Microsoft's Response to Request for Comment
Department of Commerce, National Telecommunications and Information Administration

Promoting Stakeholder Action Against Botnets and Other Automated Threats

I. Introduction

Microsoft Corporation ("Microsoft") appreciates the opportunity to provide comments to the U.S. Department of Commerce ("Commerce") and specifically the National Telecommunications and Information Administration ("NTIA") in response to its request for comments on promoting stakeholder action against botnets and other automated threats.

As a global technology company dedicated to enhancing international cybersecurity, Microsoft has long led efforts to disrupt some of the world's largest and most notorious botnets. Microsoft has also been involved in a series of efforts to secure information systems and networks to prevent botnets from compromising information technology infrastructure. These initiatives build upon Microsoft's defense-in-depth strategy, which addresses the threats posed by botnets on multiple fronts. In addition, Microsoft has worked collaboratively for years with private and public sector partners to address the threats posed by botnets, including by providing testimony before Congress and producing white papers about cybersecurity policy for emerging technologies like the Internet of Things ("IoT").[1]

II. Microsoft's Experience Disrupting Botnets

Botnets are a sophisticated type of cybercrime that allow malicious actors to take control of groups of computers without the device owners' knowledge or consent. While an individual with a compromised device may not immediately notice their device has been compromised, the impact of a successful botnet can be quite severe—a botnet can infect millions of computers at a time and enable criminal enterprises to execute many simultaneous schemes against unsuspecting victims. One of the most common objectives of those attacks is to compromise connected devices and cloud services, because this will allow the botnet to use the combined computing power of many separate resources. Once a large number of devices are part of a botnet, the botnet can be used to execute other malicious activities, such as Distributed Denial of Service ("DDoS") attacks.[2]

In some cases, the goal of a botnet operator is to disrupt online services and websites by overloading their bandwidth and rendering them unavailable. In addition, botnet operators can also target individual users. For example, botnet operators can hijack webcams to spy on people in their homes, then sell the footage on the Internet's black market. They can also use malicious

[1] For examples of Microsoft's prior testimony and publications, please see documents attached to this response as the **Appendix**.

[2] *See* Microsoft, Azure Advanced Threat Detection, available at https://docs.microsoft.com/en-us/azure/security/azure-threat-detection.

software to log the keystrokes a user enters on their device, which enables the botnet operator to steal credit card numbers or Social Security Numbers, among other personal and work-related information.[3]

However, there are ways to effectively mitigate botnet attacks. For example, Microsoft has partnered with other companies, public sector entities, and international law enforcement to effectively disrupt some of the world's most malicious botnet operations. This section provides additional detail about these efforts, including a brief background on Microsoft's Digital Crimes Unit ("DCU") and an overview of DCU's efforts to disrupt botnets. The section concludes by suggesting how existing partnerships between the public and private sectors could be further improved.

A. Background of Microsoft's Digital Crimes Unit

Microsoft's Digital Crimes Unit ("DCU") is an international team of attorneys, investigators, data scientists, engineers, analysts, and business professionals working together to safeguard people and organizations from digital threats, including botnets. Using creative legal strategies and cutting edge data analytics, DCU partners with law enforcement, non-governmental organizations, security vendors, and researchers to transform the fight against cybercrime by seeking to stop the harm, notifying those victimized, and assisting law enforcement in bringing cybercriminals to justice. In every phase of its operations, DCU is committed to protecting the privacy of individual and enterprise data while aggressively fighting cybercrime targeting Microsoft's customers, including vulnerable Internet users wherever in the world they reside, as well as our online services, infrastructure, and corporate interests.[4]

B. Microsoft's Anti-Botnet Operations

Since 2010, Microsoft has led efforts to disrupt some of the world's largest and most notorious cybercriminals and botnets. DCU's worldwide investigative team works collaboratively with public and private sector partners to fight cybercrime on multiple fronts.

- **Legal Process:** After obtaining authorization through a civil court order, DCU can launch operations designed to disrupt a botnet by severing the botnet's ability to communicate with the infected devices it controls. First, DCU seizes control of the virtual infrastructure being used to control the botnet ("command and control" or "C2"). Then, DCU directs the infected devices attempting to contact the botnet's C2 to a sinkhole maintained by Microsoft, which prevents the botnet from controlling infected machines, thus disrupting the botnet.[5]

[3] *See* Microsoft, Congressional Testimony of Richard Domingues Boscovich before the Senate Committee on the Judiciary Subcommittee on Crime and Terrorism, Taking Down Botnets: Public and Private Efforts to Dismantle Cybercriminal Networks, July 15, 2014 (hereinafter "Boscovich Testimony").

[4] *See* Boscovich Testimony.

[5] This redirection allows Microsoft to gather significant information about the botnets it disrupts: the sinkhole receives approximately 25 million unique Internet Protocol addresses per month, and the devices behind these IP addresses are responsible for—on average—250 million connections daily to the sinkhole.

- **Notify and Remediate:** Microsoft uses its Cyber Threat Intelligence Program ("CTIP") and Government Security Program ("GSP") to notify entities such as Computer Emergency Response Teams ("CERTs"), Internet Service Providers ("ISPs"), and others of threat intelligence obtained through the malware disruption operations conducted by DCU. Microsoft also uses this information to help individual and enterprise customers remediate infected devices.

- **Coordinate to Disrupt Criminal Infrastructure:** Microsoft works with public and private sector partners, including domestic and international law enforcement, to disrupt the criminal infrastructure surrounding botnets. Microsoft has coordinated with domestic and international law enforcement to seize control of domains associated with a botnet at the same time law enforcement executed seizures of the botnet's physical infrastructure. For example:

  Ramnit was a botnet designed to carry out online banking fraud by harvesting credentials such as online banking log-ins, passwords, and personnel files. Microsoft took control of more than 300 domains while international law enforcement executed physical seizures of Ramnit's C2 servers. Before disruption, Ramnit caused hundreds of millions of dollars in consumer losses and the average net loss per victim was $4,300 (USD).

  Dorkbot was a password-stealer targeting popular web services such as Facebook and Twitter. Based on information referred by DCU, international law enforcement executed a coordinated seizure of Dorkbot infrastructure throughout the world. Simultaneously, Microsoft redirected infected devices to the DCU sinkhole and began actively working with global CERTs and ISPs to ensure victims were notified and infected devices remediated—a significant task, as more than twelve million Internet Protocol ("IP") addresses associated with infected devices have connected to the sinkhole since the botnet was disrupted.

C. Legal and Public Policy Issues Surrounding Cooperation

The disruption of botnets described above has proven highly effective. Some botnets have caused billions of dollars in worldwide economic damages, while others were responsible for identity theft, stealing personal information, and sending massive quantities of spam.[6] Once the botnet infrastructure has been taken down, they can no longer inflict these harms.

However, these efforts are not entirely without challenges. Even when a botnet disruption is hugely successful, it may not result in a traditional law enforcement marker of success, such as arresting a suspected criminal or completing an investigation ("closing a case"). Achieving such results require successful attribution, because linking a botnet to an identifiable person or group of people is necessary to effectuate an arrest. This can often require resources and time commitments from law enforcement entities in disparate jurisdictions, which has challenges in effective cross-border communication and coordination. Moreover, successful attribution is not always possible, and even successful attribution may come at a significant cost. For example,

[6] Boscovich Testimony.

gathering the evidence needed for attribution may require law enforcement to allow a botnet to continue engaging in criminal activity for additional months or years prior to disruption, placing additional victims at risk and potentially losing visibility into those already victimized. As a result, law enforcement's desire for successful attribution often hampers victim notification and remediation efforts.

Given that the current performance metrics used by certain U.S. federal law enforcement agencies emphasize successful attribution and achieving the traditional markers of law enforcement success, the current system may create a disincentive for law enforcement officers to devote substantial time to botnet disruptions. To further increase cooperation in confronting the cybersecurity threats posed by botnets, the U.S. government should consider reevaluating how its law enforcement agents' achievements are measured to take into account the unique nature and importance of botnet investigations and disruptions. This issue is further complicated by the global nature of cybercrime, which adds the need of cross-jurisdictional investigation and gathering of evidence and shared credit for successful operations.

III. Securing Information Technology Infrastructure through Defense in Depth

Deploying a defense in depth strategy can reduce vulnerabilities in information technology infrastructure and prevent or reduce the impact of botnet attacks before they occur. In addition to its efforts to counter existing botnets, Microsoft also engages in a series of efforts to preemptively address the threats posed by automated, distributed threats—including botnets—on multiple fronts.

This section highlights these efforts by examining Microsoft's commitment to securing devices and reducing vulnerabilities. In particular, it identifies the ways Microsoft supports the development of secure hardware, how Microsoft's Security Development Lifecycle is designed to increase the security of software, and Microsoft's recommendations for how to improve the security of IoT deployments through a role-based approach. The section concludes by highlighting the ways deployment of cloud technology can further help secure the information technology infrastructure.

A. Security of Hardware

Hardware-based Roots of Trust ("RoT") can be used to establish trust in other components and provide reliable capabilities essential to security scenarios associated with botnets. RoTs need to be inherently trusted because their misbehavior cannot be detected, so their implementation needs to be done with special care to provide strong protections against malware. Even if a device is compromised by malware, RoTs need to continue to function unimpeded and provide their capabilities.

