Keynote: How to Secure our Ecosystem and Keep Pace with Emerging Technologies
OEA Ciberseguridad Symposium, W Hotel, Santiago Chile
Wednesday, 24 September 2019, 2:00 PM—2:30 PM
Eric Wenger, Global Director Cybersecurity & Privacy Policy, Cisco Systems, Inc.

INTRODUCTION

In August, I had the honor of witnessing in Washington DC a signing ceremony between Secretary General of the OEA, Luis ALMAGRO, and Cisco's Senior Vice President and Chief Government Strategy Officer, Michael TIMMENY. Together they launched a series of Cybersecurity Innovation Councils in Latin America—a new platform for cybersecurity education, best practice sharing, and collaboration. I am, therefore, proud to join with you all here today in the spirit of that agreement to participate in this gathering of cybersecurity experts from across this vibrant region in this beautiful city. I thank the OEA for this invitation to speak with you here today and extend congratulations for my friend Belisario CONTRERAS for the success of this event already.

Four countries were selected for the initial effort with the OEA to develop "Cybersecurity Innovation Councils": Brazil, Colombia, Mexico and of course Chile. Once operational, they will foster joint multi-stakeholder projects enabling leaders and experts from the private sector, public sector, academia, and NGOs to collaborate, drive innovation, raise awareness, and expand the sharing of cybersecurity best practices.

Education is the foundation of driving awareness and the democratization of cybersecurity. Therefore, in addition to the Councils, both Cisco and the OEA are leveraging Cisco Networking Academy in Latin America to promote educational resources that can help close the professional skills gap in cybersecurity—allowing citizens to access trainings and career opportunities in this field and help build the workforce of the future.

I would also like to thank our host country for the event. I hope to find more time to look around before I have to leave. But I did get a chance to look at your capital city from the 300 meter vantage of the Sky Costanera. One amazing feature of the exhibit is the ability to look back in time via an app. Some of the views show the scene as largely untouched until just 20 or 30 years ago. What the experience underscores is how astounding the accomplishments are of this nation in a very short period of time, including its alignment with OECD and its leadership within APEC.

Despite the relatively small size of its population, Chile is currently our 4th largest market for Cisco in Latin America. Just last year, our CEO, Chuck Robbins was here in Santiago and personally signed collaboration agreements with the ministries of interior and education to improve coordination of cybersecurity efforts and to train 10,000 technical students in cybersecurity skills over a three year period.

We at Cisco have been here in Chile for the past 25 years. We have partners across the country working with us in support of your efforts to digitize this nation. I note that you are also making great strides physically connecting Chile to the world's digital infrastructure, including the recently completed submarine cable link from Google in California to Valparaiso in Chile.

We look forward to working with the government and the people of Chile as you take on upcoming challenges, such as hosting the APEC Summit and the COP25 UN Climate Change Conference. We also offer our assistance in helping to shape the cybersecurity strategy announced earlier today by Mario FARREN the President's Cybersecurity Advisor.

<u>POWER OF CONNECTIVITY / IMPORTANCE OF DATA AND TRUST</u>

Many presentations at cybersecurity conferences are dire. I'm more of an optimist about technology. So, I hope you find the title comforting and the contents of the talk quite hopeful. That said, I don't want to set unrealistic expectations about the likelihood that I can neatly bundle up the answers for you here today. It would be nice if you could learn all you need to know about cybersecurity from a single 30 minute talk. But, alas, the world is not so simple! Reality is far more complex.

Skeptics may say that one simple solution does exist—we could unplug everything, cut all the cables, and remove the radios. We may very well decide that some "things" ought not to be tied to the Internet or to each other. But we should instead start with the following basic assumption going forward, given the rapid proliferation of networks and the widespread adoption of IoT: "anything that can be connected, will be connected."

That is really, the heart of my message. Let's improve the security of the "things" at the edge based on the assumption that they will be connected. At the same time, let's build intelligent networks that help us to reap the rewards of connectivity while also managing the risks. Even better, let's look at connectivity as an enabler of cybersecurity—and not simply as a threat to it.

