McKinsey&Company

Finding a strategic cybersecurity model

June 2017

Protecting critical and sensitive information is of paramount importance in business and government, but plans must be in place to handle inevitable breaches too.

Cybersecurity has become one of the biggest priorities for businesses and governments, as practically all of life migrates its way to data centers and the cloud. In this episode of the *McKinsey Podcast*, recorded at the Yale Cyber Leadership Forum in March, Sam Palmisano, chairman of the Center for Global Enterprise and the retired chairman and CEO of IBM, and Nathaniel Gleicher, head of cybersecurity strategy at data-and-cloud-security company Illumio, speak with McKinsey about how governments and companies can vastly improve their cyberprotections.

Podcast transcript

Roberta Fusaro: Cybersecurity has become one of the biggest priorities for businesses and governments, as practically all of life migrates its way to data centers and the cloud. In this episode of the *McKinsey Podcast*, recorded at the Yale Cyber Leadership Forum in March, we catch up with two leading thinkers on security issues. Sam Palmisano is the retired chairman and CEO of IBM, who served as vice chair of the US Commission on Enhancing National Cybersecurity. Nathaniel Gleicher is the head of cybersecurity strategy at Illumio, a data and cloud security company.

First up from the forum is Sam Palmisano, who, in this wide-ranging conversation with McKinsey's Marc Sorel, makes the case that strong cybersecurity programs are critical for improved innovation and economic growth.

Sam, thank you for joining us today. I want to talk a little bit about your work on the Commission on Enhancing National Cybersecurity. What was the original mandate? What was the process by which you came up with your findings? And what were some of the most surprising results?

Sam Palmisano: Thank you, Roberta. The thing was that President Obama had reached the conclusion that the digital economy or the Internet is so fundamental now to economic growth and society that something needed to be done to make some recommendations to enhance it

or strategically position it for the future. A great example is the Internet of Things, because it's no longer just phones and desktop computers. It's everything in life. It's self-driving cars, it's thermostats, it's music players, it's cameras.

Now you take this infrastructure and you're making billions of things that are computers, which are smart devices. But that's what they are, they're chips with software with all the vulnerabilities, unless you design for security from the beginning. And you've taken this problem and you've put it on steroids.

The complexity there is one of getting consensus to go fast and address the issues prior to billions of things being out there that aren't secure, which is the path we're headed down.

Marc Sorel: How do you think about what the private sector, and to some extent the social sector, need to do now to be part of that?

Sam Palmisano: We need to form a private-public collaboration. The reason for it, the government doesn't have the skills to do this themselves. We spent nine months crawling through their statements of skill. They can argue all they want. They don't. That doesn't mean that elements of government don't have some skill. To take the intelligence agencies out of this discussion and get to that commercial side, it doesn't have the capability. They need the capability, so they had to form a partnership. The skills exist in the academic community and in the research universities and in the technology community.

Marc Sorel: Did you all as a commission see a model in the market today for what that collaboration could look like?

Sam Palmisano: There are established entities within government that are a combination of academic, private sector, government, and technical. A lot of the technical communities come together.

General Keith Alexander ran the Cyber Command Center. There were probably 20 of us that met once a quarter for five, six years. The same guys that were running IBM, Google, Dell, Microsoft, HP, and Verizon, plus all the government appropriate people would meet quarterly. The technical people would meet even more often to tackle some of these issues, and it was self-funding. We solved problems just by pitching in because it was in the best interest of everyone to solve some of these issues, and in the best interest of the industry because you wanted to expand and grow.

To really do this, though, this was going to require funding, To solve the problem we're talking about, it's going to require some amount of money and research, like a DARPA or related fund, pick something like that as the funding source that government can coordinate, and then convene this body. Then do the work as we suggest. Now, the work is going to get complicated. Because there's two pieces to it. One is, let's say for example, to come up with a standard for the Internet of Things that you would put in this device, this object. Then within that object, you'd have this standard. Then you'd also have a nutrition label on the standard. We

called it the Cyber Star. It's like the health seal that says, "OK, if you're the manufacturer and you've complied with these standards, you get the star." You get the Cyber Star.

