**Security News Briefing 2018**

**Brad Smith, President, Microsoft**

**April 16, 2018**

**ANNOUNCER:** Please welcome President Microsoft Brad Smith.

**BRAD SMITH:** Good afternoon. Well, thank you to everybody in the room, and thank you to everybody who is watching online, either now or later. I think we have an exciting and really interesting hour ahead of us. There's an opportunity for us at Microsoft to share with you what we believe is some important news, some new steps that we're taking to advance security.

But I'm not here by myself. You'll hear me frame the issue a little bit at the outset, give you our broad perspective on the cybersecurity issue and where it's going. And then I'm going to ask Ron Green, the Chief Security Officer of Mastercard, to say a few words. And then Ron will be followed by Barry Simpson, the Chief Information Officer for the Coca-Cola Company. And then he'll be followed by Diana Kelley, the Chief Technology Officer for the Enterprise Security Group in Microsoft.

As you can see, we have a lot of chiefs here to talk with you this afternoon. After Diana shares with you our new announcements relating to the cloud, I will then walk you through what in some ways is our biggest announcement of the day, a new initiative that we think is truly groundbreaking in protecting the edge, the $9 billion Internet of Things devices that are being shipped every year with microcontroller units.

So we have a lot to cover. But let me start by giving you a broad perspective on how we're thinking about cybersecurity at Microsoft. If you think about the 14 months that have taken place since last year's RSA Conference here in San Francisco, it has been an eventful time. There were some who look back at 2017 and call the year Cybergeddon. I don't think that was misplaced, and at the same time we have started to see stuff that give us a glimpse into the future, a glimpse into what we can and should and, in fact, need to do to better protect cybersecurity around the world.

As we take stock of the world, one thing is clear, cyberspace unfortunately has become the new battlefield. We saw this in 2017 as we really saw a new generation of weapons, cyber weapons, used not just by criminal organizations, but increasingly by nation states. We saw that last May with the WannaCry attack, we saw it in June with the Not Petya attack. And fundamentally what we are seeing is not just attacks on machines, but attacks that are endangering people's lives.

In fact, we're seeing in some ways a turn for the worse in the world, because when you put this in historical perspective, when World War II ended, the countries and governments of the world united to recognize that they had not just a moral but a legal responsibility to protect civilians even in times of war. And yet when you look at these attacks last year, what we fundamentally see is, we see nation states attacking civilians even in times of peace.

For all of us who work with the technology that is this infrastructure of the future, there is a huge responsibility, a responsibility that in many ways is far greater than anything that was envisioned when computers were first invented, or when the internet first became popular.

Certainly at Microsoft, we think about the work that is needed to fulfill this responsibility in three ways. First, without question Microsoft and others in the tech sector have the first responsibility to protect cybersecurity. We build the products, we operate the services, we provide the infrastructure, and by definition when things go wrong it is our people who are the first responders for customers around the world. It is a responsibility that we need to advance each and every day.

But it's also a shared responsibility. It is not something that the tech sector can do by itself, and it is a responsibility that is shared with customers. I think that's why it is so helpful and important to hear from people like Barry and Ron about how really cutting-edge customers, who are investing so deeply in IT advances, are thinking about the work that they are doing, and they are doing with us and others to protect cybersecurity.

But even when you think about the tech sector and customers and you put us all together, another thing is clear: the private sector cannot do this alone. In part, we are talking fundamentally about attacks by nation states. Increasingly we're talking about attacks by governments that have their own well-funded cyber weapons capabilities. By definition, the private sector cannot provide all of what our countries and our communities are going to need. Hence, we need public leadership as well. We need it more than ever.

So as we think about this year's RSA Conference and coming together as an industry here in San Francisco from literally around the world, I think it's an important time to reflect on the fact that we all need to do more. As we think about what it means to do more, we need to ground ourselves in where computing is going.

As Satya Nadella, our CEO, has said, we really migrated from a worldview that was all about cloud-first and mobile-first to one that builds on that and recognizes that, in fact, we have entered already a world that has an intelligent cloud and intelligent edge.

