John Carabias: The dynamism in the attack vectors continues to grow. One thing we're seeing particularly, Steven, are attackers using AI to improve their techniques across many areas of offensive security. Phishing, impersonation, vulnerability discovery, things like evasive malware generation. This type of attack continues to grow, both in the commercial and government sectors. And so, that forensics capability and the sophistication of it, the ability to rapidly respond, is something that we're providing to a number of customers.

Steven Ludwig: Welcome to Inflection Points, a podcast series from Jacobs. I'm your host, Steven Ludwig. That was the voice of John Carabias, vice president growth and sales strategy for Critical Mission Solutions Jacobs Cyber. We sat down with him and Eric Conway, technical director for Cyber Security Capabilities and Solutions Jacobs Cyber, and we talked about all things cyber: security, infrastructure, operations, data, machine learning, and artificial intelligence.

It was a really interesting conversation about where cyber is, where it is going, and what government organizations and businesses can and should be doing around their cyber operations. The Jacobs podcast is where we meet the people that help create solutions that deliver a more connected, sustainable world. And now, with that, it's on with the podcast.

So, Eric and John, can you introduce yourselves and tell us how you got involved with Cyber? Eric, do you want to lead us off?

Eric Conway: Sure. So, my name's Eric Conway. I am the technical director for the Jacobs Cyber Business Unit, and for the last 20 years or so, I've been an engineer supporting cyber solutions in support of the intelligence community, and the Department of Defense, focusing on cyberspace operations.

Steven Ludwig: And John?

John Carabias: Yeah. So, this is John Carabias. I'm the Vice President of Sales and Strategy for our cyber business unit. Spent most of my career in the computers command control, ISR area, which is referred to as C5ISR, that really has included cyber. Over the last five or six years, I've been doing that in the DoD space, originally on the program side with a Homeland security. But most recently with DoD, and now the intelligence community, in both a technical and a business development capacity. In addition to that, I'm an adjunct professor at Loyola University in Maryland, where I teach a course on information systems to include artificial intelligence and other contemporary IT applications, like cloud and mobile computing.

Steven Ludwig: It doesn't sound like you have a lot of free time there, John.

John Carabias: No, I've also got a five month old, so free time is scarce, Steve.

Steven Ludwig: So, when I hear someone say cyber, I always think they're leaving out the rest, cyber security, but I understand that cyber is its own, complete category. Can you explain what cyber means when they use just the term cyber? Eric, do you want to take that?

Eric Conway: Sure. That is a topic of discussion quite frequently, when you have a term like cyber that's used in many scenarios. Cybersecurity is an aspect of cyber, but cyber also, I believe, encompasses communication systems, intelligence surveillance reconnaissance, or ISR.

Steven Ludwig: I'm sorry, Eric. What is ISR?

Eric Conway: Intelligence surveillance and reconnaissance.

Steven Ludwig: Great. I'm sorry, please keep going. I just want to make sure we all can understand.

Eric Conway: Sure. Yeah. So, I think cyber encompasses that. It encompasses standard information technology, which we usually refer to as IT. It includes operational technology, which we refer to as OT. Industrial control systems and all of the networks that connect all of these devices, all wrap up under this cyber umbrella. And cybersecurity is a specialty area of the securing of those networks, and those systems to prevent attacks, data theft, privacy invasions, and financial theft.

Steven Ludwig: So, from all those things that you shared, that seems there's a lot of areas requiring a ton of investment for companies or government agencies. How do those organizations figure out how to prioritize what they should look at first? Because I'm sure every thing that you mentioned, and then some, are critical. John, do you have some insight into that?

John Carabias: Sure, Steve. So, I think what we're seeing is we thought that most companies had done an analysis of their cyber transformation and accreditation journey. And we're finding, through GAO reports inside the government space, that they hadn't done some of that good blocking and tackling to make sure that they were cyber secure to be begin with.

But I think what's most interesting that we're seeing is part of digital transformation across the government IT market. We're seeing not just a move from legacy service stacks to cloud, not just a move to component containerization, where we're seeing entities begin to develop applications and build new software inside their IT environment. But we're also seeing how do we secure that once we modernize our IT infrastructure.

So, we're seeing them go on this transformation that is referred to as this digital transformation journey. And what we're trying to say, oftentimes, to our client is how do you think about the cyber vulnerabilities at the beginning of that journey? The terminology oftentimes is baking cyber in from the beginning. So, we're really trying to provide an offering that helps them take that entire journey across many of those IT elements, and make sure they're considering cyber at each one of those intervals as they adapt and incorporate those capabilities into their IT infrastructure, Steve.