There were also guys that recommended a thing called secure, they call it clean pipes. With clean pipes, there are a lot of policy implications, a lot of criminal-justice-systems implications. But technically, you could create a clean path and you could have a secure path, and you could argue for certain areas where life is threatened.

In the autonomous vehicles or drones or things where people could actually be seriously injured or die, you'd want a secure, clean path. You don't want this on the open Internet.

Marc Sorel: So you're talking about creating a separate secure environment for these privileged parts of the ecosystem.

Sam Palmisano: Right. Think of it as a commercial virtual private network but beyond that. Put that on steroids from an encryption and security perspective. For all these Internet of Things devices. Health, heart monitor, things you're putting in your body. Pacemakers, et cetera. Defibrillators. Those kinds of things. Not Fitbits that you wear on your wrist, but serious things that could do serious harm like stop your heart. You want to have that information flowing in a secure way. In an encrypted, secure way. That doesn't mean everything should be that. If you're sharing your photos with friends, I don't think you need that level or cost associated with those kinds of technologies.

Marc Sorel: You're basically saying at some level, there should be a tiering of Internets to acknowledge the degree of security required for different pieces of the ecosystem to communicate.

Sam Palmisano: That is a solution to the problem. Now you have to make it commercially viable, which gets you into things like net neutrality. But if you were to technically solve the problem, you would begin to architect portions of the Internet. You can't go recreate the past. It's just too old, it's too cobbled together. Let that be what it is.

But anything that's life-threatening or takes down the infrastructure or the world economy. Let's just start there. The premise or the assumption is that you can't solve this in the Internet as it exists today. It just was too complicated. It's too convoluted. It's too open by design. That's why it was so successful, because it was an open architecture. We had all these debates, all of the technical guys. And said, "Look. We used to do this 40 years ago." ATMs never got hacked. Money didn't start spitting out on the curb and stuff because it was a secure connection. It was, it was a proprietary network. We know how to do it technically.

But there are people that did these things for years. We've moved onto an open innovative system which is terrific because it drives innovation at a much more rapid pace. It also gives people more economic opportunity to participate. That's a big plus. But in certain areas where you're dealing with, let's say, major societal issues, we ought to go back to some of the classical approaches to how you design the systems.

Roberta Fusaro: Most people today would say, "If I had to place a bet on who's going to gain ground on whom and put space between themselves, it's the attackers that are going to continue to distance themselves in terms of capability from the defenders in terms of their capabilities." Do you agree with that?

Sam Palmisano: Eighty percent of the cybersecurity issues that have occurred in the commercial world are internal process and people. It's not the disgruntled employees who got fired and therefore they gave somebody their access codes. It's also people who didn't protect their access codes or they tape it to their computer. Or they leave it in the top drawer of their desk, and the cleaning people can go get the stuff. You would get rid of half of your problems as an enterprise if you just train your folks and put controls in place.

It's a combination of monitoring, process training, audit people. Did you follow the process? So there's an accountability in the system. That'll clean up a lot of the stuff in the commercial world. Password authentication and end points. If the civilian side of government, .gov, did those things, they would clean up probably 95 percent of their problems and save a ton of money, too.

We also talked about this idea, which never got traction in the commission report, but we thought it was a good idea where you basically would create a national ID like a credit bureau. You could create this national ID foundry where you get your birth certificate. You also get your digital identity at birth, and that digital identity is secure and protected. Now, you can modify for simple things—sharing your photos on the Internet—or you can modify it for very sophisticated things like financial transactions, your health information.

Marc Sorel: Why didn't it catch on?

Sam Palmisano: In the commission itself?

Marc Sorel: Yeah.

Sam Palmisano: What we did was said, further studies should take place, and we recommended that Treasury would look at, further look at creating this kind of an entity. We also looked at commercial insurance as well, and the purpose of commercial insurance.