What does that mean? Well, it really means that intelligence and computing power is distributed from literally the center of the computing networks of today, that being the data centers that large companies like Microsoft operate, to the very edge, the billions of IoT devices that increasingly are running more and more powerful computing units.

It is a world of multi-device. I'll bet almost everybody in this room has more than one device with them, or if not then another device at home, or at your office, or in your car. These devices are increasingly multi-sense, meaning we type into them, sometimes we do that with our fingers on keyboards, sometimes we do that with our thumbs on a touch-based device. We talk into our devices. Our devices increasingly have vision. They can hear us speak. And all of that is continuing to increase. It is being fueled by artificial intelligence from virtually every aspect of computing.

And we've entered, in effect, a serverless world. We're no longer talking to customers about how they're going to run our software on their servers, instead we're talking about an environment that connects the data center directly with devices and relies on the cloud.

In so many ways, this technological advance has promise for the future. It will do everything from helping us work more productively to enjoy our free time to literally helping us cure cancer. But it's also a time when we need to step back and think about the world that we're creating. We're creating a world where everything will be connected from your refrigerator to your thermostat to your air conditioner to your lights to your car to your office.

But we also need to recognize this: in a world where everything will be connected, we will also have a world where anything can be disrupted. And if we're not careful, a world where one thing is disrupted can quickly lead to other things being disrupted as well. Ultimately it means one thing above all else, in a world where anything can be disrupted, everything needs to be protected, literally, from the cloud to the edge.

And that's why today what we're really here to share with you is the perspective from our customers and what they are seeing and implementing to the new advances that we're announcing this afternoon, new features and functionality that will help our customers make use of a more secure cloud in ways that will help them protect their devices. And fundamentally a brand-new initiative, and an initiative that in some respects is almost different from anything Microsoft has pursued in its 43-year history, to secure the edge, to secure the edge the way it needs to be secured, and to secure it in a way that has never been secured before.

So let me turn it over next to Ron, to Ron Green. Please join me in welcoming Ron Green, the Chief Security Officer for Mastercard.

(Applause.)

**RON GREEN:** Thank you, Brad.

So what I wanted to talk to you about today was trust, and in the financial services sector trust is a critical ingredient for us to have. And for 50 years Mastercard has maintained the trust of consumers, governments and businesses when they come to conduct their payment transactions. So every minute of the day in nearly every corner of the globe, we have people that are depending on us to enable their transaction to happen.

So one of the cornerstones of that trust is security, because these consumers, the merchants, the banks, and the government are depending on us to protect the customers' information, to protect the transaction, and to prevent fraud.

So in light of that, at Mastercard security is part of everything that we do, every product we build, every service we provide, we build in security from the onset. At Mastercard we talk about security being everybody's responsibility. And we mean that within the company, but we also mean that externally as well. And by that, I mean partnership, and partnering with others in the sector, partnering with other industries, partnering with governments, those are things that are critical for us to be successful in this space.

The adversaries, the bad guys, they're upping their skills. They're getting better every day. But most importantly or what's worse is they're actually working together. They work collaboratively in a way to be more effective in their use of vulnerabilities and attacks against us. And so we don't just have -- it's not just good for us to partner, we need to, we must in order to be successful in this space.

So I will tell you, we've done a lot of really good things in the partnering space in the financial services sector. But we also partner with trusted groups like Microsoft. An example of that would be the Cyber Readiness Institute that we are jointly engaged in. And this will help us provide small and medium businesses with the skills and capabilities and just an ability to protect themselves better, because from software to conducting payment transactions, all of us, all of our businesses are integral cogs in this, and it's really important that we are able to secure not just ourselves, it's not just important for Mastercard to secure itself, but securing the entire ecosystem is very important to us.

I want to thank you for allowing me the time today to express how important it is to partner with groups like Microsoft.

**BRAD SMITH:** Thank you, Ron. And I think I was going to ask you maybe one question if you don't mind. One of the things that I think is so interesting about these issues today is, in the tech sector trust is really become a prerequisite. Trust has been a prerequisite in financial services probably since financial services were invented. What does this development of the trust equation mean for a company like Mastercard? How are you all thinking about that as you need to work at this intersection of technology and financial services?

