The need for a Digital Geneva Convention

Posted February 14, 2017 by Brad Smith - President and Chief Legal Officer

Brad Smith at RSA 2017: The Need for a Digital Gen..

This year's RSA Conference in San Francisco brings the world's security professionals together to discuss cybersecurity at a critical time. The past year has witnessed not just the growth of cybercrime, but a proliferation in cyberattacks that is both new and disconcerting. This has included not only cyber-attacks mounted for financial gain, but new nation-state attacks as well. As engineers and other employees across the tech sector meet in San Francisco, we need to ask ourselves what our response should be.

Featured Posts

Microsoft joins House Veterans subcommittee on economic opportunity for a learning roundtable

We know that we all have more to do to ... *Read more »*

Inspiring Girls to Stay in STEM and #MakeWhatsNext

As a new college graduate, my first job was to ... *Read more »*

Largest industry-funded research cooperative draws on Cascadia corridor to advance solutions to urban challenges

The cities of Vancouver and Seattle share many strengths: a ... *Read more »*

Stay Connected

Have the latest posts sent right to your inbox. Enter your email below.

Email Addı SUBS

Popular Posts

We should start by acknowledging that no single step by itself will be sufficient to address this problem. Of course, each of our companies needs to continue to do more to protect and defend our customers around the world, and at Microsoft we're focused on doing precisely that. So are others across the industry. But in addition, the time has arrived to call on the world's governments to implement international rules to protect the civilian use of the internet.

Transcript of Keynote Address at the RSA Conference 2017
"The Need for a Digital Geneva Convention"

Brad Smith
President
Microsoft Corporation

San Francisco, California
February 14, 2017

BRAD SMITH: Good morning. As we've already heard this morning, we come together in San Francisco at a remarkable time. We live in a world of constant and at times turbulent change.

And when we think about the issues that we're here to talk about this week, when we think about cybersecurity, we are clearly dealing with a growing problem – a problem in need of new solutions.

I would like to take a few minutes this morning to ground ourselves in the problem and then talk together about some of the solutions I believe we have the opportunity to pursue together.

But let's start with the problems. The problems are clear. We see them everywhere. We see them in the

Transcript of Brad Smith's Keynote Address at the RSA Conference 2017.

Just as the Fourth Geneva Convention has long protected civilians in times of war, we now need a Digital Geneva Convention that will commit governments to protecting civilians from nation-state attacks in times of peace. And just as the Fourth Geneva Convention recognized that the protection of civilians required the active involvement of the Red Cross, protection against nation-state cyberattacks requires the active assistance of technology companies. The tech sector plays a unique role as the internet's first responders, and we therefore should commit ourselves to collective action that will make the internet a safer place, affirming a role as a neutral Digital Switzerland that assists customers everywhere and retains the world's trust.

A growing problem in need of new solutions

The bad news starts with the fact that 74 percent of the world's businesses expect to be hacked each year.[1] The estimated economic loss of cybercrime is estimated to reach $3 trillion by 2020. Yet as these costs continue to climb, the financial damage is overshadowed by new and broadening risks.

Perhaps most disconcerting, recent years have witnessed the expansion of nation-state attacks. The Sony attack by North Korea in 2014 was not the first nation-state attack, but it

Safety, privacy and the Internet paradox: solutions at hand and the need for new trans-Atlantic rules

Today at the Center for European Policy Studies, Brad Smith, … *Read more »*

Is life online stifling young people's self-expression?

Young people have been cautioned: For years, they've been told … *Read more »*

White House endorses student privacy pledge in call for comprehensive privacy reform

