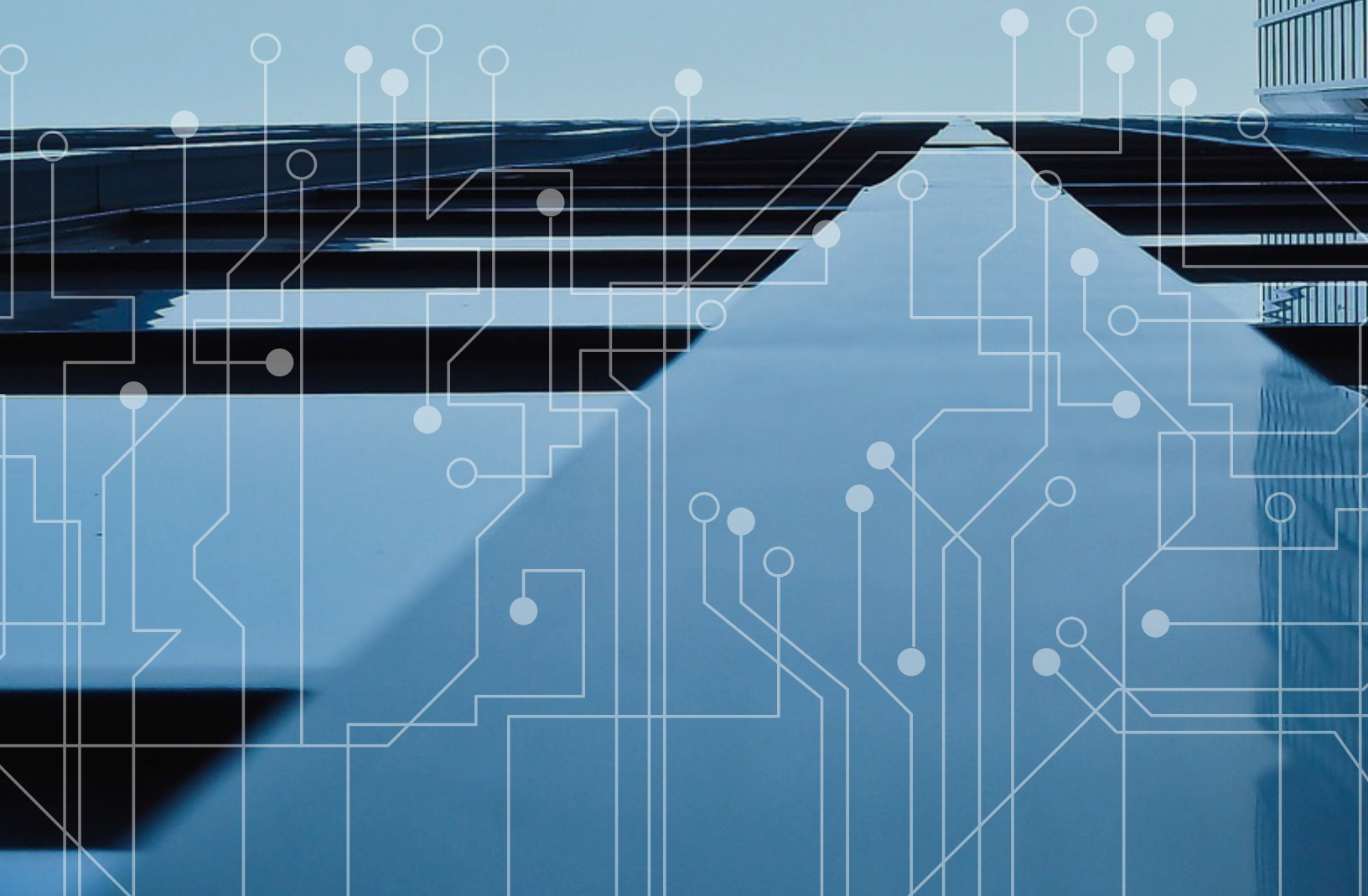
ctia Everything™ Wireless

PROTECTING AMERICA'S WIRELESS NETWORKS

APRIL 2017



EXECUTIVE SUMMARY

The wireless industry is on the front lines every day, protecting our consumers, our networks, and our technology from bad actors and cyber threats. We're proud of our investment to keep America's wireless networks safe, as well as our collaborative partnerships with key government agencies that enable industry and other stakeholders to respond quickly and effectively to threats. As the threat landscape evolves, we must continue to invest and refrain from static regulatory mandates.

