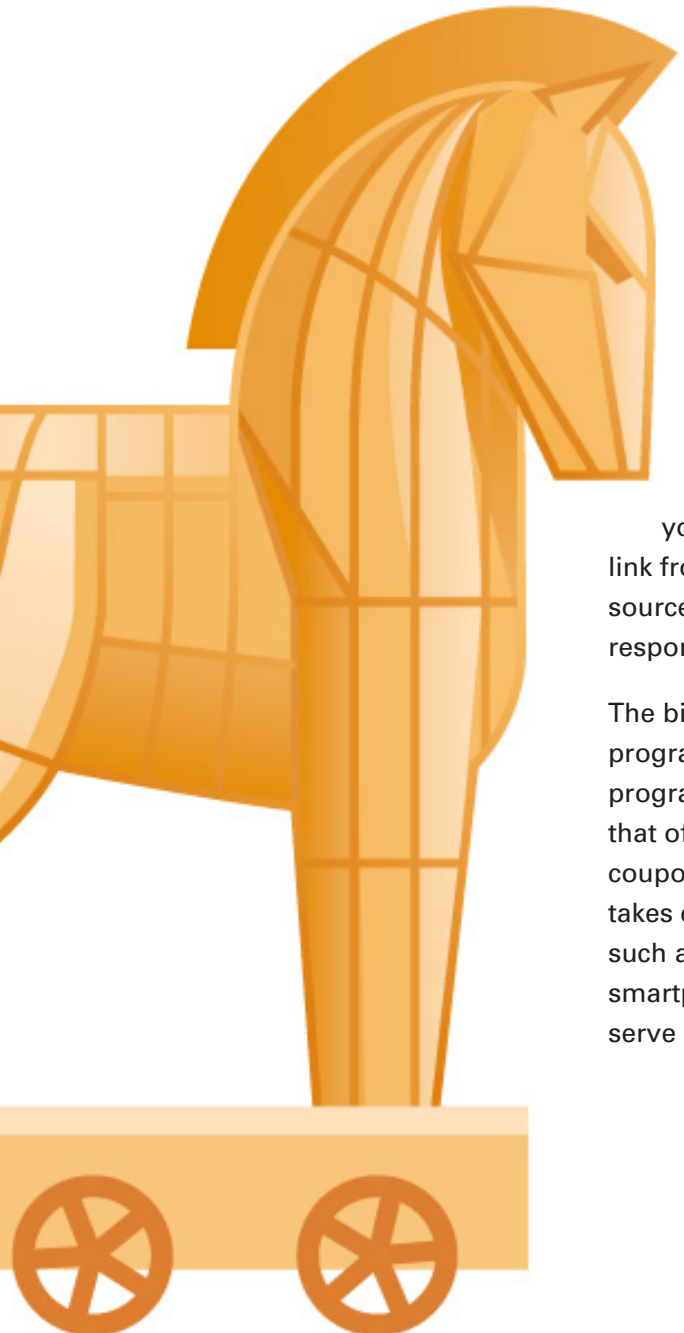
Mobile Security Threat Landscape



The mitigation strategies relative to the threat landscape above are discussed in the section on Strategy and Blueprint, as well as in the first white paper: *Today's Mobile Cybersecurity: Protected, Secured and Unified.*

Scenario One:
Connecting to Internet via Carrier Network

Smartphone and Tablet Users



As mentioned earlier, the mobile industry has invested millions of dollars in cybersecurity solutions available to consumers, resulting in a strong foundation for the future evolution of security across the ecosystem. Carriers, equipment makers, operating systems and applications providers, among others in the wireless industry, are constantly engaged in monitoring and introducing new approaches to stay ahead of criminals and hackers who try to compromise cybersecurity. Nonetheless, the threat landscape is constantly changing. In this scenario (see Mobile Security Threat Landscape) we explore how the smartphone or tablet connects to the Internet to play a game online, download a movie or engage via social media. Any of these activities can be accompanied by cyberthreats. Innocent-looking emails and text messages, even those that arrive via the user's carrier network or a secured enterprise network, can contain malware. So how do you know who you can trust? Cybersecurity experts advise never clicking on a link from unknown sources; being certain that a link from a known source is legitimately sent; and verifying the origin of a quick response (QR) code before scanning it. Here's why:

