ALLIANCES PROJECTS

UNITING STRENGTHS

EXPANDING OPPORTUNITIES

CyberSight25

Problem 3

Gen-AI Security

KEVIN JONES

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

James -
Welcome to the Alliances conversations. Part of the Alliances projects, this project is in partnership with Cyber25, an initiative that is part of the Cyber Innovation Hub at Cardiff University. Today I'm joined by Doctor Kevin Jones, who I'll pass it over to you, Kev, if you could just introduce yourself and your role.

Kevin -
Yeah. Thanks, James. Again, Jones. So I'm the global CISO for a company called Bauer Sciences. So primarily focused on pharmaceuticals, life science programmes, crop science and consumer health. And obviously, I'm sure you can imagine given the nature of the work we do, cybersecurity is critically important.
Actually, broader than that, I very heavily involved in some the cyber security community activities for CISO groups, CISO communities for information sharing.
I have a long history in innovation programmes, collaborations with academia, so probably should be quite transparent upfront so that I'm a visiting professor at Cardiff University and also I'm part of the cyber Innovation Hubs Technical Advisory Board and the Steering committee that goes around that. So lots going on around the cyber community that I'm part of as.

James -
Brilliant, Could you just provide an overview of your organisation and its objectives in the context of cyber security?

Kevin -
Yeah. I mean, there's a few things I always look at cybersecurity across really 4 domains,And from the concept of buyer, I mean it's very obvious and very clear that we have to cover cyber security in all of those domains. So I don't want to have cyber security just seen as an IT problem and it's dealt with.
By a few IT people, it's a business conversation with very technical, mostly IT related people, but actually Global landscapes for very large organisations, I mean you're talking 10s of thousands of IT servers.
Hundreds of thousands of endpoints platforms, those types of things that you're trying to protect, but also as part of that, it's the data that we have. I mean, we hold very sensitive personal information that we have to protect the intellectual property of the company. So all of that fits very well with what I would call traditional cyber security Activities, but for us, we also make a safety critical product and manufacturing in the healthcare industry. So cybersecurity embedded in the products that we make and manufacture is also critically important too and that's part of our sort of dev SEC OPS lifecycle about how we embed security there and security by default.
But also a company like ours makes things such as manufacturing and OT systems.
Certainly it is increasingly being seen as part of the CISO's remit and and even if you don't have manufacturing in organisations where OTC.
In this current landscape, with heating and ventilation systems and automation around buildings and all of those type of things will increasingly become the scope of the CISO to fulfil and for me personally, I always put people as the 4th kind of want to remind ourselves that we have to live in What I call a human centric cybersecurity world, we no longer live in a in a Realm of just technology. And we can't fix it with just technology so I come from an aerospace and defence background as well, where I spent 12 years and I know the way aerospace thinks in terms of Blackwell thinking in terms of system design and sort of cognitive burden. Those are the type of discussions the cyber security industry needs to be Having as well.

TRANSCRIPT

James -
Could you tell us what specific cyber security challenges your organisation currently facing?

Kevin -
This is one of those questions of where do you start? I think there are so many challenges in the cyber security industry, so, so probably a quick overview. I think many organisations are still on their cloud transformation journey. So we're still talking about finalising things like sassy, finalising the Zero Trust architecture implementations.
Across the piece, how do you then handle legacy systems and legacy environments that need to be sunset or things in the OT environment? You just can't patch and fix and put security in so you've got the Almost challenge of how do I protect the new whilst I'm still trying to protect and maintain some of the legacy and almost having a split architecture which which is never a good idea for security, but it's inevitable on top of that, I think the the regulatory landscapes are becoming increasingly complex across the world in fact.
So obviously you've got GDPR two things coming out in Europe. The US is increasingly coming out with cybersecurity laws and regulations, and the Patriot Act, Cloud Act, new privacy laws in the US, China, cyber security law for companies that are truly global.
So it seems that every other month these days China's coming up with a new regulatory environment for cybersecurity. India has a new cybersecurity law, Germany has a new cybersecurity law. The UK is obviously looking at how to regulate things like AI. So the, the regulatory landscape, even even at national levels is challenging. And then for many global. Kind of highly regulated organisations as well. We're seeing increasing regulations around healthcare and kind of very specific Industry regulations on top.
The good news is, many of them actually are pretty standard, good cybersecurity.
It's an information security management system, but sometimes they conflict in terms of regulations and managing that landscape is becoming increasingly complex and taking a lot of time. So those are the type of things that probably that industries are challenged with against the backdrop of an increasing Kind of geopolitical threat landscape as well.

