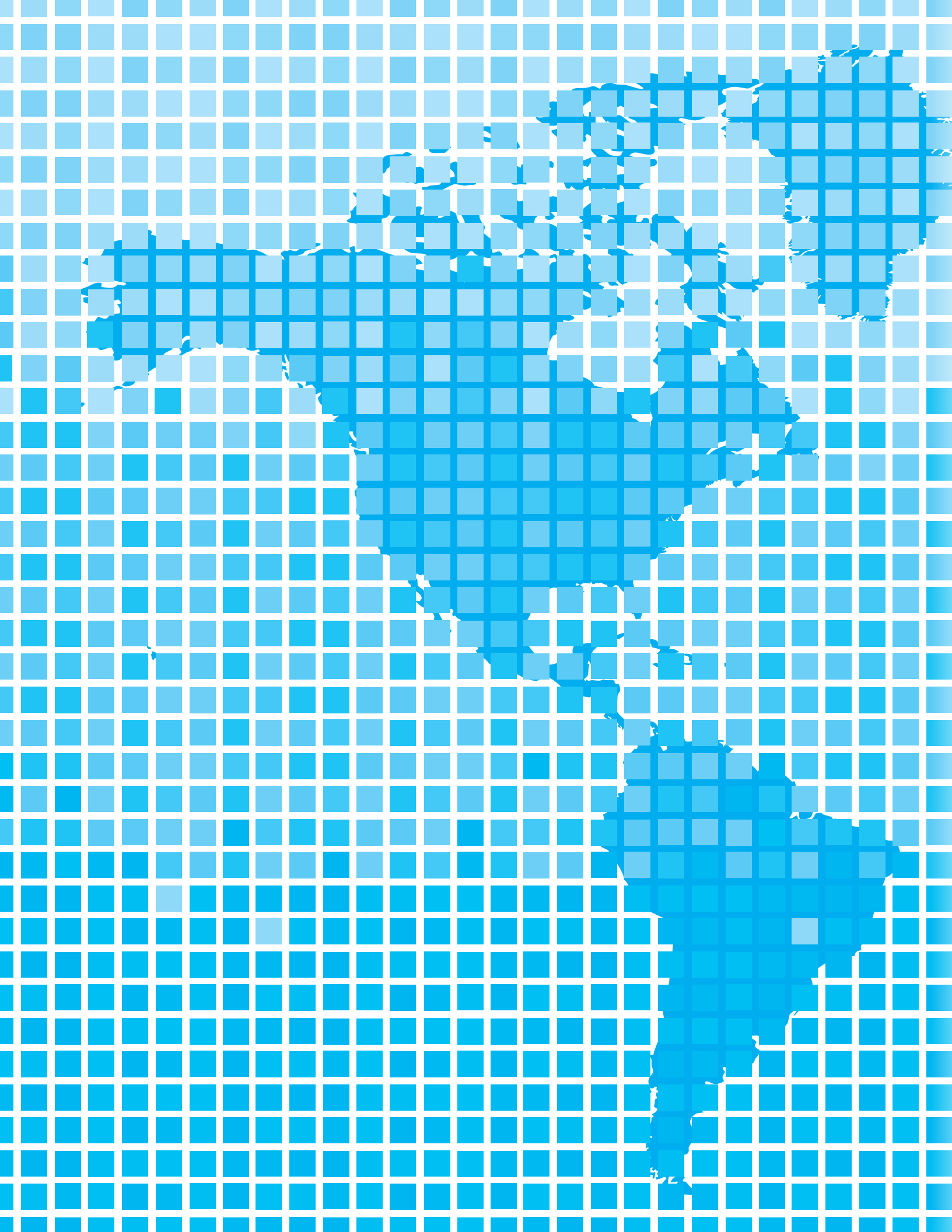
Mobile Cybersecurity and the Internet of Things

