Today's Mobile Cybersecurity

Protected, Secured and Unified

CTIA
The Wireless Association®

Today's Mobile Cybersecurity:
Protected, Secured & Unified

EXECUTIVE SUMMARY

Delivering advanced cybersecurity in mobile communications may sound simple, but the reality is a complex, constantly evolving undertaking. The cyberthreat landscape changes literally by the hour and requires constant vigilance and innovation throughout the entire U.S. mobile industry - an industry that provides 3.8 million direct and indirect jobs across the nation. It is a constant risk to be managed, where opposing forces must constantly adapt their strategies and tactics to keep the advantage. Today's mobile cybersecurity protections must be flexible and adaptable in the face of increasingly sophisticated and persistent global threats. Staying ahead of cyberthreats is far too big of a job for a go-it-alone approach, so the company members of CTIA-The Wireless Association® are working together to deliver real-world solutions driven by these market forces.

Self Interests and Shared Interests

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

This paper provides:

- *A brief overview of the cybersecurity landscape of the mobile communications industry,*
- *The extent of its interdependence in responding to an environment of rapidly changing threats,*
- *A summary of the many cybersecurity features and solutions at work today, and*
- *A sampling of the many advanced protections available for device users.*

Cybersecurity Is Everyone's Shared Goal

Everyone has a stake in maintaining effective cybersecurity across the nation's mobile communications system.

Security is only as good as the weakest link. In addition to the efforts of the mobile industry, cybersecurity depends on the awareness and daily security practices of consumers and end users across business and government enterprises. Policymakers also play a vital role in working collaboratively with the industry to encourage and maintain a flexible framework that balances the needs of stakeholders while preserving the industry's ability to stay ahead of cybercriminals and hackers. Everyone has a stake in maintaining effective cybersecurity across the nation's mobile communications system.

There is great value in policymakers, government entities and the wireless industry working collaboratively on maintaining the strongest and most resilient cybersecurity posture possible. The wireless industry looks to policymakers for a flexible and collaborative framework, where industry provides policymakers a "view from the trenches" from the individuals and entities that are fighting the battle every day. The ability to share information about cyberthreats and effective countermeasures among industry players and between industry and government is crucial, as is promoting such information sharing with effective industry liability protections. The mobile industry is in the best position to respond to the changing threats as demonstrated by the set of mobile cybersecurity solutions available today and outlined in this paper. Continued flexibility, dynamic and responsive countermeasures from the industry are essential going forward to stay one step ahead of the cybercriminals, hackers and hacktivists that target mobile communications.

A Complex Ecosystem: *Understanding the Moving Parts*

When author Arthur C. Clarke wrote "Any sufficiently advanced technology is indistinguishable from magic," he could have been talking about the amazing advances that cellular, and now mobile, communications have made possible.

Although mobile communications have changed our world in so many ways, most of us take it for granted. The complex web of technology that makes this mobile world possible might as well be magic. Mobile communications and computing for most of us means a cellphone, smartphone or tablet, and it just "works." It is a convenient tool for personal and business communications that is as indispensible as it is ubiquitous.

"Any sufficiently advanced technology is indistinguishable from magic."

— Arthur C. Clarke

However, there is one critical element of this magic where a lack of basic understanding of how mobile networks work is a problem — cybersecurity.

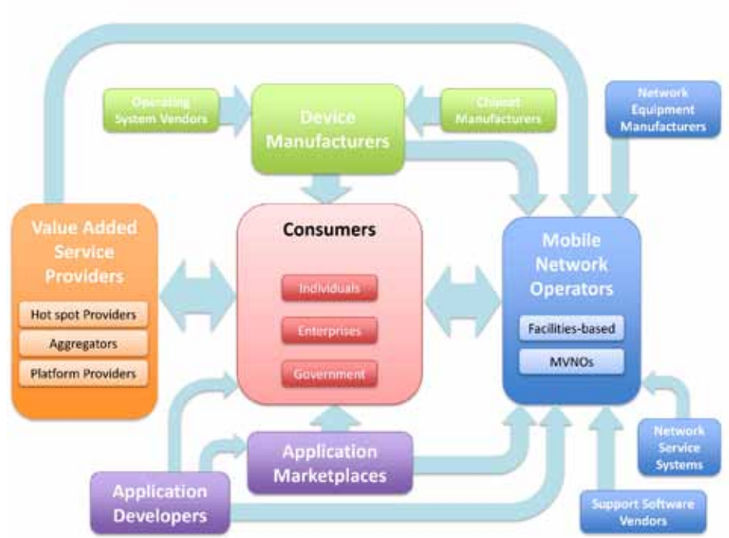
Similar to everyday precautions such as traffic signs or parental controls, it is important for consumers and end users to understand that certain common safeguards are essential to protect important and personal information. Indeed online privacy and cybersecurity go hand-in-hand since one cannot have privacy without security.

Though not well understood by the public, mobile network operators (MNOs) have been focused on cybersecurity since the earliest days of cellular communications. As a result, the key components for protecting cellular networks are well established, and form the backbone of the communications systems we rely on today. The central idea behind protecting networks is to safeguard the elements that transport information and services, including the voice, data and video transmissions that are translated into packets of information.