Traditional RoTs like the Trusted Platform Module ("TPM")[7] help provide capabilities to protect cryptographic keys, measure, and report the software loaded on a device during the boot process.

[7] *See* International Organization for Standardization ("ISO"), ISO/IEC 11889:2015, Trusted Platform Module Library, available at https://www.iso.org/standard/66510.html.

The National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-147[8] and draft NIST SP 800-193[9] introduced additional RoT for update, detection, and recovery. IoT devices should implement RoT to improve their security. RoTs can help devices recover and help operators verify recovery if botnet or malware infections do occur. Because IoT devices will be plentiful and cannot be realistically managed individually by people, they should be connected to cloud services or utilities providing provisioning, management and maintenance capabilities at scale.

Microsoft supports open global standards to develop best practices for more secure and robust deployments, and concurrently supports multiple standards. For example, Microsoft's Azure IoT solution supports devices using Hardware Security Modules ("HSMs"), the Trusted Computing Group's ("TCG") Device Identifier Composition Engine ("DICE")[10] draft specification and the TPM. While TPM is a more prevalent hardware security standard, DICE offers a scalable security framework that requires minimal hardware resources to anchor when implementing various security capabilities. DICE is especially suitable for devices in IoT that are potential targets for botnets. As technologies evolve and become even more interconnected, thinking about security from the hardware through to the customer's software helps create a more secure computing ecosystem less susceptible to compromise, including botnet attacks.

B. The Security Development Lifecycle

The security of the software being used will have significant impact on the security of IoT devices and in the fight against botnets, because applying strong security standards helps ensure quality of code and decreases the risk of exploit. At Microsoft, the Microsoft Security Development Lifecycle ("SDL") is a mandatory company-wide development process that embeds security requirements into the entire software lifecycle and provides a step-by-step approach to building secure software. This software development process—which incorporates the principles of the application security standard ISO 27034:1[11]—helps developers build more secure software and address security compliance requirements while reducing development cost.[12] Microsoft created the SDL nearly fifteen years ago as means to improve product security and ensure a consistent approach to security practices across the thousands of software engineers.

---

[8] *See* National Institute of Standards and Technology ("NIST"), Special Publication 800-147, BIOS Protection Guidelines, available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-147.pdf.

[9] *See* NIST, Draft Special Publication 800-193, Platform Firmware Resiliency Guidelines, available at http://csrc.nist.gov/publications/drafts/800-193/sp800-193-draft.pdf.

[10] *See* Trusted Computing Group, Committee Draft, Trusted Platform Architecture Hardware Requirements for a Device Identifier Composition Engine, available at https://trustedcomputinggroup.org/wp-content/uploads/TCG-Device-Identifier-Composition-Engine-rev-72_public-review.pdf.

[11] *See* ISO, ISO/IEC 27034-1:2011, Application Security, available at https://www.iso.org/standard/44378.html.

[12] *See* Microsoft, Security Development Lifecycle, available at https://www.microsoft.com/en-us/sdl.

It has since been adapted and implemented widely across industry, including at companies like Adobe[13] and Cisco.[14]

In addition, the SDL's holistic approach to secure software development can also be applied by smaller development teams for many different types of devices and online services, including Agile development environments.[15] This is particularly important because there is a current perception that Agile methods do not create secure code, and unfortunately, this perception is generally accurate. There is very little "secure Agile" expertise available in the market today. However, actively taking steps to integrate security requirements into Agile development methods can begin changing both the perception and the reality.

C. Using a Role-Based Approach to Improving IoT Security

Securing an IoT infrastructure is more difficult than securing a traditional infrastructure, in part because IoT surpasses the confines of traditional computer networks and establishes connections directly with objects in the physical world. In addition, the scale of IoT's potential reach—in terms of the number of devices, the scope and demographic span of deployments, the heterogeneity of systems, and the technical challenges of deployment into new and potentially unsecure environments—makes IoT distinct from historical information technology advancements.[16]

Connected devices hold new benefits for consumers, the public sector, and private industry but also present a number of technological and security challenges because IoT networks often involve a vast proliferation of devices; exhaustive volumes of data created by those devices; a presumption that IoT devices will likely communicate with each other; and a blurring of the roles and functions between traditional Information Technology ("IT") and Operational Technology ("OT") environments.[17]

This section highlights how, despite these complications, distinct roles and respective best practices of various stakeholders in the IoT system can lead to the deployment of a rigorous security-in-depth strategy. These stakeholders include:

---

[13] *See* Microsoft, Cyber Trust Blog, Microsoft & Adobe: Protecting Our Customers Together, June 17, 2009, available at https://blogs.microsoft.com/cybertrust/2009/06/17/microsoft-adobe-protecting-our-customers-together.

[14] *See* Cisco, The Cisco Secure Development Lifecycle: An Overview, April 5, 2010, available at http://blogs.cisco.com/security/the_cisco_secure_development_lifecycle_an_overview.

[15] *See* Microsoft, Security Development Lifecycle for Agile Development, available at https://msdn.microsoft.com/en-us/library/windows/desktop/ee790621.aspx.

[16] *See* The President's National Security Telecommunications Advisory Committee, NSTAC Report to the President on the Internet of Things, Nov. 19, 2014 ("NSTAC Report") at 2.1, available at https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

[17] For example, an industrial manufacturer that uses Internet-connected sensors to monitor production its facilities would need to simultaneously manage both IT (e.g. smart device sensors) and OT (e.g., process control board) in a harmonized manner.

- The **Manufacturers / Integrators**, who are responsible for manufacturing or assembling hardware. Best security practices for manufacturers and integrators include: scoping hardware to meet minimum requirements; making hardware tamper proof; building around secure hardware; and making upgrades secure.

- The **Solution Developers**, who are responsible for developing some portion of the IoT solution. Best security practices for developers include: following secure software development methodology; choosing open-source software with care; and integrating components with care.

- The **Solution Deployers**, who are responsible for deploying the IoT solution once it is developed. Best security practices for deployers include: deploying hardware securely and keeping authentication keys safe.

In addition to these roles, **IoT Solution Operators**, who are responsible for managing IoT deployments, have a particular set of responsibilities that can help address botnet risks and make IoT devices more resilient. Those devices—also known as "endpoints" because they sit at the edge of the network—require a consistent approach to security in order to help manage risks. Microsoft believes that there are concrete steps IoT Solution Operators can take to increase the usage of secured endpoints across devices and applications:

- **Keep the system up to date:** Where devices allow for updating, ensure that device operating systems and all device drivers are upgraded to the latest versions; this helps protect against many types of malicious attacks, including botnets. Discourage the use of devices that cannot be updated, and enforce stronger security controls around devices that cannot be updated but must be used.

- **Protect against malicious activity:** Install the latest antivirus and antimalware capabilities on each device, which helps mitigate most external threats.

- **Conduct frequent security audits**: Enable and review event logging to ensure compliance with security requirements and have adequate records to investigate breaches.

- **Physically protect infrastructure:** Restrict physical access to devices and enable logging of physical access to the system.

- **Protect credentials:** Change passwords frequently, require strong passwords that are not shared, and refrain from using credentials on public machines to make it less likely the credentials will be stolen.[18]

While IoT Solution Operators can take the important steps identified above, government entities have a special role to play in encouraging the use of secured endpoints through policy initiatives.

[18] Stolen authentication credentials are frequently the easiest way for a malicious actor to gain access to and compromise a device. *See* Microsoft, IoT Security Best Practices, available at https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-best-practices.

Through these initiatives, government entities have the ability to enact policies favoring the use of secure endpoints as a means to improve security; mitigate botnet risks; encourage deployment of IoT; convene the relevant stakeholders to address shared challenges; issue guidance assisting the public; and intervene as a regulator when necessary.[19]

D. Security Benefits of the Cloud

To protect users of our cloud services, Microsoft provides a DDoS defense system that is part of the continuous monitoring and penetration-testing processes for Microsoft's platform-as-a-service, Microsoft Azure ("Azure"). The Azure DDoS defense system is designed not only to withstand attacks from the outside, but also from other Azure tenants. Azure uses standard detection and mitigation techniques such as rate limiting and connection limits to protect against DDoS attacks.

In addition, Microsoft routinely tests Azure's capability to detect and protect against emerging threats and recover from breaches. Relatedly, Microsoft's global incident response teams work around the clock to mitigate the effects of attacks and malicious activity. These teams follow established procedures for incident management, communication, and recovery. As a result, Azure provides higher levels of enhanced security, privacy, compliance, and threat mitigation practices than most customers could achieve on their own.[20]

Microsoft's approach to cloud security is informed by threat intelligence from multiple sources, including Azure, Office 365, outlook.com, DCU, and Microsoft's Security Response Center ("MSRC"). Microsoft is able to use this wide-reaching and diverse collection of datasets to rapidly discover new attack patterns and trends, which enhances Microsoft's ability to protect Azure users from threats such as DDoS attacks and botnets.