I maintain that this is the right approach for two reasons. First, a technology developed based on the faulty assumption of permanent separation will yield hidden vulnerabilities when it is almost inevitably connected to dynamic networks at some point in the future. If we instead recognize that some "things" currently in isolation may someday be networked, we can proactively develop contingency plans in the event of an attack and secure pathways to push patches and updates.

I don't know about you, but I remember reading the Wired magazine article in 2015 about connected cars being hackable with significant trepidation. At the same time, I remember being amazed that Tesla had already delivered patches for the vulnerability over the air to its cars as they charged. That was a game changer and it illustrates the power of networks to protect devices.

We absolutely can, and should, step up our collective game when it comes to enhancing the security of the devices themselves—and I will talk about some of those efforts. At the same time, we must harness our increasing capabilities at the edge of the network if we hope to do a better job of protecting devices against attack—or against their being used as part of an attack.

We can leverage the additional capabilities offered by intelligent, intuitive networks to enhance the security capabilities of human network operators. We can accomplish this goal through the application of Artificial Intelligence and Machine Learning, using connected smart "things," that are tied together via advanced high-speed, low-latency networks, including 5G mobile networks.

Second, global challenges, like how to feed the earth's growing population in the face of climate change, will require us to come together and connect at a human level. There are devices that will light up in new ways and fuel future problem-solving innovations that we cannot yet imagine. How best to do that—to reap the benefits of being tightly connected through technology while effectively managing the risks—is the task we need to focus on together.

If we do both of these things, we really can harness technology to help us bring out the best in each other—to advance economic development, to feed more people with less water and

energy, to deliver digital services to our citizens, to educate students with marketable skills, and to foster adaptability in today's workforce. I'm hopeful we can do these things together. I hope you will join me in bringing this vision to life.

With that, let's take a deeper dive on a few topics relevant to this conversation—AI, IoT, and 5G. What these topics all have in common is a reliance on data. And this in turn, underscores the importance of security, privacy, and trust when it comes to handling that data.

Artificial Intelligence / Machine Learning

One of the things that really caught my eye about Cisco, and convinced me to come on board a little more than 5 years ago, was the pivot away from selling boxed-product hardware that enterprise customers ran in their own network. In some cases, these hardware products can now be virtualized and then run as a service. This means that functions once performed inside the customer's enterprise network may now instead be run from Cisco's own systems. It also means that the network can be more than simply a mechanism to deliver connectivity to smart devices. Rather, we increasingly see the efficiency gains and security benefits that come from building intelligence into the network itself.

Let's be clear that the rising tide of connected devices and the growing sophistication of automated attacks cannot be tackled with manual human intervention alone. We did a survey of IT professionals a few years back and found that on average they faced more than 5,000 threats per day. To combat this problem, they were using products and services from an average of 6 vendors and were using about that many separate offerings from each. The result was a sea of data that they could not possibly parse, triage, and react to in any meaningful timeframe. On

average, more than half of the threats that surveyed IT professionals deemed credible were not being addressed in the course of a typical day. And I'm confident that a repeat of that study would yield similar results today.

Yes, there are concerning impacts on the world's labor force from artificial intelligence. But cybersecurity is not one of those fields we should worry about. The data here is daunting, there are a tens of billions of devices being connected up in the next decade. Cisco's prediction is that we will see 50 Billion devices on the Internet by 2030 up from 20 Billion next year. Even if it took a few minutes per device to manually onboard, authenticate, and provision each, the process would be overwhelming. That's before we even talk about how to monitor and secure all those devices on an ongoing basis.

Already, we see significant gaps in the available pool of cybersecurity workers. ISC2, an organization of IT Security Professionals, estimated in 2017 that we will soon be short about 2 million cybersecurity workers. So, yes, let's train more. But let's also remember that this is a problem the scale and complexity of which cries out for intelligent automation, which will free humans up to focus on the problems that require our unique blend of creativity.