This cybersecurity backbone that MNOs provide, including network protection as well as security policies and filters, operate in a constantly evolving and dynamic 24/7 environment. Deployment

of next-generation technologies and constant innovation provided by the advent of the mobile Internet has increased the overall complexity for how end-to-end security is delivered. Investments by MNOs have been massive, and the benefits (in the form of well-protected networks and end users) have been recognized by continued market growth and penetration rates exceeding 100 percent in the U.S. With this rapid pace of investment and innovation, the mobile industry has evolved from a simple feature phone providing voice calls, to smartphones and tablets that connect users to a wealth of media and information via the Internet. This significant shift from when the carrier controlled virtually every aspect of the mobile device to today's diverse ecosystem represents a broad and growing collection of industry players investing in security solutions. However, as more entrants and diverse players get involved, there are greater and more complex security risks. The next graphic highlights the complexity of today's ecosystem and the corresponding interdependent security needs.

Today's Wireless Ecosystem



- **Consumers** – *Generally individuals drawn from the public and employees of enterprises or government agencies that use mobile devices.*
- **Mobile Network Operators** – *Both facilities-based and virtual network operators that render mobile services to consumers.*
- **Device Manufacturers** – *Entities that develop and manufacture mobile devices that have the ability to access networks that are provided by mobile network operators.*
- **Applications Marketplaces** – *Generally available virtual marketplace that provides for the download of applications to mobile devices, including Web applications and native applications.*
- **Application Developers** – *Entities that develop applications and make them available through the applications marketplace or through the mobile network operators, often in an over-the-top (OTT) scenario.*
- **Operating System Vendors** – *Entities that offer mobile operating systems on mobile devices.*
- **Chipset Manufacturers** – *Entities that develop and manufacture mobile device integrated circuits.*
- **Network Service Systems** – *Entities that render mobile network related services to mobile operators.*
- **Support Software Vendors** – *Entities that provide mobile network support software such as operational support systems, back-office systems and other related software.*
- **Value Added Service Providers** – *Service aggregators, Wi-Fi hot spot providers and other platform providers that can render services to consumers directly or through the mobile network operator, often in an OTT scenario.*
- **Network Equipment Manufacturers** – *Entities that manufacture network equipment such as mobile base stations, network routers, switching center infrastructure, transmission infrastructure and other network related technology.*

t is simply not possible to "declare victory" on cybersecurity in this environment; risks must be managed because they cannot be eliminated. Cybersecurity affects all of us in direct, quantifiable ways. We may not always appreciate the complexities of how mobile communication is made possible, but we know cybersecurity is important. People are conscious of it — they know what it is — if only because media coverage of cyberattacks.

Information is the currency of the 21st century and the ability of mobile technology to store and transit information demonstrates the essential importance of the mobile communications industry.

Growing interest in mobile cybersecurity is driven by a combination of media coverage and the continuing explosion of mobile devices in the marketplace. There are more mobile devices in the U.S. today than people, and the percentage of smartphone users continues to grow dramatically. Currently, more than one-third of the population carry a smartphone. Analyst firm Frost & Sullivan estimate that by 2017, 80 percent of all mobile phones in use in the U.S. will be smartphones, which means more than 200 million smartphones and tablets.

As we become more reliant on mobile communications, the need for commensurate and ongoing advances in cybersecurity measures becomes clearer. In short, the more essential and valuable something is, the more attractive it becomes to criminals as a vector of attack. As reliance upon technology rises, and consumers and enterprises entrust the mobile communications industry with their information, more investment is necessary to manage the associated security risks. Such investment is exactly what is happening in the mobile communications industry and the information it is entrusted with by consumers and enterprises. Information is the currency of the 21st century and the ability of mobile technology to store and transit information demonstrates the essential importance of the mobile communications industry.

While growing more complex and remaining a relatively open technology ecosystem, mobile communication are becoming an increasingly attractive target for attackers. As a result, there can be no single fix or single point for delivering cybersecurity. It is not possible to say, "If only the carriers could do X, or the equipment makers would do Y or the applications providers would do Z, we would be safe and be 100 percent secure." There is no "silver bullet" solution, regardless of how much money, expertise or effort is dedicated to the cybersecurity challenge. The futility of a single fix is illustrated in the diagram below, depicting just a few of the major changes in the mobile environment within the last five years. Today, cyber risks can only be successfully managed via constantly evolving collaboration, innovation and partnerships between the many players in the mobile ecosystem, including consumers.

Changes in the Environment

Understanding the Players

While familiarity with the mobile ecosystem is important, it is also necessary to understand the players and how they interact within the ecosystem. These players include all of the organizations that bring together the chain of technology assets or "system of systems" that make mobile communications possible.

However, the most important players are by far the end users and consumers. Why? No matter how comprehensive a cybersecurity apparatus is maintained, consumers and other end users must ultimately take responsibility for their actions. Users that operate their devices thoughtlessly, such as downloading applications from unauthorized locations or clicking on links in emails that wary users would recognize as suspicious, put their own data and privacy, as well as data linked to their work or social lives, at risk. In contrast, an informed user, exercising a sensible level of caution, can significantly assist in managing cybersecurity risks.