For instance, the Azure Security Center is able to detect if outbound traffic communicates to a malicious IP address of known botnets, and will alert the user if this communication is discovered.[21] In addition, Azure's cloud service is able to mitigate large-scale DDoS attacks through a distinct layer in its virtual network. This additional layer can prevent malicious traffic from reaching its target by detecting the sources of the attack and scrubbing their traffic before it can pass through to the deeper physical network layer and possibly affect network endpoints.[22]

---

[19] *See* Microsoft, Cybersecurity Policy for the Internet of Things, available at https://mscorpmedia.azureedge.net/mscorpmedia/2017/05/IoT_WhitePaper_5_15_17.pdf.

[20] *See* Microsoft, Internet of Things Security from the Ground Up, available at https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-security-ground-up#secure-infrastructure-from-the-ground-up.

[21] *See* Microsoft, Azure Security Center Detection Capabilities, available at https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities.

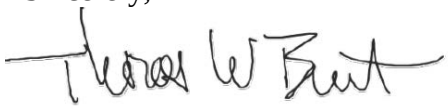
[22] *See* Microsoft Cloud Services and Network Security, available at https://docs.microsoft.com/en-us/azure/best-practices-network-security.

IV. Conclusion

Microsoft appreciates the opportunity to provide these comments to assist NTIA and Commerce in considering the options for promoting stakeholder action against botnets and other automated threats. Microsoft believes it remains important for the government to support the public-private partnerships that are currently working to mitigate the impact of botnets, take steps to encourage more cooperation, and advocate that industry stakeholders should adopt a defense-in-depth strategy designed to address the threats posed by botnets on multiple fronts.

Microsoft is grateful for the government's outreach on these issues and would welcome continuing opportunities to work with NTIA and Commerce in considering how to address action against botnets in the future.

Sincerely,



Tom Burt
Vice President and Deputy General Counsel
Corporate, External, and Legal Affairs
Microsoft Corporation

APPENDIX

Written Testimony of
Richard Domingues Boscovich
Assistant General Counsel, Digital Crimes Unit
Microsoft Corporation

Before the
Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism

Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks

July 15, 2014

Chairman Whitehouse, Ranking Member Graham, and members of the Subcommittee, thank you for the opportunity to discuss Microsoft Corporation's approach to detecting and fighting botnets. We also thank you for your leadership in focusing attention to this complicated, but important topic. My name is Richard Domingues Boscovich, and I am Assistant General Counsel in Microsoft's Digital Crimes Unit.

Before joining Microsoft in 2008, I was an Assistant United States Attorney in the Southern District of Florida for 17 years, and served as director of that District's Computer Hacking and Intellectual Property Unit. I have witnessed the evolution of cybercrime since the infancy of the Internet, and botnets are among the most malicious online threats that I have ever seen. Botnets are groups of computers remotely controlled by hackers without their owners' knowledge or consent. Botnets infect millions of computers at a time and enable criminal enterprises to invade the privacy of unsuspecting victims and steal their identities and money.

To understand the devastating impact of botnets, we can look at how they affected one victim. Consider Eunice Power, a chef in the United Kingdom, who turned on her laptop one day to find a warning that she could not access her files unless she paid ransom to cybercriminals within 72 hours. When she failed to meet the deadline, all of her photos, financial account information, and other data were permanently deleted. As she later told a reporter, "[i]f someone had robbed my house it would have been easier."

Indeed, botnets conduct the digital equivalent of home invasions, on a massive scale. Botnet operators quietly hijack webcams to spy on people in their homes, and later sell explicit photographs of the unsuspecting victims on the black market. They use malicious software to log every keystroke that users enter on their computers—including credit card numbers, Social Security numbers, work documents, and personal emails. They send deceptive emails designed to appear as though they were sent by banks that convince consumers to disclose financial account information.

Botnets are exponentially more damaging—and efficient—than traditional computer viruses. Because a botnet gets stronger as it infects more computers, a single botnet allows a cybercriminal to commit tens of billions of illegal acts in a single day. For example, the Citadel family of botnets caused more than a half-billion dollars in economic damage worldwide before Microsoft helped disrupt it last year.

For more than a decade, Microsoft has partnered with other companies and global law enforcement agencies to battle such malicious cybercriminals. I am happy to be joined today by representatives of Symantec and the FBI, who are among our key partners in this battle and who have helped us disrupt some of the world's most malicious botnet operations. Today, I will tell you about Microsoft's approach to combatting botnets by disrupting their economic infrastructure, the legal and technical tactics that we use to identify and take down botnets, our approach to protecting consumer privacy while fighting botnets, the outstanding results that have come from our public-private partnerships, and lessons learned along the way.

Botnet Prevention Requires Cooperation between Law Enforcement and the Private Sector

We do not—and cannot—fight botnets alone. As the title of this hearing suggests, fighting botnets requires efforts from both the private *and* public sector. We routinely work with other companies and domestic and international law enforcement agencies to dismantle botnets that have caused billions of dollars in worldwide economic damage. In addition to the FBI and Symantec, we regularly work with a wide range of academics from institutions that include the Universities of California at Berkeley, Santa Cruz, and San Diego as well as the University of Washington. Industry partners include CSIS.DK, FireEye, F-Secure, Kaspersky, and Kyryus. Our joint efforts demonstrate that public-private partnerships are highly effective at combatting cybercrime. Moreover, we believe that public-private partnerships are essential to addressing the increasingly complex problems presented by cybercrime; no single individual or entity can tackle these problems alone.

To that end, we monitor evolving cybercrime threats and work closely with law enforcement on a number of initiatives to help devise and execute strategies that disrupt cybercrime threats targeting Microsoft technology, people, businesses, and critical infrastructure. Microsoft also supports governments and law enforcement by providing them with technical training, investigative and forensic assistance, and the continued development of new tools to combat cybercrime. Once Microsoft discovers a botnet and disrupts its network infrastructure, it works with Internet Service Providers (ISPs) and Computer Emergency Response Teams (CERTs) to rescue and clean computers from the control of the botnets.

Microsoft's anti-botnet program uses the civil litigation system. We believe that civil litigation remedies, including injunctions, are appropriate and effective tools for stopping the harms caused by those who use criminal botnets to violate commercial and intellectual property laws. We also believe there is a vital role for law enforcement in this fight. While Microsoft clearly does not have access to criminal enforcement tools, we work to partner with law enforcement wherever appropriate. We also try to carefully structure our operations to ensure that we

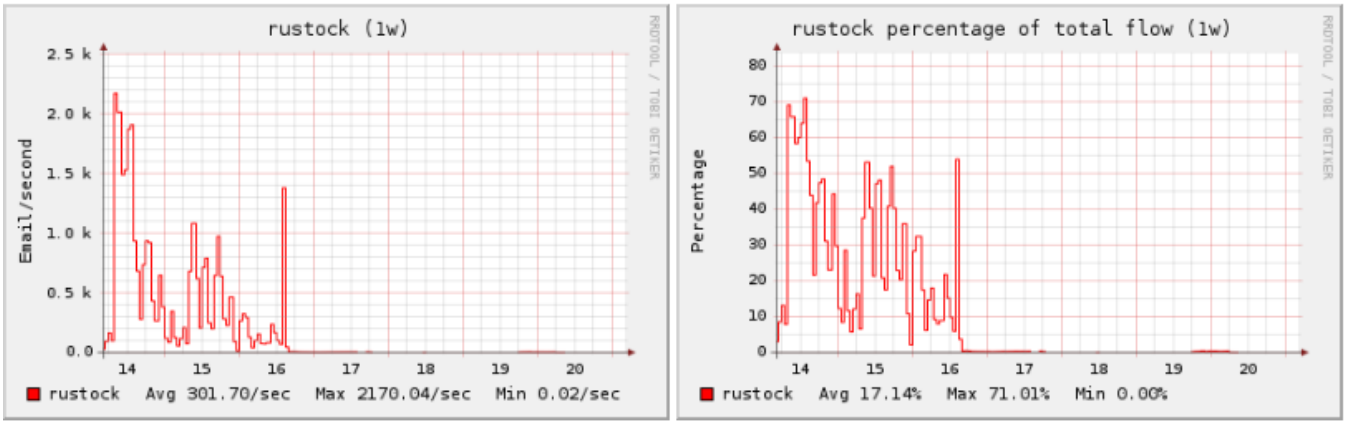
complement the efforts of law enforcement and avoid unintentionally interfering with criminal investigations or prosecutions.

Our public-private partnerships have led to significant successes. We helped to disrupt 11 botnets tied to criminal organizations committing consumer, financial, and advertising fraud, which led to the disruption of widespread criminal enterprises and the cleanup of millions of infected computers.