**RON GREEN:** Without trust we can't do business. If you think about it, as consumers ourselves, if we didn't trust someone to protect our financial interests, would we do business with them? Would we actually use a card to pay for something if we didn't trust that the payment would actually happen and then happen securely? So without trust there is no business in our space. So we think about it all the time.

**BRAD SMITH:** Well, good. Thank you very much. I really appreciate you being here.

Well, let me then turn from one customer scenario to another, and it's a real pleasure for me to welcome Barry Simpson, who is the Chief Information Officer for the Coca-Cola Company. If you think about it for a moment, everywhere around the world for over a century billions of people have had confidence and trust in what they would get when they opened a bottle that said Coca-Cola on it. Barry is taking that level of trust into a new era.

So, Barry, thank you.

**BARRY SIMPSON:** Right. Thanks so much, Brad. Thank you.

(Applause.)

I would like to give you a perspective from our company on how we look at cybersecurity, and how we have a pragmatic view of attaching security to our growth agenda. And it is really important that we focus what we do with security in our growth agenda.

From 1886 we started the company that had one product in one country. We're now a company that has over 4,000 products served in 200 countries. We had 770,000 vote shares across our franchise systems. We have a $21 billion brand. And we're a business that has really steeped itself in consumer trust and being a core part of consumer preferences.

And so when we think about security, it's all about preserving that trust with our consumer, it's about growing our business, but also being pragmatic about how we execute our security agenda across such a large, diverse system. So for us we have to have the consumer at the heart of everything we do. And it's clear that digital experiences are giving our consumers endless options to research, to buy, to interact with our brand and they can do this 24/7.

But we live in a world where we have to respect and guard our consumer's privacy, but we also have to personalize and engage them in our brand to deliver a compelling experience. So when we think of security and we think about our growth journey at Coca-Cola, we have technology at the heart of our new growth agenda.

So it's clear when we talk about growth that having digital capability at the heart of our business is really, really important. And we think about it in two ways. We think about digitizing eternally to grow with our consumers, and so that we are in our consumers' digital space. We have a personalized journey for them, and we're creating the products and brands and experiences that they expect from a company like Coca-Cola.

But we also have to grow, and we can only grow through having the right workplace experience for our associates. And so for us, we also digitize internally to make our workspace more efficient, but also more engaging and more agile, because it's very clear that he way people are working is changing.

I would like to talk a little more about some of the choices we're making as a company to create this digital workspace internally and externally. First of all, let's talk about what we're doing around our landscape. We're moving from being the company that has stitched together technology, that has been a builder of applications, to a company that is moving to strategic partnerships across platforms at scale.

We believe that that fundamental shift in technology and moving to platforms that can build ecosystems around us will give us the scale we need, will give us the speed we need, but also gives us the flexibility to partner with companies large and small to drive our growth agenda.

And so at the heart of that is simplification. If you want to go faster, you have to simplify your business. So we are dramatically simplifying our application stack all across our systems. We're also accelerating our move to cloud. We believe that cloud platforms, by their design, are inherently more secure, have better segmentation, and when you read a lot of the cyberattacks, a lot of it is about just the basic plumbing, getting the patching right. And that's getting harder and harder in a world where we're expecting to be connecting with more and more people.

We're securing our cloud platforms. We've accelerated our move to cloud. By the end of this year our company, all of our company systems will be cloud-based, and we'll be out of our corporate data center. We're also moving, as I said, to integrated platforms that scale. And I'd like to talk a little about what that means in terms of security.

So we're partnering very closely with Microsoft for our security platforms, because, once again, if you think about how we worked in the past, we would have had lots of different solutions, we would have had to stitch them all together. And we would have had to hope that with all these components stitched together that we're providing a secure environment. We just don't think we can get there fast enough, and we don't think we can do it in a way that can be complete enough without a strategic partnership with someone like Microsoft.