The biggest for-profit malware threat today is Trojans, malicious programs containing harmful code inside innocent-seeming programming or data, often in the form of emails or SMS messages that offer something appealing or helpful, such as links to discount coupons or free games. Once the user clicks on the link, the Trojan takes control and extracts information the criminal is seeking, such as data needed to access personal information stored on the smartphone or tablet. QR Codes are becoming problematic and serve as another vehicle for malicious software code.[2]

Mobile Applications: OTT Native/Web Apps and Enterprise

A class of mobile malware capable of turning a smartphone into a bot by transmitting its vital operating data to a command and control server is a growing threat.[3] The mobile botnet is then turned into a device that attacks others, resulting in: premium SMS victimization; mobile-based denial of service (DDoS) attacks; data-roaming charge victimization; and remote dialing to high-cost numbers.

Mobile malware drive-bys are a variation on the botnet. This type of malware infects via a drive-by download that turns a smartphone into a proxy or botnet, often by pretending to be a security update, or by being downloaded as part of an application in which the malicious code "sleeps" for weeks before being activated. Drive-bys and botnets are sometimes used to target specific individuals, companies or groups for attacks.

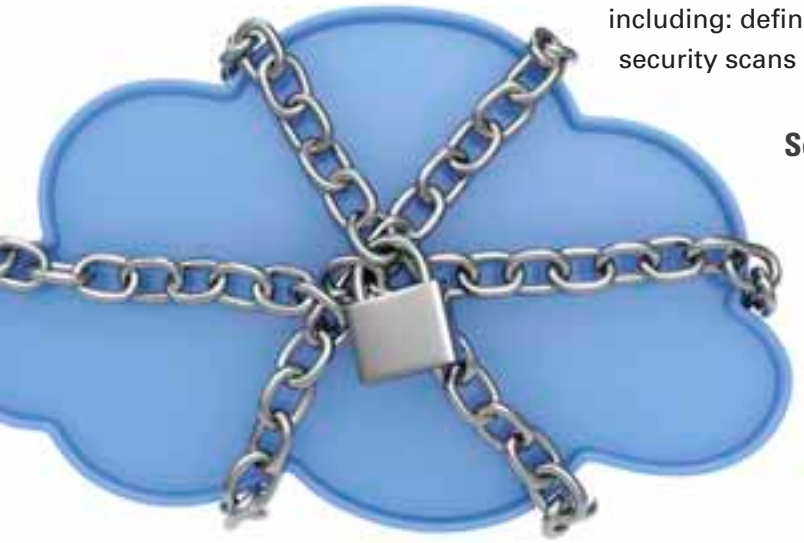
Mobile Operating Systems (OS)

The wireless industry invests significant resources in developing and securing mobile OS, beginning with secure architecture designs that share certain features used by the different mobile devices. Security solutions include:

- *A user-level permission or permission list for installations*
- *An application store or multi-distribution channel of stores for applications*
- *Application certificates*
- *Available or mandatory encryption*

Infrastructure/Network

As described earlier, the list below provides a useful sampling of the comprehensive assets and cybersecurity solutions the industry uses today to secure its services.



Security Policies and Risk Management

All the mobile ecosystem players make efforts to address security policies and risk management to safeguard their services, including: defined and documented security policies, ongoing security scans of the threat environment and security assessments.

Security Technology and Standards

There is a broad landscape of security standards that increase security levels, including those that combine general guidelines with specific directives for achieving certain standards. Examples of such standards include: Digital Encryption Standard (DES); 3GPP Standards for over-the-air encryption; IEEE 802.11i, implemented as WPA2; and FIPS-140-2.[4]

Ongoing Monitoring and Vulnerability Scans

Vulnerability scans through software and other means constantly analyze computers, computer systems, networks and applications for signs of trouble. While specifics among different types of scans vary, the common thread is to assess the threats and vulnerabilities present in targets in real time. Quite simply, stop the problem before it happens.