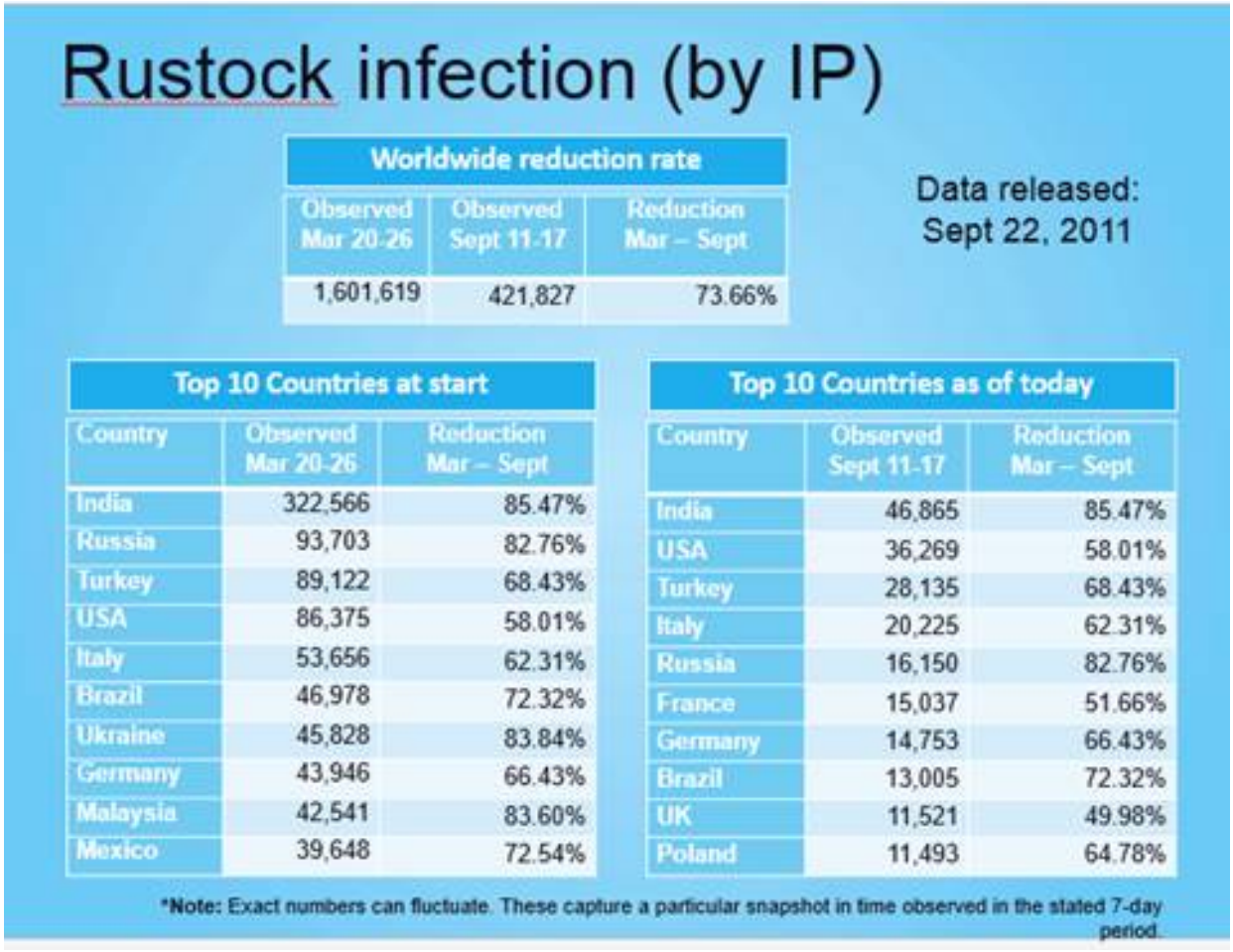
Consider the March 17, 2011 shut-down of the Rustock botnet, which at one time was responsible for approximately half of the world's spam. Microsoft worked with Pfizer, whose drugs often were the subject of Rustock spam, security experts at the University of Washington, and other law enforcement and governmental authorities, including Dutch law enforcement agencies, to dismantle this global botnet. Alex Lanstein, Senior Engineer at network security provider FireEye, said that Microsoft "did a public service" by coordinating the legal efforts to obtain control of the botnet.

The following chart shows the change in spam flow from the Rustock botnet during the week of the shut-down:

Week of Rustock Shutdown



Source: http://cbl.abuseat.org/rustock.html (visited July 11, 2014).



Rustock infection (by IP)

Worldwide reduction rate

Observed Mar 20-26	Observed Sept 11-17	Reduction Mar – Sept
1,601,619	421,827	73.66%

Data released: Sept 22, 2011

Top 10 Countries at start

Country	Observed Mar 20-26	Reduction Mar – Sept
India	322,566	85.47%
Russia	93,703	82.76%
Turkey	89,122	68.43%
USA	86,375	58.01%
Italy	53,656	62.31%
Brazil	46,978	72.32%
Ukraine	45,828	83.84%
Germany	43,946	66.43%
Malaysia	42,541	83.60%
Mexico	39,648	72.54%

Top 10 Countries as of today

Country	Observed Sept 11-17	Reduction Mar – Sept
India	46,865	85.47%
USA	36,269	58.01%
Turkey	28,135	68.43%
Italy	20,225	62.31%
Russia	16,150	82.76%
France	15,037	51.66%
Germany	14,753	66.43%
Brazil	13,005	72.32%
UK	11,521	49.98%
Poland	11,493	64.78%

*Note: Exact numbers can fluctuate. These capture a particular snapshot in time observed in the stated 7-day period.

Source: Microsoft

Similarly, last month, Microsoft and the FBI worked together to disrupt the GameOver Zeus botnet, which stole passwords via peer-to-peer technology, making it particularly difficult to track. Microsoft provided the FBI with technical analysis of the peer-to-peer network and developed a cleaning solution, as the FBI and Justice Department took control of the domains and filed criminal charges against the Russian hacker who led the botnet. As one reporter observed in an article about the disruption, "the biggest champion of the day may be collaboration between the feds and the private sector." It was this particular botnet that led to the theft of personal information that I described earlier in my testimony.

Disrupting Botnets' Economic Infrastructure

Microsoft's philosophy to fighting botnets is simple: we aim for their wallets. We disrupt botnets by undermining cybercriminals' ability to profit from malicious attacks.

At bottom, cybercriminals operate botnets to make money. Botnets are businesses, albeit illegal ones. Botnets are particularly attractive tools for criminals because they are cheap and

effective. They have a relatively low cost of entry, the marginal cost to maintain them is low, and the potential profits grow exponentially as more computers are infected.

Microsoft has seen botnets take many forms and use a wide range of tools. But a common theme among all of them is the desire to generate a profit for the botnet operators. Consider the "business models" of the most malicious botnets:

- **Zeus** botnets, a family of financial botnets that were responsible for identity theft, caused more than $70 million in financial losses, and infected more than 13 million PCs worldwide.

- **Bamital** botnet, which hijacked people's search results, taking them to potentially dangerous websites that could install malware, steal personal information, or fraudulently charge businesses for "clicks" on online advertisements. More than 8 million computers had been attacked by Bamital in the two years prior to its takedown.

- **Nitol** botnet, which used more than 500 different strains of malware to potentially target millions of innocent people and steal their personal information, including financial account data. It was discovered as part of a Microsoft study on unsecured supply chains, which found that 20 percent of PCs purchased for analysis in China from unsecure supply chains were infected with malware.

- **Rustock** botnet, which was reported to be among the world's largest "spambots," could send up to 30 billion spam email messages per day. It infected nearly 2.5 million computers worldwide.

I am proud to report that Microsoft, in partnership with other companies and law enforcement agencies worldwide, has disrupted all of these botnets—and others—and as a result has dramatically increased their costs of "doing business." By disrupting their infrastructure, we impact the bottom-line cost-benefit equation for cybercriminals. In doing so, we seek not only to protect users from the existing botnets, but to alter the financial analysis for criminals to the point that they are discouraged from establishing new botnets.

Protecting Consumers

Microsoft draws on our deep technical and legal expertise to develop carefully planned and executed operations that disrupt botnets pursuant to court-approved procedures.

Microsoft's Digital Crimes Unit ("DCU") is a team of more than 100 technical, legal and business experts that uses creative techniques and Microsoft technology to fight cybercrime and improve cybersecurity. The DCU proactively helps Microsoft customers stay ahead of new and evolving threats and challenges. Through robust partnerships and a recognition that no one company can fight cybercrime alone, DCU plays offense against online threats.

Microsoft's work in this area dates back more than a decade. In 2003, Microsoft formed a joint legal and technical team to address cybercrime, known as the Internet Safety and Enforcement Team ("ISET"), as part of Microsoft's Trustworthy Computing initiative. In 2008, ISET evolved to become the DCU, to better align with how Microsoft was tackling the evolution of cybercrime. Last year, Microsoft opened its Cybercrime Center, combining our legal and technical expertise with cutting-edge tools and technology to mark a new era in the fight against cybercrime.

The DCU uses a combination of legal and technical tactics to help fight cybercrime. In general terms, Microsoft asks a court for permission to sever the command-and-control structures of the most destructive botnets, breaking communication lines to either the domains or Internet protocol (IP) addresses that cybercriminals use to control the botnet.

Once the court grants permission and Microsoft severs the connection between a cybercriminal and an infected computer, traffic generated by infected computers is either disabled or routed to domains controlled by Microsoft. This process, known as "sinkholing," helps Microsoft collect valuable evidence and intelligence used to help notify victims that their computers are infected, as well as clean computers to remove the malicious software. These disruptions significantly impact cybercriminals' operations and infrastructure, assists victims in regaining control of infected computers and furthers investigations against cybercriminals responsible for the threat. As we execute these court orders, we work hard to avoid disrupting legitimate Internet traffic and, where necessary, we will take steps during or after implementation of a court order to achieve that goal.

