Eye on Security

A Look Back and a Look Forward

Transcript

Luke McNamara:

Welcome to another edition of The Eye on Security Podcast. I am your host Luke McNamara. Joining me today we have General Earl Matthews, the Chief Strategy Officer for Mandiant Validation to discuss FireEye's recent 2021 predictions report. General Matthews good to have you here.

General E. Matthews:

Yeah thanks Luke. Great to hear your voice.

Luke McNamara:

Well it's great to be talking about this new report that just came out that you have been part of putting together with folks from across the company and what really struck me reading this report is that it's much more than just a threat landscape, which on the intel side of the house I'm more familiar with, but it really goes into looking at how the business environment is changing, how organizations are changing, how they think about threats, and the technology that they're using particularly in this pandemic. So I guess my first question for you is in putting together something like that how do you think about taking the lessons that we've learned in the past, what we've been seeing this year, and then extracting that out forward into the next year with this sort of predictions product?

General E. Matthews:

Yeah Luke, you know I've been in this business for a really long time and I've had the fortunate pleasure of both being a CIO and a CISO, Chief Information Security Officer, and then also on

the operational side being the recipient of those kinds of services. And what's always striking to me is that we come back to basics. So the number 1 problem is still the number 1 problem, which is cyber hygiene. The number 1 threat vector is still email through fishing. So those things have been there since we started this dance what I would say in the mid-'90s in the wild, wild west of networking.

But what we are seeing here, right, is that we are always going through digital transformation so a lot of investment going to the cloud; you know COVID has challenged companies now with more remote workers than they ever had before. I think 1 of the impressive things that we've seen out of this, because you know people are working – kids are working from home too, is that the IS, the internet service provider resiliency has been remarkable to me. I just applaud them that very people are having bandwidth issues except for me when I work in North Carolina.

But when we pull all those things together, right, and the primary events that we're seeing with ransomware what we're seeing is that organizations need to go back to their basics. Do I have good, quality back-ups? How often am I doing those back-ups? How often do I restore those back-ups to make sure that they're working correctly? How am I handling data protection, especially now? We have remote workers at home, a lot of companies when this first started employees had to use their own PCs, that created a new challenge, we talked about that a little bit on the predictions report, but what we're seeing is that what is old is new and what is new is old and I think that we've just got to go back to 101 in a lot of these cases. Not much has changed; it's just where that attack surfaces at has changed.

Luke McNamara:

Yeah and you mentioned ransomware and we're definitely going to talk about that, but I think it's interesting that when you think about cyber security and that discipline at least involving 2 components, 1 being the technology stack, the assets, the networks, the users that we're trying to secure, but then all the external drivers, the economic, the geopolitical drivers, the things that make up the threat landscape, thinking about the interplay between those things we do see components like ransomware, which is not a new problem, but the way that we're having to deal with it and then like 2020 with the sort of ad hoc event that no one really expected with the pandemic if we were involved in thinking through and putting this together, these core predictions in 2019, that's not something we would've really expected but the challenges that come from all those pieces coming together please out in a way that maybe we have to think through and extrapolate what those second and third order effects of the convergence of all these different things coming together.

General E. Matthews:

Yeah it definitely has I think highlighted the role of cyber security and I think most organizations now fully understand that their entire business rests on information technology and the importance that security plays in that role is now paramount. And 1 of the things that we talked about in the predictions is security, even in this pandemic, security kind of gets pushed back a little bit despite my earlier statement because you've got to get the mission done. And I'm guilty of this myself as a CIO as hey, I'm going to sacrifice a little bit on the risk side because we need to get this mission done and we've got to get people connected and they've got to go be able to do that. And then we've got to quickly though close that gap by bringing up the cyber security and what are the best techniques that we need to be using. Is it multi-factor authentication? Is it a VPN? Is it that now we need to accelerate our desktop infrastructure to be in a virtual desktop infrastructure, VDI, because it's easier to patch on the back end than trying to have to do every little system.