Five Cornerstones of Mobile Cybersecurity

Mobile communications are a complex ecosystem comprised of a broad list of technologies and players integrated into a "system-of-systems" that enables the wireless environment that consumers enjoy today. Within this ecosystem, security is often addressed in terms of five cornerstone segments as shown below.

Next, we explore each of the five segments, the threat landscape and the proactive steps the mobile industry is taking to address the threats through solutions available today. Following this, we outline the cybersecurity industry solutions available today in the section on Solutions from Industry.

1. Consumers and End Users

Industry is working hard, and with growing success, to educate users on how to reduce their cybersecurity risks. Best practices that the industry recommends for consumers to become security savvy include:

- **Configure Devices to Be More Secure** – *Smartphones and other mobile devices have password features that lock the devices on a scheduled basis. After a predetermined period of time of inactivity (e.g., one minute, two minutes, etc.) the device requires the correct PIN or password to be entered. Encryption, remote-wipe capabilities and - depending on the operating system - anti-virus software may also serve to improve security.*

- **"Caveat Link"** – *Beware of suspicious links. Do not click on links in suspicious emails or text messages as they may lead to malicious websites.*

- **Exercise Caution Downloading Apps** – *Avoid applications from unauthorized application stores. Some application stores vet apps so they do not contain malware. Online research on an app before downloading is often a sound first step.*

- **Check Permissions** – *Check the access (i.e., access to which segments of your mobile device) that an application requires, including Web-based applications, browsers and native applications.*

- **Know Your Network** – *Avoid using unknown Wi-Fi networks and use public Wi-Fi hot spots sparingly. Hackers can create "honeypot" Wi-Fi hot spots intended to attract, and subsequently compromise, mobile devices. Similarly, they troll public Wi-Fi spots looking for unsecured devices. If you have Wi-Fi at home, enable encryption.*

- **Don't Publish Your Mobile Phone Number** – *Posting your mobile phone number on a public website can make it a target for software programs that crawl the Web collecting phone numbers that may later receive spam, if not outright phishing attacks.*

- **Use Your Mobile Device As It Was Setup** – Some people use third-party firmware to override settings on their mobile devices (e.g., enabling them to switch service providers). Such "jailbreaking" or "rooting" can result in malware or malicious code infecting the mobile devices.

These are only a few of the strategies and resources available from the industry, but the bottom line is that users play an important role in protecting their devices, especially what they download and links they click on. Consumers benefit the best from cybersecurity when they are aware of the variety of security options that are a part of their mobile devices. (See more Cybersafety Tips in the Appendix.)

All computers, including mobile devices, need to be secured to prevent intrusion.

2. Devices

Today's mobile devices are miniature computers. In addition to these truly "smart" phones, there is a growing variety of devices such as tablets and netbook computers that include wireless connectivity. These new mobile devices are more advanced than those sold even five years ago. All computers, including mobile devices, need to be secured to prevent intrusion. Applications downloaded from questionable, or even legitimate sites, can record information typed onto the device (e.g., bank account numbers, passwords and PINs), read data stored on the device (including emails, attachments, text messages, credit card numbers and login/password combinations to corporate intranets); and record conversations (not only telephone calls) within earshot of the phone. A malicious application or malware can transmit any of this information to hackers (including those in foreign countries) who then use the information for nefarious and criminal purposes, such as transferring money out of bank accounts and conducting corporate espionage. The Mobile Cybersecurity: Five Cornerstones figure on page 10 highlights some of the protections that are available today for consumers and end users of mobile.

3. Network-Based Security Policies

From a consumer perspective, network operators provide a wealth of tools that can be used to provide improved security and data protection for information that resides on the smartphone or tablet. Such tools include device management capabilities, firewalls and other network-based functionality. These tools give consumers the power to protect their information, but network service providers cannot dictate security policies for consumers to follow. However, service providers provide a wealth of consumer educational materials and practices for enhanced security protection.

Good security begins with good network policies.

From an enterprise workplace perspective, the most important element of security is network-based policy. Good security begins with good network policies. An ill-defined, inconsistent or unenforced set of security policies guarantees poor security. The challenge for businesses is that, due to the increasing bring your own device (BYOD) dynamic — when people use their personal mobile devices for work purposes such as sending and receiving email or managing documents — information technology departments need to be able to take control of corporate applications and all relevant data deployed on these devices. Many chose to do so by employing mobile device management (MDM) systems that serve to enforce company related security policies for mobile devices.

4. Authentication and Control

A lost, unlocked smartphone with pre-programmed access to a bank account or a corporate intranet can cause incalculable damage. Authentication control is the process of determining if a user is authorized to access information stored on the device or over a network connection.

Authentication is the mechanism that requires the user to enter credentials based on such things as a password or PIN, and, in the case of an enterprise, based on the organization's policy settings and active directory database. In some instances, multi-factor authentication is used to protect very sensitive data, comprising

An ill-defined, inconsistent or unenforced set of security policies guarantees poor security.

two or more of the following classic requirements:

- *Something the user knows (PIN, password, secret)*
- *Something the user has (physical token, smartcard, mobile device)*
- *Something the user is (biometric data such as a fingerprint, retina scan or photo recognition)*

As an example, this is especially helpful for anyone who wants to access banking information on a website using an unsecured terminal location, such as at a coffee shop with a Wi-Fi hot spot.