As one example, in May 2013, Microsoft worked closely with the FBI to disrupt a massive cybercrime ring associated with the Citadel botnet. As part of those efforts, Microsoft asked the United States District Court in the Western District of North Carolina to grant an emergency temporary restraining order, seizure order, and an order to show cause for preliminary injunction, to help disrupt the botnet. Microsoft argued the botnet violated a number of state and federal laws, including the Computer Fraud and Abuse Act (18 U.S.C. §1030), the CAN-SPAM Act (15 U.S.C. §7704), the Electronic Communications Privacy Act (18 U.S.C. §2701), the Lanham Act (15 U.S.C. §§ 1114), the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962), and the North Carolina Computer Trespass law (N.C. Gen. Stat. §14-458), as well as the common law torts of conversion, unjust enrichment, and nuisance.

Microsoft supported this request with evidence of how the Citadel botnet worked, and of the harm it caused to infected computers. In authorizing that request, the court: (1) enjoined the operators of the Citadel botnets from continuing to operate those botnets, (2) required domain registries to redirect a list of currently-registered domain names to secure servers, (3) required domain registries to transfer a list of currently-unregistered domain names into Microsoft's control, so they could not be used for the botnet, (4) required ISPs to log all attempts to communicate with specific IP addresses associated with the botnet, and provide documentation to Microsoft showing the persons who operate those IP addresses, (5) authorized Microsoft to cause all Citadel-infected computers attempting to connect to Citadel servers to connect instead to Microsoft servers, and install a curative file that stops the harmful

acts of the botnet, and (6) authorized Microsoft to alert end-users when an infected computer attempted to connect to any Internet site, and direct them to a Microsoft or antivirus site to download curative files.

The court's order authorized Microsoft to disrupt more than 1,400 Citadel botnets that were responsible for more than half a billion dollars in losses to persons and businesses worldwide. At the same time, the FBI took coordinated separate steps related to the investigation, marking the first time that law enforcement and the private sector worked together in this way to execute a civil seizure warrant as part of a botnet disruption operation.

Transparency and Privacy are Core Values of Our Anti-Botnet Operations

Obtaining control of botnet domains is only the first step in preventing the spread of botnets and remediating the harm that they have caused. Once Microsoft receives information about a botnet, Microsoft disseminates this data to partners so that infected computers can be cleaned. Microsoft has worked in cooperation with numerous ISPs and CERTs around the world to help notify affected customers and connect them with tools to clean their devices.

Broad distribution of this information is crucial to remediating the harm that the botnets have caused, and preventing the botnets from growing. Microsoft makes information about botnets available to ISPs and CERTs through our Cyber Threat Intelligence Program ("C-TIP"). That service allows ISPs and CERTs to receive updated threat data related to infected computers in their specific country or network approximately every 30 seconds.

Last year, Microsoft and the Secretary of State of Telecommunications and Information Society of Spain announced an important agreement under which the Spanish CERT, INTECO, became one of the first organizations to receive data from the C-TIP cloud service. All the information is uploaded directly to each organization's private cloud through Windows Azure. INTECO joined the Luxembourg CERTs, CIRCL and gov CERT, as early adopters of this program. By participating in this system, organizations have almost instant access to threat data generated from previous as well as future operations conducted by the Microsoft Active Response for Security program.

The cloud-based C-TIP program represents an evolution in such information-sharing. In 2010, the original C-TIP program began sending regular emails to participating ISPs and CERTs with threat intelligence for their customers and regions. As of 2013, 44 organizations in 38 countries received these threat intelligence emails, and momentum is building for the program. The new cloud-based program dramatically increases our ability to clean computers and help us keep up with the fast-paced and ever-changing cybercrime landscape. It also gives us another advantage: cybercriminals rely on infected computers to exponentially leverage their ability to commit their crimes. If we are able to take those resources away from them, they will have to spend time and money trying to find new victims, thereby making these criminal enterprises less lucrative and appealing in the first place.

Privacy also is a fundamental value in Microsoft's anti-botnet operations. When we execute a botnet operation, we operate within the bounds of the court order. We never look at the underlying communications sent by infected computers. Instead, Microsoft only accesses the IP address used by the infected computer, so that we can help the ISPs and CERTs notify the user of the infection and assist in the remediation. We work with ISPs so they can alert their customers directly.

In addition, Microsoft makes resources available online so that consumers can help avoid becoming victims in the first place or clean infected computers. Individuals and businesses worldwide should exercise safe practices, such as running up-to-date, legitimate software. Additionally, people should use protections like firewalls and anti-virus/anti-malware programs and exercise caution when surfing the internet or clicking on ads or email attachments, as they could be malicious. More information on how to stay safe online can be found at http://www.microsoft.com/protect. People worried that their computers might be infected with malware, can obtain free information and malware cleaning tools from Microsoft at: http://support.microsoft.com/botnets.

Improving Laws to Battle Botnets

Microsoft welcomes the Subcommittee's strong interest in this growing threat, and appreciates your efforts to provide us with more tools to fight botnets. In particular, Microsoft believes that changes to two existing laws could go a long way toward battling botnets.

First, Microsoft supports amending the Computer Fraud and Abuse Act (CFAA), which long has allowed the government and private individuals to hold computer hackers responsible for unauthorized access to computers. Unfortunately, the law was enacted in 1986, long before we envisioned the command structure of botnets. In many cases, the botnet operator develops a system that enables *others* to conduct the actual hacking. Although some botnet operators have been convicted under the CFAA, we agree with the Department of Justice that the statute would be a more effective tool if it explicitly covered trafficking in access to botnets. Microsoft also agrees with the Department of Justice that Congress should amend Section 1030(a)(6) of the CFAA to eliminate the requirement of proof of intent to defraud, which in some botnet cases is difficult to demonstrate.

Finally, Microsoft agrees with the Department of Justice that Congress should amend the Access Device Fraud statute, which allows prosecutors to bring charges against the perpetrators of phishing and other credit card fraud schemes. The amendment should apply the statute to offenders in foreign countries who directly and significantly harm individuals and financial institutions in the United States. This change would provide both additional methods to disrupt phishing botnets that originate in other countries.

✧ ✧ ✧

In summary, Microsoft's participation in public-private partnerships has resulted in the disruption and shut-down of some of the most malicious threats to public trust and security on the Internet. But our work is never done, as cybercriminals develop new and more sophisticated methods to profit from the online chaos that they create. The criminals will continue to evolve and develop more sophisticated tools. So will Microsoft. We remain firmly committed to working with other companies and law enforcement to disrupt botnets and make the Internet a more trusted and secure environment for everyone.

Microsoft

CYBERSECURITY POLICY FOR THE INTERNET OF THINGS

Authors

Benedikt Abendroth
Aaron Kleiner
Paul Nicholas

Contributors

Erin English
Jim Pinter
Arjmand Samuel
Ron Zahavi

Contents

Executive summary

This paper addresses the critical task of developing cybersecurity policies for IoT, which has particular urgency because the merger of physical and digital domains in IoT can heighten the consequence of cyber attacks.

Around the world, organizations and individuals are experiencing a fundamental shift in their relationship with technology. This transformation, often called the Fourth Industrial Revolution, has been characterized by the World Economic Forum as a fusion of the physical, digital and biological worlds, with far-reaching implications for economies and industries, and even humankind.[1] These changes create new opportunities and challenges for public policymakers, as traditional governance frameworks and models will have to be reconsidered for a different world.

The Internet of Things (IoT) is a key element of global digital transformation. There is no universally agreed-on definition of IoT, perhaps in part because the term IoT does not simply describe a new type of technical architecture, but a new concept that defines how we interact with the physical world. At a high level, IoT has been described as a decentralized network of devices, applications, and services that can sense, process, communicate, and take action based on data inputs, including control of elements of the physical world.

This paper addresses the critical task of developing cybersecurity policies for IoT, which has particular urgency because the merger of physical and digital domains in IoT can heighten the consequences of cyber attacks. The cybersecurity concerns of IoT user communities—whether consumer, enterprise, or government—provide a convenient lens for identifying and exploring IoT security issues. For example, enterprises and governments may identify data integrity as a primary concern, while consumers may be most concerned about protecting personal information. Acknowledging these perspectives is just the start; the real question is what industry actors and government authorities can do to improve IoT security.

Industry can build security into the development and implementation of IoT devices and infrastructure. However, the number of IoT devices, the scale of their deployments, the heterogeneity of systems, and the technical challenges of deployment into new scenarios require an approach specific to IoT. Because this complex ecosystem depends on many players with a broad and diverse range of security concerns—manufacturers and integrators, developers, deployers, and operators—there are emerging security best practices appropriate for each of these roles.

Government can support those efforts through the development of sound policies and guidelines. As stewards of societal well-being and the public interest, governments are in a unique position to serve as catalysts for the development of good IoT security practices, build cross-disciplinary partnerships that encourage public-private collaboration and inter agency cooperation, and support initiatives that improve IoT security across borders. There is broad evidence that this is well underway as demonstrated by supporting examples of government initiatives from around the world as reference points.

[1] "The Fourth Industrial Revolution, by Klaus Schwab," World Economic Forum, https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab (last accessed April 2017).