Cyber threats and the organizations behind them are highly resourced and sophisticated. That's why America's wireless industry works 24/7 to protect our consumers and our networks, investing significant time and money and using every tool we have at our disposal. With each generation of wireless, our networks become more secure and the technologies and tools we use to protect you become more advanced.

Now, our world is more connected than ever. With 5G and the Internet of Things (IoT) coming, we're baking security into our networks because consumers—and our country's economy—depend on us.

Cybersecurity is a top industry priority and policymakers can help with flexible, technology-neutral approaches that let us innovate quickly to protect American consumers and businesses. This will not be possible unless all stakeholders, including consumers, do their part.

IN TODAY'S CONNECTED WORLD, SECURITY IS CRITICAL TO EVERYONE AND EVERYTHING

Across the United States, nearly 380 million wireless connections join people and increasingly every part of our world together.[1] That's roughly 1.2 wireless connections for every person in the country. Those connections generate tremendous traffic over wireless networks: 9.65 million terabytes of mobile data in 2015 alone—more than doubling the prior year's record levels.[2] Indeed, since 2010, mobile data traffic has grown roughly 25 times.[3]

We're only going to grow more connected. Tomorrow's 5G networks will offer unparalleled speeds, support a massive increase of IoT devices, and enable real-time connections with minimal delays in response, enabling entirely new services and applications.[4]

The Internet of Things—bringing broadband connectivity to consumer and industrial devices, sensors, and objects—will usher in increased productivity and growth across every economic sector, from transportation and health care to public safety and energy. The number of IoT devices worldwide is projected to total around 18 billion in 2022.[5]

As wireless networks evolve, so do cyber threats. The wireless industry is always enhancing network functions and introducing new devices and applications. As networks change, cyber threats grow in number and sophistication, with new risks and exploits to address.

These threats are serious, often launched by highly resourced intelligence services abroad, organized criminal networks, and motivated entities seeking to disrupt communications networks, here and around the world.

TODAY'S THREATS

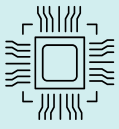
Protecting our networks is a year-round 24/7 effort as cyber threats today come in many forms, from malware and attacks targeting IoT devices to cloud infrastructure exploits and mobile threats.

Malware
Malware includes Trojan packages used to target financial information and ransomware[6] that locks a user out of their system until they pay for re-access.

Mobile Threats
These threats include attacks on mobile applications, phishing attacks to install malicious software, and attacks to trick users to divulge access credentials such as personal passwords or PINs.

Internet of Things
As the IoT expands, new opportunities for possible exploits by hackers and cybercriminals have emerged with the development of sensors, cameras, meters, monitors, and other devices that can be targeted—and exploited—by hackers and other bad actors absent core network protections.

Cloud Infrastructure
For instance, a Distributed-Denial-of-Service (DDOS) attack could use commandeered IoT devices to overwhelm elements in the cloud to restrict or deny the availability of targeted online services.



Network Attacks
Attacks could be launched by leveraging existing network protocols such as SS7 to execute surveillance and interception attacks.

Strong cybersecurity is key to delivering wireless broadband. We invest so that America can remain safe, secure, and a world leader in wireless and 5G.

KEEPING AMERICA'S WIRELESS NETWORKS SAFE AND SECURE

The entire wireless industry works together to protect our networks and our consumers.

Given the seriousness of the cyber threat landscape and how it evolves day-in and day-out, wireless network operators, device manufacturers, and operating systems (OS) and application service providers continue their effective, collaborative, and risk-based management approach that emphasizes security as an integral component. As threats increase, the wireless industry invests more in cybersecurity solutions—investments that total hundreds of millions of dollars every year.[7]

Compared to global peers, the security of America's wireless networks reflects that investment in this top industry priority. While mobile malware doubled in 2016, mobile threats amount to about two percent of all malware threats,[8] and infection rates in North America have remained in the single digits while other regions experience infection rates nearly twice as high.[9]

Wireless Networks
Today, mobile devices use different air interfaces available to connect to wireless networks—air interfaces include 3G, 4G, Wi-Fi, or Bluetooth. But not all air interfaces offer the same cybersecurity defenses. Some networks, like open Wi-Fi hotspots, present security challenges and risks, including the collection and transmission of device information, access to compromised websites, and phishing attacks that provide unauthorized device access.[10]

