Industry Leader Q&A: Cyber Security

OI's Frank Casale Talks Cyber Security with Xerox's Mark Leary

Frank Casale: Mark, welcome. I thought we would start with some basic questions. You have a very impressive background...in your words, could you tell us a little bit about your background and about your current role?

Mark Leary: Prior to coming to Xerox, I was the Chief Information Security Officer for TASC. It was a professional services firm predominantly focused on the Federal Government contracting arena.

Prior to that time I was with Northrop Grumman, a large aerospace and defense company. I was mainly involved in the IT services to the Federal Government. I spent about 12 years with Northrop Grumman. TASC itself was a spin-off from Northrop, so I was part of the leadership team that took that company private.

Frank: You obviously also have some government experience?

Mark: Over 20 years of military experience, mainly in military intelligence and also in what the Army calls Signal Corps. It is mainly the IT communications arm of the Army.

Frank: Let me play off of that. For the most part it seems like a majority of people in this space right now come from the government public sector. If you think about it, if you go back about a decade, this was something that predominantly government worried about and business executives did not worry about.

What do you think is the driver behind this cyber security and cyber threats, in general, being so high on the radar of IT executives and business executives these days?

Mark: You are absolutely right. Information security has been engrained in the government space for many, many years because of the information which they handle.

With the transformation of IT across government and the interaction they had with the citizens. Open government was promoted, but as they opened up government to the Internet, it exposed the government to a varied landscape of threats.

There have always been at the lower end of the threats those who are experimenting trying to gain access to systems, but, also, the very sophisticated threats, particularly those which are nation-state sponsored.

The government had been focused on that problem for many, many years, but I think it was actually what I call "the age of enlightenment" around 2008-2009 when the government not only noticed attacks and attempts to gain access to their networks, but also to their supply chain.

From that perspective, the government has many, many suppliers. It is not just aerospace. It is also small businesses and mid-sized businesses. What was then shared with industry was that the threats posed against the government from a nation-state sponsored perspective were the very same threats which were targeting the supply chain.

The government began to educate industry and that wave of education and information-sharing then found itself into many other different verticals that are not necessarily delivering to the government. Within other verticals, they were seeing the very same problems around the mid-2000s and 2008 period mainly in financial services and banking.

They had the financially motivated actors who were targeting those particular industries. Their data is highly monetized, right? They are very much into transactional activity that involves dollars or currency or some monetary value. They became targeted, as well. I think around 2008, industries across many different verticals became intensely aware of cyber threats and the varied types of actors who were targeting them.

Frank: How about your current role over at Xerox? Can you talk about that?

Mark: I am the Chief Information Security Officer for Xerox. Again, I have been here for just under a year. I am the Global CISO for Xerox, so I have oversight for governance and delivery of our security program across our technology business and our services business, so my role is enterprise-wide.

Frank: Is your focus 100% internally or is Xerox getting into the business, so to speak?

Mark: My focus is both internal to our security program and external to ensure that the security within the service components is embedded and part of the overall solution.

For example, on our technology side we have partnerships with many different security vendors. We have our own internal security developers who are building security into the product and into the master system.

On the services side, as we go to market with particular capabilities or solutions, I have oversight to ensure that those components which are security-related are being addressed in those solutions. As an offering from a managed security service provider, Xerox does not offer that.

Frank: That makes total sense. The media has a way of taking things and sometimes it communicates what is going on and it is not unusual that it may magnify what is going on. There are those who believe that this cyber security threat is real, and there are maybe just as many who believe that a lot of this is hype.

What is your sense? Is it a myth? Do people really need to be concerned about this?

Mark: I think based on my experience in aerospace and defense and with professional services to the government both as a supplier and then as providing those services to the government, **I think the threat is all too real. In fact, I think the general public is under-informed to the degree and scope of the problems that are facing not only the government, but also industry.**

Frank: Wow, okay. The next question here is just related to trends. I am curious, Mark... are there two or three overall trends in the industry that you think are worth noting if somebody is trying to familiarize themselves with this arena?

