ALLIANCES
PROJECTS

UNITING STRENGTHS

EXPANDING OPPORTUNITIES

CyberSight25

Problem 1

How, what, who - measuring your levels of security?

IVAN MILENKOVIC

Hyb Arloesedd Seiber
Cyber Innovation Hub

REGISTRATION FORM

ALLIANCES
PROJECTS

UNITING STRENGTHS

EXPANDING OPPORTUNITIES

Alliances

www.alliances.global

ALLIANCES X CYBER INNOVATION HUB

WHY?

As the Alliances have access to a breadth of professionals are up to speed on the reality of impacting senior Information and Cybersecurity Roles.

The Cyber Innovation Hub, held out of Cardiff University has partnered with the Alliances to elaborate on it's previous and utilise the community and their knowledge around its initiatives. We will be focusing on:

- Introducing Cyber Innovation Hub – a game changer in spinning science into cyber solutions...
- How is Cyber Innovation Hub solving the cyber problems of today and tomorrow?
- CyberSight25 – defining the solutions of tomorrow
- The Ask from the community and what do they get out of it.

WHAT IS CIH?

Introducing Cyber Innovation Hub – a game changer in spinning science into cyber solutions...

Cyber Innovation Hub is spun out of Cardiff University's Centre for Cyber Security Research (CCSR). CCSR has been operating for a decade and takes a challenge-focussed approach to applied cyber research, having developed strong industry partnerships and seen research translated into commercial processes. To date, spin out companies from this research have been limited. Largely due to a lack of capacity in the academic team to explore markets and develop commercial cases – but equally due to a lack of commercial and business skills within the team to actually take a commercial venture to market.

How is Cyber Innovation Hub solving the cyber problems of today and tomorrow?

CIH is solving this blocker by match-making the academic solution creators with entrepreneurs in the Alacrity Foundation's incubation programme. Alacrity hire business leads and train them in an intensive 12 month programme. The entrepreneurs on the programme are business-focussed, and learn how to identify commercial opportunities, understand customer needs, develop business plans, and take a solution to market. The CIH programme will wrap a team on the Alacrity programme around academic solution creators, and provide them with support and services to scale quickly. We believe this is a globally unique programme – pulling cutting edge scientific intellectual property into commercial ventures to solve the World's most pressing cyber security problems.The Ask from the community and what do they get out of it.

WHAT IS CYBERSIGHT25?

CyberSight25 – defining the solutions of tomorrow

CIH is seeking thought leadership in defining the cyber security problems of today and tomorrow, and is partnering with the Alliances team to run the CyberSight25 campaign. By 2025, we aim to have 25 well defined cyber problems, articulated by 25 of the World's leading cyber experts. This includes CISOs, CIOs, and anyone else who is living and breathing a cyber problem that they just can't find the right solution for – despite all the marketing hype!

The Ask?

There is some time required for input to CyberSight25 – so we're only seeking those who are most committed to the advancement of cyber solutions and mentoring future business founders to support the sector. The ask is as follows:

- An initial meeting to discuss the problem you would like to bring to the campaign
- Some of your time spent articulating what a "good solution" would look like – an outline to guide the CIH in developing a solution
- A 30 minute mentoring call with the CIH entrepreneurs every 2 weeks over a 6 month period during ideation and wireframing of the solution

What do you get out of it?

This is a clarion call for your knowledge and passion for the sector, to shape the solutions of tomorrow, and to mentor the next generation of cyber entrepreneurs!

TRANSCRIPT

Ivan -
I would like to believe that I have a rather diverse experience when it comes to Infosec. Fair to say, more than 20 years of various roles involved with Infosec. Again, different capacities are used to sit in a vendor land as I like to call it. I spent a good portion of my career in consulting. Being part of some large and very interesting MSP's as well, I worked in big multinationals. I worked in a small startup and everything else in between the last almost four years of my career I spent as a group season of a large. To be fair, when I say large I. I probably need. To qualify that. You know, when you talk about the company that's got more than 140,000 people across 60 countries, it kinda gives you the flavour for the scale of the challenge that I was facing actually until this month.

James -
Could you give a little bit of an insight into the objectives in the context of cyber security, that you were facing and and the things that were coming up for you?

Ivan -
When I think about where I was, we had to deal with kind of, you know, worlds top ten in pretty much any industry on one side to some very, very small. Startups, even struggling to get things off the ground and requiring some support to, you know, just get things going. And again, you know, we're talking about anything and everything from healthcare to tech to banking to manufacturing. So a very, very broad set of. Different companies that I had the pleasure of facing from where I used to sit.