Empowering M2M Communication

CTIA
The Wireless Association®



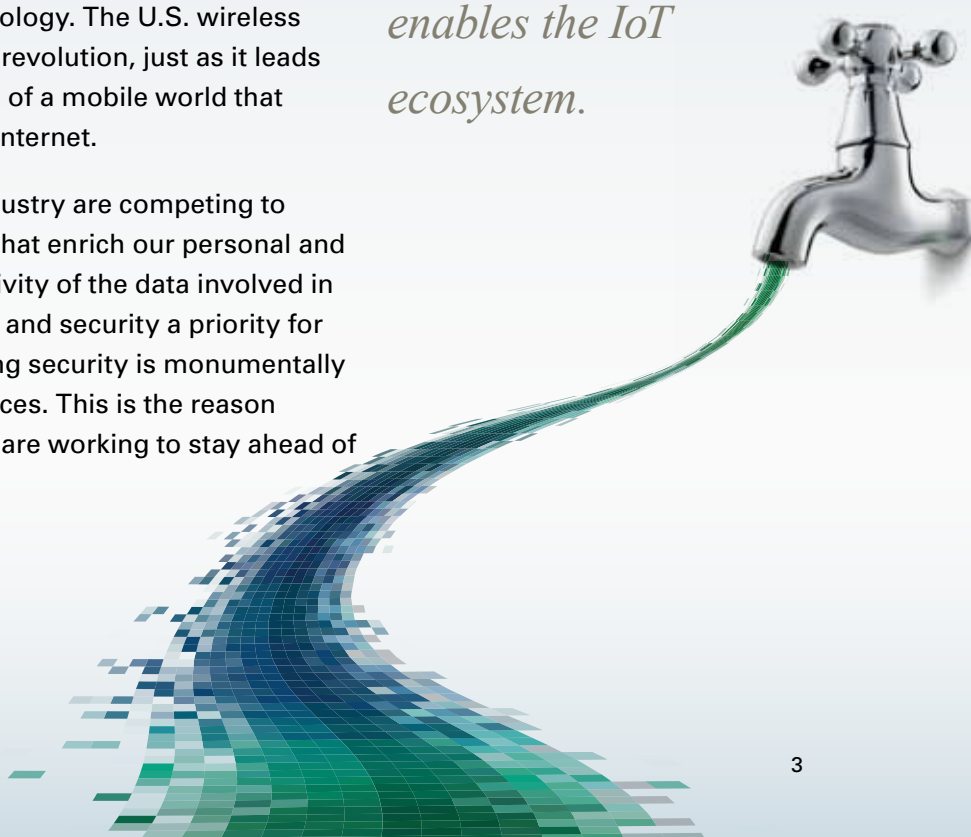
Executive Summary:

A new wave of technological advances in wireless communication is making possible a dynamic ecosystem of connected devices designed to improve how we live and work. The Internet of Things (IoT) involves information-linked networks comprised of sensors and other technologies embedded in physical objects, such as refrigerators, electronic meters, electronic tags, home automation systems, etc. IoT is expected to accelerate the connection of devices, IT systems and networks similar to how the Internet connects many of the world's seven billion inhabitants. By the end of this decade, some estimates suggest the Internet of Things could connect as many as 50 billion devices[1]—or approximately six devices per person on the planet.

While the IoT does not have a single, widely-accepted definition, it is generally agreed that it refers to a growing set of "things," or objects such as tags, sensors and devices that interact with each other and with software applications. IoT is the application domain of Machine to Machine (M2M) communications, and it provides the "plumbing" or connectivity that enables the IoT ecosystem.[2] Experts anticipate that most of this new connectedness in the M2M environment will rely on wireless technology. The U.S. wireless industry is at the forefront of this latest revolution, just as it leads in 4G technology (LTE) and the creation of a mobile world that connects people to each other and the Internet.

Companies throughout the wireless industry are competing to develop and introduce new M2M uses that enrich our personal and work lives. At the same time, the sensitivity of the data involved in delivering M2M solutions make privacy and security a priority for continued M2M market growth. Ensuring security is monumentally important for the success of M2M services. This is the reason companies across the M2M ecosystem are working to stay ahead of threats to data security.

IoT is the application domain of Machine to Machine (M2M) communications, and it provides the "plumbing" or connectivity that enables the IoT ecosystem.



It is important for end users—in business, industrial, home or personal settings—to be educated about security in an increasingly connected world. As a complement to consumer education, the mobile industry is fully engaged in keeping today's and future technologies, systems and networks secure.

The Cybersecurity Working Group maintains an ongoing blueprint developed by CTIA–The Wireless Association® in collaboration with numerous industry and government entities. This wide-ranging effort aims to ensure that society realizes the many benefits of M2M services by improving and encouraging the use of best practices and standards for data transparency, data integrity and security and the anonymization of data, where appropriate. Moreover, while the marketplace for M2M solutions remains nascent, regulators should maintain flexibility and observe industry for market-based solutions to emerge. Top-down regulation would stifle the growth and benefits that M2M communication may offer society as well as threaten the pace of adaptive cybersecurity solutions.

What Is IoT?

The **Internet of Things** is a shorthand way of describing a globally interconnected continuum of devices and objects interacting with the physical environment, people and each other.

What Is M2M?

Machine to Machine describes a set of interconnected devices that allow both wireless and wireline systems to communicate with other devices, mostly in vertical segments, i.e., the plumbing/connectivity that enables the IoT ecosystem.

Introduction

As Benefits to Society Grow . . .

Not long ago, the information technology push was aimed at helping ***people*** stay connected at home, at work and on the go. Now, the focus is on linking ***things*** to each other and to us, using sensors and wireless or wireline connections. From everyday appliances and devices that make our lives more convenient, such as mobile health (mHealth) monitoring to track our heart rates, and home applications that adjust the thermostat or start a coffee brewer, to the infrastructure that society depends upon—electricity grids, pipelines and factories—all increasingly rely on "smart" M2M connections.

We are living in a world in which virtually any and every ***thing*** can be connected to the Internet. With more than 50 billion M2M/IoT devices in use by 2020 (as compared with 62 million in 2010)[3], the United States and the world will see innumerable societal benefits and economic growth.

