Today's Mobile Cybersecurity

Industry Megatrends & Consumers

CTIA
The Wireless Association®

Executive Summary:

CTIA–The Wireless Association® and members of its Cybersecurity Working Group (CSWG) have prepared a series of papers that provide important background about today's mobile cybersecurity, on what the industry is doing to protect consumers and enterprise end users and how it will create solutions in the face of a changing cyberthreat environment. In this third installment, megatrends in information technology are reviewed in light of how they impact mobile cybersecurity. The megatrends are:

- **Mobile —** the wireless economy is expanding and with it threats from cybercriminals; industry is investing in innovative solutions to protect networks and systems, devices and software.
- **Consumers & apps together everywhere —** with consumers in control, the stakes are higher than ever for education that encourages consumers and end users to adopt security-minded behaviors; industry is responding with more ways to provide information on how to protect data and devices.
- **Virtualization —** the opportunity to create greater network and processing efficiency to address the ever-increasing demand for new and more advanced services and applications, and flexibility brings opportunities for more security solutions but also poses new security threats that require cooperative efforts to develop stronger defenses and raise awareness about protections.

The megatrends are important because cybersecurity is a team sport and collaboration across all aspects must be taken into account to protect against malware and its associated cyberthreat. Currently, the U.S. benefits from very modest levels of mobile malware infection rates compared to other regions. Based on industry reports, mobile malware infection rates are less than 2 percent in the U.S. compared to more than 40 percent in countries such as China and Russia. But this could change fast. Today's wireless ecosystem is —

- Complex, dynamic and rapidly growing — like the cyberthreats that are constantly evolving and becoming more sophisticated.
- Diverse and comprised of innovative and competitive industry players that invest millions of dollars in cybersecurity solutions, and whose vital self-interests lead them to work collaboratively to monitor trends and guide future protections.

A threefold framework is needed to support the industry's successful cybersecurity efforts:

1. Ongoing, significant public-private efforts to educate consumers and enterprise end-users;
2. Willingness to preserve flexibility so industry can respond quickly and effectively by avoiding top-down regulation that stymies innovation and stifles the best responses; and
3. Encourage collaborative framework policies between industry and government by supporting information sharing and providing effective liability protections.

Introduction

Mobile connectivity has become essential for daily living. Mobile applications, or "apps," connect us to everything in our lives. App powered accessories now link to our mini computers and reach out wirelessly to make our lives easier at our convenience.

Start your car with your smartphone? Of course. Turn up the thermostat at home while on your way back from a long business trip? Absolutely. Send your doctor your heart rate while tracking your jogging mileage at the same time? No problem. As the New York Times recently declared, the smartphone is now "the remote control for your life."

The key is that all these innovative uses depend on wireless communication. Mobility is the foundational megatrend in information technology (IT), but it is supported by other shifts that are tracked and analyzed by the wireless industry.

This paper looks at additional trends that support the rapidly growing mobility movement: the proliferation of apps, the rapid adoption of virtualization to support increased network and computer processing efficiency and the move toward self-service virtual computing resources that mirror the trend to consumerization, as users increasingly adapt wireless technology to meet their needs. These developments are then placed into the context of emerging cyberthreats and the industry recommended security practices and blueprint for future solutions.

Today's exponential growth in wireless devices and applications offers a target-rich environment for cybercriminals looking for ways to exploit these trends. In fact, cyberthreats mirror the wireless ecosystem itself—both are growing, constantly evolving and becoming more sophisticated. This means the industry has a vital self-interest in improving cybersecurity, and invests significantly in solutions based on around-the-clock monitoring and analysis of emerging risks.

Based on industry reports, the U.S. benefits from very modest levels of mobile malware infections—with more than 140 million smartphones deployed, infection rates are less than 2 percent (somewhere in the range of 0.002 percent to 1.8 percent). By comparison, rates in Russia and China are greater than 40 percent, and application stores in Russia are reported to have greater than 95 percent malware infection rates across the OS platforms. While the metrics for the U.S. are encouraging thanks to the investments the mobile industry made to provide cybersecurity solutions, the industry continues to work vigilantly to strengthen protection for its consumers and end users.

Cybersecurity begins by establishing trust.

Cybersecurity begins by establishing trust. In the mobile environment, security is built in a trusted chain until it reaches the root of trust, which is the foundation that security is based on. The analogy is similar to a door that you trust because it is locked. You trust the lock because you have the key, and the key is in your pocket. If the key is lost, the chain of trust is broken. You no longer trust the door.

Security and privacy are the two domains of protection in the digital environment. Privacy is the "what" to protect, such as consumer health and financial information and proprietary business data, while cybersecurity is the "how" to protect, for instance, encryption, VPNs, certification, and policy management.

While more Americans are aware of the need to protect their privacy and secure their mobile communications, research suggests they still are not taking the necessary steps. For example, a Harris Interactive survey conducted for CTIA–The Wireless Association finds that only about half of Americans use passwords or PINs on their smartphones.