James -
Can you describe a cyber security challenge that you face on a daily basis, what specific cyber security challenge? Is or was your organisation facing this?

Ivan -
Indeed, indeed. I guess the starting point is and and I'll tie this to the BPO world at least to start with. Normally the big portion of what needs to be done is defined in a contract. So contractual compliance becomes really a big challenge. Why? Because as I explained, you know, you're dealing with so many different companies, environments, industries, verticals, call it what you want to call it. And therefore, you know, these clients come to you with their set of requirements that you need to satisfy. And ultimately when you look across different industries and when you look across different, if you want risk appetites across the client base, those things can be very, very different. However, because the company itself then. Is in the eye of the storm. If you want, when you look, that entire ecosystem, it becomes evident that you can't only do the things that are defined in those contracts. You effectively have a duty of care if you. Want towards the clients and towards the company itself? Towards the name towards the brand. To provide the correct level of security. Even if clients don't necessarily understand why some of those things are need. And here comes the challenge. You have all those different small bubbles. If you want within your environment, within that ecosystem, as I said, and you need to find a way of actually. Normalising the information across these environments, you need to find a way of measuring things consistently across that entire environment, and you need to find a way, obviously, of then on one side, providing that information back to your management so that they can understand. How the company? Once, but at the same time you need to provide that information back to your clients, because at the end of the day, you know that trust is what kind of keeps the business going. They are really giving you in, in, in some cases, you know keys to their Kingdom. They are putting their crown jewels. In in your hands and you need to show to them that you can protect them to the, to the needed extent.

TRANSCRIPT

James -
How how did that challenge come about, you know and what are the potential risks and consequences?

Ivan -
If you think about it, the main challenge is first and foremost and with security people don't necessarily like to put it like that. And that's one of the biggest challenges we actually turn around. And kind of answer not necessarily in a straightforward way, but you know are you secure and to what extent are you secure and how are you measuring that? And I guess that's the biggest challenge. Are you measuring the right things? Are you measuring them objectively? Are the parties that need to? If you want to consume that information, are they confident that you're measuring things? As I said in the right way that you're measuring those things that are really relevant? And do they understand? You know how that fits further into their own ecosystems. So I guess you, you asked about, you know, what are the risks of doing or not doing it right. You know it's a very, very basic thing if you think about that. Sort of. I don't like the word vendor, but the ecosystem where you have a service provider on one side and a consumer of that service, you know when we talk about many, many things in that arena, we like to talk about, you know, third party risks and this and that. Do we understand what the other party is doing? Do we understand the information that they present to us because, you know, we hit them with various questionnaires and assessments and this and that. Do we understand and can we actually? Get the right level of information from those things that's really applicable to us, to the specific services that we consume and then how we go about that. And again, how does that change or how does that influence? Certain things that we are doing within our own environments when it comes to that level of security. So my big thing and and if I can, you know, distill this kind of long, long chat into one small thing. Is I want to know. What needs to be measured? I want to know how it should be measured and I want to know who in the environment is responsible for that particular measurement, and then you can really connect that into pretty much everything.

James -
Can you tell us what are the operational roles of the individuals that are impacted by the problem and who does that impact within an organisation?

Ivan -
Indeed, I guess the challenge itself is very broad and hence the answer will be along these lines. You know if you think about it in the Infosec cyber world, call it whatever you wanna call it. We frequently have those blurred lines between the IT side of the organisation and the infosec function. Sometimes that's solved by Infosec being, you know, kind of people. People perceive it as a part of IT.
You know that the only way I like to describe it truly is that infosec NIT should be proper business partners. Equal business partners if you want and and and that's probably the only way you can actually drive the improvements and how you can drive the maturity in the right way. And how you can actually see some proper returns from there and again that doesn't happen overnight, so you know. It's. I'm not suggesting you know anything here along the lines of everybody needs to make that change from tomorrow. No, it's a journey. But ultimately that's sort of a target you need to steer the ship. But nonetheless, in that context again. Answering on you know. This particular challenge, who is involved? Who is on the operational side, who can benefit and so on. Well, it's pretty much everybody. Depending on what those metrics are and and again, I'll circle back to that one because I think that's really an important discussion to have. It's going to be very slight to operational teams. It's going to be various cyber operational teams. It's going to be if you want procurement in the company, it's going to be the finance department of the company. It's going to be the marketing department. Even those are the things that we really need to. Get out, go out and then get into the business and be effective. Engage all the right stakeholders, because I think many of these, let's call them, you know, KPIs will have a bearing on various parts of the business because they're not just something that happens, you know, on the infosec side and you know

TRANSCRIPT

KPIs will have a bearing on various parts of the business because they're not just something that happens, you know, on the infosec side and you know you you let as the senior exec, you let the Infosec deal with it, you don't want to know about it, no. Can't work like that, so that's where the challenge is and that's why I think this is something that touches each and every part of. The company.