Steven Ludwig: So, that's super interesting. That's just a lot to bake in. I like that phrase, baking in cyber of from the beginning. And it seems, if I were the head of an organization or the manager of a unit or something, that's a whole lot to take in. How do you help people not become overwhelmed with the task? Especially if they're dealing with, we're seeing in the government right now, and a lot of companies, they have these huge legacy systems that are out of date, and very few people remember how to code them. So, Eric, what are you seeing in how you help people from becoming overwhelmed with that?

Eric Conway: Well, the problems have to be addressed one at a time and you have to start with assessing what you have currently in your network, or what systems you're trying to secure. So, that's usually the first step, is we start with an assessment. That helps to narrow down the problem to specifically what a particular customer has. So, for example, a local water utility, they know they need to secure their utilities against, say, ransomware attacks, but they often don't know where to start.

So, that assessment is that first step where we can say, "Okay, you have this many controllers. You have this many computers connected to your network. You have laptops here. You have control systems here." And that helps to divide the problem up into manageable segments. Then, we can apply vulnerability assessments and industry best practices, and we can do it in a more methodical way, and work through the problem one element at a time. And that way we can provide, also, a much more holistic approach to security. We can help them secure both their information technology systems, as well as their operational and their control systems. And we can do that with any customer.

John Carabias: And Steve, let me add one part to that, that we're seeing increasingly inside the US domestic government market, which is ensuring, once the technology is in place, and you've got perhaps some of the vulnerabilities identified, and those other things in place. Now, ensuring that you've got a cyber ready workforce that can maintain and operate, and has the expertise to understand what's happening on the network, and adapt to what is really a dynamic threat environment right now.

We're seeing that's a real need, as well. And we're spending a lot of time thinking through the specific needs of our different customers' permanent cyber workforces. What are those types of skills and trainings? How can they continue to adapt themselves, based on the new emerging threat vectors that seem to be coming about. We're spending an inordinate amount of time thinking about that problem, in addition to putting in place the right cyber capability itself inside any given government environment.

Steven Ludwig: That's really interesting. You know, one of the things that you just pointed out is the difference, if I'm understanding correctly, between data and all that important. And I think that's where the public thinks of the privacy, when someone breaks into a system and steals social security numbers, or what have you. But then you're talking about operations, like operations of a water plant, operations of a oil and gas pipeline, operations of a utility grid. So, that seems like those are some pretty big things that people have to look at. Is the approach similar? This idea that you do the assessment, you look at where the holes are, and then you begin to do a project plan? Is the approach for both data and operations similar?

Eric Conway: Yes, I think that it is similar. The ideas you assess, your risk, you assess your vulnerabilities, and based on the risk that you've identified, and the vulnerabilities that you've identified, and any technical gaps that you have, you then put a plan in place to address those risks, so you can mitigate the vulnerabilities. And that process holds true for operational systems, for data systems, for information technology.

A lot of this is wrapped up in national standards that have become very widely adopted. In fact, they've been adopted internationally, from the National Institute of Standards and Technologies. They have something they call the Risk Management Framework, which has quickly become the de facto standard for how to secure an information system from attack, how to reduce it from a risk based approach.

Steven Ludwig: Great. And so, I think with any major disruption in a country, either natural disaster or something, and clearly we've seen it with COVID-19, some organizations can become distracted from looking at cyber security, while others are acutely aware of new vulnerabilities, from using. Like, "Oh, we're a lot of remote meeting software, like Zoom or Google, or what have you." What have you been seeing, and what are you recommending to Jacobs clients, as they're looking at the new vulnerabilities they might be seeing in this, and how they should continue to pay attention during a pandemic or, going forward, any sort of business disruption?

John Carabias: So, certainly, some of the first questions that were asked were, "As I'm moving my workforce to a teleworking infrastructure, how do I ensure that applications like Zoom or Microsoft Teams or Google Hangouts are secure?" We did see, initially, some attacks on VPNs, and the Department of Homeland Security has done a good job of helping a lot of large corporations patch those vulnerabilities.