> ***As Neelie Kroes, the vice president of the European Commission in charge of the EU's digital agenda recently said: "The shift from an Internet of People to an Internet of Things will create unprecedented market opportunities."*** [4]

The societal and individual benefits of the IoT are just beginning to be realized with M2M innovations. More than just providing the convenience of the Internet, the IoT will provide greater efficiency by automating tasks, exchanging information, performing updates, making adjustments, maintaining thresholds and comparing variances. Machines will communicate directly with one another based on intelligent algorithms that help liberate us from routine tasks, improve end-user quality of life, reduce complexity and cycle time, improve efficiency and often enhance safety.

In addition to improved functionality, M2M communication is driving a revolution in research across every sector of the economy to analyze new information generated by the IoT. Research in medicine, science and commerce will employ new data analytics on a scale never before possible.

Research in medicine, science and commerce will employ new data analytics on a scale never before possible.

Today's M2M applications exhibit embedded intelligence, which gives us "smart" homes, transportation and healthcare delivery and real-time monitoring, which advances myriad industrial and infrastructure processes, medical applications and environmental management systems.

Four main categories of technology advances are contributing to the rapid rise of M2M communications:

- **Tagging things —** Technologies responsible for Radio Frequency Identification (RFID), Near-Field Communication (NFC), Quick Response (QR) Codes, Digital Watermarking.
- **Sensing things —** Technologies that react to environmental conditions, such as the presence of moisture (smart textiles, smart pavement, water leak detectors), heat (smart thermostats) and air quality (smoke alarms, HVAC monitors).
- **Shrinking things —** Technologies that make IT objects smaller, lighter and smarter, where embedded computing and wireless is the norm.
- **Thinking things —** Objects that access the semantic Web, which supports standardized formats to enable people to share content beyond the boundaries of applications and websites, and open cloud data to customize things.[5]

The following brief list of announcements highlights some of the ways in which M2M applications are revolutionizing our world:

- In the United States, Visa Inc., MasterCard Inc. and American Express Co. banded together to propose use of digital tokens instead of account numbers to process online and mobile purchases. Combined with EMV-chip technology, which has been widely adopted in the EU and elsewhere, the new mobile technologies are expected to improve security.
- AT&T offers M2M home monitoring and security solutions called AT&T Digital Life®. These service features include the ability to remotely lock and unlock doors, turn appliances and lights off and on and control home thermostats.
- Sprint partners with a health and wellness provider to offer M2M-enabled health and fitness monitoring services.
- In the United Kingdom (UK), Telefónica UK was awarded contracts to build the electric utility industry's largest M2M contract to-date, to roll out 53 million smart meters across the UK by 2020.[6] The UK Department of Energy and Climate Change estimates that the £11 billion program is expected to deliver net benefits of £6.7 billion in reduced energy consumption and more efficient management and deployment of electricity services across the country. [7]

…New Challenges Arise

With all these benefits come new challenges. The shift toward greater reliance on frequent, often continuous data-gathering as part of the IoT poses new cybersecurity challenges. The complexity—and automation—of M2M interconnections means that traditional security practices may need enhancements to address the growing challenges. While end-user education remains important in cyberdefense, industry players recognize the importance of cybersecurity in M2M and make it a top priority.

Research shows that as M2M connectivity grows, so do potential threats from cybercriminals and other intruders, including enemy states. The threats may be exacerbated by the growth in mobile malware where industry research shows that the number increased dramatically in 2013.[8]

M2M devices and systems are not immune to the trend of growing cyberthreats. For example, in November 2013, a new Linux operating system worm emerged that appears to be engineered to target the IoT.[9] The worm attacks a range of small, Internet-enabled devices as well as traditional computers. Variants exist for chip architectures usually found in devices such as home routers, set-top boxes and security cameras. Although no attacks against these devices have been found in the wild,[10] many users may not realize they are at risk, since they are often unaware they own devices that run Linux.

No participants in cybersecurity better understand what is at stake than the wireless industry. Currently, the U.S. benefits from one of the lowest mobile malware infection rates in the world. Based on industry reports, mobile malware infection rates last year were less than two percent in the U.S. compared to more than 40 percent in countries like China and Russia.[11] While the risk of encountering malware is

somewhat higher than actual infection rates, a similar disparity exists, with recently-reported malware "encounter" rates ranging from four percent in the U.S. to 28 percent in China and 63 percent in Russia.[12] The mobile industry makes significant investments in cybersecurity and continues to advance industry practices and solutions. These solutions are leveraged from the smartphone and tablet environment into the M2M/IoT space, and is central to the U.S. maintaining its leadership in mobile security. It is also important to understand that even as industry players collaborate to develop best practices for security, every business, including vendors, service providers and application developers, sees the competitive advantage in advancing effective cybersecurity solutions.

M2M devices and systems are not immune to the trend of growing cyberthreats.

In the end, the wireless communications industry is mindful that as each company competes vigorously to create innovative solutions along with new M2M applications, it must continue to collaborate to advance end-to-end security standards. These advances are essential because the market for M2M technology is creating an explosion of new entrants in dozens of vertical segments, including home automation, mHealth and energy smartmeters.