With that in mind, it should be no surprise to see that the services that we are selling at Cisco in conjunction with our networking hardware increasingly have a security dimension to them. We have services that enable the ability to find known pieces of malware in fully encrypted traffic during transmission without the need for the traffic to be decrypted. This is called "Encrypted Traffic Analytics" and it relies on artificial intelligence and machine learning to develop behavioral patterns associated with identified malware.

When email messages have attachments, it is increasingly common to automatically test the files in a sandboxed environment before they are sent on to the recipient. Our version works in concert with a cloud-based service (Advanced Malware Protection) that charts reputational information about these file attachments over time—because what is known about a file can change. If a file later is learned to have been malicious, the network will know where the file was distributed internally. The malicious file can be deleted from mailboxes where still unopened. Where files have been opened, administrators can be alerted so that affected devices can been be cleaned up.

Our workforce is increasingly on the go—remote workers use mobile devices, like phones and tablets, to directly access data and applications in the cloud without ever touching the "perimeter" of the traditional wired enterprise LAN network. That's why services that help extend security protection to mobile devices have become so important. For example, our Umbrella DNS filtering service, which handles about 2% of the worlds DNS queries, automatically blocks more than 20 Billion threats daily. Cisco's Duo security helps reduce the risk of password reuse by enabling multi-factor authentication and empowers enterprises to extend the security benefits of a "zero trust" architecture to mobile devices and enterprise-managed cloud services.

The common element to these services—and others like them—is that they learn over time. Such behavioral learning requires access to large-scale datasets. At the same time, we know that customers will not allow access and use of their data—even for ostensibly beneficial purposes—unless they have some certainty that their data will be adequately protected. All that is to demonstrate how and why Cisco must convince our customers that we appreciate the importance of their data to <u>them</u>—not just to us.

The foundation of our work to build and maintain trust is a recognition that trust is fragile. It is hard won and it is easily lost. Or as former IBM CEO Thomas J. Watson said, "The toughest thing about the power of trust is that it's very difficult to build and very easy to destroy." Trust also requires proof. As former United States President Ronald Reagan once said, "trust, but verify." Cisco's Chief Security & Trust Officer, John Stewart, expressed a similar notion when he wrote there is "no such thing as implicit trust." By this he means, we have moved beyond the era where a brand alone—even one as valuable and trusted as Cisco—is sufficient to address customers concerns about how their data will be handled, stored, and used. A trusted brand is necessary, but it is not sufficient. We must build on that foundation of trust elements to demonstrate trustworthiness if we expect customers and partners to securely connect their smart devices with our intelligent networks.

INTERNET OF THINGS

Turning now to IOT. As I noted earlier, even if we assume computers and systems are designed with the expectation of isolation from the Internet, the reality is that they will eventually be exposed to a dynamic threat environment. A highly publicized example of that comes from the Stuxnet attack in 2010. Kim Zetter documented the story of that attack in her terrific book, "Countdown to Zero Day." The Stuxnet exploit was intended to operate in an isolated computer network used to control Iranian uranium centrifuges—causing those centrifuges to spin wildly until they were severely damaged.

Despite precautions taken by its authors to minimize the risk of spread, the malware found its way onto the public Internet via a USB drive and "sneakernet." The lesson to be drawn here is that static solutions, such as "air gaps," do not work as a way to permanently manage

dynamic threats partly because of human tendencies to circumvent limits and to connect things.

If “air gaps” are not the answer, what is? I offer three thoughts: 1) increase the level of baseline security in the devices themselves; 2) leverage the power of AI at the level of the network; and 3) instrument the network to help inform risk-based decisions about what behaviors are expected—and should be allowed—and what behaviors are anomalous—and should be blocked.

Governments are clearly concerned about the prospects of cheaply made, poorly secured consumer IOT devices flooding the market. Governments also are focused on the changing risk profile that comes from connecting existing industrial operational technologies “OT” to informational technologies “IT” via telecommunications networks.

In the EU, we expect that the newly chartered cybersecurity agency, ENISA, will develop a certification and testing scheme for IOT. In the UK, the government has published a manufacturers Code of Practice for Consumer IOT Security. In the US, the National Institute of Standards and Technology (or NIST, which is part of the Department of Commerce) has published a draft set of IOT security baseline requirements. When completed the NIST IoT Security baselines will likely influence purchasing rules for the US federal government and regulations developed by agencies that oversee critical infrastructure operated by the private sector.