We saw some attacks on the supply chain as well, post-pandemic. So, we've helped some of our customers address some of those vulnerabilities. But as we think about what, here at Jacobs, we're calling the next normal, and the future of work, we expect this to really catapult the nature of work to being more remote. And so, some of the large questions we're asking are how can we, one, secure that, but how can we help our clients design some unique ways to think about the types of work that can be done more remotely, and the types of work that need to be done in an office space. And using an offering we have called Insights as a Service, there is some interesting analytical work we are doing that'll produce some puristics to help our clients answer some of those very questions.

Steven Ludwig: Yeah. It seems like I've spread out my risks by having all these laptops or home computers. I mean, business travelers have been taking laptops for a couple decades now, so that's not entirely new. But all these different vulnerability points has to be causing some headaches for people. Eric, are you seeing that? Or how are you seeing what John shared?

Eric Conway: You're absolutely right, Steve. What you're referring to is called the threat surface. When you analyze your risk, you look at where all the threats can come from. In traditional IT systems, the threat surface is usually defined by a well defined perimeter. Inside that perimeter, you have your corporate resources, your company resources, your network, and everything outside of that perimeter is considered to be suspicious or untrusted.

With both the advent of cloud technology that we've seen over the last decade, as well as the trends towards mobile computing. And now, with COVID-19, the telecommuting workforce, those traditional threat surfaces have changed dramatically. And that's going to usher in a completely new way of defining your security boundary for a given company, or for your corporation.

Steven Ludwig: Yeah, it sounds like there's a whole lot for people to think about, especially in this shifting environment, that we're going to see for quite a while. Now, when it comes to cybersecurity, for me, it occurs common wisdom, if there is such a thing, really thinks that, if your company or agency is the target of an organized attack from organized crime or bad actors like Iran or North Korea or Russia or China, there's not much you can do except take it and then recover. Now, this is a two part question. Is that true? And should we think of these things separately from ransomware attacks that you mentioned earlier, where people like, "We'll unfreeze your computers if you give us money."

Eric Conway: Yeah. So, ransomware. You mentioned the ransomware that we talked about earlier. The most common way a ransomware attack takes hold is usually through a phishing attack, which is when targeted emails have been sent to an unwitting user, who opens the email, clicks on the link, the link results in the download of some malicious file, which installs itself on that user's computer. And then, they do a lateral attack from that computer to another computer on the network, until they get to the sensitive servers where they can lock the server up, and then hold that server ransom.

We've been able to observe changes in just malware as well. Mass distributed malware, which is traditionally found with signature based malware detection and antivirus programs, has really evolved into identity attacks, where there are attacks on the identity of users, or application driven attacks. And these all require new ways of approaching cybersecurity, where we're using things like insight as a service. And we're using machine learning to understand the behavior of malware, rather than try to identify it from a signature based approach.

Steven Ludwig: But what can a client do, or is there much they can do, if they have a major organized attack from, as I mentioned, another country or organized crime?

John Carabias: Yeah. So, just very quickly, we do have what we call forensics capability, where we will come in and really unpack that attack to understand the raw attributes. Typically, these things have a signature that our team can corroborate with signatures of other attacks. And then there's a whole process for the way in which we attempt to mitigate that action. A lot of that is done in a very quiet fashion, quite frankly. And those are services that we have provided for both commercial and government customers. So, that certainly continues to be an important need we see within industry.

As I mentioned earlier, the dynamism in the attack vectors continues to grow. One thing we're seeing, particularly, Steven, are attackers using AI to improve their techniques across many areas of offensive security. Phishing, impersonation vulnerability discovery, things like evasive malware generation. This type of attack continues to grow, both in the commercial and government sectors. And so that forensics capability and the sophistication of it, the ability to rapidly respond, is something that we're providing to a number of customers.

Steven Ludwig: Talking to two experts like you, it really sounds like, yes, it's challenging, but there are systems and approaches in place that you can methodically begin to look at all these issues in a way that lowers the blood pressure. And it just becomes a matter of sophistication and project management. So, that's been the very interesting. Now, you mentioned AI. So, I want to talk a little bit about that. How does a company figure out or a government organization, how machine learning, better data analytics and artificial intelligence can help them? What are some questions you think that they should be asking themselves around those areas? Eric, do you want to lead off you?

Eric Conway: Yeah, sure, Steve. With artificial intelligence and machine learning, the real benefit comes from the ability to process the massive amounts of data that are coming through our customers' networks. We have security operations centers that are processing literally billions of messages per day. And the ability to have a manual analyst go through all of those messages and identify indicators of compromise, it's impossible to do with humans in the loop, or entirely with humans in the loop. And that's where artificial intelligence and machine learning can really have impact on our customers' ability to secure their networks.