Monitoring Malware and Cyberthreats

Effective multi-layered protection, in the cloud, at the Internet gateway, across network servers and on devices is underpinned by an ability to monitor and act upon malware via the maintenance of robust cyberthreat profiles.

However, there are situations in which the mobile network may have little to no visibility to possible threats, as outlined in the next two scenarios.

Scenario Two:
Connecting via Wi-Fi Location

Smartphone and Tablet Users

Consumers and end users usually make little distinction between connecting via a carrier network versus a connection via a public Wi-Fi hot spot or access point. Behavior studies suggest many consumers expect their smartphones and tablets will perform the same set of capabilities and support a similar set of applications regardless of how they are connected to the Internet.

However, as the Mobile Security Threat Landscape image shows, in the case of Wi-Fi connections, the mobile carrier network is not in the connection path to the Internet. In this scenario, consumers' devices may be more vulnerable to malware or rogue access points. Therefore, end users need to be more cautious and alert to suspicious email, Web pages and Internet links. Indeed, in this scenario, the consumer may not be afforded the same level of network monitoring for threats as they would be when connecting via the carrier network or other platform-based security monitoring.

Mobile Applications: OTT Native/Web Apps and Enterprise

Increasingly, cybercriminals target mobile devices when the consumer and end user is connecting via a public Wi-Fi access point so they may take advantage of not being subject to many of the security protections the carrier networks and other security platforms deploy in the mobile cloud. Malware solicits and collects location information and other device-specific data that allows the rogue program to take full advantage of an unsecured environment.

However, enterprise applications often require greater security for access to enterprise networks and applications. Typically, enterprise applications require passwords, multi-factor authentication, encryption, Virtual Private network (VPN) access, etc., regardless of whether the user is accessing the enterprise network through a carrier network or a public Wi-Fi hot spot.

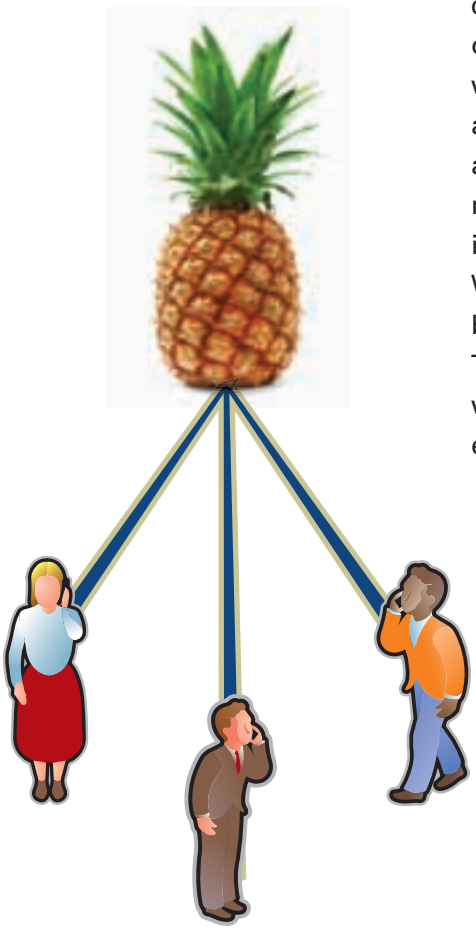
The risk occurs in the BYOD environment when an end user mixes consumer applications and enterprise applications, in particular when both types of applications share memory and other resources within the mobile device. During personal use "time," users may download malware, which can contaminate other applications on the device, including enterprise.

Mobile OS

As described above, there is little difference in this scenario in the context of the OS relative to going on a public Wi-Fi connection or a carrier network connection.