Mark: I will give you the security professional's perspective. We are currently in what I call the "perfect storm." We have a lot of the swirl within Congress and within the Executive Branch to bring along new regulatory pressures and cyber security mainly focusing on critical infrastructure. However, it is extending.

Earlier there were new regulatory pieces and acts that were put in place to govern aerospace and critical infrastructure. A lot of discussion at the Hill today is across the board, to put in some type of national regulatory framework to govern over cyber security.

Obviously, industry has some concerns around that from an over-regulatory program. The costs incurred during the SOX rollout were not inconsequential. This could have the potential of being the same type of impact on industry.

The second pressure is one that you related to in the litany of emerging technology. We do have mobility and cloud and consumerization of IT, and the rollout of these different technologies combined with new business models, from my perspective, it is a rushed market.

Any technology that is rushed to market has traditionally not had security built into it. While these new business models are adopted, it is important to understand the security implications around it.

The third pressure is the sophistication of the threat that takes advantage of the weaknesses in the new technologies being rolled out.

You look at these three pressures and they are generally the same pressures across any industry that CISOs are faced with today.

Frank: Maybe this is not the right question, but let me take a stab at it. Who should be the most stressed and concerned right now? I know one answer is "everybody in the organization." Where is kind of the center of gravity, though, of where this all needs to be handled and figured out? By that we mean a good plan, good execution, and minimal risk.

I know the CISO is the person driving it, but from the standpoint of whom you are working for internally, is it CIO? Is it the CEO? Is it the business leader?

Mark: I would say from an organizational reporting perspective, I report to the CIO. I will tell you, though, my role and my function is across the business. I meet regularly with the board and our audit committees to talk about risks to the business.

It is about the business, right? I am sure if you went to other verticals and had this discussion, they may have a different orientation. However, from a Xerox perspective, I interact quite often with the board. I interact with Ursula and our new CFO, Kathryn Mikells.

Again, a very important point to make is that **cyber security is not IT security. Cyber security is an asymmetric threat. It is a multi-threaded threat that requires all functions to look at how they are engaging with the business and building security into their processes.**

I will give you an example. One of the issues we face, one which many companies face, is the common phishing attack. This is a very specially crafted email to trick the user to click on a link and then some malicious software is loaded onto the teraframe point. They use that first entry point to then move laterally across the organization.

If you decompose that, the core issue here is the employee and education. Obviously, I am going to partner heavily with our learning and development and HR staff, right? The issue is not necessarily the malicious software itself. The point of infection and the employee's actions are what led to the infection, so I am going to heavily partner with our HR folks.

We may have potential for an attack regarding one of our business partners; maybe a specific segment of our suppliers is being targeted. I am going to partner heavily with our procurement and contracts folks to ensure that we have some way of vetting our suppliers and that their business processes and their business systems have a level of security.

We are going to have a business-to-business connection and we do not want to introduce risk by having a supplier that does not have the same degree of care around their level of security. I am going to partner heavily with procurement.

I think those two examples illustrate that the role is not just an IT security role. The role is a business executive who coordinates with adjacent functions in order to reduce the risk to the company.

Frank: That is a very good point that you make. In line with that, I also notice from your bio that you are certified both in electronic as well as physical security. Am I close with that?

Mark: Yes. Actually, I have really focused on maintaining three certifications and three degrees of knowledge. One is in the domains of physical security. That is obviously important like gaining access to a building or even a server closet.

The IT security is, I think, self-explanatory in having knowledge of that.

However, I am also certified in IT governance which is much more of a business role. I rely on my MBA and my Project Management Professionals certifications from an actual project and business management.

I think you will find that the days of an IT security guy or information security guy being just one dimension are over. The security professional, particularly at a corporate level, is more of a business executive with an expertise in IT security.

Frank: Right. How often do you fairly secure an environment where somebody walks out with something like a thumb drive of valuable information? Maybe that organization felt that they were secure, but someone was able to get a physical device, walk down the hall, and walk out to the parking lot. What is wrong with that picture?

Mark: This gets back to one of the questions you posed. What is the old mentality? The old mentality is the castle mentality. You build walls around the enterprise. You put a lot of protection in place and you are very compliance driven. I think all of that is appropriate, but I think it is only table stakes.