Steven Ludwig: John, did you want to add to what Eric shared?

John Carabias: Yeah. So just a short addition to that. We've got a matrix that we often used to say, "Look, is AI applicable here?" And that is, one, does this problem require us to make large complex calculations? Two, must we transfer a large amount of information quickly? And three, does it require us to make a series of calculations rapidly and accurately? And if the answer to that is, yes, there's often an application of AI.

And we've seen this in use cases, now, from customer service to HR, to productivity and collaboration, to analytics. On the industrial AI side, we're applying this to quality control, supply chain management, fleet logistics and routing. So, with that simple calculation, when customers bring us a problem, we're often able to say, "Yes, there's a way that machine learning can augment human intelligence to solve some discreet business problem you have."

Steven Ludwig: That's really interesting. Now, I have to admit my own ignorance and something, and I think people listening might have the same challenge, which is why I'm bringing it up. Is there a big distinction between machine learning and AI, that's easy for everyone to understand?

Eric Conway: Well, machine learning is primarily the ability for a computer to learn, to recognize certain patterns in data from being trained on large quantities of data. So, for example, you can train a machine learning model to recognize something like command and control, network traffic, and many, many, many terabytes worth of network data that's been collected. Artificial intelligence is the application of that knowledge to make decisions, to support decision making. So, it's using the machine learning models and the output from the machine learning models to make smart decisions.

Steven Ludwig: That's super helpful. So, it's one and then with the other. That's really interesting. Now, when it comes to trends in the whole area of cyber, what are you seeing right now? And what do you think's coming down the pipe, as far as cyber infrastructure that people should be paying attention to? 5G came up. I think there's been a lot about that. So, what are you both seeing? John, do you want to lead that one?

John Carabias: Sure. So, I'd start with, on the application side, application delivery scale and complexity is just growing, growing as a result of, as I mentioned earlier, component containerization. So, things like Docker and Kubernetes, where you host these software applications. There's a whole security infrastructure that must be built around that. And then, as cloud adoption continues to scale inside the government, how are you securing that infrastructure? Mobile computing, that is disrupting the traditional market and redefining both network and server security requirements. And then, as I mentioned earlier, we're seeing attackers use AI in new and interesting ways to launch attacks. So, I think those three things are the largest, most widely applicable types of trends that are occurring in the enterprise IT market for our customers.

Steven Ludwig: Interesting. Eric, are you seeing the same stuff or do you have anything you want to add to that?

Eric Conway: Yeah, I totally agree with what John was saying. And at a lower level, we're seeing our communications networks evolving, and they're evolving rapidly. We've mentioned 5G a couple times and the changes that's going to bring. And also, we see, for the last 10, 12 years, we've seen a major trend towards what we call the IT/OT convergence. That's information technology and operational technology converging. The generic use case of that would be a factory that has a bunch of controllers controlling their equipment, have now plugged these controls systems into the internet, to gain the efficiency of being able to monitor and control their operational networks from a mobile point. But the problem that brings is you've now connected your physical and your logical infrastructure, and you've made the physical plant, whether it's your robotic machinery or the pumps in a watering station, or your electrical utilities, they are all now connected to the rest of the internet, which means there are paths and vulnerabilities that make them vulnerable to attack. So, we see a big convergence there, and we see a great need across our customer base to help them secure those connections.

Steven Ludwig: This has been a fascinating conversation, and we've covered a lot of areas, and I think we could easily take an hour or two on each. And Eric and John, what I really appreciate is how you explained these very complicated topics in a way that's not only interesting for lay audience, but also offer something for people that know more about it. Now, we covered a lot of territory. Is there anything that I forgot to ask, that you'd want to add or let people know about that I failed to mention?

John Carabias: No, Steve, I think we covered all of the big, impactful trends across the cyber market, as well as some of the capabilities right now that we're delivering to our enterprise government cyber customers.

Steven Ludwig: Great. Now, how can people reach you or find out more information if they have some questions about Jacobs and your cyber capabilities?

John Carabias: Steve, you can reach us and find out more about our cyber business at jacobs.com.

Steven Ludwig: Great. Eric, John, thank you so much for your time. This has been really interesting. A great conversation.

John Carabias: Glad to be with you, Steve.

Eric Conway: Thank you, Steve.

Steven Ludwig: Thank you for listening to Inflection Points, a podcast series from Jacobs. Find out more, please visit jacobs.com. Jacobs, challenging today, reinventing tomorrow.