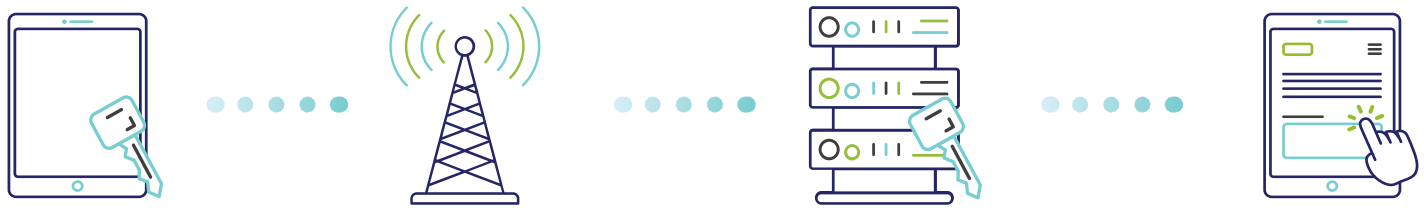
That's why America's wireless carriers equip their networks—3G, 4G, and soon 5G—with a variety of defenses[5] that protect consumers, including:

- Using standards-based encryption algorithms on air-interfaces to prevent unauthorized access to information over the air.
- Deploying authentication standards that operate as a guard, validating and authorizing the user seeking to access the network in order to ensure that only legitimate people are accessing the network. These standards use enhanced cryptographic keys to safeguard network access.
- Ciphering or coding data sent over the network to ensure it is kept free from corruption and/or modification.
- Increasing the availability and reliability of wireless networks by building in multiple redundancies, deploying back-up power solutions, and other network management techniques.
- Deploying a robust set of anti-spamming software on our networks to protect consumers from unsolicited SMS/MMS messages.
- Instituting strict access controls to limit and monitor network resources—physical and IT access—to protect against internal and external bad actors.

Mobile Devices
Today, smartphones and tablets are ubiquitous, making these mobile devices targets for cyberattacks. That's why mobile device manufacturers build in a number of security mechanisms that protect devices from cyber threats, including:

SIM Cards
An integrated circuit for storing and authenticating critical subscriber identity information, a SIM (Subscriber Identification Module) card enables a secure and reliable voice and data connection and the ability to provision new applications and services remotely.[11]

4G LTE NETWORK ARCHITECTURE



Mobile (UE) **Radio Access Network (RAN)** **Core** **Internet**

Temporary Identities
To mitigate the risk of serial numbers being compromised, networks use temporary identities that vary regularly, helping prevent interception by unauthorized users.

Anti-Theft Tools
The mobile industry's voluntary anti-theft commitment provides consumers the tools to locate, lock, and wipe their device in the event of theft or loss.[12]

Roots-of-Trust
Built into mobile devices, this hardware-based cryptographic information is used to detect malware and authenticate system software integrity.

Mobile OS/Apps
Mobile OS providers like Android, Apple, and Microsoft work with app developers to improve security while screening for bad applications at app stores in order to prevent the spread of viruses and malware. That's why mobile OS providers and app developers have created software that protects wireless devices and consumers, including:

Anti-Malware and Anti-Virus Software
This software, which varies by operating system, prevents, detects, and removes malware.

Device Security
If a device is stolen or lost, personal and sensitive information contained in the device can be made inaccessible to an unauthorized user. Tools are provided to consumers for such protection.

The wireless industry uses every tool to defend against cyber threats.

From authentication and encryption to licensed spectrum and solutions like firewalls and security gateways, wireless carriers use an all of the above strategy to protect our networks.

Spectrum
Exclusive, licensed use spectrum provides wireless network providers the ability to ensure interference protection and enable Quality of Service (QoS). Purchased by an operator at an auction or on the secondary market, licensed spectrum enables "carrier grade" quality for wireless voice, messaging, data, and video services.[13]

Licensed spectrum will also be critical to future 5G services including wireless medical consults, virtual reality sessions, and vehicular safety applications that will require QoS and low latency to ensure real-time performance.[14] The industrial IoT will also require a heightened end-to-end solution, particularly for critical infrastructure services and industries, and LTE—riding on licensed spectrum—provides the underlying platform for the necessary end-to-end security.

