The CEO Forum

The Quarterly Publication ***by CEOs for CEOs*** $19.95

Industry Cloud
Infor
Charles Phillips
CEO

Digital Infrastructure
Siemens USA
Barbara Humpton
CEO

Startups
JC2 Ventures
John Chambers
Former Executive Chairman & CEO
Cisco Systems

Healthcare
EmblemHealth
Karen Ignagni
President & CEO

Cybersecurity
Forcepoint
Matthew Moynahan
CEO

10 CEOs Transforming Business Through INNOVATION

Culture
Round Room
Scott Moorehead
CEO

Media
Worth Media
Juliet Scott-Croxford
CEO

Telecommunications
Nokia
Risto Siilasmaa
Chairman

Technology Innovation
Avnet
Bill Amelio
CEO

Data Ownership
SRAX
Chris Miglino
CEO & Founder

Matt Moynahan CEO **Forcepoint**

Forcepoint opened the company's Cyber Experience Center in Boston in April and hosted a ribbon-cutting ceremony featuring, left to right: Massachusetts Governor Charlie Baker, Forcepoint CEO Matthew Moynahan, Raytheon Chairman and CEO Tom Kennedy, and U.S. Senator Edward Markey of Massachusetts.

"You have to be vigilant 24/7 in our space."

The CEO Forum Group selected Forcepoint as the innovation leader in cybersecurity for creating the new approach of human-centric cybersecurity. This new model focuses on the intersection of users and critical data, and has stopped countless attacks before they could happen.

Robert Reiss: Until recently I had not heard of the name Forcepoint, but you've created a different model in cybersecurity. And, frankly, over a trillion dollars has been spent on cybersecurity and it seems everyone is still getting attacked.

Matt Moynahan: I'm not surprised you didn't know it. It's a new name. The combined expertise from our early companies is 25 years, but the new Forcepoint is fairly new, only two-and-a-half-years old.

Forcepoint is a purpose-built security company from several different companies designed to change the way you solve the security problem. Our approach is around understanding what really matters most to organizations, which is their people and their interactions with content and critical data. So, you're right, a trillion dollars has been spent. It could be considered one of the biggest failures in modern industry, but the threats are so advanced that the thinking needs to change.

"The first thing for you to think about as the CEO is: What data do I have that could be important to my company, critically important, such that if it was stolen, it might impact the market value or brand of that company?"

Explain the Forcepoint model.

Quite simply, we've changed the way we try to secure things from thinking about infrastructure, which is the old way: trying to prevent people from getting in – classic walls and moats. It's been proven that you cannot secure the internet. You cannot secure a corporate infrastructure fully, so people are getting in. Second, the number one attack vector right now to get in is stealing people's identity; credential theft.

In summary, instead of trying to monitor all the technology in your company, we try to provide a safety network for your employees, customers and partners by understanding what normal behaviors are. So that when those identities or credentials have been stolen, we're able to tell when hackers are inside of your company because their behavior is different than that of your good employees. It's a behavioral-centric approach to how we stop bad things from happening.

So it's a double whammy, it hits the individual and the corporation?

Exactly. So we said let's flip this model on its head. Let's try to understand what do people typically do? What do good people do, what do bad people do? Let's go create an understanding of what "good" looks like instead of worrying about all the technology. When we see outlier behavior, where it would suggest that someone's identity has been stolen and there's two Roberts on the network, it allows us to understand who the good Robert is and protect the company. So, it's just a different way to think about what you need to secure.

From our standpoint, it's really around understanding what bad people have penetrated your organization, what data are they touching, and how do you stop that, while at the same time allowing the good employees, which are the vast majority, to go about their day without friction in the business processes.

Are most of the bad people already in the company, or are they from outside the company?

There are three types of bad. One is really bad actors, and those could be in the form of nation states or various types of hackers that have penetrated the company and gotten in. The two other types of bad things that happen are typically done by good people. There is accidental leakage. People make mistakes all the time. The second type are adversaries that have stolen identities and gotten in. Understanding the behavioral patterns of people inside of your company really allows you to surface the needle from the haystack, so to speak, without all the blinking lights of worrying about infrastructure. We're very excited by this.

Since everyone is probably being attacked at all times, what should a CEO do first?

Almost every company is a target at some point in time. The world is powered now by data. The first thing for you to think about as the CEO is: What data do I have that could be important to my company, critically important, such that if it was stolen, it might impact the market value or brand of that company? So, naturally, folks will immediately go to things like customer data or blueprints of products we're building or engineering designs. That's absolutely critical. But it gets a little bit more sophisticated than that. What data do I have or do I produce that, if it got in the wrong hands, could do damage to me personally as a CEO?

First and foremost, what sort of data exists about me from my own personal brand as leader of this company, which obviously is attached to the company brand or company data, that if it got in the wrong hands could have a significant negative impact?

What types of vital information should CEOs be aware to protect?