So from that standpoint it's good because it also helps accelerate us getting to what's on our roadmap a lot quicker than we might've done had there not been the pandemic. But I think at the end of all of this it doesn't really matter what's happening geopolitically; it's that we always have to think global but we have to act local. So just like you and I have done a number of times on election security, right, and so now we're through the election and knock on wood we got through it without any major disaster happening or incident happening because we paid attention to it just like we did in Y2K, but we know the adversaries geopolitically, the Iranians, the Russians, and the Chinese, were all intent on trying to upset our elections. And so we've got to think global but we've got to act local.

Luke McNamara:

Yeah, that's a good point and to your point earlier about what's old is new again and what we've kind of teased already about ransomware that seems to be an interesting example where it's not a new problem, it's 1 we've been dealing with for some time, but there's also some nuance to that where components of how we're seeing the actor activity play out this year with respect to combining the sort of data theft and naming and shaming the leaking sites that we've seen has evolved in a particular new way how that extorted behavior is playing out. And again there's nothing necessarily incredibly complex technically from that but the success that these actors are having seems to be drawing new actors in and it's becoming a problem for a lot of different sectors, organizations across different industries.

I'm curious how you've seen how boards have changed how they've thought about security in the middle of the pandemic but also because of ransomware and has that changed their thoughts in how they deal with the disruptive threat that's very immediately known when you've been hit by it, your customers, your vendors, everyone knows as your organization may

experience disruption and have to shut down components? How do you see that play out in the board and how organizations are thinking about security now?

General E. Matthews:

Yeah, I think it continues to be highlighted as a key business factor, a key risk factor. And I would've thought that the WannaCry crisis a few years ago was going to be the wake-up call to it, but when you actually look back and you see how much money they made out of that ransom it was like less than $1 per system that got compromised. The difference now, why I think there's the wake-up call, is that that cost is going up dramatically. Millions of dollars now are being asked for this ransom and unfortunately I think that there's been an overreliance on cyber insurance in order to try to cover that and that is not happening. The cyber insurers are not necessarily covering that for a variety of different reasons we don't have to go into today, but I just think that the demand for these higher ransom amounts, the amount of organizations that are actually paying it has gone up dramatically; the US pays more than any other country. We don't treat ransomware like we treat terrorism when you know for terrorism and hostages we usually don't pay the ransom but we seem to be willing to pay the ransom with our data on that and especially municipalities, public sectors are really highlighted on that. Of course now we've seen in the news the first case of a loss of life due to ransomware with the attack on the German Hospital and the patient had to be diverted to another hospital and ended up dying. And so I think there is a far more awareness now and I think that they're asking more questions about what is our susceptibility to ransomware.

What I'm not seeing, right, is the kids of questions from the board asking, "Hey, how can you quantitatively tell me that we're protected from ransomware? Where's the data? I know you security guys tell me that we are," and as far as I'm concerned they would not accept that answer from HR or finance or manufacturing without seeing the key performance metrics to go along with it. In order to have those key performance indicators you have to have data. That capability actually exists today not just in a snapshot of time. So I see the awareness but I still don't see the level of questioning that they should be asking.

Luke McNamara:

Well we're definitely going to get into discussing validation and how that is evolving and playing out this year, but 1 thing I wanted to zero in on, in the webinar that I would recommend everyone check out around this predictions report, you brought up something that I think has been an underappreciated component of a lot of the ransomware attacks, several of the big families that have been making the news this year, and I think it's kind of been lost in the details but that's the increasing risk that OT assets are being put under by some of these families that are including process kill lists specific to OT assets and devices and the potential

for more lower skilled actors to potentially be entering this space. Could you talk a little bit about that and what you see playing out as that goes forward?

General E. Matthews:

Yeah, I'm actually particularly concerned about this as we head into 2021. We talked about it in the predictions report where all of us who were on there were in agreement that ransomware is not going to go away in 2021. But the part that was particularly worrisome for me was operational technology networks and industrial processes in our most critical infrastructures. And when we look at the number of malware families that are being incorporated to disrupt operational technology it's going up significantly.