Introduction

Digitization and the increasing connectivity between devices, citizens, and their governments continue to transform many aspects of our societies and economies in meaningful ways. Smart cities benefit from sensors that can measure air quality, traffic flow, and energy consumption. Smart manufacturing becomes the norm in Industry 4.0, where intelligent machines are networked so they can exchange and respond to data to independently manage industrial production. The Internet of Things is a transformational concept.

In 1999, Kevin Ashton, co-founder of the Auto-ID Center at the Massachusetts Institute of Technology, envisioned an Internet of Things based on RFID chips that could enable "things" to communicate with each other.[2] Since that time, declining hardware costs, miniaturization of sensors, the emergence of hyper-scale cloud computing, and the proliferation of Internet connectivity have created an environment where IoT usage can grow at a geometric rate. Estimates vary, but some have projected that they will nearly double in the next three years from about 28 billion devices today, to more than 50 billion by 2020.[3]

It is not just the sheer number of IoT devices that will have an impact, but how they connect the physical and cyberworlds. IoT breaks the confines of traditional computer networks and establishes connections directly with objects in the physical world. The core concept of this phenomenon is that IoT allows for "things" to connect to the Internet, ranging from the significant—airplanes, elevators, solar panels, medical equipment—to the mundane—toys, soap dispensers, and porch lights.

To the extent that IoT is an extension of current platforms and networks, many of the same risks to the confidentiality, integrity, and availability of data still apply. However, many connected devices will be deployed into environments with older legacy systems that cannot be easily managed and updated, or they may fall under multiple regulatory jurisdictions with different requirements, or into consumer environments with fewer resources for significant security management.[4]

These challenges provide ample reason to bring governments and the technology industry together to increase the security of IoT networks and devices generally, and to ensure an adequate security baseline that addresses all IoT elements. This paper offers an overview of the security challenges related to IoT and provides guidance on the roles that both industry and government can play in ensuring its security and building a foundation of trust in the Internet of Things.

---

[2] Kevin Ashton, "The 'Internet of Things' Thing," *RFID Journal* (June 22, 2009), http://www.rfidjournal.com/articles/view?4986

[3] "Internet of Things (IoT): number of connected devices worldwide from 2012 to 2020 (in billions)," Statista, accessed April 2017, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide

[4] The President's National Security Telecommunications Advisory Committee (NSTAC) Report to the President on the Internet of Things, Nov. 19, 2014, Appendix E, https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf

What exactly is the Internet of Things?

There is no universally agreed-on definition of IoT, perhaps in part because the term IoT does not simply describe a new type of technical architecture, but a new concept that defines how we interact with the physical world.

The US National Security and Telecommunications Advisory Committee (NSTAC) has defined IoT based on three shared common principles: [5]

Devices
Devices within a network are instrumented so they can be addressed individually.

Platform
Devices are interconnected by way of a shared platform, such as a cloud service.

Intelligence
Devices may perform functions adaptively, on their own or with other devices and applications, based on programming and inputs from the physical world.

[5] NSTAC Report, page 3.

Security concerns about the Internet of Things from a user perspective

The cybersecurity concerns of IoT user communities will differ. But these concerns provide a convenient lens for making sense of the IoT security issues, and can help policymakers develop an understanding of how different users frame and express their IoT security concerns. Empathizing with the user's perspective enables more responsive policy approaches, and helps calibrate guidance and requirements so that they effectively address security concerns without limiting IoT innovation.

Therefore, we propose a framework organized by the three core groups of users—consumers, enterprises, and governments—and provide an illustrative (though not exhaustive) view into how they use IoT.

Consumers

Consumer IoT users may use connected devices in their homes, automobiles, clothing and accessories, and other aspects of their daily lives. Typically, consumer-level IoT uses are characterized by:

- Individuals or groups of users that use shared hardware with relatively limited computing power. For example, several members of a family may share the same Internet-connected device, such as a television or a security system where people share a common account or might have their own accounts.
- Engagement with user-generated data and machine-generated insights through a cloud-based application delivered on websites and small-screen devices. Users may, for instance, track their physical activities through wearable sensors and then use an application for insights into their fitness gleaned from the sensors.
- Sensitive data shared by the user to generate value out of the connected devices. For example, putting an Internet-connected video camera at home can help people monitor for burglars or watch their pet, even though the camera may also capture personal moments that users would not want others to see.

Security concerns in these scenarios often focus on the exposure of private activity or sensitive personal information. In some cases, governments have intervened to ensure that manufacturers implement a reasonable level of cybersecurity defense and truthfully represent security practices.

For example, in 2013 the US Federal Trade Commission (FTC) settled a complaint against a manufacturer of home video cameras that had misrepresented the products' security posture. According to the FTC, "The cameras had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address." The FTC noted that, among other poor security design choices, the manufacturer had "failed to use reasonable security to design and test its software, including a setting for the cameras' password requirement. As a result of this failure, hundreds of consumers' private camera feeds were made public on the Internet."[6]

---

[6] "Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy," Federal Trade Commission, last modified on September 4, 2013, https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles

Enterprises

Enterprises leverage IoT to improve business processes (supply chain, inventory, maintenance), enhance customer experiences (retail, delivery), and take innumerable other innovative approaches to resolving business challenges. The concept of Industry 4.0, also referred to as a technology-powered Fourth Industrial Revolution, is evidence of this trend.

For example, Rockwell Automation, a firm that provides industrial automation solutions, automated the collection and analysis of data from remote installations across the supply chain of petroleum companies.[7] Similarly, elevator company thyssenkrupp worked with Microsoft to create a line of connected intelligent sensors that monitor millions of elevators around the world in real time, enabling the company to improve their reliability and cut maintenance costs.[8]

Like consumers, enterprises are concerned with vulnerabilities and threats that could lead to compromises of privacy. But they also have other concerns, many of which stem from the challenge of managing IoT security at enterprise scale:

- Operations depend on data integrity and availability, therefore potential for data corruption by attackers can have severe consequences. For instance, a medical device could be hacked to provide false information to the doctor, or a car could receive sensor data indicating that there is no car in the adjoining lane. In addition, ransomware can be particularly damaging to enterprises with its resulting denial of access to data.
- Traditional cybersecurity threats can be significantly more powerful because of IoT, such as distributed denial of service (DDoS) attacks that can make an online service unavailable by overwhelming it with traffic from multiple sources. For example, when an IoT deployment on a college campus was compromised, thousands of connected devices were turned against the campus's own network in a DDoS attack.[9]
- Managing security updates in always-on scenarios such as production environments that operate around the clock 365 days a year, where temporary shutdowns for security updates may cause significant disruptions to system availability.
- Whether the cloud services supporting IoT can demonstrate compliance with international standards, such as ISO 22301 for business continuity management, ISO/IEC 27001 for information security management, and ISO/IEC 27018 for data privacy in the cloud.[10]

As IoT continues to gain traction in the enterprises, questions of security are top of mind for business decision makers. Many enterprises are struggling to determine how secure their end-to-end IoT infrastructure is, and some of them even delay the implementation of IoT technologies until best practices and standards can be established and confirmed. One method to move forward with an IoT deployment is to conduct security evaluations of an entire IoT stack, including the security capabilities of connected devices, to gain insights into potential vulnerabilities.[11]

---

[7] "Fueling the Oil and Gas Industry wih IoT," Microsoft Corporation, last modified on December 4, 2014, https://blogs.microsoft.com/iot/2014/12/04/fueling-the-oil-and-gas-industry-with-iot

[8] "Microsoft HoloLens enables thyssenkrupp to transform the global elevator industry," Microsoft Corporation, last modified on September 15, 2016, https://blogs.windows.com/devices/2016/09/15/microsoft-hololens-enables-thyssenkrupp-to-transform-the-global-elevator-industry/#xULXoLwKMCjvkm2J.97

Governments

Given the breadth of societal roles that governments fulfill, their uses for IoT may be even more diverse than those of enterprises. The many areas in which governments see potential applications of IoT span from e-governance that uses technology to improve services for citizens to environmental protection using sensors to monitor the bacterial levels of rivers and lakes. Smart cities have given rise to a broad range of IoT-powered scenarios that rely on connected devices and sensors—for example, connected street lamps that not only provide light but also measure environmental factors —that will change how city officials deliver services, and how municipal government and citizens interact in the physical world.

Governmental concerns about IoT security are likely to be similar to those of enterprises, but with particular scrutiny given to key areas:

- Meeting baseline security requirements for government through standardized processes, like FedRAMP, the US federal government's program to authorize cloud services for US government agencies.
- Resilience against threats directed at government infrastructure, such as nation-state attacks that rely on deep network penetration to undermine functionality, compromise data, and cause other negative impacts.
- The duration of security support for IoT products and services, ensuring that a product's end of support (or end of life) is sufficiently predictable for long-range planning.

Government reliance on IoT has already been tested in high-profile situations. For example, the San Francisco Municipal Transit Agency experienced a ransomware attack in November 2016 that shut down its ability to collect fares. Fortunately, because the agency had backed up its data, no ransom was paid and the systems were quickly restored to normal.[12]

As these examples demonstrate, the IoT is subject to an array of security challenges that could limit development and slow progress toward broad usability. Both industry and government have roles to play in addressing these challenges. Industry can build security into the development and implementation of IoT devices and infrastructure, and government can support those efforts through the development of sound policies and guidelines.