Industry understands the importance of getting out ahead of this problem rather than waiting for government officials to establish requirements through inflexible laws and prescriptive regulations. At Cisco, we are proud to join many esteemed global technology companies—some partners and some frankly fierce competitors—in multi-stakeholder efforts to define baseline security requirements for IoT devices.

In the OT space, we joined the "Charter of Trust," which brings together a multinational, multi-sector group of companies, including Cisco, Daimler, Dell, Deutche Telekom, IBM, Mitsubishi Heavy Industries, NXP, Siemens, with three important objectives for improving IOT security: 1) Protect the data of individuals and companies; 2) Prevent damage to people, companies and infrastructures; and 3) Create a reliable foundation on which confidence in a networked, digital world can take root and grow. The Charter of Trust effort recently expanded to include an associate membership for government agencies, beginning with the BSI in Germany and CCN National Cryptologic Center of Spain.

In the more consumer-oriented IOT space, we helped found the Council to Secure the Digital Economy (CSDE)—composed of USTelecom, the Consumer Technology Association (CTA), and 13 global information and communications technology (ICT) companies, including, AT&T, CenturyLink, Cisco, Ericsson, IBM, Intel, NTT, SAP, Oracle, Samsung, Telefonica, and Verizon. This organization in turn convened technical experts from 19 leading organizations throughout the ICT sector (collectively called "C2"). The C2 group itself is an impressive assembly, including: BSA, US Chamber of Commerce, CTA, ITI, NCTA USTelecom and UL to develop and advance industry consensus on baseline security capabilities for new devices, which were recently published.

As I noted, improving device security is foundational. But there is also a vital role for the network to protect devices that may not be able to protect themselves against being attacked. In addition, poorly secured devices can also be used to launch attacks. For example, recall the "Mirai" botnet about two years ago, which leveraged poorly secured DVRs and cameras to launch Dedicated Denial of Service (DdoS) attacks against other computers and network infrastructure.

Cisco is leading the effort to develop standards that will enhance coordination between device makers, network vendors, and system operators. One such standard developed through the Internet Engineering Task Force (IETF) is called called Manufacturer Usage Descriptions (MUD). Using this standard, “thing makers” can declare expected behaviors for their devices. Then the network can become a plane for visibility and control, which will enable decisions as to whether a device is acting in an expected or anomalous fashion.

Let’s take the example of a connected lightbulb, if we compare the behaviors declared by the device manufacturer with actual observations we may see activity not expected from a light bulb—like making telephone calls or ordering pizzas. We could then deem those behaviors anomalous and block them. The IETF standard will make this process more efficient and authoritative enabling device manufactures to describe expected behaviors in a standardized, structured, and testable format. Any activity that does not match an expected, white-listed behavior could simply be blocked without manual human intervention.

At Cisco, we are excited about this approach and are working to make it commercially available through an association calle IoTopia, which is driving adoption of open standards for security by design, device intent, autonomous onboarding, and lifecycle management. The US government is also working on this MUD standard. The US National Institute of Standards and Technology is following up on a joint recommendation by the Departments of Commerce and of Homeland Security to study the efficacy of the MUD standard as a network risk mitigation strategy. With the participation of about 20 different companies, they built a simulated network environment. Upon completion, the results will be published along with an extensively documented guide to enable further research and practical applications.

Trusted 5G Networks:

Finally, I want to talk for a moment about the coming adoption of 5G mobile networks, which will again offer new security opportunities and challenges. Much of the talk about 5G characterizes it as a race—perhaps one we are losing or already have lost. But the "Race to 5G" is a misnomer. The transition to 5G is not happening all at once. Instead, it will happen in waves or phases that will take years.

The first part of that effort relates to allocation of spectrum. These networks will likely be made up of various blocks of spectrum—each with different characteristics. Once spectrum is allocated by national governments, radios can be deployed and handsets can be sold. This will boost speed and drop latency by virtue of the increase reliability of the Radio Access Network (or RAN) and the ability to perform computing functions at the edge of the network.