But the one I probably want to touch on today and I think is really future looking is around AI security and specifically generative AI or Gen AI security. It's something that's kind of the technology that becomes available so quickly.
The trick is to be as close as you can and not too far behind of the technology landscape as a CISO, but this one seems to have come so quickly. So, getting to grips with what is going on in AI, how it's going to impact the business. And how we secure this is going to be a real challenge that I'm talking to a lot of Caesars about at the moment in terms of what, what are we doing for best practice? How are we trying to catch up? What are we implementing? So I think that's probably one of the biggest challenges we can.

James -
How would you say that that challenge has come about and what are the potential risks or consequences of that challenge?

Kevin -
So for Gen AI, actually there's it's easier to break this down into slightly different viewpoints, since the first viewpoint I think is.
This concept of Gen AI available to all has really come about in the last six months. Everybody's now using it, trialling it, testing it. So the first thing for me is how do we protect our data?
And implement sensible ways that the business can utilise the power of Gen AI. It's going to fundamentally change the way Companies work and the way we work over the next 12 to 18 months, I'm absolutely convinced. People who know Me Well will sometimes say that I'm a bit of a cynic of new technologies. There's been a few bubbles over the last three, five years that I've said. I don't really see that as a game changer. This one I do.

TRANSCRIPT

At the moment There a lot of the technology still Seems to be being used.
Kind of like a very advanced search engine, but as this generative part comes out and people start really generating files, these videos, PowerPoint presentations, whatever it might be documents for the company. I think that's when this tower will really be harnessed. But obviously they're built on models so they can only learn.
Based on the data you provide to the model, so the first challenge with all of these things is how do we protect the company data from going to 3rd party loss being used by other companies or competitors because it's just been uploaded because the people want to use the technology and trial the technology.
It's sort of like the normal third party risk management. And I can see companies trying to catch up and do contracts with these companies. Then you've still got data leakage or data inference actually becoming a problem with Gen AI. So that's the first bucket. I think that's gonna be a real challenge, but it's something we can probably manage Using existing techniques.
The second one for me is if the adversaries have this technology and it becomes a commodity, what does that do for our existing security stack? And I think that's a different challenge to the first one. And we're starting to see Gen AI being used against other companies. These where they're using voice generation or some kind of advanced phishing e-mail, I think social engineering attacks particularly will be hugely more complex, more sophisticated. And kind of real, they're going to be more difficult to defend against in that context. So I think that's I think we'll have to watch and see how that plays out as this Gen AI becomes a commodity for the adversary.

The third one, Which again I think is a slightly different view and a slightly different perspective is really going to be about how we then use Gen AI to improve what we have on the security side and this kind of creates this AI battle. It's a war for AI in terms of defence and attack. And again, it's kind of history repeating itself In what we've seen many, many times before in the security space, but can it make us more efficient, more effective to use autonomy and then AI to generate reports and threat intelligence and feed that?
That means, for stock analysts, for example, they can really be spending their time not writing reports. For writing those things, that of course means we need to develop our own models, because you're not going to upload that type of data to a third party cloud environment to hope that it generates you the right answers. So we're gonna have to develop our own models and that really brings me onto kind of the next one, which is again a slightly different viewpoint. But you can see they're all linked as well.
Which is companies are going to want to develop? Gen AI and more traditional AI tooling very quickly to have kind of their competitive advantage in the next two years. And maybe that's even too long. So I know we are certainly looking at having our own Gen AI platform internally that we build our models and interconnect with our data. Which then brings us to the question of. In the future, let's take a two to five year timeline. These models are going to be fundamental to how companies operate and the security protection of them is going to be absolutely key. So this is one of the challenges. I think the cyber innovation hub can particularly help With which is. How do you do something like a dev SEC OPS for AI models so everything shift left security by design around ensuring that the right data is going into them. The models are built with security in mind. Maybe explainable AI goes into that piece. So we could do security monitoring of the models. Then you've got to consider how the how the actual engine could be manipulated by an adversary. The future, I think is is around data integrity. We've seen about confidentiality and availability have been the battleground really for the last.
234 years as we move into a world of AI, it shifts our focus onto data integrity as well. And that for me can only be achieved really by good design principles, security principles, DevOps, fully embedded through the pipe into operation of those AI models and break them down into composable.
But I think it's a perfect example of where something like cyber innovation hub that wants to look at the future to kind of almost predict what we're going to need. It's a really good example, but only if you have all four of those kind of buckets, if you like, is it going to be?