Role of Mobility in M2M Communication

The M2M world of today seems limited only by the imaginations of application developers, device manufacturers, operating systems developers, infrastructure vendors and service providers.

Wireless connectivity is frequently the most efficient, flexible and cost-effective option.

The virtuous cycle of innovation and investment in M2M development embraces both wireline and wireless connectivity, but mobile uses are predominant. By 2018, M2M devices are projected to account for more than 40 percent of connected devices in the United States, as compared to 19.7 percent globally.[13] Wireless connectivity is frequently the most efficient, flexible and cost-effective option, especially in geographies lacking reliable wireline access. The result is that this growing segment of the IoT is made possible by mobile connectivity.

The wireless industry is investing in security solutions (see CTIA Whitepapers[14]) and is making ongoing advances in the wireless cybersecurity blueprint that resulted in the U.S. having one of the lowest smartphone malware infection rates. These solutions and advancements are, and will be, directly applied to other connected devices.

To ensure that society realizes future benefits of the IoT, the wireless industry is committed to continuing efforts to develop best practices and create solutions that will support security, transparency and data integrity, including the protection of sensitive and personally identifiable information. As interest in this expansion of the IoT has grown, so has attention to the cybersecurity and data privacy implications of M2M devices.

M2M Challenges

There are several key areas that pose challenges to M2M adoption and security across many industries and verticals.

Ecosystem:

- **Standardization:** Devices often have to communicate to each other, to upstream management systems (traditional or cloud-based) and to users. This alone presents a challenge in standardizing communication and management protocols, which is further complicated by the different network platforms and connectivity paths which are used. Devices and users may be on Wi-Fi, 3G, 4G or hard wired broadband systems, any of which could be public or private, at any given time.
- **Fragmentation:** It is difficult to define an "ecosystem" as platforms vary significantly. A set of best practices and guidelines may not translate from one industry to another or even across vendors or regions.
- **Complexity:** In part because of this ecosystem variation and regulatory complexity across sectors, industry growth and innovation may not keep pace with market demand. This has a varying degree of impact accross global regions, depending on industrial, economic and political trends.
- **User Experience:** There is a lack of a unified user experience across systems. This makes it challenging to support consistency as administrators (at the industry or consumer level) move from system to system.

Device:

- **Size:** There are often limited device resources (e.g., power, CPU, memory, etc.) available to implement security measures.
- **Hardware:** Because of the diversity in chipsets and operating systems (OS) used, there may be restrictions in implementing chipset/OS-level security measures that are consistent across devices.
- **Data Constraints:** Many devices use integrated methods to identify, encapsulate or compress data. This may result in data handling limitations.

Confidentiality, Integrity & Availability:

- These are the traditional three tenets of security, which apply today as much as ever.
- Securing the communication channel is critical, especially when sensitive data are gathered. Encryption should generally be used, but in some cases, there may be interface/driver limitations. As device churn happens over time, older units should be replaced with those which are capable of more advanced security (e.g., Virtual Private Network (VPN) terminations).
- Authentication of devices AND users when accessing systems and individual portions of data should be encouraged. Devices should be able to authenticate requests from the cloud and attest to their own identity and integrity as well. Depending on the industry, Role-Based Access Control (RBAC)[15] may be required.
- Limited connectivity and availability is not unusual in some M2M deployments. This is especially true in low-power machines that rely on solar or are only active at specific times/conditions. Alerting systems should be able to ascertain expected downtime versus continuous connectivity.

Emerging Cyberthreats

Threat vectors in the growing M2M space are diverse and distributed across broad domains from healthcare and home automation, to energy, transportation and industrial controls. Smartphones and tablets are targets of sophisticated and constantly varying threats. Similarly, threat vectors in the growing M2M space are equally diverse and more complex because of the range of devices that are potential targets for cyberthreats. Targets may include anything that depends on M2M, such as glucose meters and pacemakers for individual health monitoring; controls for home heat pumps and thermostats or front door locks; and a wide array of control systems for industries and critical infrastructure. A diverse array of wireless technologies enable these M2M linkages, and include the familiar Wi-Fi, 3G and 4G networks that support the mobile communications environment we depend upon today.

The growing presence of M2M linkages, particularly in critical infrastructure industries, is rapidly expanding the market for M2M network security services, which by some estimates is expected to reach nearly $1 billion in annual spending by 2018.[16]

This trend is occurring as mobile cyberthreats continue to expand globally. In the third quarter of 2013, several cybersecurity reports noted an increase in banking-oriented attacks, and an increasing sophistication in the appearance of malware so they more closely resemble legitimate applications.[17] But the greatest concern is the continued spread of multi-platform malware such as the Perkele trojan, which began appearing at the beginning of 2013.[18] This Trojan is a cross-platform threat that can attack PCs, laptops and mobile devices, using them to intercept communications to defeat two-factor authentication, such as that used in online banking.

...the greatest concern is the continued spread of multi-platform malware...