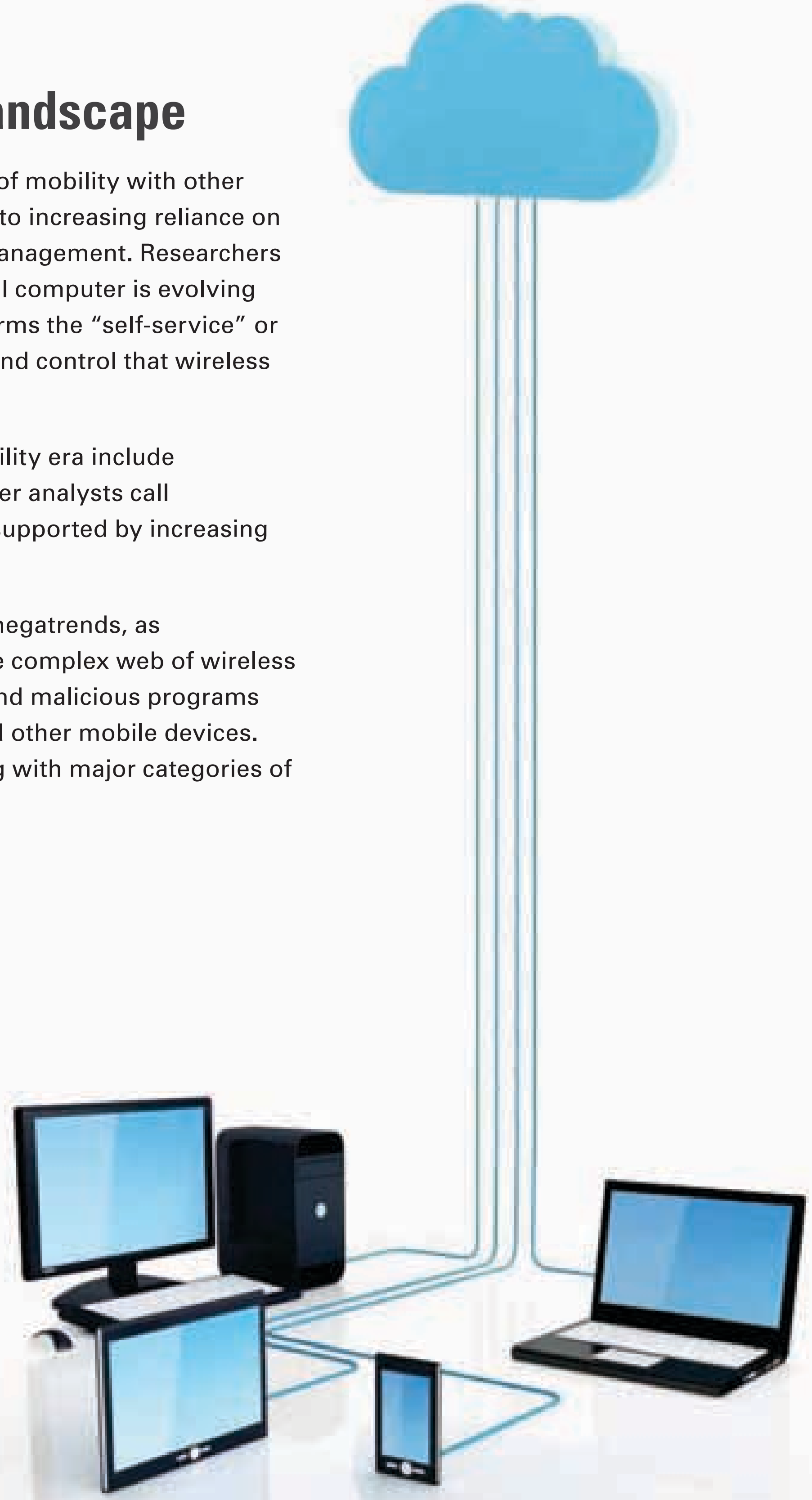
This means educating consumers and enterprise end users on the vital role they play to maintain the chain of trust needs to be a constant, collaborative effort, along with maintaining cybersecurity in today's dynamic and growing mobile environment. Achieving cybersecurity is not a once-and-done race, but rather a marathon that requires everyone's participation and commitment—consumers and enterprises working with government and the mobile industry.

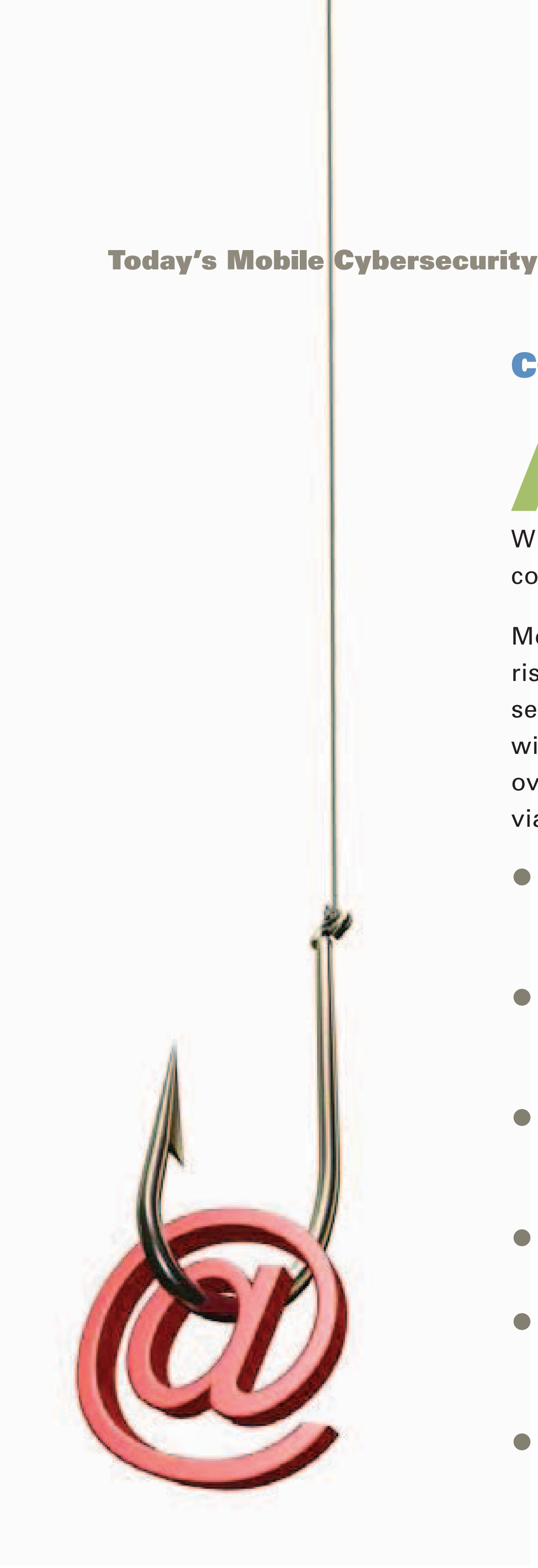
Megatrends and the Mobile Cyberthreat Landscape

IT research highlights the reinforcement of mobility with other information patterns, including the drive to increasing reliance on social media, the cloud and "big data" management. Researchers at Gartner suggest the era of the personal computer is evolving as consumers migrate to using what it terms the "self-service" or personal cloud to support the flexibility and control that wireless devices bring to daily activities.