James -
Have you attempted to solve this problem internally and if so, why was it not successful?

Ivan -
Of course we have, and I wouldn't necessarily say it wasn't successful. I'd say it was a journey and a. If you want. There's still plenty to go and and and visit on that journey. You sort of, you know, solve certain things and you discover some other things and whatnot. We actually went as far as to create an entire catalogue of. Various KPIs. We started with, you know, water all those things that we can possibly think of that might even remotely be useful for certain discussions, if you want or might be useful to, to give us a bit more information about how something happens in a particular way or where the problem is. Might be occurring. And then we tried. It was really like a properly big catalogue. And then we tried figuring out who are the people in the company that those KPIs can be useful to. Who are the people in the company that can have a say or? That are you. Know, as I mentioned already, that they are possibly responsible for delivering some of that stuff. And then we tried engaging the business in a way that, you know, you go to, let's say, a CFO put this big ugly list in front of him and try to have a nice discussion. Listen, we think this, this and that is relevant. To you, and this is how and why would you agree? Can you see anything else? And so on and so on. And it was actually a fantastic experience. It took us. Quite a bit of time to come to something that made sense to the business as a whole. Yeah. And. And and to make sense to most of the senior leadership of the company and I guess that's an interesting point there. And then I had the luxury. Of working and and and and driving the infosec for a. Rather, a rather large company with a fantastic team of people, many of which I kind of cherry picked. You know, I was just blessed with the quality of people I was surrounded with. And when I think about it. One of the reasons why we were able to actually do as much as we did was exactly that. Plenty of very high quality people and the business to a very large extent. Let you know what we are trying to do and they were engaged properly and so on. If I then try to think you know how things happen out there slightly outside of that context, you have infosec professionals who work in much, much smaller environments where budgets are hugely challenging. Whereas because they are spinning multiple plates, they don't necessarily have time or maybe knowledge or maybe. You know the. The resources, whatever that might be to do something big like that. So my take on this is. Can we, as the professionals, come together and try to find the solution where we can distill a set of those metrics well defined KPIs and things where, as I said, three important things, what? Must measure. How to measure it, which is very important because you know the second you start talking about some subjective things, everything goes through the window, something I learned in my. Career is you. Know I might be weird myself, but I don't trust a single person. Number coming from a person, unless I actually see that number coming directly from a system somewhere. So the second you can introduce subjectivity, people do it. It's just in our nature. It's a very weird thing. And and and. You start having you know, a gap that you might not understand. Down the line. So as I said, what you need to measure how you need to measure. So it's not necessarily some very hard prescriptive things and whatnot, but very nice clear guidelines and ultimately who's responsible for that number. And if we came up with this basic framework, again, there will be things that are different for different industries for different sizes of environments and whatnot. You know, let's, let's call them. Auxiliary metrics or I don't know it can be, as I said, something industry specific or whatever, but. There must be a set of very basic things that we can come up with and that we can put in front of everybody else, and I don't know if we're talking about the context of, you know, the UK. Is it something that I'm drawing a parallel with what SEC does in in the US would listed companies, you know, can somebody like? Go to the people and say this is the basic set of metrics that everybody must measure and that's going to tell them, you know, some, some, some very bad. Things, and ultimately that might empower scissors and various

TRANSCRIPT

other infosec professionals to actually focus on how to improve some of those things. And what else is needed really in the context of their business. But it just might save them some time and effort in trying to convince the business. Why must those things be looked at?

James -
Is there anything on the market then that that that you've identified that you could that but didn't procure and and and if so, why, why? Didn't you procure them?

Ivan -
Great, great question. What I've seen on the market are various and don't get me wrong, fantastic solutions that are only taking into account, you know, small parts of that picture. So you will have solutions that focus, I don't know, maybe on the endpoint. Or that maybe focus on people or? This or that I haven't really seen a solution where you have all those things brought together in the way that you can draw the data from various systems and that you know you can, you can really just consume it at the end of the day. I think with all the AI and things happening.
Right now, I I think it's possible to make something where we should be able to very, very quickly make sense and normalise if you want those numbers. So the challenge is. How do you take the information from that very possibly diverse ecosystem and bring it to that one thing? Yeah, I don't think such a thing exists out there at the moment. Furthermore, to answer the second part of the question, you know, what did we do about it? We had to come up with something custom. And yes, we were, you know, taking various numbers and information and pushing everything into our security data like platform. And then you know, driving some of those things and effectively improving and pushing the envelope but. I'll go back to what I already said. You know, I was blessed with a fantastic team. I had a, you know, a data expert. I had some very smart people that I could count on to make some sense and to drive those things. And we created some, you know, beautiful dashboards and it made sense. For everybody in the company. But can someone you know if you have a single IT security manager in a company that, as I said is, probably spinning every plate there is out there, do they have the luxury of doing something like that? I don't think so. So I guess if someone can solve that one and we can, you know. You. You. I. Guess we don't need to aim for, you know, some sort of, you know, all bells and whistles. Solution and whatnot. Important to have something that will work out-of-the-box. It's important that you start with something that you know that's, I guess, pluggable that you can bring additional things if and when and as you see fit and adjust things for your environment. But as long as it can answer those basic things and it. Allows you to grow.