The purpose of commercial insurance was that if you agreed on the standards, and therefore you complied with those standards, you should be able to get higher liability coverage at a lower rate than somebody who didn't.

Our view was that would drive up the adoption rate because people are going to want to find an insurance policy for cyber. That's going to happen. How do you get these companies to make the investments to move up the risk-protection curve? Well, you make it to their advantage by having insurance that says, "We could audit those standards. And if you've complied with those standards, like burglar alarm systems or fire alarms in your home, you're going to get higher liability coverage at a lower rate." That's to make it an economic-based system versus a government-mandated system. The commission was very biased toward private-sector

solutions versus government-mandated solutions. You need a private sector or an economically driven set of motivations to solve the problem.

Roberta Fusaro: This has been a fascinating conversation. Thank you, Sam, for taking the time to be with us today.

Sam Palmisano: Oh, thank you. It was great being with you.

Next up from the Forum, is Nathaniel Gleicher, who describes how businesses can learn a lot from the model of protection used by the US Secret Service.

Roberta Fusaro: Welcome, Nathaniel. Thank you for joining us today for the *McKinsey Podcast*.

Nathaniel Gleicher: No problem. Glad that I could join.

Roberta Fusaro: Your company has been providing cyber options for four or five years now, and I'm wondering how you've seen the market change over that time in terms of what customers are looking for or technologies that have emerged.

Nathaniel Gleicher: There used to be a perception that cybersecurity was black magic, particularly outside of the technical community, and that outside of that community, people would sort of say, "I don't understand this. Just make it work." As long as you don't hear anything, no news is good news. The increasing scope and scale of breaches and the degree to which organizations are moving into these exposed environments has changed that. If you look at business leaders, I think they are focused on how do you quantify the risks that you face, and how do you measure the benefit that you're getting from the solutions you invest in? It's a much more quantification-driven industry than it used to be. I don't know that we're very good at quantification yet. But the desire to quantify is an important change.

Roberta Fusaro: Apart from quantification, are there other hot topics in cyber that you're seeing or managing right now?

Nathaniel Gleicher: Sometimes I think we do cybersecurity like fourth graders play soccer. Chase the ball across the field, the whole group runs. There are always hot topics. What's interesting to me is that we've known for a while there are a few steps that if you took them, environments would be much more secure.

If you think about encrypting data, using strong passwords, white-listing your applications, segmenting your environment, patching your vulnerabilities, and people generally haven't done that because it's been hard to figure out how to do that at scale across these large organizations.

One of the biggest challenges that we face in cybersecurity today is that we don't really have a single, coherent strategic model to describe how to protect an environment. There are a lot of tactical models, so if you look at the SANS top 20, if you look at NIST, if you look at some of these other frameworks, they will tell you, you should be investing in encryption. You should be

investing in segmentation. You should be investing in certain kinds of detection. They'll tell you all the tools you should use and you can think about how to line them up, but it's very tactical. It's hard to find a model that lets you pull back and think about the threat as a whole.

I'm starting to see groups of companies trying to solve that problem, trying to think, how do you do these steps that don't seem all that sexy, but that actually drive to security.

Roberta Fusaro: What are some of the potential remedies?

Nathaniel Gleicher: If you look at security disciplines through the ages, whether it's law enforcement, executive protection, physical security for locations, military security, any of these sort of well-built disciplines, the foundation of every security discipline is understanding the environment you're protecting and exerting control over that environment.

In cybersecurity, we are not good at understanding the environment we're defending. Most organizations don't understand the network. They don't understand what's connected and what's communicating with what. Because of that, they have relatively few options to control that environment. I mentioned before a few simple things people could do to strengthen their environment. Those are all about control, and what I mean by control, people often think there's prevention, keeping the bad guys out, and then there's detection and response, catching them once they get in.

Those are both important components. In general today, people would tell you, you can't invest all in one or the other, that prevention by itself isn't enough. People are going to get in. What people miss in that debate is the reason detection and response works is because you understand your environment, and you control it.