The driving forces creating this new mobility era include increasing consumer control, what Gartner analysts call **"consumerization"** and **"app-ification,"** supported by increasing use of self-service virtual computing.

Cyberthreats accompany each of these megatrends, as cybercriminals attack any weak link in the complex web of wireless connections using an array of malware and malicious programs that can gain access to smartphones, and other mobile devices. The following highlights each trend along with major categories of security threat.





CONSUMERIZATION.

As consumers have become more dependent on mobile devices, they have become more emboldened and empowered, adapting the technology to suit their needs. Without the proper risk education and the right information, consumers can make it easier for attackers to succeed.

More than ever, consumers need to be informed about the risks and the steps they should take to protect their privacy and security as they conduct more of their lives and work online in a wireless environment. For instance, using third-party firmware to override settings on mobile devices can lead to malware infection via device firmware attacks. Other threats include:

- **Device loss/theft —** A unsecured device, i.e., without a password or PIN, remote wiping software or location software, is an easy target if lost or stolen
- **Baseband chipset attacks —** Attacking the smartphone's basic communications functions through a hacked cell connection or tricking the handset into relying on a faked network
- **Mobile malware —** Downloading a variety of viruses and trojans inside infected apps or opened by clicking on malicious links or text messages
- **Mobile fraud —** Using Short Message Service (SMS) trojans to bill unsuspecting consumers for premium SMS
- **Spam/spim —** Forgetting "caveat link," consumers unwittingly click on links in suspicious emails or text messages that can infect their devices or lead them to a baited website
- M**obile OS attacks —** Made easier when consumers turn off default settings, or "jailbreak" or "root" their devices

APP-IFICATION.

As Gartner analysts put it, the move from PC applications to mobile apps is having a dramatic effect on all aspects of the marketplace. One application now can be used in multiple settings by the user, raising the possibility of greater than ever cross-platform portability, and not surprisingly, more opportunities for malware infection. This trend raises the bar for cybersecurity for consumers and enterprises as more businesses and government agencies permit bring your own device (BYOD) users in their IT environments. While IT managers often use mobile-device-management systems to allow device monitoring, location, remote lock and wipe, access control, etc., threats may still come from:

- **Rogue Wi-Fi access points —** A fake Wi-Fi that mimics a legitimate hot spot, intended only to exploit the ability of mobile devices to connect automatically, and can even occur without the user's knowledge (often called a Wi-Fi "honeypot")
- **Wi-Fi access —** Network security is limited in public Wi-Fi access points, so for all its convenience, using apps in public hot spots can more readily invite man-in-the-middle (MitM) attacks, among others, that can steal information or even hijack the device
- **Marketplace compromises —** Apps infected with malware are on the rise, which means consumers should only download apps from trusted sources, and carefully review the app's uses of data beforehand
- **Third-party compromises —** Apps can be infected at any point prior to being downloaded by the unsuspecting consumer
- **Impersonation —** Malware that sends messages impersonating law enforcement, such as the FBI, and demanding payments to "settle" investigations

> *... the move from PC applications to mobile apps is having a dramatic effect on all aspects of the marketplace.*

VIRTUALIZATION.

This trend supports the mobility movement because, among other efficiency improvements, virtualization enables lower-power devices to access much greater processing power, thus expanding utility and increasing reach beyond the limitations of devices. It also means added challenges for enterprise IT security experts who have to protect the increased options now available to end-user environments. In addition, education and training for end users, as BYOD increases exponentially, becomes even more important to avoid such threats as:

- **Carrier infrastructure attacks —** Compromised infrastructure can be used to mount Distributed Denial of Service Attacks (DDoS) on a large scale against public sector and business enterprises
- **Carrier service attacks —** Compromises to carrier services across wide geographies can result from successful DDoS attacks on carrier network infrastructure
- **Malicious network use —** A compromised virtual network can become a botnet used to attack more systems and networks
- **Wi-Fi compromises** — Infecting unprotected devices at public or "honeypot" Wi-Fi locations with malware that then attacks others using the virtualized network service
- **Third-party compromises —** Attacking the virtual network service through cloud providers and business partners
- **Marketplace compromises —** Attacking the virtual network service through equipment and applications

The availability of virtual storage and computing resources for individual users opens a new set of opportunities for the industry to increase protection while providing the important elements of virtualization that enable every consumer and end user to have access to scalable and nearly infinite resources for whatever they need to do from their devices. To strengthen cybersecurity, the industry uses virtual machine (VM) deployments that allow software applications to execute in isolation from others.

To strengthen cybersecurity, the industry uses virtual machine (VM) deployments that allow software applications to execute in isolation from others.

In other words, each VM may access only its own data and no more. In this way, virtual servers and virtual networks can avoid risks of infection from a single contaminated VM.