We're routinely protecting blueprints of really sensitive

products. It could be sneakers, it could be refrigerators, it could be jet airplanes, it could be trading algorithms for hedge funds. If that information gets out, it's very, very easy for that to be replicated.

Every single day, if you look, there are nations all around the world who don't have the same respect for intellectual property that this country may have, or there are multiple use cases for this type of technology and it is under attack. That's number one. Number two, we do look for other types of information that could be used to do harm to your company like press releases that could cause stocks to trade in advance. Any type of information that could be abused, you really need to, first and foremost as a CEO, get your arms around that.

As you work on the human side of breaches, what's an example with a CEO?

I'll give you a real world example of a CEO for a fairly prominent company. It was on a Saturday. This gentleman was off from work, checking his email over the phone while at his son's soccer game. His son scored his first goal so he's very proud, naturally. The CEO then went and posted a quick message to his Facebook account, which he didn't use that much, and said how proud he was of his son scoring the goal. He immediately had a "parent" of one of his son's teammates send him an email saying that she caught the first goal on video and how proud she was of him, and if he wanted to get access to that video, he should please send his email.

Now, it happened to be China who sent that email, not a parent of his son's teammate. This gentleman never used Facebook much, but this is how intense the scrutiny is over CEOs, boards of directors, and key employees. They are the number one attack vector to get inside of a company. Going back to the approach that Forcepoint has, once your identity has been stolen and there are two CEOs on the network, how do you identify which one is the real CEO? And it's through behavioral patterns.

Behavioral patterns – how do you do that?

Every person has a certain rhythm to the way they go about living, right? You could view it as simple as a habit. When you get up every morning, what do you do? Do you check your phone? Do you log into work? Check your email? Drink a cup of coffee?

I get it. Brilliant. I assume this is done through digital?

Audience gathers at the Forcepoint Cyber Experience Center for a "State of Cybersecurity" fireside chat with CEO Matt Moynahan.

Forcepoint's new Boston location features the company's state-of-the-art executive briefing center and global center of excellence for behavior analytics.

"Think of us as painting a picture of normal behavior patterns of a human being. We use that to protect them. So when someone has stolen the identity and gets on the network and is doing bad things to a company, we can tell what good and bad is. Hackers don't know how you go about living your daily life. So, it's very, very hard. It's easy for them to steal your identity; it's hard to replicate who you are."

There's also a technical wizardry behind the scenes, but it has to be done with respect to the privacy of all individuals. First and foremost, it's collecting fragments from the way people go about and interact with digital technology. Think of us as painting a picture of normal behavior patterns of a human being. We use that to protect them. So when someone has stolen the identity and gets on the network and is doing bad things to a company, we can tell what good and bad is. Hackers don't know how you go about living your daily life. So, it's very, very hard. It's easy for them to steal your identity; it's hard to replicate who you are.

So we paint a picture of that behavior and then when things get bad we will in fact let the companies know. Those companies will then go and let that employee know that their identity has been stolen, and maybe change a password or take protective measures. It's really almost creating a personalization, a curated type of security for each and every person on your network to make sure that you protect them from some of these new modern threats.

And who do you deal with in that company…the Chief Security Officer? The CIO?

Depending on the size, in a smaller organization it might be the head of IT who may also be responsible for security. In larger organizations that would be the Chief Security Officer, Chief Risk Officer, or CIO.

In summary, instead of trying to monitor all the technology in your company, we try to provide a safety network for your employees, customers and partners by understanding what normal behaviors are. So that when those identities or credentials have been stolen, we're able to tell when hackers are inside of your company because their behavior is different than your good employees. It's a behavioral-centric approach to how we stop bad things from happening.

When you look at security, what's wrong with our approach today?

I think the security industry, as you mentioned earlier, needs to be changed. There has to be a paradigm shift in

The Forcepoint booth was a hub for meetings and demonstrations at the 2019 RSA Conference in San Francisco.

"We started everything from our mission and vision to understand cyber behaviors, and we needed to make sure that the mission-oriented culture was driven through everything we did, and any customer interaction felt that."

the way people think about things because the old way clearly isn't working.

You became CEO in 2016. What were some of the first things you focused on?

It was really interesting coming into an environment where there were three companies when I came in, and then we went and purchased five. It was a very rare opportunity to go put in place the first culture for the combined company.

Typically you don't get that, typically you have to be a startup, otherwise you're coming into a large organization when the culture is already baked. So this was actually the rare opportunity of putting in a culture for the first time. Actually it turned out to be a competitive advantage for us because we said, "Let's create a mission-oriented culture to solve this specific problem and align everything we do around accomplishing that problem for our customers." So we started everything from our mission and vision to understand cyber behaviors, and we needed to make sure that the mission-oriented culture was driven through everything we did, and any customer interaction felt that.