TRANSCRIPT

James -
I think you touched on this briefly in, in, in your explanation. But what are the operational roles of the individuals impacted by this problem?

Kevin -
Yeah, cyber security is always a team sport in whatever we do. It's a team sport. You don't solve the problem of cyber security with a few IT people sitting in an office by themselves trying to configure firewalls. I mean, maybe that worked 20 years ago, doesn't work today. So in this grand world of AI, you're certainly going to need the developers.
And bringing them into designing and developing security by default You're gonna need data custodians to be able to understand what type of data we're putting into this Model we're going to data scientists to see if the model is accurate and valid.
I spoke earlier about human centric cybersecurity, so people using these Tools, these techniques. We've got to understand what are the dangers, what are the consequences for getting this wrong? Putting your data in here, or even if you get a good output from Jenna. How much do I trust that? Do I have a confidence value in what's being generated? And can I use that? So you need all of those as well as it. To be honest, it's a systemic Kind of ecosystem challenge, which I think makes it really exciting.

James -
Is there anything you have started to do internally on this challenge?

Kevin -
No, I mean developing Gen AI platforms. So we're already looking into tools and techniques that we would use and many of them actually do exist in the cyber security world. It's good for coding practise, good development practise, integrating security, monitoring, data tagging and classifications.
So you can get some of those ideas already embedded into what you would do to protect the model. I think there's some gaps still as an industry as a whole and talking to other pesos, I think it's Probably universal challenge around how we do explainable AI, how we do security, monitoring of AI and how we actually protect the models themselves because the models are just as important in future as the the intellectual property, kind of that it's going to leverage because that is the core of of the future systems and the future Operations. So there are some real challenges that I think the industry needs to solve and obviously companies like ours are very willing to work with vendors and providers that can not only leverage only what we think exists today, but what could exist tomorrow.

James -
Are you starting to see this sort of solution or product come into the market or hearing about it being talked about that it is something that needs to be done?

Kevin -
Yeah, definitely. Conversations going on in CISO forums and CISO groups. And there are a couple of vendors already starting looking at. It's certainly the dev OPS part of how to do AI but I don't think that the Answer is out there, yet to be honest.

James -
In your opinion, what would good look like in terms of a solution for this?

TRANSCRIPT

Kevin -
It's a difficult thing to do because we haven't got Dev SEC OPS right in normal code yet in terms of developing applications. That's one of the reasons we still see Huge amounts of vulnerabilities out of everywhere, in every software, and increasingly so because.
How we do good coding practices, how you do good commits and automated testing, verification and validation throughout the code and deployed in the right way with security controls and that's where automation can help. But we as an industry don't have that right yet across the board.
We need the same things for Dev SEC OPS for AI, just with some nuances around. Kind of the operational part. So how do we ensure consistency in the model? How do we ensure that good data input verification, validation and and those checking is done so?
In my Mind it can be done with good standards, good patterns, good technologies that are actually really monitoring these things and making AI Possible or models composable. So I'm thinking more akin to the kind of you'd have microservices in a good DevOps environment. How do you do that with an AI Gen AI model? But interestingly, it's the same principle as well because in operation.
Just like today, we'll do vulnerability scanning, pen testing, whatever it might be of an application, we still need to find ways of doing that For AI, and that's kind of the the how you do that against against a model, I haven't quite figured that out yet, but I've got a good theory about the end to end deployment of of what's needed. Just not the technology is Not there yet.

James -
If you identified this solution, would you consider procuring it?

Kevin -
Yeah. I mean certainly having been to discussions with a number of pesos across the board, it's a solution everybody's looking for.
I would kind of put a bit of caution around it that no one solution is going to solve the problem here. There's no silver bullet, Some of it is design principles and some of its culture in organisations as well. So there's the non-technical parts that really have to be done very, very well for this to work. And then I think you're probably going to need two or three different technologies throughout the stack that are going to give you that end to end Coverage from design mitigation controls around its usage, actually probably embedded in the AI model as well. Sometimes to make sure that the model is not giving information it should give and it has safeguards around its use. And then as I said, security monitoring incident response, those type of technologies need to be there. So I see this more as kind of everything from from governance process but also through the technology stack. And yeah, I think if you had those components that you needed and it would be an easy easy decision for people to be piloting that. And certainly we'll be looking to work with partners to help us deliver secure Gen Ai.