Other trends reported by industry security firms in 2013 include:

- A rise in ransomware that targets mobile users in the form of fake antivirus software with such subject lines as "free call updates" pretending to scan for malware.[19]
- Increased commoditization of malware, including "easy bake" malware kits that make it possible for inexperienced and not technically savvy perpetrators to turn into online criminals.[20]

These new threats strive to defeat two-factor authentication, and may be capable of delaying the downloading of a threat from the cloud in order to evade malware detection and other forms of initial detection by the application store. Such increasingly sophisticated threats illustrate the challenge for cybersecurity experts. They must constantly work to adapt and devise new approaches to thwart attacks on mobile networks and systems and ensure applications and devices can be operated safely.

Some Scenarios

Here are several examples of M2M connections and corresponding illustrative **protective countermeasures**.

Connections

Wearable smart devices
Watches, glasses | **encryption, authentication techniques**

Smart meters
Information transport to utility provider | **encryption**

Home automation for convenience and protection
Monitoring and remote control, secure access and alarm system | **encryption and VPN**

Retail NFC
Near-field communication applications | **encryption, malware security, access controls**

Even the whimsical convenience of a coffee machine, a texting system for the coffee machine | **encryption, authentication techniques to deter mischief or unauthorized use**

Applications

mHealth
Telemedicine, blood pressure monitor, pacemaker control, or glucose level monitor | **encryption, access controls, compliance with relevant security requirements**

Automotive
Smartphone to vehicle, vehicle-to-vehicle | **central monitoring to vehicle encryption, access controls, authentication techniques**

Cloud-based device control
Tablet/smartphone | **locate, lock and remote wipe**

Industry Approaches to Preserving Cybersecurity

Mobile industry participants are committing significant assets to provide comprehensive cybersecurity solutions.

In addition to the industry's security efforts discussed above, the industry manages M2M cybersecurity through 24/7 monitoring and threat assessment; design and testing; encryption; vulnerability management; and policy/data sharing. The wireless industry actively drives innovation through advances in:

- **Monitoring and vulnerability scans**
  The goal is to assess and anticipate threats in real time and prevent problems from happening.
- **Advanced security technology standards**
  These span general guidelines to specific directives and together create a landscape of security standards that is continually evolving in response to the threat environment.
- **Enhancements to security policies and risk management**
  This specialty field develops and provides enhancements to security and risk management protocols; improves definitions and documentation; and provides security assessments based on ongoing scans of the threat environment.
- **Advances in monitoring of specific cyberthreat profiles**
  Robust profiles of specific and emerging cyberthreats are essential to quickly mounting effective defenses and countermeasures.

Mobile industry participants are committing significant assets to provide comprehensive cybersecurity solutions.

Ongoing Efforts to Counter Cyberthreats

Many of the same techniques and best practices in use in today's mobile communications ecosystem are adapted and leveraged for use in the M2M wireless context.

This list is intended to be illustrative of the range of solutions that are part of the ongoing cybersecurity blueprint developed in conjunction with the CTIA Cybersecurity Working Group:[21]

- **Security Audits**
- **Encryption and Virtual Private Networks**
- **Immutable Root-of-Trust**
- **Enhanced Security Features**
- **Software Update Distributions**
- **Multiple Air-Interface Security**

Mobile industry participants are committing significant assets to provide comprehensive cybersecurity solutions.

Many, if not all, of these technologies and solutions may be applied in the M2M domain, thereby keeping the industry and the end uses of these connections one step ahead of the threats.

The rapid expansion of M2M connectedness elevated the focus on cybersecurity and data privacy protections among government agencies and policymakers. Among the most important steps being taken are collaborative discussions with industry players to better understand the current state of the industry and where market innovations in M2M uses are headed. In addition, public and private sector groups are committed to ongoing identification of cyberthreats and advancing efforts to maintain security and data privacy in ways that preserve societal benefits.

Policy Approaches to M2M Cybersecurity

In the United States, there are many data security laws and regulations where applicability to the IoT and M2M may have to be studied and reviewed as to their sufficiency and appropriateness. Examples of these include: the FCC's Customer Proprietary Network Information (CPNI) Rules; Gramm-Leach-Bliley Act (GLB) Act; Electronic Fund Transfer Act, (EFTA); Children's Online Privacy Protection Act (COPPA); Federal Information Security Management Act (FISMA); North American Electric Reliability Corp. (NERC) standards; Health Insurance Portability and Accountability Act (HIPAA); the Health Information Technology for Economic and Clinical Health Act (HITECH); and the Patient Safety and Quality Improvement Act (PSQIA, Patient Safety Rule).[22]

Early in 2013, the importance of security was elevated once more with President Obama's announcement that his Administration would develop a national cybersecurity framework to protect critical infrastructure.

The National Institute of Standards and Technology (NIST) lead the process with industry to develop a voluntary, non-regulatory cybersecurity framework to address critical infrastructure, which encompasses the new challenges posed by the IoT and M2M. The NIST Framework was announced on February 12, 2014 and industry looks to leverage the framework broadly across the 16 industry sectors that it addresses. Consistent with Presidential Executive Order 13636,[23] the mobile industry and the telecommunications sector played a leading role in the development of the framework. Both in the context of security and privacy, the framework is an important milestone for the evolution of M2M/IoT.