Another fascinating part to that Luke is that for the most part when we look at operational technology they have distinctly unique and proprietary protocols in those systems. But as they start to modernize and adopt more IT capability into the ICS and SCADA control systems the attackers really know how to attack those today where they don't have to dedicate a lot of resources to being specialized and have the training to attack our legacy systems. As they start to modernize I think it's going to become a more rich target environment including for manufacturing where there's a lot of OT but we really haven't paid attention to it from a securities standpoint in trying to make those systems more robust. And even when I was the CISO of the Air Force we had lots of long, dedicated conversations about some of our most sensitive systems did we really want to modernize them to an IP-based capability or did we want to leave a significant portion of them still in the analog world but still modernize the system. So it's an interesting debate but I just see it's going to be a problem next year.

Luke McNamara:

Yeah and I mean it's certainly a lower end of the barrier to entry of a space where I think historically a lot of the primary concern had been around Nation State Actors, even specific Nation State Actors that seemed to hold more specialized knowledge around targeting those specific systems that you mentioned and we seem to be entering 2021 in this environment where at least there's a lot of plausible deniability now for a wide range of threat actors but to include Nation States to be able to carry out some very disruptive attacks maybe at a greater frequency than we've seen in the past and just the volume of criminal activity could kind of provide again that deniability to those types of operations.

General E. Matthews:

Yeah I think for me when I consider this area I think this is where there's a direct tie to the

entire supply chain effort that's happening. And you know supply chain risk is nothing new, I just think there hasn't been a lot of significant attention paid to it on there and what we're seeing is really the bad guys now targeting the original equipment manufacturers or the suppliers to get to the whale that they want to get and we can think of Target a number of years ago got in through the HVAC system because it was tied together. And so there was some effort around that but I see what's happening now is just as organizations make it harder for the bad guys to get in they're searching now what is the next weakest link for me to go because I don't want to spend all this time here. Okay, well who are their major suppliers? Who are their major sub-suppliers? And I think they're being very specific targeted towards those suppliers and doing the reconnaissance that they really need to have because if you think about it we really haven't seen a ransomware go around the world like we did for WannaCry and NotPetya and that's because they're being specifically targeted now, the organizations are, with the right type of thing to break in and I'm just really concerned about the supply chain in that regard and I was a victim of that.

Luke McNamara:

No, this is something I want to discuss further because this is not something that we really went into in the report, in the predictions report, but it's something that I think continues to be an area that people are concerned with. I know specifically to the information supply chain when we look at managed service providers, when we look at telecoms, when we look at vendors that may be pushing down software packages into their customers' environment there's certainly a lot of cases and examples where we still see APT actors and others see value in targeting and compromising those sorts of entities. But then there's the whole hardware space, which I think continues to be an area where there's a concern but it also may be a little bit of black box. How do you see, again thinking about this from the perspective of how your experience interacting with boards and as someone who's had to secure very large organizations, how do you see people thinking about okay, there's everything I have to do to secure my own network, my own users and everything, but now I've got to worry about my suppliers, my vendors, and people that may be suppliers and vendors to them? How do you see that space evolving?

General E. Matthews:

Yeah, I see it going down actually a couple of roads. One of them comes back to cyber insurance. I'm starting to see an uptrend in organizations looking at high value contracts from very key suppliers to have separate cyber insurance specific to those contracts because generally the umbrella cyber insurance contracts for that company may not necessarily pay off for that 1 high value contract. So I've – in my public speaking I'm recommending to

organizations that on their critically high value contract they should have cyber insurance on that.

Within that I'm advocating then that as part of your contract that you determine when a customer gets audited versus them providing you the time table of their audits, so it's kind of like an out-of-cycle inspection. "Hey, I want to do an audit of your cyber capabilities," and I think the cyber insurance companies hopefully will say, "Oh that's a great idea. We should go in there," because then that helps really quantify the cyber insurance premium and what it is we're actually covered.

And kind of alluding here too right on these high sensitive contract is a lot of times the security procedures behind that need to be dedicated to that particular project. So I'll just give you the example when I was at US Transportation Command and I was the CIO there and we had a significant intrusion into 1 of our networks. It all got publicized that it was a US Trans Com when in fact it wasn't; it was with our supplier. And that supplier was providing a key algorithm in 1 of our command and control programs. Well it also turns out that this supplier was a subsidiary of a larger defense contractor. So the larger defense contractor certainly had the capability to extend their security capabilities down to their subsidiary and they chose not to.