Infrastructure/Network

Network security infrastructure is very limited in public Wi-Fi access points, since they are designed primarily to provide fast and direct connectivity to the Internet. While consumers enjoy the benefits of ready access to the Internet, public Wi-Fi often represents the weakest link. Connection and data traffic are usually unencrypted at Wi-Fi access points, such as those in airports, cafes, hotels and other public places, and they are increasingly the targets of machine-in-the-middle (MitM) attacks to steal consumers' personal information. Other exploitations are exemplified by the "pineapple" Wi-Fi access point as a means to mimic a legitimate Wi-Fi hot spot, but exploits the ability of mobile devices to connect automatically. This type of risk requires no user interaction and often occurs without the knowledge of the end user of the connection being established.



Scenario Three:
Connecting via PC

Smartphone and Tablet Users

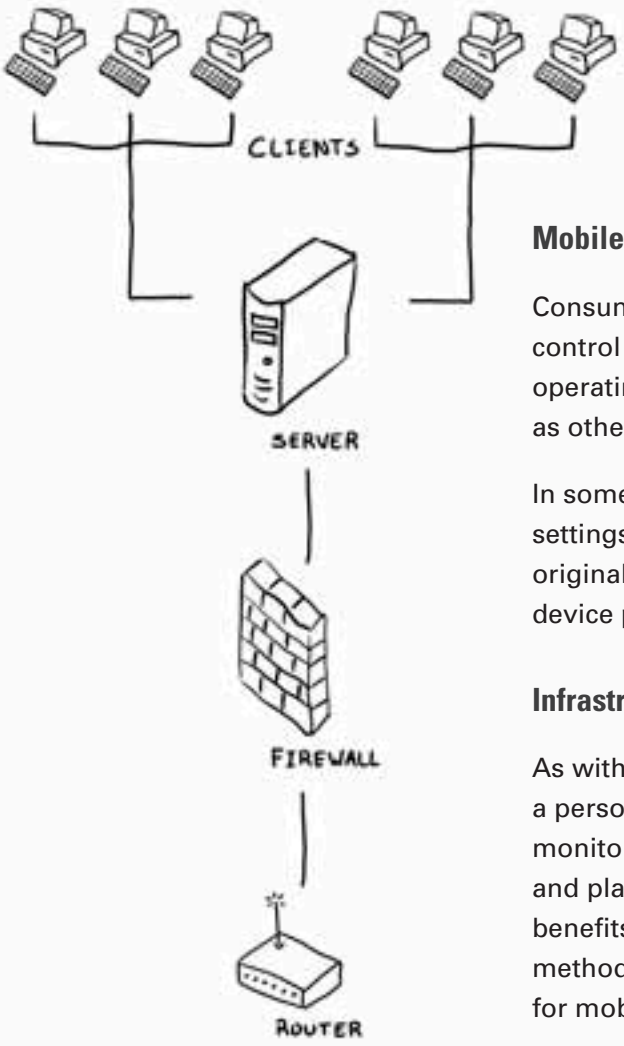
Consumers and end users sometimes "tether" their smartphones or tablets to their personal computers. Often this scenario is used to manage the backup of device information onto a computer; manage pictures, music or videos; or sometimes to root or jailbreak the device (i.e., gain control of the mobile devices' OS).

In this scenario, risks are heightened because the mobile carrier or other security platforms may not have visibility into transactions and functions that occur between the mobile devices and a computer. Also, the consumer may have downloaded applications, software updates or other programs from the Web to a PC without the benefit of the carriers' and platform providers' security.

Mobile Applications: OTT Native/Web Apps, and Enterprise

Similar to the risks of connecting to the Internet via a public Wi-Fi hot spot, the personal computer is also targeted by cybercriminals and malware developers as a conduit to mobile devices because PC-to-mobile-device "sideloading" is free from the carrier networks' and other security platforms' security protections in the mobile cloud.

Malware downloaded to the device in the context of a personal computer may run the risk of contaminating other applications on the device and can extend to enterprise applications.



Mobile OS

Consumers and end users often use their personal computers to control and manipulate memory storage and files on the device operating system, as described earlier for backup purposes, as well as other stored settings, data, etc.