If you don't know where your high-value assets are, and if you don't know what connects to them, how someone would access them, it's incredibly hard to know what you need to protect. If you don't have the resources to control that, you're defending an open field. So you have hundreds and hundreds of paths you need to defend, potential connections you need to worry about, and the attacker gets to move first. On the flip side, if you invest to understand your environment first, and control your environment first, it actually makes detection and response better.

Roberta Fusaro: What are some ways to identify the crown jewels, the things that really do matter? I can imagine that that could be an incredibly difficult task, given all the assets that companies manage.

Nathaniel Gleicher: It's different for every organization, to some degree, but it's about understanding business risk. The question is, what are the assets that I defend, or that my business relies on, such that if they were exposed or compromised, it would fundamentally harm the way I do business?

Whether that's health care data about your customers, or customer information, whether that's the systems on which your business runs, whether that's the exchanges across which you

connect, every business has a different set of factors they need to judge. But often, if you think in terms of business risk, we're pretty good at figuring that out because businesses have been measuring and concerned about risk for quite some time. It's just a question of translating that and understanding the technical implications.

A model that I like to use when I think about this is the way the Secret Service protects the president. The president is a lot like a high-value asset in a data center, in that he's very valuable, very targeted, and also very exposed. The Secret Service doesn't get to take the president, put him in a box somewhere, and have him not talk to anyone. He's constantly talking to people, so the job is really about managing risk, which is similar to the way we're protecting assets in the data center.

When the Secret Service is protecting the president, if you imagine the president speaking in an auditorium, the Secret Service shows up months before the president is going to be there. The first thing they do is they map the auditorium to understand that if the president's going to be here, speaking on this stage, here are all the attack vectors. Here are all the ways someone could reach the president. An auditorium is built for openness, so there are going to be a lot. The Secret Service tries to control that environment, to shrink the number of attack vectors. The reason they do this is, as we said before, if you have to watch a hundred attack vectors, it's really expensive, and you're really spread out thin. If you have to watch 20, you're in much better shape as a defender. So you can say we don't leave this doorway open, and no one's going to sit in this portion of the auditorium. You can close things down to simplify your environment. That's important for a lot of reasons, but the biggest reason is it makes detection much easier.

If there's a section of the auditorium where no one is supposed to sit, that doesn't necessarily mean no one will show up there. People always do strange things. But if someone does, you know they've broken a policy. It's not a false positive. There's no risk of confusion. You can simply react, and it lets the Secret Service act much more quickly because rather than basing their actions on uncertain analysis, they're basing it, they create firm boundaries. When someone breaks a boundary, they know what to do. If the Secret Service wanted to, they have a lot of resources, they could put a metal detector at every seat in the auditorium.

They could put one at every single seat. They could get the best metal detector in the world. The problem is, they would never do that. They would get thousands and thousands of alerts and lots of them would be because someone had a particularly heavy watch on, or had change in their pocket. Whatever it might be. In order to test those alerts, they would have to send Secret Service agents out into the auditorium to check each one. And Secret Service agents are really expensive, and they're rare. It takes a long time to train them. They're hard to find. What you really want to do, is take your precious resource, your Secret Service agents, and you want to direct them at the hardest, smallest slice of the problem.

So take that and apply it to the data center. If you are detecting everything everywhere, and you don't have control over the environment, you're going to get a lot of alerts. The statistics we see right now back that up. Organizations get 500, 1,000 critical alerts a day, which is a huge number of alerts that supposedly you have to deal with.

On average, organizations say they have the capacity to investigate something like 1 percent of them. So you're investigating 1 percent of all these critical alerts. Quickly you start to turn things off because that data is dirty. If you're following the model, you would do the same thing the Secret Service does. You don't put a metal detector everywhere. What you do is you control the environment. You limit the places people can be, the paths they can take, so you know where to watch. So you know if this is my high-value asset in my data center, then if anything strange happens there, obviously it should be my highest priority. If anything strange happens in something connected to it that might be a secondary priority. You can start to prioritize these alerts and focus on the problems that matter more.