Most of the security professionals in my peer group have basically abandoned that paradigm. The paradigm of today, particularly because of the threat landscape and the sophistication, is that you make an assumption that the enterprise is already compromised. It is completely assumed that it is and you work from there.

You change the dynamic. Rather than building walls around the enterprise, you protect the data that resides within it and outside of it. We have a lot of deperimeterization with mobility and cloud and it has become more and more about the data and protecting the data.

When you start to change that mindset of the traditional "I'm going to build an IT security capsule wall around the enterprise" and move toward protecting the data as it moves across our enterprise, with our business partners,

and even with our customers, it is an entirely new dynamic, an entirely new paradigm that you have to move toward. I think most are.

Frank: Okay, great. Those are very good points. I want to talk to you about budget. Many of our members struggle with one thing, the ones that get it. They see they need to spend money to do much of this. This is a relatively new area for many of them and there seem to be no bench marks or industry numbers in the sense that "you should spend this percentage of your IT spend" or "this percentage" of some other number.

Do you have any thoughts or advice as to what someone should budget for cyber security or threat minimization?

Mark: First, I would point out that there are some metrics out there around percentage of IT security spend as a percent of IT spend. Usually, you see Gartner and Forrester and other research groups which go out and do surveys and produce some basic metrics.

They are important from a benchmark perspective, but you have to look at the way the research was done, the survey group, and the sample that was taken. Is it representative of my industry? I think the conversation needs to shift.

One, the benchmark is important. We would want to always go back and use benchmarks because we want to know what others are spending. That will give us an indication as to whether our spending is the same as theirs.

I think the much more important conversation is when you go through the annual budgeting process and you are talking with the CFO and with the business partners. You go back to the business and the threats where the business is not meeting its objectives. Then you get more of an enterprise risk management discussion.

Security is very difficult to quantify. How do you quantify deterrence theory to cause them not to take an action? It is very hard to measure from a dollar perspective. Those in banking could probably do it because they are very transactional-based.

You have the discussion with the business leaders on what their business goals are, what their objectives are, and then you map those risks which are IT or cyber related to them that may prevent them from reaching those business objectives. You then look at what investments need to be made in order to burn that risk down. Then you get to a point of where the risk appetite is and how much should be spent.

There are two ways to look at it. One, you have the important conversation with the business around the

risk of them reaching those objectives from an IT and IT security perspective. Then you use those benchmarks from Gartner and Forrester and the corporate executive board and other forums as a check point. The worst thing you can do is drive toward that percentage of spend that Gartner reports as their benchmark. I think that is less meaningful than having the business discussion.

Frank: Okay, there goes that MBA of yours getting in the picture again. You make total sense there. At the end of the day, I agree with you. It has to be looked at from a business perspective. What may have a certain impact on a publishing company would have a different impact on a bank or a financial services institution, right?

Mark: That is right. You are aware that the FCC came out with the new ruling around cyber security risk that it is now discloseable. They are actually promoting the disclosure around that. Again, this is another business aspect. Those risks that we meet with the appropriate risk management plan and those that we accept, we have to disclose.

Frank: Mark, I have two more questions. I want to relate this to outsourcing. You referred before to the "perfect storm". I have to think that the fact that most Global 2000 companies also do a heck of a lot of outsourcing, it is not only, “Hey, do you have your act together?” but do they have their act together. I am sure this has an impact on the overall risk scenario.

What do companies need to do these days as part of selecting vendors to whom they will outsource and/or what should they insist upon with outsourcing providers that they may have been working with for years?

Mark: That is definitely on our radar, managing supplier risk whether it is a product or a service. What environment is that service or product being delivered from? It could have on-premise providers, as well. What degree of assurance is built into that service and product?

You can use very different ways to measure it, but you have to have at least a framework in order to measure it. This is where you want a relationship with contracts and procurement to ensure that they entail or comprehend in their solicitation those security requirements that we would expect.