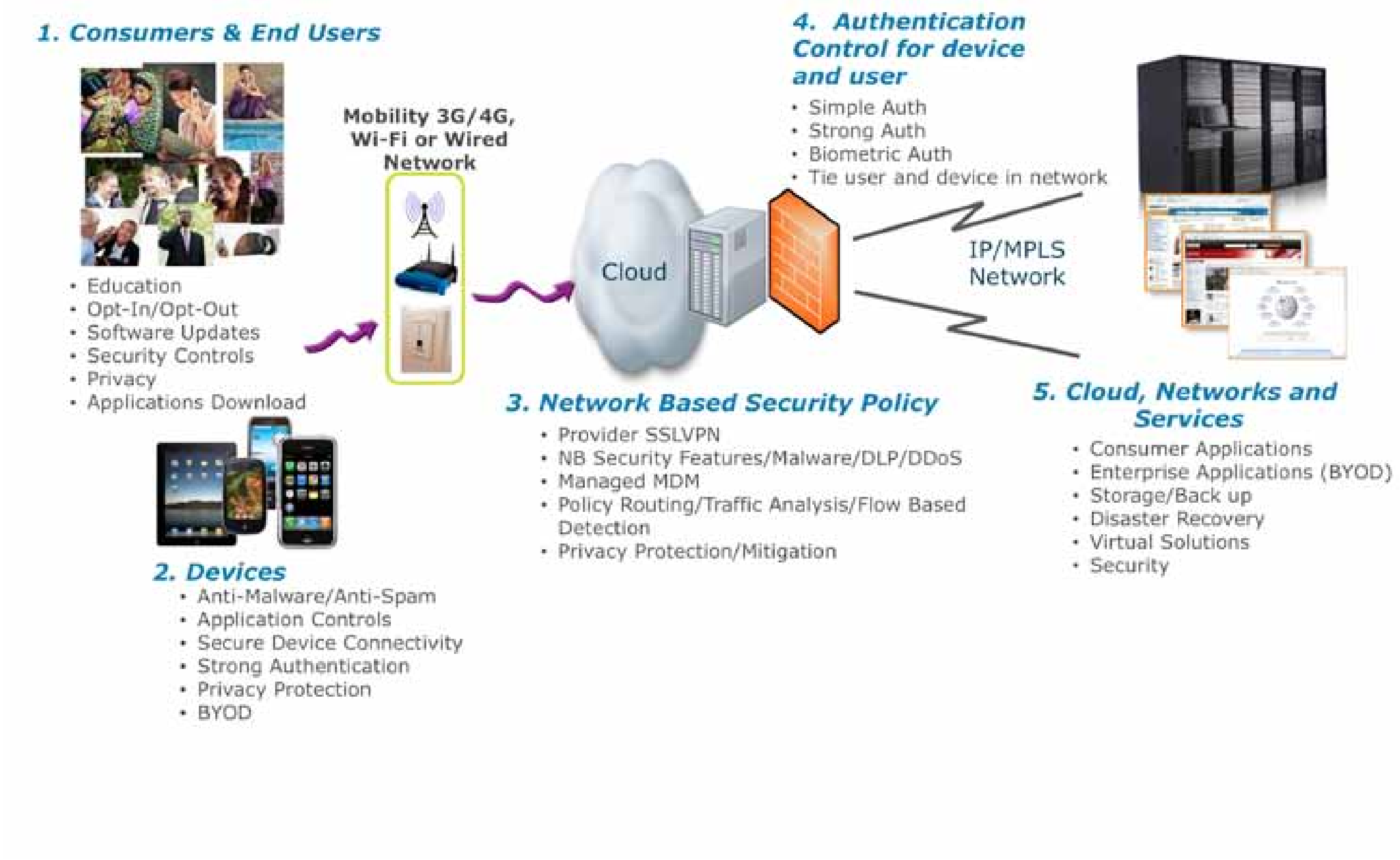
This means virtualization brings both strengths and vulnerabilities to the growing mobile environment. By supporting virtually limitless workspace in which users' data is stored and distributed across a number of computing platforms, risks appear in over-the-top (OTT) applications that store subscriber data. This means data is potentially available to sophisticated cyberhackers using compromised servers and websites and other mechanisms.
For example:

- **Infectious hacking/malware —** Infected data can be transmitted across the Internet, unleashing malware that can spread to other data uses and virtual storage systems, or co-opted by hackivists
- **Impersonation (MitM) —** Compromises that improperly and unwittingly support cybercriminal actions by duping end-users
- **Malicious sites —** Spreading malware from infected websites that is designed to exploit virtual storage and systems

These megatrends in mobile communications technology, and the corresponding threats they attract, are the focus on ongoing and significant investments by the wireless industry.

State of Industry Solutions

Industry participants include a broad range of technologies and players integrated into a complex "system-of-systems" that supports the wireless ecosystem consumers enjoy. Security within this environment is often viewed in terms of five cornerstone segments: consumers and end users; devices; network-based security policies; authentication controls for devices and users; networks and services.



1. **Consumers and end users —** The industry understands that security depends on the user, so it works hard to provide the best guidance to consumers and end users based on industry best practices. This advice begins with how to configure and use mobile devices (PINs, passwords, keeping the device settings and defaults) to how to check permissions and understand the security and privacy settings (or absence of) before using networks or downloading apps and the caveats to being aware as the user emails, texts, connects via Wi-Fi and goes to the cloud or Internet.

2. **Devices —** These miniature computers need to be treated with the same security-minded features as PCs, including passwords, authentication and credential protections and security software to protect against malware.

3. **Network-based security policies —** Solid network policies are at the foundation of good cybersecurity. Network operators provide guidance, support and tools to consumers and enterprise IT managers and their end users to enable them to protect their information. Their efforts are increasingly important as the environment moves to more use of virtualization and self-service cloud computing.

4. **Authentication and controls for devices and users —** Proper identification of users to authorize legitimate access to information stored on a device, or over a network connection from the device to a cloud is vital to maintaining cybersecurity. Primary responsibility for ensuring this level of security rests with consumers and enterprises and their end users.