In addition, wireless industry certification regimes[15] are critical for validating key security functions, like over-the-air software updates and patches, which help secure managed-IoT environments and set the foundation for 5G and next generation wireless services. The wireless industry is evaluating options for certifying that key security capabilities are implemented in devices being attached to networks, to help mitigate risks to devices, networks, and end-user applications.

Standards
Wireless network security standards processes are comprehensive and have proven effective. Driven by industry participation, standards-setting and standards-developing organizations are developing global standards that will provide dynamic, resilient, and safe wireless networks to counter security threats for a connected world.

Key standards-setting organizations include the following:

3GPP is developing security and privacy standards for wireless technologies, architectures and protocols.[16] 3GPP is also developing several cryptographic algorithms, which are a part of the end-to-end security solution and will provide for ongoing enhancements to mobile cybersecurity.

IETF is developing security requirements for network protocols for end-to-end device security and the IoT.[17] These efforts build on several successful security protocols and standards IETF has developed, such as IP Security, Transport Layer Security, and Simple Authentication and Security Layer.

ETSI is responsible for the standardization of cybersecurity standards internationally and for providing a center of relevant expertise for information and communications technologies, including mobile.

In addition, the National Institute of Standards and Technology (NIST) convenes the private sector to develop an industry-driven methodology—the Cybersecurity Framework—to assess and manage cybersecurity risks and outcomes. This framework is intended to help private sector organizations that provide critical infrastructure with guidance on how to protect it, along with relevant protections for privacy and civil liberties.

Network security and monitoring tools are key.

Wireless Radio Access Network
The radio access network (RAN) provides the radio communications between the mobile and the core network. Base stations provide the air-interface radio connection between the mobile device and core network, perform mobility and handover, and ensure good performance and allocation of shared radio resources.

To prevent intruders from accessing air interface communication information, or eavesdropping in other words, wireless network operators equip their RAN with functions that ensure the security of the radio communications functions and interconnection to the core network. Specifically, RAN security features include:

Mutual Authentication Functions
To detect and prevent "spoofing," these functions use an Authentication and Key Agreement protocol between the mobile device and the RAN that allow the device to authenticate the network, and the network to authenticate the device.[18]

IPSec Encryption
Using a protocol called IPSec, the RAN can encrypt communications in the back-haul connections to the core network and also detect and mitigate unauthorized access, helping ensure radio access and prevent denial of service attacks.

Access Controls
These tools enable the detection of unauthorized access to RAN resources and the ability to deny access if appropriate. Wireless carriers use an all of the above strategy to protect our networks.

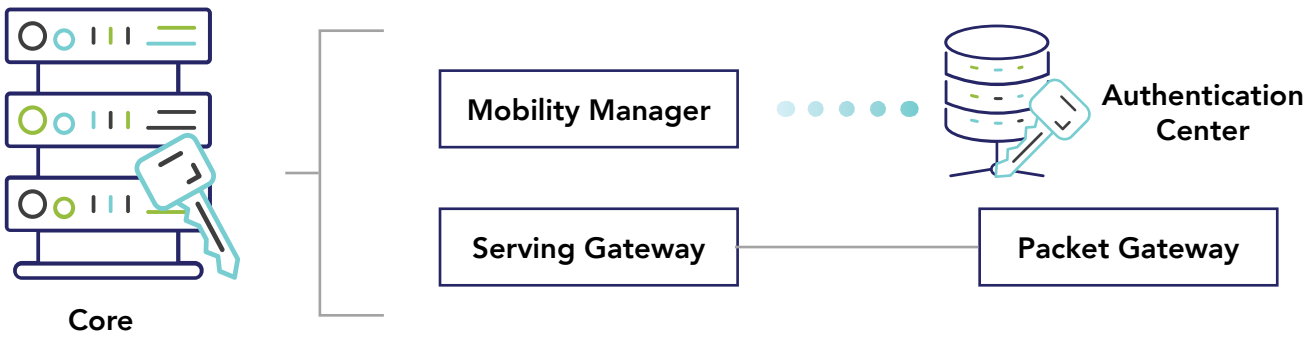
Wireless Core Network
The core network consists of data gateways or routers, mobility management platforms, policy and billing, and the home subscriber database.

The data gateways and major routing platforms carry IP traffic from many connected devices through the core network and out to cloud services or the Internet.