James -
If you identified that solution, that is good, that does what you've just outlined, would you consider procuring that for, for your organisation or a future organisation?

Ivan -
Yeah, absolutely. Look, if I could save, you know, plenty of time and first and foremost very quickly go back to the business. Listen, these are the areas that we must be looking for. And it is because. It's almost, you know, let's be very optimistic. Let's make it an industry. Standard, so you know. If we know we need to do this, and if these are our numbers, again, it's very easy to engage with everybody without going around in circles. So that you can actually start focusing on the problem and on the gaps rather than, you know, convincing people why they should be looking at something. So on. Therefore, I mean, you know straight away I can. I can see how much I could save in terms of. Money and effort and how much I can help the company buy by focusing on the problem straight away. So yeah, I would.

TRANSCRIPT

James -
Moving on to sort of the cyber innovation hub side of things then and the involvement from their side and bearing in mind obviously that the idea of this is to be able to. Have those problem statements that you've just outlined there. Then the cyber innovation Hub will, you know, will be looking to sort of. Help them in any way that they can. That sense of. Of building or creating a solution. You know how to do. You envision the cyber innovation hub. Being able to contribute to solve this challenge that you've that you've high.

Ivan -
Sure. I guess in my view there are two possible avenues there. One is again, this is an area that's you know close to my heart and I'm familiar with some fantastic work done already in the industry by I won't name them, but. Very large analyst company, let's call them like that out there. And they kind of, it was last year, they actually came out with a very nice piece of work that talks about the outcome driven metrics. So in a way, it's a starting point, you know, and it's almost if you want the seed for what? We believe we should be doing. There is a challenge with it, however, the challenge is not everybody's got the budget for big analyst companies to tell them these are exactly the things you should be looking at and this is how you do it. And by the way, you need to pay us a tonne of money to help you get the programme off the ground. As you can imagine. So I think the first part. Of the involvement and engagement could be pioneering this as almost I'm. I'm not gonna say an open source framework doesn't. Necessarily work like that. Pushing the agenda and convincing the industry that you know, these are the basic things that everybody must be looking at. Yeah. So it's almost like maintaining the framework of metrics and maintaining it in a way that everybody accepts it as a. Can that be easily done? I don't know. Something certainly to discuss. But then the second part is and we actually get to talk about technology. Now you have the beautiful metrics I already told you. I don't trust things coming from people and from various emails and. Beautified, beautified KPIs, no just doesn't work like that. Is there a need for a product that can actually be out-of-the-box? Provide, you know, connections to the basic systems that you need out there. You know everybody's got the antivirus of sorts and everybody's got, you know, some sort of e-mail security product and this and that and whatnot. Can we have something and and again, you know similar things do exist on the market. But as I said, they are very focused on, on particular segments of this. But can we have something that effectively consumes the data from various sources? Can we have something that I'm not tied to a particular ecosystem because you know not everybody out there uses Microsoft for everything? Yeah. Out there uses, you know just. Best of the breed, top three. Whatever Dr products and. Not so. Can I have something that, yeah, out-of-the-box consumes this information but also allows me to tweak and tune and and and connect multiple products that I might have and so on. But at the end. It gives me the output that I'm after and it gives me the same output whatever the ecosystem behind it.

James -
How would that success be measured by you through any solution developed for it?

Ivan -
Again, 2 avenues there, one not necessarily tied to the solution itself and that would be the adoption of a particular metric.
If you want the width and breadth of. Where we manage to go to get them embedded, because I think that's the way to go and and and for many reasons. But the second one ultimately is you know if you can tie a solution to it and provide something that can effectively digest. Different inputs and give you an objective view of where your environment is. And if it can give you hints as to you know what are the areas you can start again straight away you know that's that's where the values are. These you get the score the software itself can try to understand how easy to improve it. And what? Are the areas that need to be addressed, and so on. Let's try and you know, let's try to bring it all together, but a successful solution should be able to give you some straightforward hints. Give you, as I said, those objective values for the metrics that should be there and ultimately. You know, help you to drive the entire security. Look forward to it.