5. Cloud, Networks and Services

Networks deliver many of the applications and services that consumers enjoy today. As illustrated, the complex security solutions the industry provides encompass multiple types of network access connections: the cloud, the Internet backbone, core network and access network connections.

- ***The Cloud*** *allows public and private sector consumers to use applications and information in a remote data center, where large clusters of systems work in parallel to process and store data. Consumers directly access cloud services over the Internet. In traditional computing, most of the data and software needed to carry out specific functions resides on individual machines, which are operated by their respective users.*

  The complex security solutions that the industry provides in the figure shown on page 10 (Five Cornerstones of Mobile Cybersecurity) encompass multiple types of network hosting and transmission points, including data centers. These centers are large-scale warehouse environments that hosts thousands of network servers, which either function independently or are interconnected by parallel hosting and processing software (cloud computing software), to complete complex computing functions. Data centers are a core element of the Internet backbone, as they host the web pages and web-enabled software/applications that consumers utilize when they access the Internet through the multitude of network options available in the marketplace. Data center operators are responsible for the management and security of both physical and virtual assets, as well as the implementation of organizational security and compliance policies.

- **Internet Backbone** — *The Internet backbone is comprised of the principal data routes between large telecommunications networks and core routers. These data routes are operated by a mix of primarily commercial (i.e., private sector) operators, and for certain purposes, government agencies and academic institutions. In the private sector, Internet services providers (ISPs) deliver Internet exchange traffic (i.e., email and Web content) via privately negotiated interconnection agreements.*

- **Core Network** — *The core network forms a "bridge" between the Internet backbone and the next step in the chain, access networks. One of the main functions of core networks is to route phone calls across the public switched telephone network (PSTN). Among the technologies used in core and backbone facilities are data link layer and network layer technologies.*

- **Access Network** — *The access network connects users to their immediate service provider. The access network refers to the series of wires, cables and equipment lying between the point at which a telephone connection reaches the customer and the local telephone exchange. In mobile communications, this definition has expanded to include wireless base stations, which comprise the Radio Access Network (RAN) and Wi-Fi access points, which are often the end users first touch point to a network. With the advent of 4G technologies (i.e., HSPA+, WiMAX, LTE), the edge of a mobile operator's IP network now extends all the way out to the base station itself, blurring the line of responsibility between traditional core and access networks.*

Solutions from Industry:
Expanding Cybersecurity Defenses

Cybersecurity is vital for every player in the wireless communications ecosystem. Since its inception, the industry has invested billions of dollars in the ongoing development of cybersecurity resources. For the constituent parts of the wireless industry — including carriers, equipment makers, operating systems, applications providers and others — delivering advanced cybersecurity and staying ahead of the bad guys is both a defensive and offensive strategy.

Yes, delivering advanced security is a defensive necessity for maintaining operations, but it's also a tremendous offensive asset as a competitive differentiator and overall engine for growth. The wireless communications industry is incredibly diverse, but a common thread across inhabitants of the sector is its elemental focus on security — and not just what comprises security today, but what will be required for tomorrow and beyond.

The list below provides a useful sampling of the comprehensive assets and cybersecurity solutions available today to protect devices and networks.

What Industry Does to Secure Its Services

Security Policies & Risk Management

- *Security policy development and risk management for wireless communications is very nearly an industry unto itself. Today, all the players have efforts to address security policies and risk management that include: defined and documented security policies, ongoing security scans of the threat environment, security assessments and many more risk management efforts to safeguard the products and services the industry provides.*

Security Technology and Standards

- *There is a broad landscape of security standards that increase security levels. Combining general guidelines with specific directives for achieving certain standards is also common across the industry.*

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.*

Monitor and Reporting on Malware and Cyberthreats Profiles

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

Industry Cooperation through CTIA's Cybersecurity Working Group *(CSWG)*

- *An illustration of the kind of security-enhancing cooperation that takes place across the mobile communications industry is CTIA's Cybersecurity Working Group (CSWG), which is comprised of experienced senior representatives from leading companies, including:*

- **Alcatel-Lucent**
- **Asurion**
- **AT&T**
- **Carolina West Wireless**
- **Cavalier Wireless**
- **Cellcom**
- **CellularOne of Northeast Arizona**
- **CETECOM**
- **Cisco**
- **Ericsson**
- **HTC**
- **Microsoft**
- **Motorola Mobility**
- **Nex-Tech Wireless**
- **Nokia**
- **NSN**
- **P3 Communications**
- **Qualcomm**
- **Samsung**
- **Sprint**
- **Sybase**
- **Symantec**
- **Syniverse**
- **TCS**
- **T-Mobile USA**
- **U.S. Cellular**
- **Verizon Wireless**

- *Meeting on quarterly basis, with informal communications happening on a much more frequent basis, CTIA's CSWG is just one example of providers within the mobile communications industry working together for a shared goal: delivering advanced cybersecurity for all users.*

The industry also works to educate consumers about the available solutions as evidenced by the CTIA Cybersafety Tips in the Appendix.

Cybersecurity Solutions for Consumers and Enterprises and Consumer Education

While the industry has done a great deal to secure its services, it has also heavily invested in solutions that offer protection and security for consumers and enterprises. These solutions are generally available throughout the mobile ecosystem and, as described below, offer a more complete picture of what is available today. The industry also works to educate consumers about the available solutions as evidenced by the CTIA Cybersafety Tips in the Appendix. The solutions offer protections that consumers can avail themselves of based on their unique needs and requirements.