So 1 of the key things that I come back to when we talk about supply chain is hey, the risk assumed may not be the risk taken and in this particular case the risk taken by the defense contractor was actually our risk and we didn't get a vote in that. And then when we started peeling this back and we started looking at some of the common security practice that should be in place what we found out was the guys who were working on the software were using the exact same PC to check their email, to check their corporate HR site when that PC should've done nothing but be dedicated to the development of that software and if they needed to go do other business they should've went over to another terminal.

And then the final part of this with the supply chain then is really putting in strong cyber language into your contracts and that actually came out of our effort from having been exposed and then that has now led up to what's in the DFAR language now for defense and industrial-based companies.

Luke McNamara:

And thinking about this specifically for that space, I mean I know – I'm familiar with a lot of the activity we've been seeing for years on groups like APT10 or APT40 where the theft of IP we can understand would have a very long-lasting potential lead time till arrival product is maybe introduced or how that IP is being weaponized in some way down the line. When we think about the potential risk that potentially the defense and industrial base and militaries have to contend with in supply chain is it something where activity that we're seeing now today could

potentially be something that as complex as the system is and the strategy that you mentioned makes a lot of sense for trying to dealing with some of that risk, is it a risk that maybe we won't fully see play out into an actual threat for some time?

General E. Matthews:

Yeah, absolutely and you know 1 of the things that again back to that CIO job that I wasn't worried about a destructive attack; what I was worried about was the ATPs causing me enough doubt into our data that it would slow us down and was the integrity of our data where it was supposed to be. And so I think what you have outlined here is entirely possible where we won't know the effect until we're actually trying to do something strategically around the world or with our company, right, from a competitive standpoint that then something will happen. And I'm not talking to you all about a trojan or a back door; I'm talking about something greater than that. And I definitely think that's what's happening and I think we've all heard before, we've already seen the greatest transfer of wealth in our lifetime actually and probably in the world over the last 10 or 15 years through all the theft of intellectual property.

Luke McNamara:

So I knew we'd eventually get there and we've kind of touched on this along the way, but validation, the validation piece of this since this is I know a lot of what you spend your time focused on and thinking about here at Mandiant and FireEye. What is the state of the validation space today in terms of how organizations are thinking about it, in terms of their overall security strategy and posture, and then what you see in terms of adoption? What are we seeing this year?

General E. Matthews:

Yeah, so first let me kind of define what it is that security validation is. It's really an evidence-based –

Luke McNamara:

That would've been –

General E. Matthews:

Yeah, that's okay, no problem at all. It's an evidence-based approach to managing your cyber security lifecycle and it's being done by demonstrating the impact of modern threats and malicious activities in the context of your production environment. And so what that allows you to do now is really proactively identify what are the configuration issues in my security stack and then it exposes then what my true gaps are around my technology but also with my people and process because sometimes we forget about the people and process part of that. And so for the first time we can really start quantifying the cyber hygiene problem that I brought up at the very beginning, which still remains the number 1 problem.

And we have long said that if we could get cyber hygiene under control that would be 85 percent of the effort that our people had to do every day. And we have made a lot of strides towards what we've heard continuous monitoring in this regard and I would say continuous monitoring really was the first kind of step of security validation, which is really understanding what assets it is that I have on my network because you can't defend what you don't know about. The issue with continuous monitoring is that it's actually not telling me is the box working the way that I think it's supposed to be working. And so if we take continuous monitoring and add the word 'and validation' now we can instrument an environment emulating the enemy tactics, techniques, and procedures, running real binaries in my production environment, and start telling me, "Hey, is my firewall actually configured the way it's supposed to be configured or the way that I want it to be configured based on my risk framework?"

And so now we can actually start generating data, creating good, key performance indicators because kind of back to an earlier question you asked what does the board – the board should be asking, "Hey, how well are we doing with data ex-fill of either personal identifiable information or financial information?" right? How is that? And today as a CISO you're responding back, "We have our data loss prevention software and we have it configured and we had an audit and here's what it is." Well what happened when the audit was over because that's a snapshot in time? "Oh, I applied a new patch, an upgrade to my DLP, and by the way the patch said it applied correctly but it actually isn't." And so now we can actually produce the data through automation on exactly how are my controls working.