5. **Networks and services —** Virtual computing resources, including the move to self-service, the Internet backbone, core network and access network connections all play important roles in securing the complex interconnected environment.

Solid network policies are the foundation of good cybersecurity.

In addition to the solution segments described above, providers across the industry provide end users, at both the consumer and enterprise level, with access to 24/7 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.

As we have seen, the mobility movement is attracting many industries to provide their customers easier access to services and products using wireless devices. Mobile banking is growing in popularity, but that also means it's attracting more criminal interest. While banks are using a variety of tools, such as one-time password (OTP) authorization systems, cybercriminals are devising online fraud schemes to circumvent them.

Any device with an IP address may be susceptible to malware attacks

Also, applications for mobile devices now offer the ability to remotely monitor and control functions at home, such as energy settings and usage rates. Malware that contaminates a mobile device may be able to also infect devices that it communicates with, such as smart meters and other functions within the home including an alarm system. Any device with an IP address may be susceptible to malware attacks.

These newer apps join established wireless-enabled uses when traveling on airlines or passenger trains and highway vehicles, and consuming a variety of entertainment media on-the-go.

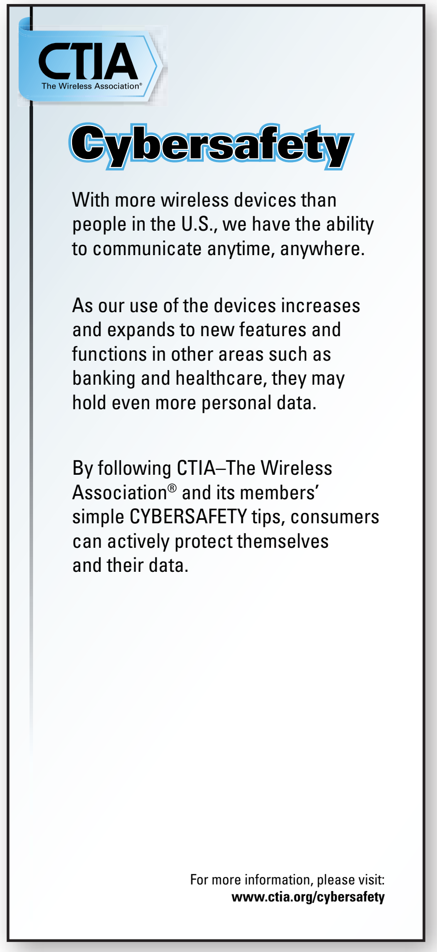
What can happen in typical consumer use situations to compromise cybersecurity, and how industry-recommended steps can avoid these problems, serves to illustrate the robust state of current cybersecurity solutions.

Attack and Response – The Good, the Bad and the Ugly

The illustration outlined below describes a typical malware attack on a smartphone and two possible responses: mitigation countermeasures based on CTIA Cybersafety Tips for Consumers, and possible outcomes if the attack remains undetected or countermeasures are not implemented.

Example Malware Infection of Smartphone:

- SMS message causes a user to click on a malicious Internet link that opens though a browser, or malware contained in an email attachment is opened by a user checking client email.
- As a result, malware infects the smartphone and obtains access to account login and password credentials stored on the device.
- The information associated with the login and password accounts are transmitted to the hacker/cybercriminal.
- Once the information is received, the hacker/cybercriminal has the ability to impersonate the user associated with the accounts based on the stolen login and password credentials.
- The hacker may log on using the account information delivered by the malware and may exploit the account through such actions as:
  - Sending spam to the contact list in the account;
  - Hacking into linked social networking accounts, e.g. Facebook, Twitter, etc.;
  - Searching for other personal information such as financial account information;
  - Downloading personal pictures and videos and posting on public websites;
  - Searching for information to exploit identity theft, e.g. DoB, SSN, etc.


CTIA
The Wireless Association®

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.

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

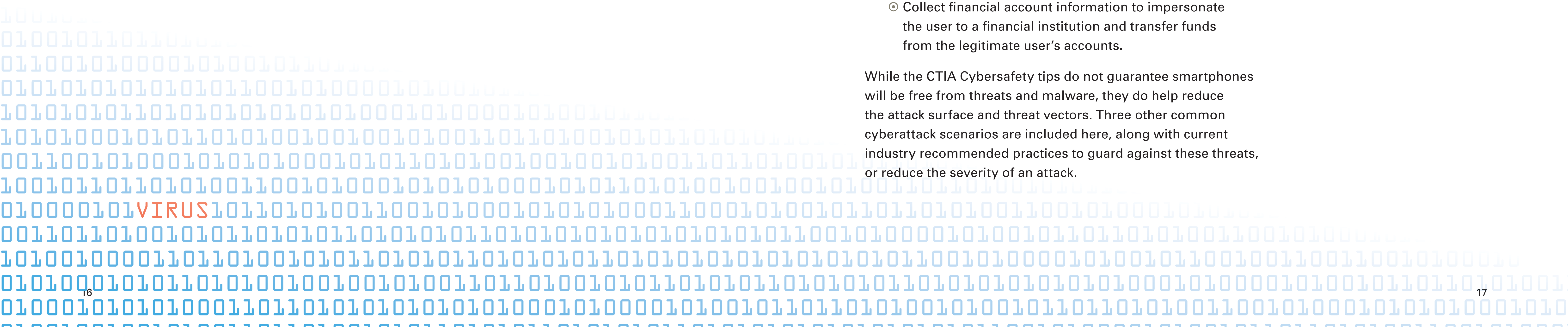
User Follows CTIA Cybersafety Guidance (Model Citizen):

- This user avoids links or emails that are not trustworthy or questionable, only downloads apps from credible sources, and deletes the SMS/text message or email prior to any malware infection taking place.
- Sensitive and personal information are encrypted (in some form) and therefore not readily accessible in the event the smartphone is infected with malware.
- The smartphone has not been rooted or jailbroken, and therefore the malware does not have the ability to directly exploit the smartphone's operating system.
- Backup for the smartphone's personal content is in place so that in the event that the smartphone is infected, the user can readily reset the smartphone to its default factory setting, thereby wiping the malware from the device. Once the reset is completed, the backup information can be used to restore the smartphone to its settings prior to the malware infection.
- If these precautions have been taken, the user can update and change the credentials associated with the account information that has been compromised.
- In addition, the user can review and monitor access to the accounts that have been compromised to confirm that the attack has been remediated.