1. Lost or Stolen Smartphone Database

(EIR – Equipment Identity Register)

A nationwide database, built and maintained by wireless companies, prevents smartphones reported as lost or stolen from being activated for voice and data services on a carrier's network. The idea is to reduce, if not eliminate, device theft by making it impossible to use a stolen smartphone.

2. Password Mobile Device Lock

All devices have the ability to require a password or passcode in order to access the device. Unfortunately, not everyone uses them or often the feature is turned off by the user. Wireless players have made significant progress in educating consumers and end users to utilize password protection. Additionally, new features like minimum password length and password complexity requirements add an extra measure of security.

3. Remote Lock of Mobile Device

Users can remotely lock their smartphones in the event the devices are lost or are unattended. Also, if users misplace their phones they can activate a remote ring that produces a tone, even if the sound on the device is turned off.

4. Remote Wipe of Mobile Device

There are applications available for end users to erase all data from devices that are presumed lost or stolen. There are even capabilities where a selective wipe can remove all work-related data, while retaining the personal data.

5. Anti-Malware/Anti-Virus Software

Depending on the device's operating system, anti-malware and anti-virus software may be available to prevent, detect and remove malware of all descriptions, including: viruses, malware, adware, backdoors, malicious apps, dialers, fraud tools, hijackers, keyloggers, malicious layered service providers (LSPs), rootkits, spyware, Trojan horses and worms.

6. MDM Policy Management

Given the increasing number of wireless devices used within organizations, mobile device management (MDM) is a crucial discipline for enterprise and government IT departments. MDM software secures, monitors, manages and supports mobile devices. It is fueled by a tight coordination between security policies and operations. The measures that organizations take to implement mobile device security tend to focus on ensuring that devices are configured to match corporate policy. Examples include: requiring devices to be protected by a compliant password before a device can interact with an enterprise server for functions such as email; ensuring the information on the devices can be wiped remotely; and enforcing strict policies on downloading of applications to require or prevent specific applications on the devices.

7. Encryption Data at Rest
(e.g., FIPS140-2)

A variety of encryption mechanisms and standards exist within the mobile industry to support encryption of data that resides locally on a mobile device. Encryption transforms information using an algorithm to make it unreadable to anyone except those possessing the correct login or key information. An example of an encryption standard is the Federal Information Processing Standard 140-2 (FIPS 140-2), which sets out U.S. government requirements that IT products should meet for sensitive, but unclassified (SBU) use. It defines the security requirements that must be satisfied by a cryptographic module used in a security system protecting unclassified information within IT systems. FIPS 140-2 is published by the National Institute of Standards and Technology (NIST).

8. Encryption Data in Transit
(e.g., 3GPP standards)

Encryption is also used to protect data in transit as it moves from the mobile device to the mobile network, for instance, e-commerce data being transferred over smartphones and tablets. The mobile industry relies upon standards that are defined by the 3rd Generation Partnership Project (3GPP), which is a collaboration among groups of telecommunications associations that created and maintain globally applicable third generation (3G) mobile phone system specifications. These specifications are based on evolved Global System for Mobile Communications (GSM) specifications within the scope of the International Mobile Telecommunications-2000 project of the International Telecommunication Union (ITU). These standards are in use today for 3G and 4G technologies. For example, in 4G mobile networks there are three standards which dictate the handling of traffic. There are as many standards for the encrypted transit of data as there are touch points within networks. Responsibility for these standards can range from the application itself to the device, the transport, the core, the cloud, etc. and careful attention is needed on the interweaving of these standards.

9. VPNs

A virtual private network (VPN) is a technology for using the mobile Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible. A VPN provides security so that traffic sent through the VPN connection stays isolated from other devices on the intermediate network. VPNs can connect individual users to a remote network, application or multiple networks. VPNs typically require remote access to be authenticated and make use of encryption techniques to prevent disclosure of private information.

10. Secure Email Solutions

Secure email uses encryption to protect email messages from eavesdropping or mistaken recipients. There are a variety of proprietary solutions as well for secure email access.

11. Parental Controls

Mobile devices help children and parents stay in touch and bring new levels of safety and peace of mind for families, but as appropriate, parents also want to be able to monitor and manage the way their children use mobile device. That's why the mobile communications industry has led the way in developing effective, easy-to-use controls that offer parents the oversight they need, while keeping their children in touch.

12. Secure Applications

Making certain that applications installed on mobile devices are properly vetted and free of malware or viruses is critical. However, because no platform is perfect and many users find themselves seeking applications that are situated on a non-vetted platform new emerging application audit technology services are providing users and enterprises with additional security.

In addition to these solutions, providers across the mobile communications industry provide end users, at both the consumer and enterprise level, with access to 24/7 end user support services.

13. Cloud-Based Services and Secure Solutions

The massive migration to cloud-based services has resulted in an explosion of development and investment in cloud-focused security solutions. The mobile industry has made significant investments in cloud-based security solutions. In addition, secure access services' built-in audit features help users reduce the burden of managing security features and compliance in the case of an enterprise.