So we're moving our directory structures. We've simplified them, and we've moved them to the Azure AD platform. We moved our Office 365 system to the latest versions, and we're moving to Advanced Threat Protection. And this really lets us understand what's happening across the systems. And, like I said, we're a part of a large franchise system, and when you think about attacks for our system, they can be the simple attacks, we're seeing phishing attacks, simple and sophisticated, and growing in number. And so having Advanced Threat Protection across that environment is extremely important to us as well.

We're also seeing sophisticated attacks out there. And this is a battle where we just can't keep throwing more troops at the battle. We just have to be smarter at how we work across our technology landscape. And so using artificial intelligence, using the power of the Azure platform to help to detect threats, to understand patterns, and then to scale that across our franchise system is delivering certainly benefits now, but we see the benefits scaling more in the future, particularly as we see the threat landscape continually increasing.

When we think about what we do internally, we're bringing consumer-grade technology to all our associates within the company. That's what they expect. People expect the same ease of use they have outside of work to have that same ease of use inside of work. And so, security has to be both rigid yet also flexible. We like to talk about having frictionless security within our company. So when we deploy solutions, such as Windows, pan across our organization, it's really important that we do this in a way that makes it a seamless experience for our end consumers, our associates.

So things like Windows Hello, things like Microsoft Authenticator, they bring intuitive ease-of-use ways of securing devices and giving us that full multi-factor authentication across our organization that we need to protect our environment, yet we're also freeing up people to be able to work anywhere at any time on any device to work with our system.

With simplification, this move to platform, this building of ecosystems for security is also letting us move faster. If we think about the pace we need to change at for security and how we need to adapt to the threat landscape, our historical approach of having multiple solutions on multiple platforms is really difficult to manage at pace, and at scale.

Our recent rollout of MSA across all of our global landscape, we were able to do that in less than two months, because we made the choices on platform and because we made decisions around how we want to partner to scale for our systems. So I think when we think about cybersecurity it has to be about simplification. The move to cloud is extremely important to us. And this ecosystem of security technologies that work together really allow you to scale at speed and to adapt in an ever-changing environment.

Thank you.

(Applause.)

**DIANA KELLEY:** Thank you, Barry. Thank you.

Thank you, everyone, for being here. I'm Diana Kelly and I don't know if what you just heard sounded familiar, what you heard from Barry and what you heard from Ron; companies struggling with engaging their customers but building trust and finding a way to simplify. In my role I talk to customers every single week and these are the core themes that we are hearing back from them. They're saying to us, Microsoft, can you help us to simplify, can you help us to move smarter and be faster with our remediation. We also hear a lot about the struggle, the struggle is real.

So the number of different products that companies have to deal with; whose first RSA is this? OK. The show floor is going to be fun because there's no end of products on that show floor. I mean there's so many different options to choose from. But customers really are looking for a level of simplification and being able to bring together all of these signals from all these different products, share intelligence across their space so that they can make better decisions. A lot of companies, their security operations folks, they're drowning in data. They don't know how to triage, how to get to it, and if you want to think about the -- look at one number of drowning in data, this is an example. Windows Defender AV defends against 5 billion -- 5 billion -- unique threats a month. That's a lot of threats. Could you imagine a team of people going through that number of threats without having some sort of aid with automation?

So we see the cloud as a security imperative for enterprise. In order for enterprise to leverage out trust, to get the simplification and the integration they need, they need to move to the cloud. And to leverage the security that can come from the cloud. What about all that signal I was talking about before? Where can we collect all that signal? Where can we use machine learning and AI to be able to go through that signal? That's going to be in the cloud.

The cloud is a place where you have more secure data storage, where you can have identity management on the control plane and centralize security and threat intelligence information. Cloud is a business imperative and security is also.

Microsoft takes a unique approach to being able to provide what enterprise needs in terms of additional trust, additional efficiency, and additional security.

And we do this in three core ways. The first one is intelligence. Bringing that intelligence together, leveraging it across our different platforms.

The second is in the platform itself. Bolt-on security. How many times have you heard bolt-on security? Who here thinks bolt-on security is the best thing, it's the way to go? Let's all bolt it on. No. I'm getting some smirks. (Laughter.) And I know you. It's OK to smirk.