The National Highway Transportation and Safety Administration (NHTSA) is committed to improving safety and mobility on the nation's roadways. Connected vehicle technology shows great promise in transforming the way Americans travel.

Through wireless technology, connected vehicles, ranging from cars to trucks and buses to trains, will one day be able to communicate important safety and mobility information to one another that helps save lives, prevent injuries, ease traffic congestion and improve the environment. NHTSA has increased its engagement with vehicle cybersecurity and is developing resources in this area.[24]

The North American Electric Reliability Corporation (NERC), since 2007, developed a set of 83 mandatory NERC standards that establish and enforce reliability for the bulk-power system of North America, as well as protect the industry's critical infrastructure from physical and cyber threats. In 2009 NERC updated the Critical Infrastructure Protection (CIP) elements of the reliability standard; including identification and protection of both physical assets and digital (cyber) systems.

Wireless Industry Efforts

CTIA is actively engaged in the public-sector initiatives, as well as with standards and solution-building efforts across the wireless and telecommunications industry through its Cybersecurity Working Group (CSWG).

CTIA's ongoing collaboration with government agencies and industry groups serves to monitor and address cybersecurity threat trends and solutions in light of the rapidly growing M2M market.

The industry's competitive environment works in favor of advancing cybersecurity because each player understands the advantages of marketing products and services that deploy the current best practice.

In fact, the industry's size, global diversity and focus on security matters is reflected in the number of initiatives that CTIA and its members are currently involved with, including (but not limited to):

ATIS | The Alliance for Telecommunications Industry Solutions is a technical and operations standards-setting body for the entire information and communications technology (ICT) industry, including critical security and interoperability issues involved in M2M connections. This work is conducted through the ATIS M2M Committee.

TIA | The Telecommunications Industry Association recently released TIA-4940, "Smart Device Communications (M2M) Reference Architecture," and is working with the OPC Foundation to support new standards for interoperability.

3GPP | Third Generation Partnership Project, which adopts standards for mobile communications, is also looking into standards for M2M wireless communications.

OMA | Open Mobile Alliance, which coordinates input to the oneM2M[25] standards organization.

OneM2M | Global standards development organization developing the M2M service layer.

GSMA | GSM Association, supports projects regarding embedded SIM devices and Connected Living Programs.

BBF | Broadband Forum, standards that govern the control signaling abstraction layer.

IEEE | Institute of Electrical and Electronic Engineers, standards for M2M wireless communications.

ITU | International Telecommunications Union, global standards initiative in M2M service layer.

Overall, the industry's principal concern is that oversight and controls remain flexible and supportive of a nascent market that brings great promise to make peoples' lives safer and easier, and benefit society as a whole.

Conclusion

The M2M revolution outlined here illustrates the dynamism of the mobile environment and the need for a collaborative government-industry approach to advance cybersecurity and data protections.

...in a world of connected devices, the focus should shift from how information is collected and communicated to how it is protected and shared.

As we have seen, many of the techniques available today to maintain cybersecurity are being effectively used for M2M connections. The examples are visible in many realms in the latest generation of smart meters used by electric utilities, in increasing adoption of telemedicine and electronic health records, and telematics for industrial automation.

What is needed is the continuation of a broad-based modern approach as defined by the voluntary NIST Framework, involving a government and industry partnership to guide ongoing industry development of cybersecurity best practices and solutions.

An overly rigid, prescriptive approach that focuses on requiring particular standards to achieve better security risks enabling the very end it seeks to avoid. Such "solutions" tend to create uniform, standardized approaches to security challenges, which make it easier for cybercriminals to master once and copy endlessly their successful attacks, even turning malware development into cybercrime enterprises on an industrial scale.

Recommended practices that drive current industry solutions are constantly being updated to reflect the latest analysis of threats. In addition, research and development is ongoing to create new countermeasures and solutions that protect consumers and end users, and the networks and components of the wireless ecosystem.

For M2M the National Cybersecurity Framework should be preserved as technology neutral, and not vary depending on the type of device or technology being used to gather or transmit data.

Equally important, the framework for M2M cybersecurity should remain flexible enough to allow companies to continue to innovate and bring forward new M2M applications and new solutions to counter emerging threats.