14. BYOD Solutions

(Secure Container Software Solutions)

As with cloud, the rapid, ongoing expansion of BYOD models of operation has resulted in a corresponding investment in the development of secure container software solutions, which provide a separate and secure virtual environment on mobile devices.

15. Authentication and Identity Management

For sensitive information, solutions exist for stronger-than-password authentication. Since a user's single password can be stolen or guessed, users can use two-factor authentication. In addition to a password, a digital identifier or time-based random number is required that can prevent hackers who stole a password from accessing the account. Many consumer products provide for two-factor authentication, some through text or an application. There are a number of mobile applications, such as banking applications, that have embedded this two-factor authentication into their consumer systems.

In addition to the solutions described above, providers across the mobile communications industry provide end users, at both the consumer and enterprise level, with access to 24/7 end user support services. When used in conjunction with ongoing consumer education programs, these services help deliver advanced security to address the evolving and complex mobile cyberthreat landscape.

Conclusion:
Implications for Policymakers

Effective cybersecurity – whether for a nation, business, organization or individual – is the result of a partnership between the entity being protected and those in the industry that makes mobile communications possible. All of the participants, from the consumer to the manufacturers, carriers, applications developers, software providers, etc. have a role to play. At every step of the process, there is a shared responsibility for making cybersecurity a priority. The good news is that as a result of the historical, ongoing and concerted efforts of industry, regulators and lawmakers, public knowledge of the need for heightened cybersecurity has grown and continues to grow.

While achieving political consensus is always a challenge, there appears to be a widespread understanding among policymakers that a single legislative "fix" for cybersecurity does not exist; therefore, a flexible approach to legislation in the wireless arena is necessary. The threat landscape is, by definition, a non-static one. Enabling cybersecurity, as a result, cannot be achieved by following a set list of mandated criteria. Even if such a list were to exist, it would be outdated the same day it was established.

Maintaining security in a wireless environment is a constantly evolving dynamic.

Cybersecurity threats and vulnerabilities can change from day to day, and even hour to hour. The effective steps for managing cyber risks today are unlikely to suffice for very long. Maintaining security in a wireless environment is a constantly evolving dynamic. Experience has demonstrated repeatedly that this challenge is best left to those who know the most about it and have the most at stake. In both cases, these are the experts in the wireless communications industry.

However, policymakers play an important role in cybersecurity. Policy efforts that are informed by the realities of the cybersecurity atmosphere — no silver bullet, no single fix, many moving parts and all of them interdependent — are a must. Similarly, policies that seek quick-fixes, one-size-fits-all outcomes or so-called solutions that restrict the flexibility that the wireless industry requires to

respond quickly to new and emerging security challenges can cause unintended harm to the very businesses, consumers and institutions it seeks to assist. Obviously, we encourage policymakers to focus on a real-world approach, and provide guidance and oversight, but tap those closest to the networks to configure our nation's cybersecurity posture in a fashion that is flexible and adaptive to the changing threat environment.

Developing and deploying advanced cybersecurity solutions to manage risk both maintains consumer confidence, and is the best defense to stay ahead of cybercriminals and hackers.

As outlined in the Cybersecurity Solutions from Industry section of this document, the wireless communications industry — although fiercely competitive — has always been united in the core belief that security is absolutely critical. Developing and deploying advanced cybersecurity solutions to manage risk both maintains consumer confidence, and is the best defense to stay ahead of cybercriminals and hackers. It is this simple reality that drives the industry to spend hundreds of millions of dollars every year on cybersecurity measures — a level of investment that will continue to grow over the years.

Without question, there is great value in policymakers, government entities and the wireless industry working together, collaboratively, on the shared goal of maintaining the strongest and most resilient cybersecurity posture possible. Overall, the wireless industry looks to policymakers for a flexible and collaborative framework, where industry can provide policymakers a "view from the trenches." The ability to share cyberthreat information among industry players and between industry and government is crucial. As is the critical need to promote such information sharing with effective liability protections for the industry. The mobile industry is in the best position to respond to the ever changing threat landscape as demonstrated by the existing set of mobile cybersecurity solutions available today. Continued flexibility, dynamic and responsive industry countermeasures are essential going forward to stay one step ahead of the cybercriminals, hackers and hacktivists that would target mobile consumers.

The partnership among policymakers, government agencies and industry is very much in keeping with the nature of communications networks, where every element is connected, interdependent and reliant on one another to effectively address mobile cybersecurity for the nation.

Cybersafety

For more information, please visit:
www.ctia.org/cybersafety

With more wireless devices than people in the U.S., we have the ability to communicate anytime, anywhere.

As our use of the devices increases and expands to new features and functions in other areas such as banking and healthcare, they may hold even more personal data.

By following CTIA–The Wireless Association® and its members' simple CYBERSAFETY tips, consumers can actively protect themselves and their data.

C – **Check** to make sure the websites, downloads, SMS links, etc. are legitimate and trustworthy BEFORE you visit or add to them to your mobile device so you can avoid adware/spyware/viruses/unauthorized charges/etc. Spyware and adware may provide unauthorized access to your information, such as location, websites visited and passwords, to questionable entities. You can validate an application's usage by checking with an application store. To ensure a link is legitimate, search the entity's website and match it to the unknown URL.