So, no, how do we do security the best? When we build security in, when it's part of the platform, when it gets simplified and we can leverage that. So building it in across all levels in the devices, in the hardware if possible, in the operating systems -- building it into each layer so that it's easier to deploy, easier to manage, and can help the simplify the process.

And then partnership. We've heard it from Barry, we heard from Ron, partnerships matter -- partnering with enterprises so we understand what they need and we can help them. It's also partnering with other technology vendors. We know we're not the only technology vendor in the world. We know our customers are working with multiple vendors, so we are working with those vendors, too, as a partner in order to, again, simplify and create that intelligent fabric for organizations.

And when we talk to enterprise, enterprise is telling us that the most important thing for their security readiness is this cloud intelligence. It's the ability to share that data back.

When we talk cloud intelligence, we mean every part of our cloud. So we get information from Windows, from Bing, from Azure Active Directory, and we even bring information from Xbox for security into our Intelligent Security Graph.

Have you heard of the Intelligent Security Graph? Yes? Okay. So the Intelligent Security Graph offers unique insights. What is it? For us, it's the central nervous system of the Microsoft Security Solution Set. Unique insights. Literally trillions of signals. So here's the five billion potential threats that I talked about earlier, scan through 18 billion Bing pages every month, 400 billion e-mails are analyzed anonymously -- that took me a second to get through -- analyzed anonymously. And we provide enterprise security for 90 percent of the Fortune 500.

So bring together the signal from the Intelligent Security Graph to provide information that will help companies remediate and detect problems more quickly.

The other thing that's really nice about this graph is it helps to democratize this information. So in the past, larger companies and enterprises were able to get some level of deeper collected intelligence, but smaller companies were not able to afford that level of intelligence. So we can provide to all of our customers information from the Security Graph.

But you hear about speed and time and what does that really mean? You can remediate faster with the Graph. Remediate faster -- how about milliseconds?

So early in the year, Dofoil, which is a crypto-mining campaign, so it was a bot that got onto a system and mined crypto because this is now a way to make money. If you're an attacker, maybe it's more profitable for you than phishing these days to do the crypto mining, but you need a lot of systems to do it in.

So on March 6th, in milliseconds, 80,000 instances of Dofoil were blocked -- milliseconds. Faster remediation, reality, milliseconds. And over the course of the next 12 hours, 400,000 were blocked, and Windows users were not impacted by this crypto-mining campaign.

But what are we here to talk about? How the Intelligent Security Graph Powers the announcements that we're making today from Microsoft. And we're making them in three areas that matter to the enterprise. The enterprise has said, "I need help with this."

Making those smarter choices. How do you inform the IT department so they can make those choices? The faster remediation, dealing with all of this signal, and a lot of it noise, and being able to remediate more quickly.

And then simpler integration. Can you help -- can you bring it all together for me? Can you make it simpler for me to use across a partner ecosystem and across my Microsoft estate?

So let's start with smarter choices. The first one is Secure Score. This is now the Microsoft Secure Score. If you've heard about the Office 365 Secure Score, this is an extension of it. And companies can use it to measure themselves and look at what kind of controls they've got in place, what security they've got in place, and then give them a score. And they can compare the score against two things that enterprises, especially the C-suite, love to measure themselves against.

The first one is: How am I doing against my peers? So you can say, I'm a financial services organization, I want to see -- I know what my Secure Score is, can you show me what my peers -- you don't see the name of the peers, you just know other financial services institutions.

What's the other thing most of us think when we see a score? How can it get better? How can I do better on the score? So we also provide actionable recommendations that companies can use in order to increase their score.

The Attack Simulator, we're also announcing as available today. The Attack Simulator allows companies to make smarter choices by allowing them to send a phishing or ransomware campaign -- a faux, it's not going to actually lock up their system -- but a phishing campaign or a faux ransomware campaign against their organization so they can simulate the attack and then educate the users if the user clicks through, educate those users, raise their security awareness, and potentially tune the policy.