So it started with the people, and we do have this concept called radical candor, which is essentially giving people straight talk with the intent of helping them improve their performance….not with the intent of being critical or political or backstabbing. And in a company that's coming together that didn't have historical execution fabric or execution DNA as a single company, we really needed people to talk straight talk. If you did it in a bad way the company would have been pulled apart. But if you create this culture where people do it in a good way, the gravitational forces pull it together. And that's what we've been doing.

So how is it working?

It's fantastic. We routinely get emails from people who have joined the company recently that talk about how welcoming it is and how it's rewarding and intrinsically motivating. You can't just be nice. It's got to be this intrinsic motivation to help build a company. I think people feel like they're personally vested in doing that.

We do a lot of work in many, many different industries ranging from governments to financial services to what have you, and the things that we've been able to prevent from happening have ranged from suicides to cases of active terrorism.

"We really needed people to talk straight talk. If you did it in a bad way the company would have been pulled apart. But if you create this culture where people do it in a good way, the gravitational forces pull it together. And that's what we've been doing."

When you monitor behavior you can surface a lot of things. Everything becomes a use case of human behavior. If you see someone walking down the street that looks happy, you know they're happy. If they look sad, you're like, "Hey, what's the root cause of that?" On the Internet, you don't have the physical cues. You can't see people to go help them or watch out for them. So essentially, when you monitor behavioral patterns on the internet, yes you can do some things like stopping identify theft and credential theft. But you can also do some amazing things like stopping acts of terrorism. You can stop things like suicide, because everyone's got different signs. It's almost like understanding the symptoms of a problem.

In the digital world, you don't see it typically. If you surface that in a way where the proper folks – whether it be HR or a general manager – can go help someone, you can do that type of thing.

So let's talk about your leadership philosophy. I know you like lobster hunting. Anything you could learn from lobster hunting that ties into leadership of cyber security.

It's an eat or be eaten type of industry!

Touché.

I've eaten many lobsters, and I've enjoyed it, but they're very prickly characters. One thing I've liked about cyber, and it's kept me in there for 20 years, is that it's a very, very hyper-competitive industry, and you have to be vigilant. Almost going back to Andy Grove, 'Only the paranoid survive.'

It's very, very true. I think you see several of our larger competitors out there who, quite honestly, have stopped innovating, and that has opened the door for us to come in and do something that is paradigm-shifting. You have to be vigilant 24/7 in our space. The nice thing is when you're motivated to change the world in a mission-oriented type of way, you have that sort of extra kicker. It's not just about making a profit, this is around actually trying to change the world and we feel that here.

People are feeling that sense that you can make the world a better place.

The immersive and interactive Forcepoint Cyber Experience Center showcase brings to life today's evolving threat landscape for enterprises and government agencies.

Absolutely, absolutely.

Let's shift to sports. I know you're a big Patriots fan, and I'm seeing now you actually look a little bit like Tom Brady. Any leadership lessons you could learn from the Patriots?

It's about not getting enamored with superstars and thinking more in terms of the system that you put in place. I think that's really important. It's not just the Patriots. There have been several dynasties you can point to. In rugby we have the All Blacks, and there's several of those reference models. We try to make this a sum of the parts type of company and culture. When everybody knows their job and knows what's expected of them and comes to work every day trying to do their job, great things can happen. We operate in an industry that has 30% normal attrition rates. When someone leaves, you've got to have the next person step up and fit into that system and what's expected. There are lessons to be learned from those types of organizations.

Let's go back and summarize what CEOs need to do to prepare for cybersecurity attacks.

The threat environment has completely changed over the past two decades. It started out with people trying to defame Amazon and wreck websites, to credit card theft, which now feels completely minor in the big scheme of things. There are major things that are happening ranging from terrorist events to intellectual property theft designed to bring companies down. The first thing for a CEO is really to be aware; don't think you're not a target because you are. There is someone out there that finds value in something your company is creating, for some reason. Try to identify what that is.

Start with your data, most importantly, and then try to take a look at your workforce and try to put in place increased protections for those that are interacting with that critical data to keep your company from harm.

A pleasure having you, Matt, on the CEO Show.

Thank you Rob, I appreciate it.

Robert Reiss and Matt Moynahan – Interviewed March 31, 2019.

Matt Moynahan is the chief executive officer for Forcepoint. Under Moynahan's leadership, Forcepoint launched a bold new approach to cybersecurity, centered upon enabling customers to focus on what matters most: understanding people's behaviors and intent as they interact with critical data and systems everywhere.

Before he joined Forcepoint in 2016, Moynahan held a series of senior leadership positions including as president of Arbor Networks, a DDoS service provider; founding president and CEO of Veracode, an application security services provider; and vice president of Symantec's Client & Host Security and Consumer Products & Solutions divisions, leading the latter to $2 billion in annual revenue.

Moynahan holds a bachelor's degree in economics from Williams College and a Master of Business Administration degree from Harvard Business School. He currently serves on the board of directors of Care to Compete, a nonprofit organization supporting athletes with brain damage and chronic traumatic encephalopathy, and is a member of the Big Brothers Big Sisters program.

FORCEPOINT