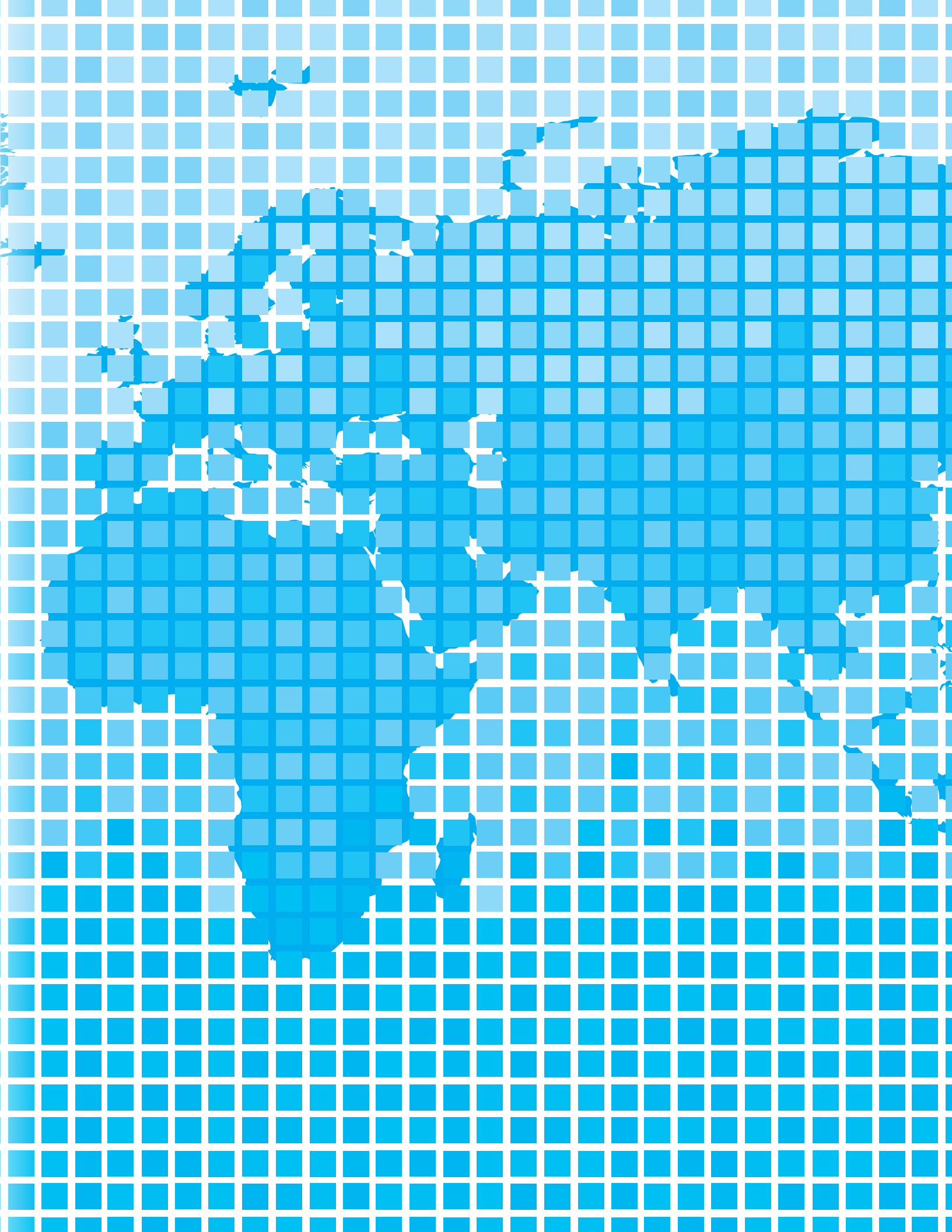
Public-private partnerships that create industry best practice frameworks will nurture innovation and safeguards in this new sector for the Internet of Things where the benefit to society of M2M communications can be fully realized.

Finally in a world of connected devices, the focus should shift from how information is collected and communicated to how it is protected and shared.

Endnotes

1. *Samuel Greengard, "The Internet of Things Means Business, Baseline Magazine, Feb. 19, 2014, available at* http://www.baselinemag.com/innovation/the-internet-of-things-means-business.html.
2. *Eric N. Barnhart, P.E. and Charles A. Bokath, "Considerations for Machine-to-Machine Communications Architecture and Security Standardization," IEEE Xplore® Digital Library (2012) available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6156367.
3. *See Steve Hilton, Analysys Mason, Analyst Corner - Consumers to Expedite an M2M World, Wireless Week, March 28, 2011, available at* http://www.wirelessweek.com/articles/2011/03/analyst-corner-consumers-expedite-m2m-world, *and see Ericsson White Paper, More Than 50 Billion Connected Devices, February 2011, available at* http://www.ericsson.com/res/docs/whitepapers/wp-50-billions.pdf.
4. *Dan Verhaeghe, "From M2M to The Internet of Things: Viewpoints from Europe," TechVibes, July 7, 2011, available at* http://www.techvibes.com/blog/from-m2m-to-the-internet-of-things-viewpoints-from-europe-2011-07-07 *(quoting Neelie Kroes).*
5. *Id. citing Dr. Lara Srivastava, Professor in Media and Communications at Webster University, "Europe and the Internet of Things," presentation in Budapest, May 16, 2011.*
6. *See Anne Morris, Telefónica confirms €1.78B UK smart meter deal, Fierce Wireless, Sept. 25, 2013, available at* http://www.fiercewireless.com/europe/story/telef-nica-confirms-178b-uk-smart-meter-deal/2013-09-25.
7. *Id.*
8. *See e.g., TrendLabs Security Intelligence Blog, Looking Forward into 2014: What 2013's Mobile Threats Mean Moving Forward, Jan. 20, 2014, available at* http://blog.trendmicro.com/trendlabs-security-intelligence/looking-forward-into-2014-what-2013s-mobile-threats-mean-moving-forward *(estimating the number of malicious or high-risk apps as having grown to 1.39 million).*
9. *See Kaoru Hayashi, Linux Worm Targeting Hidden Devices, Symantec Blog, Nov. 27, 2013, available at* http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices.
10. *Malware is said to be "in the wild" if it is spreading or detected among infected computers or devices in the general public, and not restricted to a laboratory environment.*
11. *See e.g., Lookout, State of Mobile Security 2012, available at* https://lookoutl.com/resources/reports/state-of-mobile-security-2012, *at 9-10 (U.S. and Russia). See also TrustGo™ Q4 Mobile Mayhem Report 2012, Jan. 10, 2013, available at* http://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). See also NQ Mobile 2013 Mid-Year Mobile Security Report at* http://blog.nq.com/2013midyearsecurityreport/.