Our next theme is faster remediation. We know SecOps has too much to go through, too much to triage, and to investigate. If you've got 1,000 alerts, how do you know which are real and which aren't? You and to go and investigate. This can take a lot of time, and we've got very understaffed SecOps organizations in a lot of enterprises.

So with the upcoming Windows 10 update, there's a new Windows Defender Advanced Threat Protection, automated investigation. So you don't need a person to go now investigate it. It's going to do the automated investigation and automated remediation.

And if you don't like the automated remediation part, that's okay. I used to be a network admin, so I always hear on remediation, that's okay because if that's something that the company doesn't feel comfortable with at first, we have a "check with me" function within Windows Defender ATP automated investigation and remediation, and at that final part before the remediation takes place, you could do a "check with me" with a human if that's something that the company chooses to do.

The integration of threat detection really does help with this faster remediation. And an example here is with the e-mail protection, let's say you're using Office 365. An e-mail comes in, Office 365 checks the link in the e-mail. Is it malicious? It's not malicious, okay, put it through. Gets through to the user, the user clicks. Guess what? Office is going to check it again. And the reason is that attackers are smart enough to know that sometimes companies check when the e-mail comes in, but they don't check during click. So we check at click.

Let's say it's turned malicious. Okay, that's malicious. That gets reported up into Office ATP. But what if you've got an end user on Windows who's using some other e-mail? They have a personal e-mail that they use on their Windows device? Well, Windows Defender also gets alerted about that malicious URL so you have that integration, again, through the layers, Office ATP sharing it with Windows Defender ATP to provide more holistic protection.

Conditional access is another piece of faster remediation. So we've had conditional access for a while. This is where you can make an ongoing risk assessment of a user logging in and attempting to get sensitive data based on a number of factors like what device they're using, what time of day it is, which geographic location they're in, if geographically they logged in from New York an hour ago and now they're trying to log into Singapore, could be a little hanky. And so this is what conditional access does for us.

Now, Microsoft 365, we are adding in device-level assessment to conditional access. So Windows Defender ATP reports that there's been a compromised device, this also goes into the conditional risk score, and at time of login, can be used to determine whether or not you allow that login, and can prevent a compromised machine from accessing your sensitive corporate data.

Simplification. Better integration. Anybody here use -- you probably heard Microsoft is on a mission to end the traditional passwords and the proliferation of passwords, and Windows Hello is one of the main ways we're doing that.

So we are announcing today that with the latest Windows update, we will have support for FIDO 2.0, and that's going to allow in certain work line instances, so use cases where you have 10, 20 different people logging into the same machine, they can all log into the same machine using their biometrics thanks to this partnership.

And partnerships across other vendors, too. The Microsoft Intelligent Security Association, again, announcing this today, and this is our working with our key partners to provide better solutions, simplified solutions that increase your security posture.

So an example would be with Lookout and Sentinel One and Ziften, these have end point solutions.

We have Windows Defender ATP, but not every device that a company uses is Windows Defender. So if you've got OSX or you've got iOS on your iPhone -- if it's on your iPhone, it's iOS -- you're using Android. Our partners will report that end point information up into Windows Defender ATP console so that you can look at it in the same console. It's that kind of partnership that really delivers what enterprises are asking for in terms of management simplification and security.

And we're announcing the Microsoft Security Graph API. You've heard about the Security Graph, now here's the API. This means that we can partner with some of our core trusted technology partners and integrators to be able to allow them to leverage all of that information that's within the security API.

And we're also hoping to engage the rest of the industry in using the information from this API to help inform their products, and against threat intelligence across the entire ecosystem. And we've got three of those partners here today -- Palo Alto, PWC and Anomaly, to showcase what they've done with the APIs so far.

I'm going to be back in a couple of minutes to tell you a little bit more about that, but right now, I'm going to hand it back to Brad because he has one more very exciting announcement.

**BRAD SMITH:** Thank you, Diana. I want to turn to what I think is the biggest announcement that we have today, which is Azure Sphere. I just want to give you a little bit of context, and let me pick up where I left off before. It really is a new world. It's a world where we're seeing the Internet attacks every day on all of the connected devices that are running across the planet.