So that's the initial part of what security validation is about but as we look at it and then we go to the next stage it's, "Huh, so I know how my controls are working and I'm doing a better job of detecting than I am of blocking. Why is that?" So now this gives me an opportunity to optimize my security controls so that I can match it to my risk framework. And why I always keep coming back to the risk framework is because on some portions of our network the data may be perishable so I want a high level of detection but not as much blocking going on because that's giving me an early indicator of what the bad guys might be doing. But on my high value segment I want those things to be almost equal detection and blocking.

Then once I have a good understanding of that from a validation standpoint now I can actually move to what we refer to as rationalization. Why do I have all these overlapping controls? I'm not getting a very good return on investment because I'm only using 25 percent of this capability out of this product. If I could tune this A and C and get rid of B or conversely tune A and B and get rid of C because it's agnostic, it's all about how you have it configured based on your architecture, now I can actually start increasing the return on investment I have.

Then the final leg of the security validation is really at a known goods state then being able to take those things that I'm using for testing, what we call actors, re-roll them into monitors, create an automated playbook, I want this firewall, this port on that firewall to meet these conditions, and I want you to run that test every 3 hours. As long as those conditions are met I don't want to be told about it but as soon as that condition were to change I want to know about it. That's how automation is going to help us augment our teams and then when we do that then your red teams can actually do far more red team actions than they could've ever done before but to me more importantly they can focus on that other 15 percent of the bad guys.

Now the second part of your question was about what kinds of industries, right, are we seeing, what kinds of sectors and right now the 2 sectors that have really adopted security validation is the financial sector and healthcare and you can understand why. The financial sector, they're really worried about protecting the money, personal identifiable information, but they also tend to be the leaders in adopting newer technologies because they have the financial resources to do that in the financial industry. Healthcare on the other end who doesn't have the same vast resources to apply to cyber security actually is adopting it quicker because not only of patient information but because there's a susceptibility to ransomware and they know that fraud is also 1 of the number 1 things. So when you add fraud to ransomware to patient information they're quickly adopting how we're addressing security validation.

Luke McNamara:

It makes so much sense coming from the intel standpoint where in the past if they have a report on APT34 and some new tactic that they're doing and you pass that over to a customer, maybe there's some YARA rules attached to it or some other components of intel that are actionable to them in some way but there's still a difficulty in answering that question of okay, with me as the organization, the security controls that I have in place today if I don't know that I've been hit by this target, if I'm not seeing it, how would I know that if I were to be hit and someone in my organizations were to be sent a spearfish from that APT today that we'd be able to handle it and deal with it from a _____ sense.

General E. Matthews:

Yeah, it actually does and up till now I admit my faults readily. I was willing to put another product into the security stack but I wasn't never willing to take anything about because I really frankly didn't know what was going to happen to it. Now I can use automation to validate that and show exactly why I need to do something. And there's a huge disconnect between what a vendor claims their capability is and what it actually does when I get it into my architecture. There's a huge disconnect between out of the box functionality and its potential to go in there.

I think that no one can really confidently say that every tool in their security arsenal is really adding value so those are the kinds of things that we need to do and I firmly believe Luke that due to COVID and the economic impact on companies cyber security is not going to be left untouched this round. I think the board and CISOs are going to start to have a greater understanding about what is happening and how much money we're spending on cyber security and what is the real return on value and this is where security validation can really come in and help organizations be able to show here's the value that we're getting out of product 1, 2, or 3 and during the Cyber Summit I actually conducted a seminar on rationalization to show organizations how they could actually do that.

Luke McNamara:

And 2 of the sectors you had mentioned earlier that you see as being kind of early adopters in particular, those are also sectors that deal a lot with compliance or have to deal with that a lot. How do you see that compliance and regulation potentially shaping adoption in addition to the economic drivers you mentioned with diminished resources and budgets in the security space?