In some instances, the computer is used to alter the original settings of the device's OS. Altering the OS programming from the original provider setting and accessing user-specific data on the device poses the most significant risk of malware contamination.

Infrastructure/Network

As with public Wi-Fi access points, the scenario of tethering to a personal computer is one that may have no visibility to the monitoring and security functions implemented by the network and platform providers. While consumers and end users enjoy the benefits of simple and ready access to the device via their PCs, this method presents another weak link in the ability to provide security for mobile device applications and data.

Strategy & Blueprint

The industry strategy for staying on top of trends in cyberthreats and reducing risks to the mobile ecosystem is based on encouraging partnership with government, raising the level of education of consumers and enterprise users and building on the significant industry know-how, investments and solutions to keep updated a blueprint for future mobile security advances. The blueprint is in response to the threat landscape described in this paper and the goal is to continually improve the mobile industry's cybersecurity profile.

On behalf of CTIA, the CSWG believes that well-informed consumers and enterprise end users are the nation's strongest defense against cyberthreats. The working group bases this conclusion on regular reviews of consumer and enterprise user behaviors and use trends, and combines it with detailed analyses of cyberthreats to provide a solid framework for considering the path ahead for solutions, including education programs and technical solutions to meet emerging threats. This is only part of the detailed cybersecurity blueprint that CTIA member companies continue to advance.

1. **Ongoing Consumer Education:** Surveys consistently show that the more consumers understand the risks in the mobile environment, and the many layers of protection currently available, the safer their actions become. Industry and government efforts are needed to emphasize that mobile cybersecurity awareness and education are central to the protection of privacy online, especially for children and young people who surf the Internet from mobile devices and use social media more frequently than their parents.

   In addition to educating parents and youth, consumer education needs to focus on all demographic groups. Studies also show security risks associated with backward-compatible older generation mobile phones. High numbers of these older devices are resold and remain in use in the United States and represent attractive targets for cybercriminals.

The mobile industry provides a wealth of consumer information online, in "how-to" videos and other instructional material to help purchasers of new or resold mobile devices understand how to protect their personal information and preserve their privacy. This educational information is updated frequently to reflect new cyberthreats or insecure practices by users. In addition, the industry works to continually make software permissions easier to understand.

2. **Consumer/User Credential Protections:** Dissemination of guidance to encourage industry players and consumers to institute and use encryption and multi-factor authentication on mobile devices for greater protection of user data, whether it is stored in the cloud or in secure elements on the devices.

3. **Enhanced Security Features:** Development of multiple layers of security for mobile devices that range from a basic, built-in level to premium levels of security features.

4. **Software Update Distributions:** Development of recommended mechanisms for timely distribution of software updates to consumers and end users, including consumer education on how to verify authenticity.

5. **Multiple Air-Interface Security:** Consideration of notifications to consumers and end users on their devices for greater consumer awareness of the risks when those devices encounter access to unencrypted Wi-Fi; unsecured network connections (3G/4G); or equipped with less than secure backward compatible standards, such as WEP-wired equivalent privacy (versus WPA2-Wi-Fi). In addition to notifications, technology based approaches to address differing security policies across multiple air-interfaces are areas of continued effort and research.

6. **Side-loading:** Consideration of mobile device access by personal computer platforms for installing, updating or modifying applications and the risks associated with possible malware contamination.

7. **Login/Password Locks:** Consideration of femtocell "backdoor/root" login password locks so that mobile devices can be better secured in typical offload scenarios.

8. **Root-of-Trust and Policy Enforcement:** Consideration of built-in enhancements to foundational security for next-generation smartphones and tablets, covering functions and data structures used to authenticate and authorize users and processes using keys and certificates, including root–of- trust, policy enforcement and application programming interfaces (APIs).

9. **M2M and NFC:** Addition of security protections to guard against cyberthreats in the machine-to-machine (M2M) and near-field communication (NFC) zones in the mobile environment, as these areas are increasing targets for financial crimes.

10. **Text Messaging/SMS:** Consideration of security capabilities as enhancements to existing SMS protocols and technologies.