It's a world where we're starting to see just how serious the damage can be when these attacks take place.

It was in 2016 that the Mirai attack basically enabled hackers to take control of 100,000 devices and use it to launch a DDoS attack by turning those devices into part of a botnet.

It was an attack, that on a single day, basically took the east coast of the United States off of the Internet.

It is that kind of prospect that we have to take new steps to guard against. It's even more important when we put this in the context of the world that we're entering that literally is powered by billions of these MCUs, the microcontroller units that I spoke about before.

As I mentioned, there are going to be nine billion of these MCU-based devices shipped this year. Think about that. For every person on the planet, there will be more than one of these MCU devices shipped. They literally will be in the toys of our children, they literally will be in our kitchens and our refrigerators, they will be in every room in our house.

Already, if you have a device at home that has a button or a status light or it does something that turns on but lacks a high-res color display, it has an MCU.

Now, today, fewer than 1 percent of those MCUs are connected to a network or the Internet. But that is changing, and it's going to continue to change. And what it fundamentally means is that our homes and our offices and the infrastructure of the future will literally be only as secure as the weakest link.

If we're going to address that security in an effective way, we need to really build security from the chip all the way up to the cloud. And that's one of the reasons we're building on the expertise that we've had for so many years at Microsoft. Not just the software that you think about with products like Windows and Office, but the kinds of security steps that we've been taking for 15 years at the chip level to secure devices like the Xbox.

What we're doing today with our Azure Sphere announcement is really going where no company has gone before. And it really starts, above all else, with one very important proposition. As we think about these devices, we need to take cybersecurity from an art to a science.

And that's what our researchers have been doing as we think about what it takes to ensure that these billions of devices are secure, we've developed seven priorities. Seven properties, if you will. Seven properties that can only be advanced effectively if we focus on cybersecurity at the hardware level, at the software level, and at the service level in the cloud.

So let me take a couple of moments and walk you through each of these seven and why they're so important and what they mean.

First, it starts with ensuring that there is a hardware root of trust. What that means is that we're able to protect the secrets, the information on the device with hardware that has physical countermeasures against side-channel attacks.

If you've been following, as we all have, the events of this year, we've all learned about the importance of side channel attacks at the chip level, so we need to start with protection at the chip level to protect against these kinds of side-channel attacks. So we do that with protection at the hardware layer.

The second property that we really need is what we call "defense in depth." Fundamentally, that means that there are multiple mitigations and responses to attacks or breaches, not a single line of defense.

Now, we do that by building in these lines of defense at both the hardware and the software level, at the operating system level.

The third property is really a focus on having a small trusted computing base. I'll give you an example.

What it means is you can have private keys stored in hardware-protected vaults that are inaccessible to software. So if you're trying to launch a software-based attack, you find that the software cannot access these private keys at all.

The fourth is having dynamic compartments. What that means is that one has hardware-enforced boundaries that really prevent breaches in one software compart from going to another software component. So you can see how this is another area where hardware and software protection and innovation really need to come together.

And then there are three properties that one can address effectively only if we take effective action at the hardware, the software, and the cloud-based level.

The first of these is about certificates. We've, increasingly, become I think used to these in many institutions, certainly large enterprises, but the notion of relying on certificates instead of passwords to establish identity for mutual identification. And we can do that by combining these advances at all three of these layers.

The next is about online failure reporting. And when you think about this, it just is obviously fundamental. Where there is an attack that results in a failure, we need the ability to generate a report about that failure automatically and instantaneously through a failure analysis system.

And, finally, in some ways, the last key to making all of this work is renewable security -- the ability to provide an update to even the smallest device on the planet so that security and a secure state can be updated automatically.

The fundamental fact of life is this: If we're going to ensure that these billions of devices are protected in people's homes and around the world, we need to address every one of these seven properties, and each of these three layers is needed to ensure we do the job the world requires of us.

What we're announcing today is Azure Sphere. It is an end-to-end IoT solution. It goes where, as I said, no company has gone before, by addressing each of these seven properties, and doing so at these three different layers.