User Fails to Follow CTIA Cybersafety Guidance:

- The user experiences malware infections on a smartphone through SMS/text links, infected email attachments, infected applications downloads.
- The user's personal and sensitive information is not encrypted, and backup is not in place.
- The user may not be aware that the malware infection has taken place and the infection persists on the device for some time.
- Account information and user credentials are repeatedly stolen by the malware and sent to hackers/cybercriminals.
- Account information and user credentials are exploited to do such things as:
  - Send spam to the user's contacts;
  - Send attachments containing malware to the user's contact list;
  - Search accounts for personal information to commit identity theft;
  - Disclose personal information to public sites;
  - Remotely lock the user's device and commit ransomware (i.e., attempt to demand a fee to unlock the device);
  - Impersonate the user through social networks;
  - Collect financial account information to impersonate the user to a financial institution and transfer funds from the legitimate user's accounts.

While the CTIA Cybersafety tips do not guarantee smartphones will be free from threats and malware, they do help reduce the attack surface and threat vectors. Three other common cyberattack scenarios are included here, along with current industry recommended practices to guard against these threats, or reduce the severity of an attack.



Use-Case Scenario One: *Connecting to the Internet Via a Carrier Network*

Carrying an Unsecured Lifestyle App

Mobile apps are available that offer exciting new possibilities to help countless Americans enrich their lives by locating their friends or even helping them keep track of their running mileage and expended energy. Many of these lifestyle apps rely on a geolocation service to plot the mileage or match locations among friends using the same app. These mobile lifestyle applications also open a new channel to privacy invasions and compromise of personal information by hackers.

These mobile lifestyle applications also open a new channel to privacy invasions and compromise of personal information by hackers.

For example, a consumer decides to download an app to her smartphone to aid in keeping a record of her jogging and exercising. Because she failed to activate the device's security features, the data it records is vulnerable. A cyberattack results in the theft of data, including her personal identity information and geolocation data on her pattern of regular movements when she goes out jogging.

This is one of many cyberthreats in the growing use of personal apps that has the mobile industry increasing its emphasis on cybersecurity.

Recommended protections in this scenario include ensuring the device offers password protection and end-user authentication procedures, as well as detection capabilities in the event the device is compromised, so that the device can be remotely located, locked, and when appropriate, wiped of the individual's personal data. In addition, having the data backed up through a trusted mechanism (e.g., some carriers offer a backup and restore capability) provides the ability to restore the data to the "clean" smartphone once the malware is removed, or a new device is provisioned.

Use-Case Scenario Two: *Connecting to Internet Via a Wi-Fi Location*

Getting Caught in a Wi-Fi "Honeypot"

An enterprise end user is on a business trip, and is staying at a hotel that doesn't offer free Wi-Fi. In what he thinks is a stroke of good fortune, the businessman realizes there is a free Wi-Fi hot spot in the hotel lobby. He uses the connection to access the Internet to send a personal email to a friend, and goes to his bank account to transfer funds to his debit card.

At that moment, a cybercriminal uses a MitM attack to steal the international mobile equipment identity module (IMEI) code and Subscriber Identity Module (SIM) information from his smartphone. This allows the cyberthief to perpetrate identity theft and impersonate the legitimate user—all without the victim's knowledge. With the SIM information, any one-time passwords (OTPs) intended for the victim's phone number are available to the fraudster-controlled device. This can result in compromise to the victim's financial or personally sensitive information.

Industry guidelines urge consumers to use public Wi-Fi networks and hotspots sparingly, and preferably only when the source is credible. In addition, automatic Wi-Fi location functions should be disabled from mobile devices, and activated only at the consumer's control. In the event public hotspots are used, additional security precautions should be considered, such as the use of VPNs, encrypted SSL (secure sockets layer) connections, or other encryption and authentication mechanisms to protect against potential cyberthreats.

Use Case Scenario Three:
Improperly Secured and Lost Device

Failure to Physically Secure a Device

Some end users think of cybersecurity as hacking attacks and detection software. In reality, one of the most common ways for an unsavory character to gain access to a consumer's personal information is simply to come across an improperly secured device.

For example, let's say a consumer is in a taxi: He takes out his smartphone to send an email to the person he's going to meet, and distractedly leaves it behind on the seat when he leaves the taxi. The next passenger picks it up and notices the device doesn't have password protection enabled. This passenger gets into the device and finds that the victim is automatically logged into his virtual network email account and his bank account. Now, he's in trouble.

Industry guidance always begins with encouraging consumers and end users to maintain passwords and login credentials on their mobile devices. In addition, online email and bank accounts should have unique logins that cannot be easily guessed or replicated. Other solutions can include multifactor authentication schemes and encryption software.

The ability to remotely locate, lock and wipe the device to thwart fraudulent access is very important in this scenario so that account passwords aren't compromised. This protection also provides sufficient time for the consumer to access his accounts online and change the relevant credentials, as well as to implement other security measures to detect and prevent any unauthorized access.