11. **Device Enhancements:** Consideration of developing security features for tablets as well as smartphones, based on trend in increasing malware threats to tablet users. This is in spite of larger threat volumes currently associated with smartphone usage.

12. **Disrupt Malware Spread:** Development of both technical solutions and educational guidance to thwart the commoditization of malware tools.

These are some of the many cybersecurity strategies and activities being undertaken by CTIA member companies based on the research and recommendations of the CSWG. As the mobile ecosystem evolves and new threats emerge, strategies and solutions are changing.

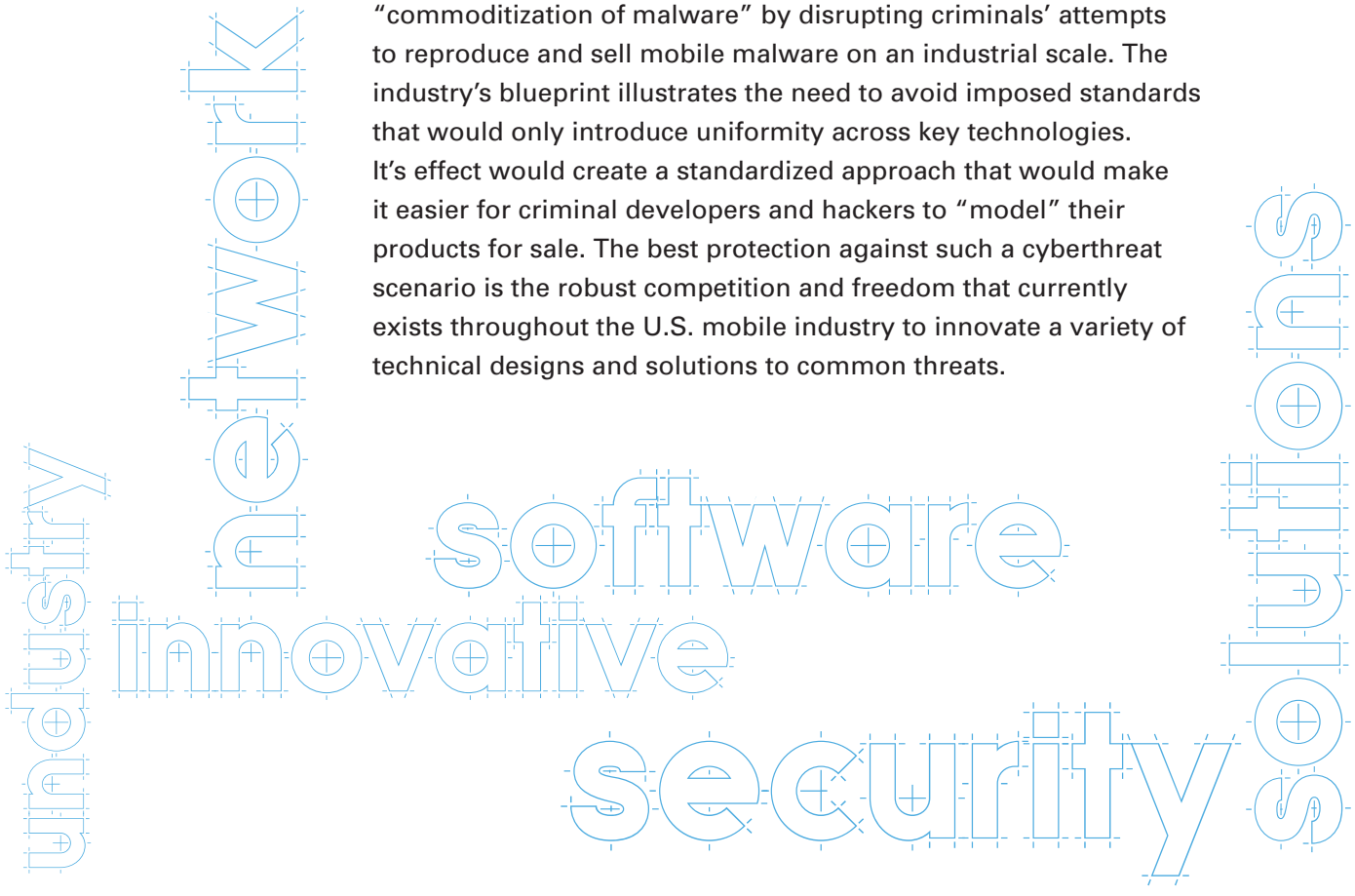
Conclusion:

The magnitude and nature of the challenge of delivering security in the mobile environment requires the active participation of the entire landscape of mobile communications stakeholders. Industry and government. Consumers and enterprises.

This is why the industry is committed to the cybersecurity blueprint to guide the development of solutions for the future, while maintaining the flexibility the industry must have to quickly adapt to changes in the risk environment.

No stakeholder in the fight against cyberthreats has a greater interest than the mobile communications industry to protect its users. In fact, a recent nationwide survey of IT decision makers, conducted on behalf of CTIA, found the majority think the industry is doing a good to excellent job of addressing cybersecurity concerns and providing solutions.[5]

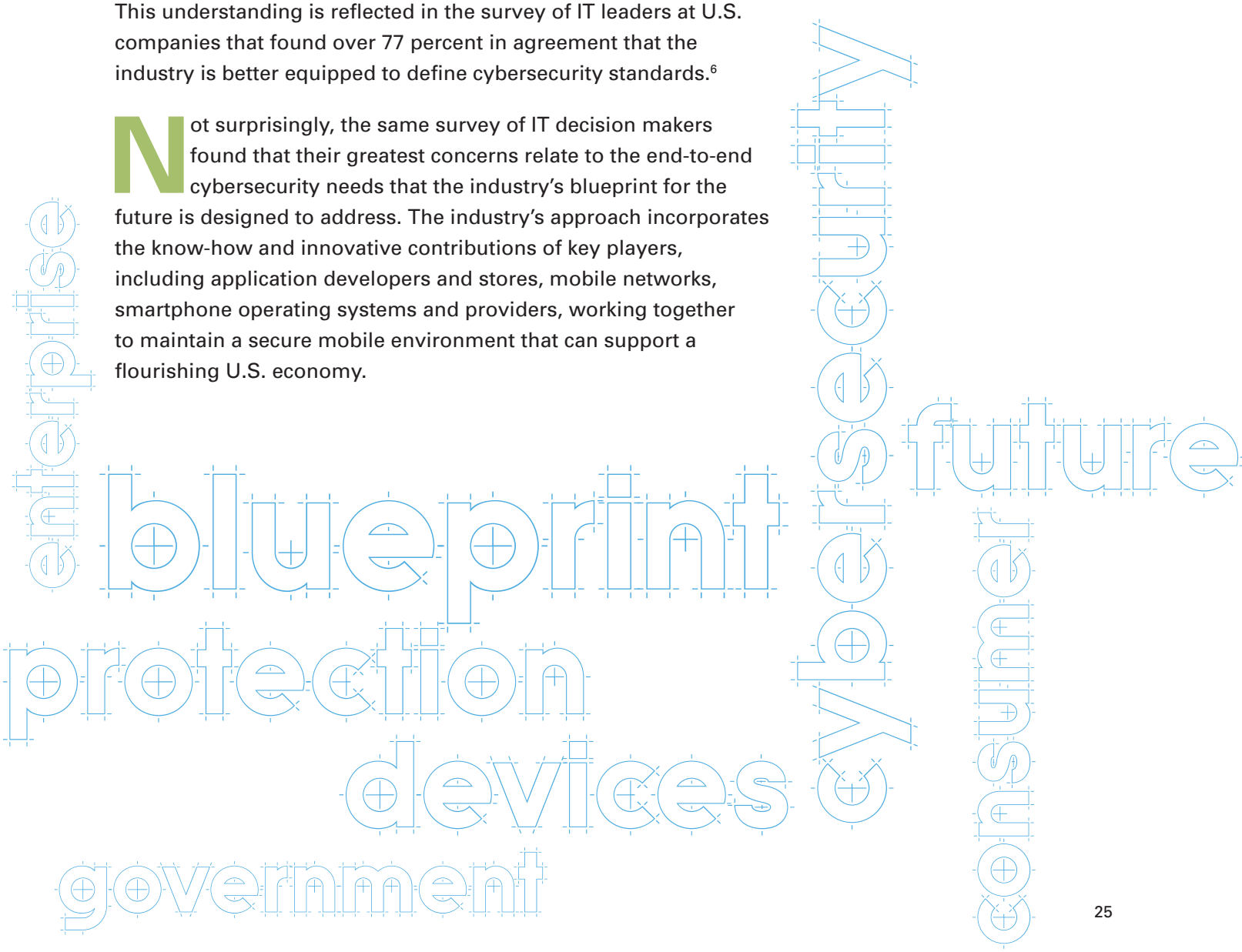
The industry's blueprint focuses on prevention of the "commoditization of malware" by disrupting criminals' attempts to reproduce and sell mobile malware on an industrial scale. The industry's blueprint illustrates the need to avoid imposed standards that would only introduce uniformity across key technologies. It's effect would create a standardized approach that would make it easier for criminal developers and hackers to "model" their products for sale. The best protection against such a cyberthreat scenario is the robust competition and freedom that currently exists throughout the U.S. mobile industry to innovate a variety of technical designs and solutions to common threats.