The Azure Sphere has three different pieces. I'll talk about each, but in brief, it has the Azure Sphere certified MCUs, the new chips, it has an operating system, the Azure Sphere Operating System, and it has a cloud service, the Azure Sphere Security Service.

So let me give you a little bit of information about each of these. The first is the Azure Sphere MCUs. This is a new class of MCUs. It is five times as powerful as legacy MCUs.

When we're talking about an MCU, we're talking about something that is literally a computer on a chip that is as small as somebody's fingertip. And as you can see, it's as thin as somebody's fingertip.

The researchers at Microsoft Research have made advances to strengthen the power of these chips and to put that power to work to protect people's security around the world.

In fact, what we're doing to jumpstart this new ecosystem that we so clearly need is to license this technology and intellectual property royalty free to any silicon manufacturer that wants to build these new Azure Sphere chips. In fact, already, MediaTek is starting to fabricate these chips. These chips will be shipped in 2018, more partners will follow.

And what we've been able to do with these hardware advances is really engineer security at the root, at the chip level in three ways.

First, we're putting this increased power to work with connected, built-in networking. That is, obviously, a prerequisite for these security advances.

The second is we're securing this with the silicon technologies that we pioneered in Xbox, silicon technologies that make the chip more secure.

And, third, we've added crossover processing capabilities -- capabilities that really enable ambient intelligence in an MCU package for the very first time.

So if the only thing we were talking about today is this new step to advance security at the chip level, I think we would be doing something important. But that would not be a complete solution. We need the other two pieces of Azure Sphere as well.

So the second is really the Azure Sphere Operating System. This is a new operating system, it's based on a custom Linux kernel -- a custom Linux kernel that has really been optimized for an IoT environment and is reworked with security innovations pioneered in Windows.

Of course, we are a Windows company, but what we've recognized is the best solution for a computer of this size in a toy is not a full-blown version of Windows, it is what we are creating here. It is a customer Linux kernel, complemented by the kinds of advances that we have created in Windows itself.

For anybody who has been following Microsoft, I'm sure you'll recognize that after 43 years, this is the first day that we're announcing that we'll be distributing a customer Linux kernel. It's an important step for us, it's an important step I think for the industry, and it will enable us to stand behind the technology the way I believe the world needs, because what we will do is ensure that these devices are secured throughout their ten-year lifetime with the continuing improvements and updating to the Azure Sphere Operating System.

Of course, that is possible only because of the third piece, which is the security service -- the cloud-based service. This is a service that will guard every Azure Sphere device. It will broker trust for device-to-device and device-to-cloud communications. It will detect emerging threats, and critically, it can and will renew security the way our customers need.

If you look at what we're doing with this Azure Sphere Security Service, we're really able to take those properties that I described and make their advances real.

So as you saw, when I talked about certification and authentication, because we have this service, we're able to use certificate-based authentication for all communications.

We're able to use the automated processing of on-device failures to detect emerging security threats, or able to respond to threats with fully automated, on-device updates of the operating system and applications.

There's another critical aspect of what we're doing with the security service that we're making part of Azure Sphere, and it, too, reflects, frankly, a new way of working.

What we're doing is we're making this service compatible not only with Azure as a service, but with customers' other legacy or proprietary or cloud-based services.

So if a customer wants to continue to integrate these MCU-based devices with AWS or the Google Cloud or cloud services from IBM or Oracle or Alibaba or literally anyone else, they can do that.

In essence, when you really step back and think about this, this announcement I think reflects two things that are very fundamental: The first is the ability to take cybersecurity to the edge of the world's computing networks, the edge that will become more and more vulnerable if we do not take these kinds of steps.

But the second thing it really does is it enables us as a company to put security first.

We're working with operating system technology in new ways to do that, we're working with our competitors' services in new ways to do that. We're working with hardware companies across the chip ecosystem in new ways to do that, and we're doing it in ways that share technology and intellectual property in new ways as well.

I do believe that it enables us to make an important contribution to what the world needs from us, and that is to work with everyone to put security first and help to create a safer world.

So thank you.

END