The risk is that many devices can simultaneously attempt to connect, effectively creating a denial of service attack, or attackers could steal a master key that would give access to the entire network.[19] That's why wireless operators deploy a number of tools used to monitor, guard, and protect the core platforms and subscriber database, including:

- Firewalls that block certain types of network traffic, forming a barrier between a trusted and untrusted network—analogous to a physical wall that blocks and isolates the spread of an attack.
- Intrusion prevention systems and intrusion detection and prevention systems that monitor network activities for malicious activity—helping identify malicious activity, record information about the activity, and block or stop it.
- Malware monitoring and detection to target hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

WIRELESS CORE NETWORK SECURITY



- Virtual Private Networks that enable traffic to be sent through a secure connection, isolating that traffic from other devices on intermediate networks. Capable of connecting individual users to a remote network, application or multiple networks, VPNs require authentication for remote and use encryption techniques.

These functions within the core network are highly secure in terms of physical security and access controls, requiring gated facilities, guards, secure card entry, sophisticated login/password controls, and other measures. Not only are security functions a high priority, the core network is managed by trained and specialized personnel who are security and risk management experts.

Cloud-Based Security
Whether running apps, storing data, or delivering services, the cloud—a network of servers—have proven popular and efficient for delivering carrier grade text messaging, social networking, banking, e-commerce, and mobile health. These servers and the mobile applications and services they enable have become a target for new threats, and this matters because the all-IP architecture and openness of the Internet provides broad and diverse entry points to the mobile network for possible attacks.

That's why wireless network providers work to ensure the security of their network vis-à-vis cloud-based services and applications, including:

- Secure interconnection and transport from the core network out to the cloud and Internet.
- Mutual authentication techniques, limiting and monitoring the number of entry points into the mobile network, and using highly secure communication links as appropriate.
- Collaborating with the entire network ecosystem because if a customer goes to a risky website and downloads files with malware, the other parts of ecosystem must help detect and clean the infected files.

Security has become stronger as wireless networks evolved.

As wireless carriers keep innovating, so do our security measures. From the 2G networks of twenty-five years ago to today's 4G networks, the wireless industry has increased digital coding, encrypted the air link, strengthened mutual authentication, and added cryptographic techniques.

With standards work ongoing for decades, each new generation of technology brings security improvements incorporated across a broad set of global standards:

2G/3G
Both 2G and 3G provide for network-based authentication of mobile devices as well as data encryption capabilities. Improvements added in these generations of mobile service included authentication and encryption that deterred eaves-dropping and fraudulent service theft.

4G
4G provides a strong security platform, involving an end-to-end security architecture that leverages the advances of earlier mobile generations from the device through the network and into the cloud. 4G incorporates strong cryptographic and authentication techniques such as mutual authentication between various elements of the architecture to ensure a secure environment.

5G
As we move towards 5G, wireless network providers are working with industry standards bodies to build on existing security features and include new innovations into the network design and development process from the beginning. 5G networks will be designed to build on the security approaches already in widespread use across today's 4G mobile ecosystem and will adapt to the changing threat landscape.

Global mobile industry standards bodies have identified new opportunities to enhance our security protocols. With the wireless industry working cooperatively for advances in encryption and security protocols for threat detection and mitigation, these groups recommend that 5G incorporate:

- Physically independent structural blocks organized to form an end-to-end all-IP-based system, creating distributed network security that supports an open architecture and distributed security control.
- Fragmented or diverse ownership of end-to-end network assets requiring improved mutual authentication across network elements.
- Flexible security based on open architecture where larger networks often need to be connected to smaller networks, and smaller networks offer simpler and more efficient ways to implement security protocols.
- Advanced security and encryption technologies built into mobile devices, as well as advanced authentication schemes, like biometrics.

WIRELESS EVOLUTION

1G

Application
Voice

Consumer Benefits
Nationwide Cellular/Wireless Service

2G

Application
+ Text, Email, Limited Internet

Consumer Benefits
+ Secure Voice, SMS, Longer Battery Life

3G

Application
+ Social Media, Video Streaming

Consumer Benefits
+ Secure Internet, Access to Data, MMS, Video Messaging

4G LTE

Application
+ HD Video, VR, AR, High-Speed Data

Consumer Benefits
+ All IP, Broadband Smart Phones, Low Latency, Backward Compatible