Strategy & Approach for the Future

The wireless industry, through cooperative industry efforts like CTIA's CSWG, stays abreast of trends in cyberthreats as well as where mobility megatrends are leading the industry. The working group, comprised of experienced senior representatives from 34 leading companies, conducts research and analyses, and develops and promotes best practices industrywide.

The CSWG also conducts ongoing consultations with a variety of government agencies, including the Department of Homeland Security and the National Institute of Standards and Technology, among others, to discuss cybersecurity threats, trends and solutions in light of industry developments.

Such cooperative government-industry efforts have helped to ensure robust cybersecurity solutions for American consumers and to establish a blueprint that will keep the mobile environment secure for the future. Current research suggests these efforts are succeeding.

Compared to rates in other developed and developing countries, the United States has been less impacted by mobile cybercrime. Most research suggests that less than 2 percent of mobile devices in the U.S. are infected with malware (representing over 1.4 million devices).

But as noted previously, cybersecurity is a marathon requiring ongoing efforts of all industry players, government and consumers and end users.

CTIA
The Wireless Association®

NIST

U.S. DEPARTMENT OF HOMELAND SECURITY

...cybersecurity is a marathon requiring ongoing efforts of all industry players, government and consumers and end users.

A. Educating Consumers and Enterprise Users

Surveys consistently show that once consumers can connect the risks they hear about in the mobile environment to their own lives and experiences, the more willing they are to take advantage of the many layers of protection currently available.

…a majority of consumers (more than 50 percent) are still unsure of what steps to take to protect their mobile devices and secure their information…

Surveys like the Harris Interactive research done for CTIA show a majority of consumers (more than 50 percent) are still unsure of what steps to take to protect their mobile devices and secure their information, which means there is more work to be done on consumer education.

Also, the Harris work reveals that younger consumers, including children, are quicker adopters of apps and mobile innovations generally, and are more likely to engage in the activities that draw cyberthreats. Still, consumer education needs to focus on all demographic groups because threat analyses have exposed security risks associated with backward-compatible older generation mobile phones. Significant numbers of these older devices remain in use and are the most vulnerable to attack.

Specific outreach is needed by enterprise IT leaders to strengthen protocols and procedures used to enhance cybersecurity in BYOD settings.

B. Ongoing Efforts to Counter Emerging Cyberthreats

The chain of trust is essential to cybersecurity. As part of its charter to work across industry to develop standards and best practices for an immutable root of trust, CTIA's CSWG has placed consideration of root of trust enhancements high on its priority list for the cybersecurity blueprint.

Root-of-Trust and Policy Enforcement: Developing the next generation of built-in enhancements to this foundational level of security is important for newer models of smartphones and tablets. Under consideration are enhancements covering functions and data structures that authenticate and authorize users, and processes using combinations of keys and certificates, and which could include policy enforcement and application programming interfaces (APIs).

The industry's blueprint for future solutions also includes a number of significant efforts to stay ahead of the threat curve. Here are additional highlights of new security directions —

Consumer/User Credential Protections: Creating and recommending guidance that encourages the industry and consumers to institute and use encryption and multifactor authentication on mobile devices for greater protection of data, whether it is stored remotely or in secure elements on the devices.

Enhanced Security Features: Encouraging multiple layers of security for mobile devices, including tiered approaches that begin with basic built-in levels of security to premium levels of features for added protection.

Software Update Distributions: Developing recommended procedures for distribution of software updates to consumers and end users on a timely basis, including consumer education on how to verify authenticity. The timely and automatic updating of security features and enhanced capabilities become key to continually staying ahead of threats and hackers.

Multiple Air-Interface Security: Creating and encouraging notifications to consumers on their devices to raise awareness of the risks of encountering access to unencrypted Wi-Fi; unsecured network connections (3G/4G); or when their devices are equipped with less-than-secure backward compatible standards, such as WEP-wired equivalent privacy (versus WPA2-Wi-Fi). In addition to notifications, research continues to develop technology-based approaches to address the variety of security policies that currently exist across multiple air-interfaces.

M2M and NFC: Developing additional protections 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.

The timely and automatic updating of security features and enhanced capabilities become key to continually staying ahead of threats and hackers.

Conclusion

The megatrends touched on in this paper illustrate the dynamism of the mobile environment and the need for a cooperative government-industry, all-in approach to continue advancing cybersecurity.

The mobility wave is bringing with it new enhancements for how we live our lives, as apps for every conceivable convenience are appearing almost every day. While these advances are more visible to consumers, the "back room" changes that support the mobile ecosystem are moving just as rapidly. IT management and storage in a wireless context, as illustrated by the advancing adoption of virtualization and now self-service computing, are changing the way enterprises view software allocations, storage and server capabilities, and as a result, the need for fresh thinking about security.

If there is one constant in mobile cybersecurity, it is the rapidity of change. Efforts to create uniform, standardized approaches would only make it easier for cybercriminals and hackers to replicate malware like an industrial virus.

If there is one constant in mobile cybersecurity, it is the rapidity of change.

The mobile industry focuses on the research necessary to support recommended practices that highly competitive players then are at liberty to mold into innovative security solutions. In this way, the devices, the networks, infrastructure, platforms and other components of the wireless ecosystem stay ahead of cyberthreats using a variety of technical approaches.

A cooperative approach that encourages everyone to stay focused on cybersecurity keeps the innovations coming, and protects intellectual property, while using the recommended framework that will stay ahead of cyberthreats.

Policies that promote open communication and assure legal protections for the industry are essential components to creating and sustaining the level of engagement required as these megatrends play out in the wireless environment.