Y – **Year-round,** 24/7, always use and protect your wireless device with passwords and PINs to prevent unauthorized access. Passwords/PINs should be hard to guess, changed periodically and never shared. When you aren't using your device, set its inactivity timer to a reasonably short period (i.e., 1–3 minutes).

B – **Back-up** important files from your wireless device to your personal computer or to a cloud service/application periodically in case your wireless device is compromised, lost or stolen.

E – **Examine** your monthly wireless bill to ensure there is no suspicious and unauthorized activity. Many wireless providers allow customers to check their usage 24/7 by using shortcuts on their device, calling a toll-free number or visiting their website. Contact your wireless provider for details.

R – **Read** user agreements BEFORE installing software or applications to your mobile device. Some companies may use your personal information, including location, for advertising or other uses. Unfortunately, there are some questionable companies that include spyware/malware/viruses in their software or applications.

S – **Sensitive** and personal information, such as banking or health records, should be encrypted or safeguarded with additional security features, such as Virtual Private Networks (VPN). For example, many applications stores offer encryption software that can be used to encrypt information on wireless devices.

A – **Avoid** rooting, jailbreaking or hacking your mobile device and its software as it may void your device's warranty and increase the risk of cyberthreats to a wireless device.

F – **Features** and apps that can remote lock, locate and/or erase your device should be installed and used to protect your wireless device and your personal information from unauthorized users.

E – **Enlist** your wireless provider and your local police when your wireless device is stolen. If your device is lost, ask your provider to put your account on "hold" in case you find it. In the meantime, your device is protected and you won't be responsible for charges if it turns out the lost device was stolen. The U.S. providers are creating a database designed to prevent smartphones, which their customers report as stolen, from being activated and/or provided service on the networks.

T – **Train** yourself to keep your mobile device's operating system (OS), software or apps updated to the latest version. These updates often fix problems and possible cyber vulnerabilities. You may need to restart your mobile device after the updates are installed so they are applied immediately. Many smartphones and tablets are like mini-computers so it's a good habit to develop.

Y – **You** should never alter your wireless device's unique identification numbers (i.e., International Mobile Equipment Identity (IMEI) and Electronic Serial Number (ESN)). Similar to a serial number, the wireless network authenticates each mobile device based on its unique number.

Glossary

3G & 4G: A general term that refers to new wireless technologies that offer increased data speeds and capabilities using digital wireless networks.

Adware: On its own, adware is harmless software that automatically displays advertisements. Unfortunately, some bad actors may choose to integrate spyware and other privacy-invasive software in adware.

App (Application): Downloadable tools, resources, games, social networks or almost anything that adds a function or feature to a wireless device that are available for free or a fee. Some applications may also offer users the ability to purchase content or enhanced features within the application.

Cache (or Cookie): Many websites store the initial visit so that when the mobile device user visits again, the data from the same website can appear faster.

Cloud: Cloud computing allows users and enterprise companies to store and process data and deliver applications on the network. In traditional architectures, most of the data and software needed to carry out specific functions resided only on the computer or mobile device. Under cloud architectures, careful consideration is needed to ensure data and applications are protected from abuse.

Cybersecurity: Protection from unauthorized access or malicious use of information in the mobile or telecom ecosystem, which may include networks, devices, software, applications or content.

Cybersafety *(for consumers)*: Proactively installing, using or visiting available applications, software or trustworthy content to protect or prevent unauthorized use of personal information that is stored or accessed on a mobile device.

Cybersafety *(for wireless industry)*: Throughout the wireless industry ecosystem (networks, devices, software, apps or content creators and other platform providers), the ability to share information and tips on how to protect the industry's networks, infrastructure and customers from unauthorized access; prevent tampering with mobile devices, software, apps or content; or malicious attempts to steal or use unauthorized information. When appropriate, this may include sharing information with the government, academia and industry experts.

Cyberthreats: Potential vulnerabilities that bad actors can exploit to compromise data, extract information or interrupt services.

Encryption: Digitally scrambling information so it can be transmitted over an unsecure network. At the other end, the recipient typically uses a digital "key" to unscramble the information so it is restored to its original form.

ESN (Electronic Serial Number): A unique number placed on and within a mobile device by its manufacturer. It is used within a wireless network to identify and confirm the device. The ESN standards were defined by TR45 for AMPS, TDMA and CDMA mobile devices.

Executable scripts: Instructions that a program or operating system reads and acts upon.

Firmware: A collection of non-volatile memory and software program code that resides in consumer electronic devices such as smartphones, tablets, television remote controls, and in personal computers and embedded systems such as those in smart meters, navigation systems and vehicles. Among other activities, firmware ensures that if the device is reset, remote wiped or loses power, it doesn't lose its memory nor does it have to be restored.

Hacking: Illicitly exploiting a weakness in a networked information system to access or alter data or interfere with network or device functions. A hacker may be motivated by a number of factors, such as the challenge or profit.

IMEI (International Mobile Equipment Identifier): A unique number placed on and within a mobile device by its manufacturer. It is used within a wireless network to identify and confirm the device. The IMEI standards are defined by 3GPP in Technical Standard 21.905.

Jailbreaking: Involves removing software controls imposed by the operating system by manipulating the hardware and/or software coded onto the device.