Today, I had the privilege of listening to the president's … *Read more »*

Latest Tweets

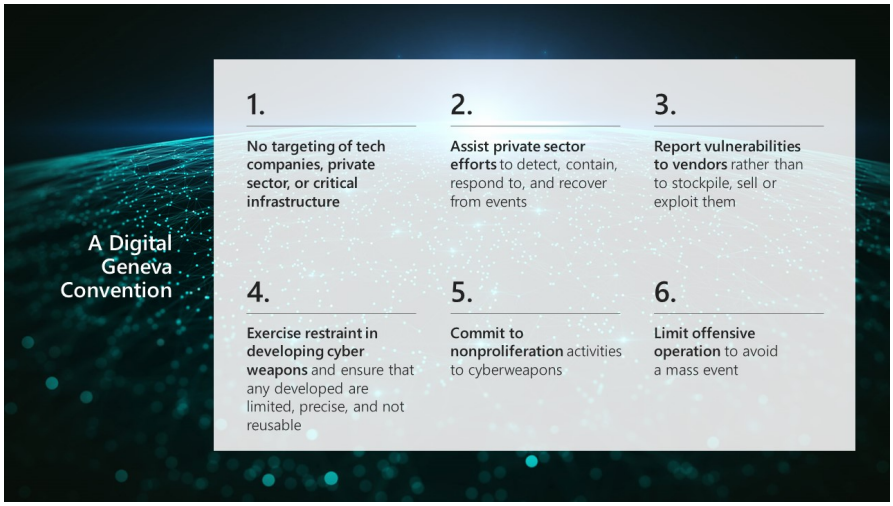
RT @MicrosoftIP: Check out how MSFT is partnering with automakers like @Toyota to power the digital transformation of connected car https:/…

RT @Microsoft She could be the one to crack the code or find the cure. #MakeWhatsNext https://t.co/kO1A5NhfJa

World Water Day 2017 – Transforming the Way the World Uses Water: https://t.co/VPqzFjvHe4

MT @MicrosoftSV Celebrating #WomensHistoryMonth with #WomenInTech — A Letter to

represented a visible turning point. While prior attacks had focused on economic and military espionage, the Sony attack in 2014 involved retaliation for free expression in the form of a (not very popular) movie. It was followed in 2015 by even more visible international discussion about nation-state attacks aimed at the theft of companies' intellectual property. And last year the issue broadened again to include hacking incidents connected to the democratic process itself.



Responding to the rise in nation-state cybersecurity attacks

We suddenly find ourselves living in a world where nothing seems off limits to nation-state attacks. Conflicts between nations are no longer confined to the ground, sea and air, as cyberspace has become a potential new and global battleground. There are increasing risks of governments attempting to exploit or even weaponize software to achieve national security objectives, and governmental investments in cyber offense are continuing to grow.

In fundamental ways, this new plane of battle is different from those of the past. It starts with the fact that cyberspace does not exist in a clearly tangible form in the physical world. But beyond this, cyberspace in fact is produced, operated, managed and secured by the private sector. Governments obviously play all sorts of critical roles, but the reality is that the targets in this new battle – from submarine cables to datacenters, servers, laptops and smartphones – in fact are private property owned by civilians.

There's an additional consequence that results from all this. The tech sector today operates as the first responders to nation-state attacks on the internet. A cyber-attack by one nation-state is met initially not by a response from another nation-state, but by private citizens.

The situation has also worsened in one additional and important way. For two-thirds of a century, since 1949, the world's nations have recognized through the Fourth Geneva Convention that they need to adhere to rules that protect civilians in times of war. But nation-state hacking has evolved into attacks on civilians in times of peace.

This is not the world that the internet's inventors envisioned 25 years ago. But it's the world that we inhabit today. And as the private citizens thrust into this challenge, the question for all of us in the tech sector is what we will do to address it.

Stronger individual tech sector responses

Microsoft, like companies across the tech sector, is aggressively taking new steps to better protect and defend customers, including from nation-state attacks. This includes new security features at every level of the technology stack, reflecting the $1 billion that we're spending annually in the security field.

Email is currently at the heart of the cybersecurity battle, as an estimated 90 percent of all hacking begins with an email phishing attack. Reflecting this importance, last year we added Advanced Threat Protection for Microsoft Exchange Online. This identifies recognizable malware and suspicious code patterns in emails and stops them before they can do damage. We then added Office 365 Threat Intelligence to provide enterprises with information on the top targeted users, malware frequency and security recommendations related to their business. And last week we added new data governance features for Office 365 that include alerts that will be sent automatically to users when someone attempts to copy and download their inbox. We'll be adding new features and offers in the coming months that provide additional protection.

In many ways, however, security-related product features are just the start. Data analytics and machine learning have become game-changing defense mechanisms for detecting nation-state attacks. Microsoft's datacenters are connected to over a billion computing end points and receive over a trillion data points every day. Advanced Threat Protection alone processes 6 billion emails each day. This provides the foundation for world-class early warning systems to detect cybersecurity attacks.