---

[9] "IoT Calamity: the Panda Monium," Data Breach Digest, Verizon, 2017, http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-sneak-peek_xg_en.pdf

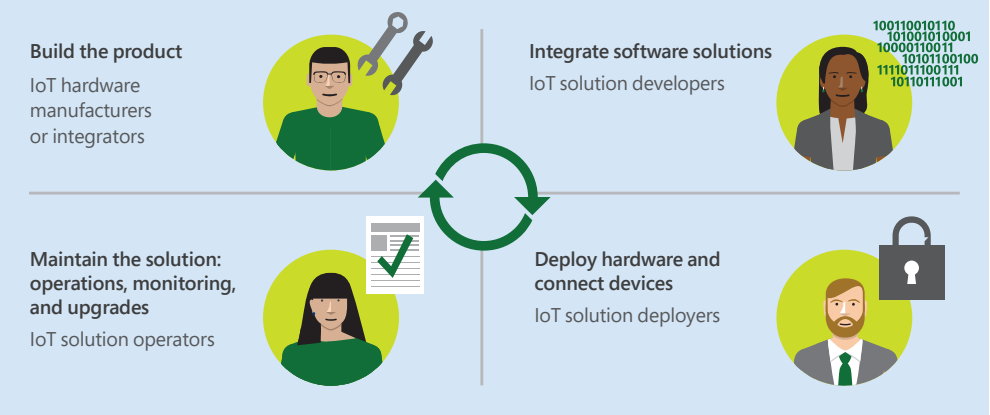
[10] For example, the Microsoft Azure IoT Hub was recently awarded nine industry-leading certifications to demonstrate the company's commitment to supporting users with their compliance needs. https://blogs.microsoft.com/iot/2016/12/07/azure-iot-hub-awarded-9-industry-certifications-for-public-cloud-computing/

[11] For instance, Microsoft announced the Security Program for Azure IoT, which brings together a curated set of security auditors customers can choose from to perform a security audit on their IoT solutions. https://blogs.microsoft.com/microsoftsecure/2016/10/26/securing-the-internet-of-things-introducing-the-security-program-for-azure-iot/

[12] "San Francisco Rail System Hacker Hacked," Krebs on Security, last modified on November 16, 2016, https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked

Industry: Enhancing IoT security through a role-based approach

The IoT ecosystem depends on several key roles - manufacturers and integrators, developers, deployers, and operators. The graphic below outlines these roles and their contribution to the IoT ecosystem.



One way to grasp the security issues each role must address is to examine appropriate security practices for each one. At Microsoft, our experience with IoT networks has helped us identify best practices relevant to each of these roles. While they are not intended as direct recommendations for policy initiatives, they can help policymakers understand the complexity of the IoT ecosystem and how security responsibilities can be distributed across it.

IoT hardware manufacturers or integrators

These are the manufacturers of IoT hardware, integrators assembling hardware from various manufacturers, or suppliers providing hardware for an IoT deployment manufactured or integrated by other suppliers. Microsoft recommends several practices to secure IoT hardware:

- **Scope hardware design to minimum requirements.** To avoid opening the device to unwanted attack vectors, hardware design should include the minimum features required for operation of the hardware and nothing more. For example, include USB ports only if necessary for the operation of the device as unnecessary access points can enable attackers.
- **Make hardware tamper-proof.** Build mechanisms that can detect physical tampering, such as opening the device cover or removing a part of the device, and send an alert as part of the data stream uploaded to the cloud.
- **Build security into hardware.** Build security features such as encrypted storage or integration of cryptographic keys into devices.
- **Make upgrades secure.** Firmware upgrades during the lifetime of the device are inevitable. Building devices with secure upgrade paths and cryptographic assurance of new firmware versions will help ensure device security during and after upgrades.

IoT solution developers

Developers of IoT solutions are typically either part of an in-house team or a system integrator who specializes in this activity. They may develop various components of the solution from scratch, integrate off-the-shelf or open-source components, or adopt preconfigured solutions with minor adaptations. To secure IoT solutions, Microsoft recommends the following practices:

- **Follow secure software development methodology.** Development of secure software requires end-to-end thinking about security from the inception of the project, including choice of platform, language, and tools, to its implementation, testing, and deployment. For example, the Microsoft Security Development Lifecycle provides a step-by-step approach to building secure software.[13]
- **Choose open-source software judiciously.** Open-source software can enable quick development of solutions. However, when choosing open-source software, consider the activity level of the community for each component. Look for an established community that actively supports its software and is responsive to addressing vulnerabilities and other issues that are uncovered.
- **Integrate with care.** Many software security flaws exist at the boundary of libraries and application program interfaces (APIs). Functionality that may not be required for the current deployment might still be available via an API layer, so make sure to check for security flaws at all interfaces of components being integrated.

IoT solution deployers

Deployment involves setting up hardware, connecting devices, and installing software in devices or in the cloud. Use these best practices for more secure deployments:

- **Install hardware securely.** IoT deployments may require hardware to be installed in unsecure or unsupervised locations such as public spaces. In those situations, the deployer must ensure the hardware is protected from tampering. For example, if USB or other ports are available on the hardware, make sure that they are covered securely to keep attackers from using them as entry points.
- **Keep authentication keys safe.** Each device requires an ID and associated authentication keys generated by the cloud service. Keep these keys physically safe even after deployment; a criminal can use a compromised key to impersonate an existing device andsend false data to the operator.

[13] Microsoft Security Development Lifecycle, https://aka.ms/msSDL

IoT solution operators

Once deployed, IoT solutions require monitoring, upgrades, and maintenance. This is most often done by an in-house team of IT specialists, hardware operations and maintenance teams, and domain specialists who monitor the behavior of the overall infrastructure. These best practices will help maintain the security of devices over the long term:

- **Keep the IoT system up to date.** Ensure that device operating systems and all device drivers are upgraded to the latest versions. Microsoft provides automatic updates for its operating systems including Windows 10; other operating systems, such as Linux, may offer this service, or organizations may need to schedule updates themselves.
- **Protect against malicious activity.** If the operating system permits, install the latest anti-virus and antimalware software on each device to help protect against external threats. Make sure that these are updated regularly.
- **Audit frequently.** Audit IoT infrastructure for security-related issues on a regular basis. Most operating systems build in event-logging that must be reviewed frequently to assess the state of the network, including whether security incidents have occurred.
- **Protect the physical IoT infrastructure.** Security attacks against IoT infrastructure can be launched using physical access to devices, for example, the malicious use of USB ports. Logging physical access is a key way to help uncover these physical breaches.
- **Protect cloud credentials.** Cloud authentication credentials used for configuring and operating an IoT deployment can also be a way for a bad actor to gain access and compromise an IoT system. Secure and user-friendly authentication for the user can mitigate the risk of credential theft and account compromise, such as multi-factor authentication or biometrics.

Government: Advancing IoT security through policy

As stewards of societal well-being and the public interest, governments have a special role to play in delivering the vision of a secure IoT and supporting its development. Governments also have unique capabilities to convene stakeholders to address shared challenges, promote best practices through guidance, and intervene as regulators. Indeed, governments around the world have leveraged these capabilities in different ways to address the growth of IoT.

Microsoft offers several recommendations to help governments develop policies that advance IoT security. Governments can:

- Serve as catalysts for the development of good IoT security practices.
- Build cross-disciplinary partnerships that encourage public-private collaboration and inter-agency cooperation.
- Support initiatives that improve IoT security across borders.

We also include supporting examples of government initiatives from around the world as reference points. Given the nascent state of IoT policy development, this will help governments learn from each others' approaches and perspectives as their IoT initiatives move forward.

Encourage the use of good IoT security practices

Raise awareness of best security practices and guidelines

Not every business has the knowledge and expertise to make smart decisions about security when developing and deploying IoT devices and services. Governments can enable better security outcomes by promoting best practices that range from security-by-design principles to sector-specific product development and risk assessment guides.

Examples

- The US Department of Homeland Security offers broad guidance on improving security in the design, manufacture, and deployment of IoT devices. This guidance is not limited to a particular sector and is not regulatory in nature, which makes it accessible to audiences across the IoT ecosystem.[14]
- The Internet and Security Agency of the Government of Korea published a guide that identifies 15 security principles for the development of IoT devices. They cover the whole lifecycle from their design and development to their installation and operation (and ever retirement). The government plans to update this security guidance as IoT technology evolves. [15]

---

[14] Strategic Principles for Securing the Internet of Things, US Department of Homeland Security, November 15, 2016, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[15] "IoT Common Security Guide," Korea Internet Security Agency, last modified on October 6, 2016, https://www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=1&mode=view&p_No=259&b_No=259&d_No=80&ST=&SV (Korean).

Develop enhanced guidance for safety critical sectors

Greater investments in cybersecurity and system resilience apply in particular to devices that support human life, critical infrastructure, transportation, and other essential functions, whose inability to function and lack of resilience could have dire consequences.