Malware: Malicious Software is computer language codes created by hackers to access or alter data or interfere with network functions. It may manifest itself as worms, Trojan horses, spyware, adware, apps, data files or Web pages with executable script.

Glossary

MIN (Mobile Identification Number): The MIN, more commonly known as a wireless phone number, uniquely identifies a wireless device on a wireless network. The MIN is dialed from other wireless or wireline networks to direct a signal to a specific wireless device. The number differs from the electronic serial number, which is the unit number assigned by a phone manufacturer. MINs and ESNs may be electronically checked to help prevent fraud.

Mobile Network Operator (MNO): Service provider licensed by the FCC to deploy and operate commercial mobile networks that support a host of services from voice communications to high speed wireless data to video multimedia applications.

Mobile Virtual Network Operator (MVNO): A company that buys network capacity from a network operator in order to offer its own branded mobile subscriptions and value-added services to customers.

Operating System (OS): As of July 2012, there are more than 10 wireless operating system platforms. They include: Android (Open Handset Alliance); BlackBerry OS (Research in Motion); BREW (Qualcomm); Java (Sun Microsystems); LiMo (Open Source Linux for Mobile); iOS (Apple); WebOS (HP); Windows Mobile (Microsoft); Windows Phone (Microsoft); and bada (Samsung).

Parental Control Features and Tools: Services offered by wireless providers or third parties that allow parents to manage or monitor how their kids use wireless products and/or services. These tools include content filters and password protections that may be built-in or downloaded as an application to a wireless device. CTIA has listed many of the parental control features and tools that wireless carriers offer here http://bit.ly/Jzph90

PIN (Personal Identification Number): An additional security feature for wireless phones, much like a password. Programming a PIN into the wireless phone can be accomplished either through the Subscriber Information Module (SIM) or other permanent memory storage on the wireless device that requires the user to enter that access code each time the phone is turned on and/or used.

Privacy Settings: Ability to determine how personally identifiable information (PII) is used by wireless applications, devices and services. Consumers should always review the privacy policy of a wireless application, device and service so they know when and how their PII will be made available to third parties such as their friends, commercial partners or the general public.

Provider: Also known as a carrier, service provider or network operator, a provider is the communications company that provides service to end user customers or other carriers. Wireless carriers provide their customers with service (including air time) for their wireless phones.

Public Switched Telephone Network (PSTN): The traditional public telephone network, composed of multiple telephone networks, which themselves are made up of telephone lines, switches, cables and a variety of transmission media (fiber, microwave and satellite facilities). This originally analog, but now almost wholly digital network, was predicated on switching calls rather than establishing dedicated circuits between calling and called parties. Ultimately it is the collection of electronic switching infrastructure and transmission and network termination equipment that comprise the traditional voice communications network as distinguished from the Internet that was predicated on the transmission of data packets.

Radio Access Network (RAN): The portion of mobile networks that provides for controlled access to radio and spectrum resources by mobile devices. The RAN is usually comprised of radio-base-stations, routers and other interconnecting infrastructure that supports seamless interoperation of mobile devices as they traverse the system from location to location and region to region.

Rooting: Rooting allows a device owner to obtain full privileged control within the operating system to overcome any software parameters or other limits on the device. With this access, a hacker may alter or overwrite system protections and permissions and run special administrative applications that a regular device would not normally do. Once rooted, the device is jailbroken.

SIM (Subscriber Identity Module) Card: A small card that fits inside some wireless devices and communicates with a wireless network using a unique code. A SIM card may be removed and transferred to another wireless device.

Glossary

Spam: Unsolicited and unwanted emails or text messages sent to wireless devices. While carriers are constantly filtering their networks to stop spam text messages, spammers are evolving and changing their methods to try to get through. If you receive a spam email on your mobile device, file a complaint with the FCC (http://www.fcc.gov/cgb/consumerfacts/canspam.html). The FCC's CAN-SPAM ban only applies to "messages sent to cell phones and pagers, if the message uses an Internet address that includes an Internet domain name (usually the part of the address after the individual or electronic mailbox name and the "@" symbol)". The FCC's ban does not cover "short messages," typically sent from one mobile phone to another, that do not use an Internet address.

Smartphone: Wireless phones with advanced data features and often keyboards. What makes the phone "smart" is its ability to better manage data and Internet access.

Spyware: A type of malware that functions without a user's knowledge or permission. Spyware frequently captures user activity and data, either storing it in obscure file locations or sending it to another location on the Internet.

Text Message (Short Message Service (SMS); Texting): Subscribers may send and receive a text, usually 160 characters or less, on their wireless devices.

Virtual Private Networks (VPN): A VPN allows a user to conduct secure transactions over a public or unsecure network. By encrypting messages sent between devices, the integrity and confidentially of the transmitted data is kept private.

Viruses: A computer virus is unwanted code that is capable of replicating and transmitting itself from one source (e.g., smartphone, tablet, computer) to another.

Wi-Fi® (Wireless Fidelity): Wi-Fi provides Wi-Fi-enabled devices (e.g. laptops, tablets, smartphones) with wireless Internet access to the immediate local area and is used in homes, businesses and other similar settings. Wi-Fi does not use 3G/4G wireless networks.

WWW.CTIA.ORG