INVESTMENT IN SECURITY— GENERATION BY GENERATION

1G

Threats: Analog, Fraud, Eaves Dropping

2G

Threats: Attacks on Encryption
General Improvements: Digital, Air-link Encryption

3G

Threats: Exploit Clear Transmission of IMSI, Hacking In/Out Going Calls
General Improvements: Mutual Authentication Between Mobile and Base Station

4G LTE

Threats: Includes Internet IP Based Security Threats
General Improvements: Strong Encryption Techniques With Built In Security Mechanisms

GETTING CYBERSECURITY RIGHT TO ENSURE AMERICANS ARE PROTECTED

All of us have key roles to play in protecting our online security and privacy.
Everyone—consumers and businesses, industry and policymakers—has a stake in cybersecurity and a responsibility to help protect against cyber threats. CTIA convenes our industry, helping identify risks and strategies to address cyber threats. Through our Cybersecurity Working Group, the wireless ecosystem works with key government agencies from the National Security Agency to the Department of Homeland Security.

The wireless industry also works together to respond to challenges. For example, responding to mobile device theft in 2013, network operators, device manufacturers, and OS companies made the "Smartphone Anti-Theft Voluntary Commitment"[20] to protect new models of smartphones against unauthorized use if they are lost or stolen.

The industry also educates consumers by providing best practices to protect their data, ranging from how to configure devices to be more secure to how to understand the security on different types of networks.

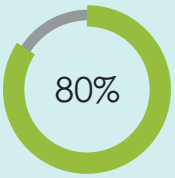
The more consumers understand the risks online and the many layers of protection currently available, the safer they become. By following simple security practices, consumers can help make their wireless experience safe and secure.

Using PINs, passwords and other features can help protect your mobile device and personal information, and apps are available that can locate, lock, and/or erase your wireless device if it gets lost or stolen.

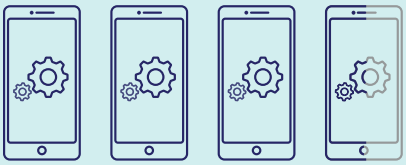
Policies to help protect Americans and the wireless networks we depend on.
Wireless companies must monitor, protect, diagnose, and fight potential cyberattacks in real time, and that's why policymakers should promote flexible, technology-neutral solutions and focus on cyber threat information sharing with appropriate liability protections.

To ensure we can continue to innovate as fast as cyber threats do, we need voluntary, collaborative, industry-led efforts—avoiding mandates that quickly become outdated.

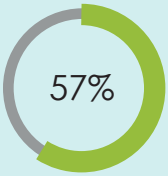
CONSUMER USE OF WIRELESS SECURITY FEATURES CONTINUES TO RISE



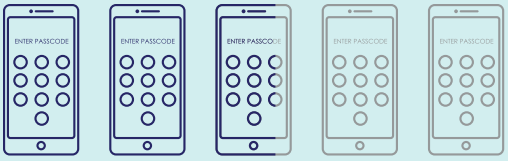
Today, nearly 80% of consumers enable security on their smartphones, an **increase of 54%** from five years ago.



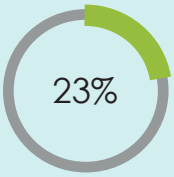
77% of consumers run software updates for their smartphones every time or almost every time.



57% of those who have enabled remote lock/ locate security have done so because they now have a smartphone with that capability.



59% of smartphone owners now say their device has remote lock/ locate capability.



Users with anti-virus or anti-malware software have grown 23% since 2015.

Source: Harris Poll.[21]

While many federal agencies have roles to play, the Department of Homeland Security is critical in convening industry and government stakeholders to work together toward a common framework to address cybersecurity.

The ability to share information about cyber threats and effective countermeasures among industry players and between industry and government is crucial, as is promoting such information sharing with effective industry liability protections. After Congress passed the Cybersecurity Information Sharing Act[22] in 2015, CTIA has focused on moving beyond information sharing trials to automated sharing via new technologies.

Specifically, CTIA's Cyber-threat Information Sharing Pilot is working to facilitate integration with the DHS Automated Information Sharing (AIS) portal. This effort aims to automate the sharing of threat information among carriers to rapidly and effectively mitigate cyber-threats.

We urge policymakers to keep up this collaborative approach with the wireless industry on important and complex 5G security issues in order to encourage actions that can be taken in standards groups and other organizations. As we move toward 5G, the next-generation of wireless, flexibility will be critical to meeting the challenge of protecting our networks and our consumers against the dynamic global threat landscape.