Examples

- The US Food and Drug Administration has issued guidance to encourage management of cybersecurity vulnerabilities for medical devices that are already on the market.[16] In particular, it supports limiting the impact of cybersecurity incidents on devices, thereby reducing patient risk by applying the NIST Framework for Improving Critical Infrastructure Cybersecurity.[17]
- In Japan, the National Center of Incident Readiness and Strategy for Cybersecurity recommends measures to protect against the physical consequences of compromises in or breaches of IoT security, such as when safety concerns flow as potential consequences from cybersecurity concerns. It highlights that IoT security incidents can have impact in the physical world, for instance through large machines that could harm workers operating them, and should be addressed appropriately.[18]

Invest in IoT security training, education, and raise public awareness

Government investments in workforce development and awareness-raising campaigns can help increase the scale and impact of industry-led efforts.

Examples

- Building the IoT ecosystem will depend on a knowledgeable workforce. There are a number of steps that governments can take to encourage schools, universities, and training programs to adopt curricula that advance the knowledge of information security in general and IoT security specifically. The UK Government Office for Science, as one of is ten recommendations for government policymakers, includes promoting the integration of computational thinking in the curricula of schools and training programs.[19]
- The US Federal Trade Commission, drawing on lessons learned from its own data security cases, has developed a business education initiative, "Start with Security," which gives enterprises of all sizes ten effective security measures they can take to protect their data.[20]

---

[16] Postmarket Management of Cybersecurity in Medical Devices, US Food and Drug Administration, December 28, 2016, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[17] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (NIST), February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[18] General Framework for Secure IoT Systems, National Center of Incident Readiness and Strategy for Cybersecurity, Government of Japan, August 26, 2016 https://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf

[19] The Internet of Things: making the most of the Second Digital Revolution, UK Government Office for Science, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

What about certifying or labeling IoT devices based on security?

The primary goal of a certification program should be to improve security by providing more information to consumers and incentivizing the broader IoT marketplace. Organizations have called for a certification or product labeling approach to IoT device security. The U.S. Presidential Commission on Enhancing National Cybersecurity called for the creation of a cybersecurity "nutritional label" to inform consumer purchasing decisions.[21] Similarly, the European Commission has contemplated a Trusted IoT Label and the establishment of minimum security baselines for IoT devices.[22]

An effective IoT device security certification or labeling program should embrace three key principles:

- **Informed by a robust multistakeholder consultative process.** Stakeholders from across the IoT ecosystem should be integrated into an open and transparent process for developing a certification program. Device manufacturers, software providers, user advocates, and security researchers are among those who should be included along with government representatives.
- **Aligned with international standards.** Certification programs should align with international standards and standardization efforts, not duplicate or contradict them. For example, the OPC Foundation already operates a certification process for its industrial interoperability standard.
- **Flexible implementation.** IoT deployments vary widely. There should be flexibility in how adherence to a certification program is communicated to consumers, whether on a box, website, or other means.

[20] "Start with Security: A Guide for Business," US Federal Trade Commission, June 2015, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[21] Report on Securing and Growing the Digital Economy, Commission on Enhancing National Cybersecurity, 2016, https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

[22] "Commission Staff Working Document, Advancing the Internet of Things in Europe," European Commission, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0110

Build cross-disciplinary partnerships to enhance IoT security

Encourage collaboration between the public and private sector

IoT policy issues are often driven by IoT's unprecedented scale, which can impact a diverse range of stakeholder groups in new ways. For example, realtors may face new challenges in marketing and selling a smart home if its connected elements cannot easily be transferred over to a new owner, while retailers may grapple with how compromised IoT devices impact customer satisfaction and loyalty. Including a broadly representative group of stakeholders can be particularly useful in developing, updating, and maintaining IoT security guidance.

Examples

- The German Plattform Industrie 4.0 convened more than 100 private and several public-sector organizations to create a framework and recommendations for how to implement and manage the digitization of industrial manufacturing, including its security. As part of the network, one working group on the security of networked systems is addressing the implications of cyber attacks on the production process, and offering guidance for small and medium-sized companies on how to secure their infrastructure.[23]
- The US Department of Commerce has created a multi-stakeholder process to address the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things. Their goal is to foster a more security-focused IoT market, particularly with respect to support for security updates and product patching.[24]

Create an interagency task force to coordinate security efforts

The impact of breakdowns in cybersecurity cuts across organizational boundaries, so creating an interagency or inter-ministerial IoT task force can balance perspectives on security and risk management. Such a task force could develop policies and coordination efforts that address these cross-organization security issues.

---

[23] "The background to Plattform Industrie 4," Germany Federal Ministry for Economic Affairs and Energy, 2017, http://www.plattform-i40.de/I40/Redaktion/EN/Standardartikel/plattform.html

[24] Multistakeholder Process on Internet of Things Security Upgradability and Patching, US National Telecommunications and Information Administration, September 2016, https://www.ntia.doc.gov/files/ntia/publications/2016-22459.pdf

[25] Eric Wood, "The Internet of Things can't work without cooperation," Microsoft Corporation, January 29, 2015, https://blogs.microsoft.com/work/2015/01/29/internet-things-cant-work-without-cooperation/#sm.0011nu14713g1fjexb2137e347suk

[26] Industrial Internet of Things: Unleashing the Potential of Connected Products and Services, World Economic Forum, January 2016, http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

[27] "What is OPC?," OPC Foundation, last accessed April 2017, https://opcfoundation.org/about/what-is-opc

[28] "Security Check Performed by German Federal Office for Information Security," OPC Foundation, June, 2016 http://opcconnect.opcfoundation.org/2016/06/bsi-security-check

[29] "About ENISA," European Union Agency for Network and Information Security, last accessed April 2017, https://www.enisa.europa.eu/about-enisa

Support initiatives that improve IoT security across borders

Promote the development of secure, open, consensus-based standards

As new IoT technologies develop, there will be an increasing need to ensure interoperability between new IoT systems and legacy technology systems. Without commonly accepted standards, IoT could potentially fall short of the promise of a connected world.[25]

The World Economic Forum reports that one of the greatest barriers to IoT adoption by many businesses is a lack of interoperability, which can significantly increase complexity and cost.[26] While some Internet protocols can be adopted from existing standards, IoT has specific security requirements that must be addressed separately. Governments can encourage the development of open, voluntary, consensus-based, and globally relevant standards that foster greater interoperability.

Examples

- In the manufacturing sector, the OPC Foundation developed the open-source OPC Standard that companies can follow to help enable the secure exchange of data in automated industrial settings.[27] (The OPC Foundation includes many of the world's largest automation and industrial suppliers, including Microsoft.) After performing a check of the OPC Unified Architecture's (UA) security functions, the German Federal Office for Information Security confirmed it was designed with security in mind and no systemic security vulnerabilities were found.[28]

Harmonize approaches to IoT security across national borders

Manufacturers of IoT devices want to market their devices worldwide, no matter where the underlying code was developed or the devices were manufactured. Governments are in a position to reduce the possible costs for small and medium-size IoT manufacturers to meet IoT security requirements by harmonizing them across countries.

Examples

- The European Union Agency for Network and Information Security (ENISA), a center of expertise for cybersecurity in the EU, is advising member states, countries outside the EU, and the private sector on cybersecurity issues.[29] Based on recent trends of critical infrastructures implementing an increasing number of IoT technologies, ENISA also offers guidance for specific user groups, such as Smart Cars, Smart Homes, Smart Airports and Smart Cities across the EU.[30]
- The Alliance for Internet of Things Innovation, launched by the European Commission and several IoT players, is facilitating the dialogue between several IoT stakeholders to establish a thriving IoT ecosystem across the EU. In its report on policy issues, working group four provides recommendations on how governments can leverage existing efforts, such as the Network and Information Security Platform or the NIST Cyber Physical System Public Working group, as well as security-by-design and best development practices amongst others.[31]

---

[30] "IOT and Smart Infrastructures," ENISA, last accessed April 2017, https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures

[31] Report AIOTI Working Group 4 - Policy, Alliance for Internet of Things Innovation (AIOTI), October 15, 2015, https://aioti-space.org/wp-content/uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf

Conclusion

Securing IoT requires collaboration – across borders, sectors, and organizations – with a sense of urgency. However, the relevant stakeholders, implications of potential policies, and indeed, the relevant technologies themselves are still evolving. Policymakers must therefore take a long-range view of problems and solutions, while moving with agility in the face of a changing landscape.

Dialogue is the most important ingredient for meaningful progress in IoT cybersecurity policy. Policymakers have significant opportunities to create spaces where challenges can be explored and solutions identified, whether through public consultations led by governments or non-governmental organizations, collaboration across stakeholders towards common frameworks or standardized approaches, or other forums. These processes can increase understanding of different perspectives and ultimately lead to policy proposals that are relevant to key constituencies and supported by them.

Looking forward, cybersecurity policy for IoT will only increase in importance as the world grows more connected. The IoT user communities noted in this paper – consumers, enterprises, and governments – will face new security challenges stemming from IoT, including situations where users may not even be aware that they are interacting with a connected device. Addressing these scenarios requires careful consideration of how to balance security needs with opportunities for innovation.

Microsoft looks forward to supporting the growth of a secure IoT ecosystem through advancements in technology and policy, in partnership with stakeholders from across the public and private sectors.


Microsoft