The core of the network is and will remain important—even as we move more functionality to the edge. For now, the "core" of the network supporting the operation of the edge or RAN is the same as the 4G core. But we will see again another significant advancement in the capabilities of the network once we refresh that network core. Cisco plays a key role in ensuring the speed, reliability, and security of 4G networks today and 5G radio networks as they are being built. But we will bring new capabilities to 5G networks when the core is also refreshed.

All this begs the question of why we should care about 5G. Is 5G just faster 4G? Much of the conversation today focuses on consumer wireless broadband speed and performance boosts that will come from the build out of 5G networks and the deployment of 5G mobile handsets.

Advances in the consumer market are always exciting, but...let's not lose sight of what these technologies can bring to the industrial and enterprise spaces.

Honestly, it is hard to know what will be the "killer app" of 5G today any more than we could have foreseen the development of broadband video streaming services, like Netflix or Hulu, when we brought fiber to the home or 4G to Mobile devices. There are high-speed, low latency applications that will boost productivity and innovation in the enterprise that we cannot yet imagine...enabled by customized "flavors" of 5G delivered in the form of specialized "slices" of the network.

What we can predict with some certainty is that there will be more intelligence at the edge of the network—sometimes referred to as "mobile edge compute." More computing power near the edge of the network means that traditional notions of "core" and "edge" may start to blur. This will change the security landscape in at least two ways. First, there will be more threat surface because the devices at the edge won't necessarily push decision making into the center or core of the network. Instead, more data and metadata will be generated and consumed at the edge.

Second, there is a potential for significant improvements in security if we leverage the distributed nature of the network to layer in visibility and control over the security of devices operating at the edge. Together, these two changes underscore the importance of building 5G mobile network using trusted parts from trusted vendors.

Governmental concerns around 5G break down into three fundamental areas: First, how to improve the security of the devices at the edge of the network that will be connected to 5G.

Second, how to ensure reliability and trustworthiness of the vendors supplying technology that will make up their 5G networks. Third, how to manage non-technical risks to ensure a diverse marketplace of trusted suppliers who can compete on a level playing field for business.

This first point ties to what I said earlier about all the IoT and OT "things" we will attach to the network via 5G and a complementary technology called WiFi6...and the importance of industry-led efforts to establish baselines for security of those devices, like the "Charter of Trust" and "C2". At the same time, this leads us to security concerns around the importance of 5G networks that are unique. Not only do the devices themselves need to be built with security and trust by design and by default, but governments are looking to ensure the security and trustworthiness of the vendors supplying the equipment used to operate this network.

As for the network itself, there are technical approaches to managing vendor supply chain risk that focus on review, testing, and certification of equipment to achieve product assurance. Some argue you can mitigate the threat of data exfiltration by layering in encryption to protect confidentiality of communications, or by reviewing source code, or by segmentation and isolation. But these approaches will not prevent access to metadata—which are often as telling as contents of communications. Also they will not protect against attacks aimed at disrupting or halting operation of edge network devices.

This is why when thirty-plus nations gathered in Prague earlier this year to discuss how best to ensure the security and resilience of 5G networks, they focused on both technical and non-technical aspects of risk. The non-technical approaches they discussed included transparency of funding, of ownership and of the rule of law governing operation of vendor businesses. Requiring standards-compliant, interoperable, open interfaces, like those advanced

by the Open RAN Alliance (of which Cisco is a member), is also one particularly noteworthy effort aimed at reducing risk of future vendor lock-in.

CONCLUSION

The global challenges we face together implore us to collaborate in connecting the world more tightly together with technology. While our world is complex, technology properly deployed can reduce complications we experience in our daily lives. AI, IOT, and 5G are among the tools at our disposal. And we cannot afford to leave them on the table. Instead, we must work together in the spirit of the MOU that we signed with OEA calling for the establishment of Cybersecurity Innovation Councils, to both improve the security of the "things" themselves and to harness them to secure networks. I thank the OEA again for the opportunity to join you today and I thank all of you for your attention.