Wireless communications companies invest millions of dollars to enhance the security of their networks, software, hardware and devices. This means carriers, manufacturers, applications providers, operating systems and platform providers, among others, pursue unified efforts in addition to independent investments to continually advance the industry's blueprint. All players share an economic interest in delivering effective cybersecurity and ensuring the entire interdependent mobile ecosystem delivers sustained, high-value security for all users.

This understanding is reflected in the survey of IT leaders at U.S. companies that found over 77 percent in agreement that the industry is better equipped to define cybersecurity standards.[6]

Not surprisingly, the same survey of IT decision makers found that their greatest concerns relate to the end-to-end cybersecurity needs that the industry's blueprint for the future is designed to address. The industry's approach incorporates the know-how and innovative contributions of key players, including application developers and stores, mobile networks, smartphone operating systems and providers, working together to maintain a secure mobile environment that can support a flourishing U.S. economy.



Endnotes

1. *See e.g.,* **http://www.securityweek.com/stratfor-re-launches-corporate-website-after-cyber-attacks**, **http://www.theworld.org/2012/01/cyber-attack-israel-websites/**, **http://m.cnet.com/news/fbi-warns-users-of-mobile-malware/57532937?ds=1** *and* **http://www.darkreading.com/mobile-security/167901113/security/news/240006056/top-5-deadliest-mobile-malware-threats-of-2012.html.**

2. *See e.g.,* **http://www.abc.net.au/technology/articles/2011/06/08/3238443.htm** *and* **http://www.mobilemarketer.com/cms/news/content/11296.html.**

3. *See e.g.,* **http://www.informationweek.com/security/mobile/rise-of-android-botnets/231601419?nomobile=1** *and* **http://www.symantec.com/connect/blogs/androidbmaster-million-dollar-mobile-botnet.**

4. *See e.g., Universal Mobile Telecommunications System (UMTS) - 3G Security; - Cryptographic Algorithm Requirements (3GPP TS 33.105 version 3.5.0, release 1999), available at* **http://webstore.ansi.org/RecordDetail.aspx?sku=ETSI+TS+133+105-v3.5.0-2000-10;** *WiFi Protected Access II; and Federal Information Processing Standard (FIPS) Publication 140-2.*

5. *See "IT Experts Say Government & Wireless Industry Need to Work Together on Cybersecurity," Oct. 9, 2012, available at* **http://www.ctia.org/media/press/body.cfm/prid/2214** *("89 percent said that the mobile industry is fair, good or excellent in addressing cybersecurity and offering solutions").*

6. *Ibid.*

WWW.CTIA.ORG