Within Microsoft we've forged a unique, internal three-part partnership as part of the 3,500 security professionals from

across the company. The Microsoft Threat Intelligence Center (MSTIC) is our reconnaissance arm, combing through the constant stream of data from our more than 200 cloud services and third-party feeds. Using machine learning, behavioral analysis and forensic techniques, this dedicated team creates a real-time picture – a security intelligence graph – of cyber activity related to advanced and persistent threats to Microsoft and our customers.

When a threat is detected, MSTIC alerts our Cyber Defense Operations Center (CDOC), an "eyes on glass" command center staffed 24 hours a day, seven days a week by rotating teams of security and engineering professionals from across our product and services portfolio. This team of specialists serves as our frontline, taking immediate action against threats to defend our own systems and protect customers.

As we identify threats, we're not only working with customers, but using legal process, led by our Digital Crimes Unit (DCU), to respond in new and innovative ways that disrupt attacks, including those launched by nation states. Last year MSTIC identified an attack pattern that led to a group associated with a nation-state that had registered internet domains using names that included Microsoft and other companies' trademarks. We went to federal court, obtained court orders and successfully sought appointment of a Special Master to oversee and expedite additional motions in our case. Working under this judicial supervision, we can notify internet registries whenever this group registers a fake Microsoft domain and request that control of that domain be transferred immediately to a sink-hole operated by DCU.

Using this novel approach, we can disrupt the nation-state's use of these domains within 24 hours. Since last summer, in response to extended nation-state attacks, we have taken down 60 domains in 49 countries spread over six continents. In each instance we stopped the flow of data to the hackers from any customers whose computers were hacked, we notified the customers of the nation-state attack and we helped them clean their environment and increase their security.

Across the tech sector, companies are racing to provide stronger cybersecurity protection for customers, including from nation-states. Each of our advances is making an important contribution. But we're nowhere close to being able to declare victory. Governments are increasing their investments in offensive cyber capabilities. We therefore need to recognize a

critical truth – this is not a problem that we can solve solely with each of us acting alone.

Calling on governments to do more

The time has come to call on the world's governments to come together, affirm international cybersecurity norms that have emerged in recent years, adopt new and binding rules and get to work implementing them.

In short, the time has come for governments to adopt a Digital Geneva Convention to protect civilians on the internet.

The foundation for new and international rules is now in place. Over the last two years there has been important progress in developing global cybersecurity norms. For example, in July 2015 governmental experts from 20 nations recommended cybersecurity norms for nation-states "aimed at promoting an open, secure, stable, accessible and peaceful ICT environment."[2] These include key principles that bar governments from engaging in malicious activity using information and communications technology or similarly damaging other nations' critical infrastructure.

Importantly, leading governments have also proven that they can address these issues through direct and frank bilateral discussions. Following highly visible and even challenging negotiations, in September 2015 the U.S. and China agreed to important commitments pledging that neither country's government would conduct or support cyber-enabled theft of intellectual property.[3] This paved the way for the Group of 20 to affirm the same principle more broadly at its meeting just two months later.[4] And additional inter-governmental discussions are continuing to progress further today.

All of this points the way to potential new steps ahead. First, there is a new opportunity for vital bilateral action. Just as the United States and China overcame mutual challenges and made important progress in 2015 to ban intellectual property cyber-theft, the United States and Russia can hammer out a future agreement to ban the nation-state hacking of all the civilian aspects of our economic and political infrastructures.

Second, governments around the world should pursue a broader multilateral agreement that affirms recent cybersecurity norms as global rules. Just as the world's governments came together in 1949 to adopt the Fourth

Geneva Convention to protect civilians in times of war, we need a Digital Geneva Convention that will commit governments to implement the norms that have been developed to protect civilians on the internet in times of peace.

Such a convention should commit governments to avoiding cyber-attacks that target the private sector or critical infrastructure or the use of hacking to steal intellectual property. Similarly, it should require that governments assist private sector efforts to detect, contain, respond to and recover from these events, and should mandate that governments report vulnerabilities to vendors rather than stockpile, sell or exploit them.

In addition, a Digital Geneva Convention needs to create an independent organization that spans the public and private sectors. Specifically, the world needs an independent organization that can investigate and share publicly the evidence that attributes nation-state attacks to specific countries.

While there is no perfect analogy, the world needs an organization that can address cyber threats in a manner like the role played by the International Atomic Energy Agency in the field of nuclear non-proliferation. This organization should consist of technical experts from across governments, the private sector, academia and civil society with the capability to examine specific attacks and share the evidence showing that a given attack was by a specific nation-state. Only then will nation-states know that if they violate the rules, the world will learn about it.