Endnotes

1. *See e.g., Lookout, State of Mobile Security 2012 report, available at* **https://www.lookout.com/resources/reports/state-of-mobile-security-2012**, *at 9-10 (U.S. and Russia). See also TrustGo™ Q4 Mobile Mayhem Report 2012, available at* **http://www.trustgo.com/en/?option=com_jce&view=popup&tmpl=component&img=/images/en-GB/q4_mobile_mayhem.jpg&title=** *(re Chinese application store infection rates).*

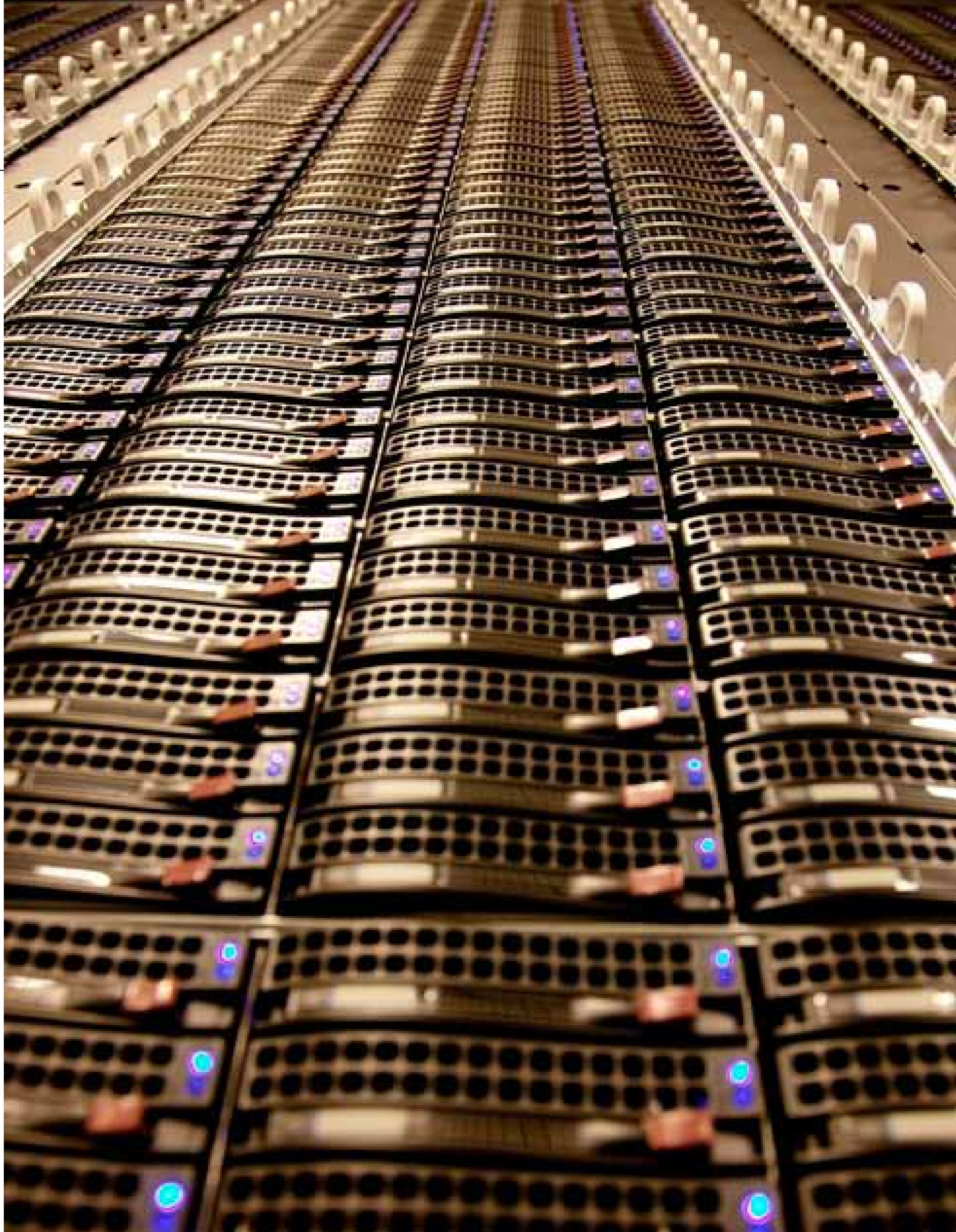
2. *Brian X. Chen, "Smartphones Become Life's Remote Control," New York Times, January 12, 2013, B1, available at* **http://www.nytimes.com/2013/01/12/technology/smartphones-can-now-run-consumers-lives.html.**

3. *See e.g., Lookout State of Mobile Security 2012 report, op cit., at Figure 5; see also Georgia Institute of Technology, GTISC Emerging Cyber Threats Report 2013, available at* **http://www.gtcybersecuritysummit.com/pdf/2013ThreatsReport.pdf**; *and see Dan Needle, Mobile security firm cites 'an onslaught of 14,000 new malicious apps,' TabTimes, Sept. 13, 2012, available at* **http://tabtimes.com/feature/ittech-security-privacy/2012/09/13/mobile-security-firm-cites-onslaught-14000-new-malicious** *(citing TrustGo™ Summer Mobile Mayhem Report 2012: "10 marketplaces in Russia have greater than 95% virus infection rates"); Lookout, Why Malware Writers Dig Russia and China, Oct. 24, 2012, available at* **https://blog.lookout.com/blog/2012/10/24/malware-infection-rates-vary-by-geography/**; *and Kaspersky Security Bulletin 2012: The overall statistics for 2012, Dec. 10, 2012, available at* **http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012**.

4. *Harris Interactive found that 50% of smartphone owners used a password or PIN, compared to 49% of tablet owners.*

5. *See e.g., Brian Taylor, "Gartner: Five Megatrends As Personal Cloud Replaces PC Era," Talkin' Cloud, Mar. 14, 2012, available at* **http://talkincloud.com/gartner-reports-new-pc-is-personal-cloud**.

6. *See e.g., GTISC Emerging Cyber Threats Report 2013, op cit, at p.6.*



CTIA

The Wireless Association®

WWW.CTIA.ORG