12. *See Lookout Mobile Threats Made to Measure: The Specialization of Mobile Threats Around the World, Feb. 20, 2014, available at* https://www.lookout.com/static/ee_images/Mobile_Threats_Made_to_Measure_Lookout_Report_2013.pdf*, at pp. 11 and 17 (a single device may encounter malware more than once, and may not necessarily be infected).*
13. *See Cisco VNI Mobile Forecast Highlights Tool, 2013 - 2018 (Feb. 2014), available at* http://www.cisco.com/assets/sol/sp/vni/forecast_highlights_mobile/index.html*.*
14. *See CTIA Policy & Initiatives, Policy Topics, Cybersafety and Cybersecurity, available at* http://www.ctia.org/policy-initiatives/policy-topics/cybersafety-and-cybersecurity*.*
15. *See National Institute of Standards and Technology, Computer Security Division, Computer Security Resource Center, Role Based Access Control (RBAC) and Role Based Security, at* http://csrc.nist.gov/groups/SNS/rbac/*.*
16. *Signals and Systems Telecom Ltd., The Wireless M2M Bible: 2013-2018 (2013) at Figure 9 (Global Wireless M2M Industry Revenue by Sub-Market ($ Million): 2011-2018.*
17. *See Trend Micro The Invisible Web Unmasked: TrendLabs 3Q 2013 Security Roundup, available at* http://about-threats.trendmicro.com/us/security-roundup/2013/3Q/the-invisible-web-unmasked/*.*
18. *See Kaspersky Labs IT Threat Evolution: Q1 2013, available at* https://www.securelist.com/en/analysis/204792292/IT_Threat_Evolution_Q1_2013*.*
19. *See Kaspersky Labs It Threat Evolution: Q2 2013, August 15, 2013, available at* http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_IT_Threat_Evolution_Q2_2013*.*
20. *See F-Secure Mobile Threat Report: January-March 2013, available at* http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Thre at_Report_Q1_2013.pdf*.*
21. *See the CTIA Cybersecurity Whitepapers available at* http://www.ctia.org/policy-initiatives/policy-topics/cybersafety-and-cybersecurity*.*
22. *See e.g., Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd. 6927 (2007), and Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Declaratory Ruling, 28 FCC Rcd 9609 (2013); Gramm-Leach-Bliley Act, Pub. L. 106-102 (113 Stat. 1338) (1999) (codified at 15 USC § 6801-6810); Electronic Fund Transfer Act, Pub. L. 95-630, 92 Stat. 3641 (1978); Children's Online Privacy Protection Act, Pub. L. 105-277, 112 Stat. 2581 (1998); Federal Information Security Management Act, Pub. L. 107-347, 116 Stat. 2899 (2002); North American Electric Reliability Corporation standards, available at* http://www.nerc.com/pa/stand/Pages/default.aspx*; Health Insurance Portability and Accountability Act, Pub. L. 104–191, 110 Stat. 1936 (1996); the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act, Pub. L. 111-5, 123 Stat. 115 (2009); and the Patient Safety and Quality Improvement Act, Pub. L. 109-41, 42 U.S.C. 299b-21 et seq. (2005), and the related Patient Safety Rule at 42 C.F.R. Part 3.*
23. *Executive Order 13636 Improving Critical Infrastructure Cybersecurity (February 12, 2013), available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity*.*
24. *National Highway Traffic Safety Administration, Preliminary Statement of Policy Concerning Automated Vehicles, May 30, 2013, available at* http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf*.*
25. *See oneM2M WI-0003 Roles and Focus Areas, available at* http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CC4QFjAA&url=ftp%3A%2F%2Fftp.onem2m.org%2FWork%2520Programme%2FWI0003%2FoneM2M-WI-0003-VocabPrinciples-V1_2.DOC&ei=n_LKUvamIZC_kQeTtIDACQ&usg=AFQjCNFk_UsX-DIvzLOShPQ339Tn-Kqxbg&sig2=gkYhkOFGp62N5nHqNaktQA&bvm=bv.58187178,d.eW0*.*



WWW.CTIA.ORG