TRANSCRIPT

James -
Would there be any other K.

Ivan -
I I guess. Might challenge here is you know what are the KPIs we're talking about? Are we talking about the KPIs that that I'm suggesting we should have as the industry baseline or are we suggesting the KPIs that are gonna be? Tied to the. To the product itself and we can have a very long discussion on. The topic I guess you know kind of this time around coming from from the. KPIs relevant to the product, yes, I can. I can certainly see, you know some some basic things being very relevant there along the lines of. What's what's supported? How many different? Pieces of a puzzle, or how many different systems out there you can actually include in that picture. What are the you know, what are the various sources you can you can consume the information from and and so on and so on. So we can we can, you know, have some, some, some very technical stuff there. I wouldn't necessarily touch on what I believe are the right KPIs that must be looked at as part of the baseline metrics. That's gonna be, you know, very early opening a big kind of worms because I see all sorts of things out there. And I know quite a few companies doing some some great work on, you know, kind of trying to convince people why certain things should be looked at and some other shouldn't. And then you will have, you know, many, many professionals out there. Sort of not pioneering, but you know, really pushing their own metrics for the sake of, you know, this is what works in my environment and so on and so on. I think that's a much, much broader debate. And actually I would, I would like to have that one out there in the open and I think we need more clever people to debate. Peace rather than me just. Give you my view on it because it might be, you know, rather narrow given that you know, I I haven't seen everything out there. So I would really like to see some sort of a follow up on that particular one. You know what are those metrics that we should take as the baseline whatever the industry whatever the. The business size and so on, that must be objectively measured. And yeah, I I think you need to look at planning something for that one James.

James -
Well, I really appreciate it, Ivan. It's been great to talk to you

Ivan -
Take care, James.

KEY POINTS

Contractual Compliance as a Cybersecurity Challenge:

- In the Business Process Outsourcing (BPO) world, contractual compliance is a significant challenge.
- Dealing with various companies, industries, and risk appetites poses difficulties in meeting diverse client requirements.
- The challenge is to provide the correct level of security beyond contractual obligations to maintain trust with clients and uphold the company's reputation.

Measuring and Normalizing Security Metrics:

- The challenge involves normalizing information across diverse environments and measuring consistently.
- Finding ways to provide information to both internal management and clients is crucial for transparency and trust.
- The need to measure the right things objectively and ensure understanding across different business ecosystems is a central challenge.

Blurred Lines Between IT and Infosec:

- The challenge extends to the blurred lines between IT and information security functions within organizations.
- Infosec and IT should function as equal business partners to drive improvements and maturity effectively.

Operational Roles Impacted:

- The challenge impacts various operational teams, including cyber operational teams, procurement, finance, and marketing departments.
- Key performance indicators (KPIs) have a bearing on different parts of the business, requiring engagement with diverse stakeholders.

Internal Attempts to Solve the Problem:

- The organization has attempted to address the challenge internally, creating a catalog of various KPIs.
- Engaging with different departments and stakeholders to align on relevant metrics took time but was eventually successful.

Market Solutions and Limitations:

- Existing market solutions focus on specific aspects of the cybersecurity landscape (e.g., endpoints, people) but lack comprehensive integration.
- The speaker emphasizes the need for a solution that can consume data from diverse sources and provide an objective view of an organization's security posture.

Envisioning a Cyber Innovation Hub's Contribution:

- The Cyber Innovation Hub could contribute by pioneering an open-source framework for outcome-driven metrics.
- The involvement could focus on maintaining a framework of metrics that the industry accepts as a baseline.
- Additionally, a successful solution from the Hub should provide objective values, insights, and hints to improve security postures.

KEY POINTS

Success Metrics for the Solution:

- Success would be measured by the adoption of metrics across the industry and their incorporation into various organizations.
- A successful solution should provide objective values for metrics, help understand areas of improvement, and offer actionable insights.

Consideration for Procuring a Solution:

- Ivan would consider procuring a solution that aligns with the outlined needs, saves time, and provides actionable insights for the organization.

Challenges in Defining KPIs:

- The challenge lies in determining whether KPIs are related to the industry baseline or specific to a product.
- Ivan is open to discussing technical KPIs related to the product but acknowledges a broader debate on baseline metrics that need industry consensus.

Call for a Broad Debate on Baseline Metrics:

- Ivan suggests a need for a broader debate on defining baseline metrics for the industry, involving input from various experts and professionals.