ENDNOTES

1. CTIA's Wireless Industry Summary Report, Year-End 2015 Results (2016), at http://www.ctia.org/industry-data/ctia-annual-wireless-industry-survey.

2. Id

3. See id.

4. 5G networks will be 10 times faster than 4G networks, respond 5 times as quickly, and connect 100 times the number of devices. Thomas K. Sawanobori, CTIA, The Next Generation of Wireless: 5G Leadership in the U.S., at 5 (Feb. 9, 2016), at www.ctia.org/docs/default-source/default-document-library/5g-white-paper.pdf.

5. Ericsson Mobility Report 2016, at 33 (Nov. 2016), at https://www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november-2016.pdf.

6. Ransomware is malware that installs itself on a mobile device without the knowledge of the user and extorts payment once device information is locked, usually encrypted, and held hostage in exchange for a ransom payment.

7. CTIA, Today's Mobile Cybersecurity: Blueprint for the Future, at 6 (Feb. 2013), http://files.ctia.org/pdf/Cybersecurity_White_Paper_2.pdf.

8. See McAfee Labs Threats Report, at 36-37 (Apr. 2017), at https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf.

9. Id. at 38.

10. Other risks include the International Mobile Equipment Identity (IMEI) and International Mobile Subscriber Identity (IMSI) being intercepted and used to track a mobile device.

11. Manufacturers limit access to SIM cards to minimize risks from the challenges of the application ecosystem.

12. Smartphone Anti-Theft Voluntary Commitment, CTIA (2016), at http://www.ctia.org/initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment; Capabilities that the mobile industry deploys to protect networks and consumers from threats and bad-actors.

13. As we move further into use of all IP architectures with voice being provided over a data channel using Voice-over-LTE (VoLTE), Quality of Service (QoS) attributes are used to prioritize the packets so voice quality is maintained at a high level over other traffic like e-mail and web browsing. Licensed spectrum enables operators to provide VoLTE for consumers and businesses. Video conferencing is another example of a service that depends on licensed spectrum to maintain QoS for both the video and audio in real-time services.

14. Thomas K. Sawanobori, CTIA, The Next Generation of Wireless: 5G Leadership in the U.S., at 11-12 (Feb. 9, 2016), at http://www.ctia.org/docs/default-source/default-document-library/5g_white-paper_web2.pdf. See also Mary-Ann Russon, What will 5G be used for? Self-driving cars, connected home appliances and incredibly smart cities, Int'l Bus. Times (Nov. 7, 2015), at http://www.ibtimes.co.uk/what-will-5g-be-used-self-drivingcars-connected-home-appliances-incredibly-smart-cities-1527420.

15. See e.g., Certification, CTIA (2016), at http://www.ctia.org/initiatives/certification.

16. SA3 – Security, 3GPP, http://www.3gpp.org/specifications-groups/sa-plenary/sa3-security#term0_1 (last visited Apr. 10, 2017).

17. See e.g., Best Current Practices for Securing Internet of Things (IoT) Devices, IETF (Oct. 21, 2016), at https://datatracker.ietf.org/doc/draft-moore-iot-security-bcp.

18. Such authentication functions include SNOW 3G (designed by Lund University, Sweden), and the Clock cipher standard (NIST, USA), or Stream cipher.

19. This is a more serious but significantly less likely scenario: Attackers may be able to steal K (128-bit master key) from the Carriers' Home Subscriber Server (HSS) or obtain it from UICC manufacturer. Safeguarding security keys is one of the most guarded measures established by SIM card providers and operators. It is incumbent to ensure secure loading of electronic keys onto the SIM cards at the manufacturing site and highly secure loading into the network home subscriber database.

20. Smartphone Anti-Theft Voluntary Commitment, CTIA (2016), at http://www.ctia.org/initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment.

21. These studies were conducted by Harris Poll on behalf of CTIA in 2012 among 505 smartphone owners and in 2017 among 936 smartphone owners, who are adults, 18+ in the U.S. Full weighting and methodology available upon request.

22. Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, Division N §§ 101-11, 129 Stat. 2242 (2015).

ACKNOWLEDGMENTS

Key contributors to this report were Tom Sawanobori, John Marinho, Eshwar Pittampalli, Kevin Ryan, Brittany Serrano, and Leah Morrison.