General E. Matthews:

Yeah, this is where I really think the board will start paying attention once they get exposed that a capability exists for them to generate the data like we're doing with Mandiant Security Validation. I firmly believe it will be a foundational technology in every organization within the next 5 years; it really should be. It should actually be where they start from and the reason why is because if you're a board member of a public company you have a fiduciary responsibility to make sure that you're in compliance with whatever the compliance or regulation you're supposed to because you're going to be held liable for it. And so if you can start then bridging the gap between internal audit, external audit, and the security team and start producing quantifiable data back to your risk framework, show them hey – so for instance PCI. PCI has a lot of different controls and so you can choose which controls within the PCI compliance you want to use and then that's what the auditors are going to be looking for is validation that those controls are in place. Now we can say, "Not only are those controls in place but those controls

are in place and they're working and oh by the way, here's my quarterly report that shows every quarter that it's working."

We have had a couple of customers who they've taken their audit report, briefed it to the board, next quarter they come back, they brief it to the board, and so when they get their audit they go fix everything and then they go brief it to the board, "Here's what we found and then here's what we fixed. We fixed it all." They come back the next quarter and half a dozen things on that same finding from last time is on this quarter and the board goes, "Hey, we thought you fixed it." "Well we did fix it," but there's something called environmental drift that happens every single day because there are hundreds of changes happening on your network and when those changes aren't well communicated and we can show that they're not, things are going to break and it's not from malicious reasons. It could be that someone replaced a piece of equipment, they got distracted, they missed the checklist on a firewall or we applied a patch and the patch broke or you know IT is 1 of the things that we're famous for is we move servers around on the network and so that changes the SPAN ports to change. Well if the security team doesn't know that it was over there they keep evaluating the SPAN, "It's all good, it's all good," when in effect it isn't. Another big problem that we see all the time, right, is from timing. But anyway, I digress, let me come back to compliance.

I really think that we can through automation help organizations take their risk framework, match the controls, and show the efficacy of those controls through automation and it'll make everyone more streamlined and happy about what the actual condition is of their security controls. And so I'll just digress 1 more time: we released in April a Global Cyber Security Effectiveness Report and what came out of that report was that people's perceptions of how their controls were working is not actually how they are. So they thought they were in a higher state of preparedness when they actually were not.

Luke McNamara:

And you add to all that chaos the disruption caused by the pandemic and us working from home, which will no doubt continue at least in the near future and that's a whole other layer of kind of problems in that category that organizations have to deal with in ensuring that what they have is actually working as it's supposed to be mandated. So I guess 1 final closing question, I know in a product of this size there was probably a lot that was left on the cutting room floor in terms of predictions that didn't make it in and there is I think to go back to our discussion around ransomware 1 data point in there that was mentioned that gives me some solace, which is the component they discussed about point-of-sale malware and point-of-sale targeting, how that used to be a much bigger problem and then some of the defensive controls around that, some of the encryption around that data made it less lucrative for the adversary. And we've seen that shift kind of away from that most notably actually ironically with FIN11, a group that was targeting that sort of system into ransomware along with the rest. Any

predictions that didn't make the cut that you feel going into next around ransomware or something completely different?

General E. Matthews:

Yeah, well so I want to reemphasize something that's in the report that we talked about with ransomware and that is we'll see an uptick in ransomware as-a-service, meaning that you can go to an organization and have them execute on your behalf the ransomware as-a-service or you just get a subscription and you just start launching MAZE attacks or Ryuk attacks against whatever organization you want to; that's how easy it's going to be. What we didn't talk about in the report is I see a demand for greater visibility on how controls are actually working, I see greater visibility for more automated, cross platforms versus point product solutions, and we're proud at Mandiant Solutions that we now have 1 portal for Mandiant Solutions whether you're getting Mandiant Advantage, which is the first capability of our threat intelligence that comes out of there. Mandiant Security Validation will be added to that because we can now operationalize the APTs within 2 clicks. You can actually go test your environment that will be there, if you have Mandiant Consulting you'll be able to get that there, Managed Defense, that will all be in 1 portal for our customers and this is where I think what CISOs are actually looking for. I don't need another point solution; give me a platform that integrates this stuff and that's what I'm really proud of that we're doing at Mandiant Solutions.

Luke McNamara:

Fantastic. Earl, always great to chat with you and hopefully the next time we do this it'll be in person.

General E. Matthews:

Yes, that would be wonderful Luke. Great to see you too.

Luke McNamara:

Take care.

General E. Matthews:

All right, bye-bye.