Building a trusted and neutral Digital Switzerland

Finally, those of us in the tech sector need to act collectively to better protect the internet and customers everywhere from nation-state attacks. As the first responders to threats that in part target our own infrastructure, it's important for global technology companies to adopt concrete commitments to help deter and respond to nation-state cyberattacks. As the Fourth Geneva Convention relies on the Red Cross to help protect civilians in wartime, protection against nation-state cyberattacks requires the active assistance of the tech sector.

We need to start with a clear premise. Even in a world of growing nationalism, when it comes to cybersecurity the global tech sector needs to operate as a neutral Digital Switzerland.

We will assist and protect customers everywhere. We will not aid in attacking customers anywhere. We need to retain the world's trust. And every government regardless of its policies or politics needs a national *and* global IT infrastructure that it can trust.

This commitment to 100 percent defense and zero percent offense has been fundamental to our approach as a company and an industry. And it needs to remain this way in the future.

If we're going to turn these words into effective action, we need to come together as an industry to adopt our own clear principles and to help put in place the steps needed to make these principles real. For example, we should commit ourselves to collaborative and proactive defense against nation-state attacks and to remediate the impact of such attacks. We should pledge that we'll continue to take no efforts to assist in offensive actions anywhere. We should make software patches available to all our users, regardless of the attackers and their motives. We should adopt coordinated disclosure practices for the handling of product and service vulnerabilities. And we should work together to support international defensive efforts, like the new international organization described above.[5]

There is strong progress on which we can build. For example, we at Microsoft have been collaborating with other leading cloud companies like Amazon and Google to combat cloud abuse such as spam and phishing sites. We're working together on a common abuse reporting schema to accelerate the reporting of abuses we may see on each other's networks. On issues such as customer notification of potential nation-state attacks, we've all learned from important work where Google and Facebook have been early and impressive leaders. More broadly, there is good work and common collaboration springing up everywhere, from new startups to the industry's largest companies.

Finally, as we consider these questions, it's worth reflecting on at least one aspect of some of the other recent issues that have united the tech sector.

The recent debates about immigration have brought to the surface an important truth. As an industry, the tech sector has literally brought the world together under its own roof. For example, at Microsoft in Washington state, a strong majority of our employees were born in the United States, but we also have employees who have come from 157 countries. I've long

arrived at the office each morning feeling that I work at the United Nations of Information Technology.

Our company is not unique. As an industry, we've brought people together in ways that can promote mutual understanding and respect. We need to harness this global understanding to protect people everywhere, earning their confidence as the world's Digital Switzerland.

—

[1] http://www.isaca.org/cyber/Documents/State-of-Cybersecurity-infographic.pdf

[2] http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[3] https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

[4] http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/, at paragraph 26. The G-20 provision affirmed the same provision agreed to by the U.S. and China, stating "that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."

[5] For a more complete discussion of these principles, see https://blogs.microsoft.com/on-the-issues/2016/06/23/cybersecurity-norms-nation-states-global-ict-industry/#sm.000fn948avqfd2m11711pov1fd3a2

About the Author

Brad Smith

President and Chief Legal Officer

Brad Smith is Microsoft's president and chief legal officer. Smith plays a key role in representing the company externally and in leading the company's work on a number of critical issues including privacy, security, accessibility, environmental sustainability and digital inclusion, among others.

Back to top

Share this post:

Related Stories

At US Safer Internet Day launch event in Philadelphia, youth commit to being kinder online

Youth and teens attending the official U.S. launch event of Safer Internet Day 2017 embraced
Read more »

Next Generation Washington: Our perspective on this year's state legislative agenda

As we begin a new year, lawmakers from across Washington state have been sharing the
Read more »

Expanding partnerships and transparency on human rights

As our society becomes increasingly interconnected, it is more critical than ever that we foster
Read more »

Corporate Blogs

Corporate Citizenship Blog
Internet of Things
Cyber Trust Blog
Microsoft on the Issues
Next at Microsoft
Official Microsoft Blog
The Fire Hose

Windows

Office

Office Blogs

Business & Enterprise

Dynamics

Devices

Microsoft Devices
Xbox Wire

Services

Skype Blogs
Bing Blogs

Server & Cloud