Really, we look at it from two different ways. The first is equivalency. We naturally have policies around how we operate and how we maintain our environment and how we engage with suppliers. Is there a degree of equivalency there? We ask for some evidence or interviews in order to gain a level of confidence that it is in place.

Beyond that, there is evidence that can be submitted beforehand. There are numerous certifications around ISO standards and audits around the SSAE and SAS audits that are conducted to ensure controls are in place. We request those types of evidence.

Where you get into a very sensitive component of a sensitive system—and I am speaking more from my aerospace background—you may even require some degree of testing. It is not outside the realm of possibility.

I know one of my peers in the banking industry has about 20 individuals doing assessments on their suppliers' sites, generally about 80 a year. This is a portfolio of 800 suppliers, so that is 10% or so. Still, he is looking at it from a risk perspective of how important that supplier is and doing some formal assessments around there.

I think the most important point is to have a framework in place on how you engage with your suppliers and an outsourcing arrangement. Then have some way of vetting and including that information into the bid and into the weighting criteria to award a particular contract.

Once you are part of that conversation or part of that process, then, again, you reduce the risk to the government.

The other side is the perspective of the outsourcer, right? **I have seen more and more outsourcers—Xerox being one—building security in, not bolting it on as additional. We are delivering a secure product or service as a default,** not as them opting out. It is already opted in on their behalf on our product and our service.

From a business perspective, I consider that a discriminator. That is a competitive advantage when you are able to add value that is very important. It is in the press; everybody is concerned about it. If you articulate the value as a discriminator, then it does give you a competitive advantage when you go into competition for particular outsourcing opportunities.

Frank: That's great. Mark, I am curious. If you look in your crystal ball, what do the next two or three years look like? I am not trying to "lead the witness" here, but my concern is that this gets worse from the standpoint of the marketplace. I am stepping back and thinking of Global 2000 and even mid-market companies.

My concern is that this gets worse before it gets better. Am I off the mark there? What do you think?

Mark: I refer back to my earlier "perfect storm." My crystal ball is very cloudy right now because of the churn in the market. I see both the downside and the upside.

The downside is that the threat landscape is dynamic; it is ever-changing. Quite frankly, three years is a long term. From a threat perspective, it is almost monthly, if not daily, that the threats are changing, right? That is pretty scary.

I came into the office yesterday and was listening to NPR. They were covering the hacker convention in Las Vegas where they had talked about hacking a car. Actually, cars park themselves now, so that is pretty concerning if they can actually hack a car and try and steal it. The threat is there.

The upside is that many companies have recognized security as a valued attribute of any offering or product. I see a lot more of the building of that security in, the auditing, and the standards alignment.

I am seeing a lot of offerings now where you would say, "You are taking on a lot of risk. That is an emerging technology. It has not really been vetted as something that is viable." They are actually coming to market and they have a story to tell around security.

The threat is always going to be pretty dynamic, but I do think that suppliers, whether it is products or services, are paying attention. They are, if not vocalizing the importance of security in their product, certainly showing evidence that they are demonstrating it.

I think you could go back to the story around Microsoft which is very successful, I think. I think Microsoft gets some bad press because they do have some what we call "patched Tuesdays." Every month, a patch may come out for their software.

However, they have a very stringent way of developing product and going to market. If you look at the way it was, possibly in the 90s, and compare it with today, they have dedicated themselves to an approach towards security. I think this is the same way that other companies have adopted because of the ability for a company to turn itself around from a security standpoint to be somebody that is kind of flayed in the public press around their product to one that has a model that others are adopting as a success story.

I think other companies are looking at it and evaluating how they are going to market and how they are approaching security as a discriminator in that offering.

Frank: That sounds wonderful. Mark, thank you so much. This is a very exciting arena and you have a very impressive background. I appreciate your perspective. I know many of our members will benefit from this, so I appreciate your time. Do you have any parting comments?

Mark: I think we get back to the earlier point. How much of this is real and how much is hype? I will tell you it is extremely real. I think industry as a whole recognizes that and is addressing it from their perspective and what they are offering to the market.

For more information on Outsourcing Institute offerings & events, contact us at inquiries@outsourcing.com