Roberta Fusaro: What are some of the policies or regulations that are emerging that business executives need to concern themselves with?

Nathaniel Gleicher: In a lot of ways, 2017 will be a year of regulation in cybersecurity. Not exactly the regulation people think about. I don't know that it'll come from DC. SWIFT, the financial-transactions organization, recently put out controls that all of its members need to comply with to segment and protect their SWIFT application.

This is in response to all the criminal activity targeting SWIFT applications. That's one. The New York DFS, the financial regulator, put out controls around cybersecurity quite recently. The European Union recently put out a new general data-protection regulation, which has a whole range of controls built into it, but there are specific pieces around where is data stored, and how is it stored, which raise serious concerns for companies.

There are a lot of pieces coming out from different places, that depending on what industry you sit on, you need to watch. The pattern that I'm seeing, though, is each of these has components that require organizations to do a better job exerting control over the data in their possession.

Organizations have said, "My data just pools in all these places. I don't even know where it is. It moves through these systems too fast for me to follow." It has been acceptable for companies not to know answers to these technical questions. You're seeing these regulations start to come out that push back on that. There's this increasing requirement on organizations to understand what's happening in those systems, and where that data's going.

Roberta Fusaro: How might this increased oversight affect companies' ability to innovate? So many new business models are data- and analytics-driven.

Nathaniel Gleicher: There's this old apocryphal joke that if we built cars like we built computers, cars would go 500 miles an hour, get 500 miles a gallon, and blow up once a week. We've made this choice, historically, around computer and Internet innovation that the consequences of unreliability aren't all that high.

We'd rather have rapid innovation, but what's happening now is more and more you see the technical world, the Internet world, colliding or reconnecting with the physical world, whether it's autonomous cars, whether it's health innovation like you're seeing, whether it's integrating smart solutions into the home, whether it's integrating smart solutions into our transportation framework.

There are more and more opportunities integrating technology and smart solutions into the financial systems that our society runs on. There are more and more opportunities for surprisingly small bugs to cause very big chain effects in the physical world. The push and pull that you're seeing is how do you maintain the pace of innovation that has been so valuable, and such an engine of economic growth, an engine of competitive edge for us, while still mitigating the risks of all of these autonomous systems, and more and more sophisticated systems that are impacting the physical world.

Roberta Fusaro: What are the opportunities for VCs and start-ups in this changing environment?

Nathaniel Gleicher: There are huge opportunities in pointing artificial intelligence solutions and orchestration solutions at problems that are incredibly hard to do at scale for large organizations. We tend to think of cybersecurity as a technology solution because that's convenient.

The truth is, it's really an organizational solution. If you only have one computer, obviously anyone can make a computer secure by turning it off. But if you have one computer, if you have one system, a sophisticated defender is going to be much better able to protect that than if you have a thousand systems and hundreds of employees, or 10,000 systems, and hundreds or thousands of employees.

The challenge is getting large organizations to operate in a coherent fashion, when large organizations are made up of people, and we aren't always good at operating in a coherent fashion. What organizations really need, and where there's real potential, is how do you make it so those things we talked about at the beginning, encryption, strong passwords, segmentation, white-listing applications, patching vulnerabilities can be done reliably, consistently and at scale because if we can do that, we would solve a large chunk of our security problem.

Roberta Fusaro: Nathaniel, thank you so much for joining us today.

Nathaniel Gleicher: Thank you for having me. ☐

Nathaniel Gleicher is the head of cybersecurity strategy at Illumio, and **Sam Palmisano** is chairman of the Center for Global Enterprise and retired chairman and CEO of IBM.
Roberta Fusaro is a senior editor of McKinsey Publishing, and **Marc Sorel** is a consultant in McKinsey's Washington, DC, office.

Copyright © 2017 McKinsey & Company. All rights reserved.