James -
How would you envision the cyber innovation hub contributing to solving this?

Kevin -
So as I said at the beginning, I really have a little bit of an unfair advantage on this question because I'm actually part of the cyber relation hub and I sit there. So for me the concept of the cyber innovation Hub is a brilliant one. There are some fantastic places around the world where you have usually clusters Of excellent cybersecurity skills plus entrepreneurial talent.
And that means you end up solving problems quickly and problems that really customers want. And not just coming up with a good technical idea and saying I think I think this is good and Then investing heavily In the technology and saying I'm going to continually improve the technology and then try and take into market the the areas around the world that do this exceptionally well usually have some kind of community or team or external engagement with end customers and they hyper focus on the entrepreneurial Part as well as the technology part.

TRANSCRIPT

So the innovation hub for me is all about how you bring those two things together, anchored here in Wales, To be able to have a kind of not only startup but acceleration programme for cyber businesses, because Wales particularly has a lot of the good components, you need it.
It's got A number of fantastic universities there, there are a number of prime organisations that are here, big manufacturing, Big cybersecurity players in the market, they can advise and and bring those pieces in, but we also have a very good tradition in Wales of trying to generate startups and The the thing For me, for the hub is we need to turn cyber security
to be something that can really scale, grow. You've got this ability to push forward, so challenges like this are absolutely vital to the innovation hub because as if you have access to a group of CISO'S who say actually, yes, this really is a problem, this is not just a nice technological solution. You can partner together to develop such solutions tested not only in test beds, but in real businesses. And help build out those startups and that ecosystem around. And once you get it right, then more and more challenges come and people will be willing to invest in the ecosystem even more. Trust is the word I would use, to trust the ecosystem. The good ideas come out from around Wales. So I definitely want to see the innovation hub tackle Problems like this, but not necessarily problems that are already in a saturated market.
I mean a good example would be that everybody wants to do automation and AI. Now for security detection. As an innovation hub, it's certainly something the skills here would be but deciding on if you want to go in that domain Or is it going to be the prevalence of quite a saturated market where actually a lot of the big players are already starting to do that? And I think something like this innovation hub could be looking at Gen AI where there is good Opportunity to to go in that direction in that domain.

How we protect data in the cloud probably was a good place to be 1218 months ago that there's 5060 companies already trying to tackle that problem. So find those right things that the innovation hub can add value with. So we're not just another player and and certainly it's not something that's trying to Develop a silver bullet. Either it's finding what can be done well that fits and fixes problems, and then it's scalable

James -
How would you measure the success of the solution developed through this collaboration with the Innovation hub?

Kevin -
Yeah. I mean the first thing is the solution has to work. So. So yes, we should get feedback from customers that says this is something that's really valuable if it's deployed, it's it's stop some form of cyber attacks or to reduce some sort of business risk.
But I also go back to this idea that it's got a dovetail with entrepreneurship. So there has to be also interest from potentially VC's or or other companies that this is a good idea and there's further investment coming into the opportunity because an innovation hub has to be sustainable. So I would say there's two different types of indicators, really one is, yeah, customer feedback, customer satisfaction. What is the company growth through?
Onboarding new customers and sales pipelines and those type of things is definitely one. But then you've also got to say, OK, it's. Is there a kind of more of an entrepreneurship KPI that we need to consider for these things?

TRANSCRIPT

James -
You just touched on the KPI's there. Is there anything else that you'd add to that that you'd have in mind to measure that success apart from those?

Kevin -
I think they're the most important ones, to be honest. Yeah. And there's others, which are kind of, what does it do for the area of reputation? But they're really difficult to measure. So yeah, I would. I would hyper focus on those as kind of the KPIs. You shouldn't have too many KPIs. And if you do, you're probably trying to Please too many people and that's normally a bit of a problem for a startup especially so hyper focus on the customer and then kind of also on the entrepreneurial ship and growth. Those would be my two areas.

James -
I really appreciate the time today, Kevin. I really do. But before I let you go, is there anything else that you would add or emphasise regarding this cyber security challenge and the collaboration with with the innovation hub?

Kevin -
I mean, I'm close to the innovation hub. I know it well. I know the concept well. I think probably the big thing for me is for those of you who aren't, get involved. Look at the website for Cyber Innovation Hub to pose your own challenges. Invite the team maybe into your organisation, because the more these entrepreneurs can learn about real world challenges, the problems that they can solve and room to grow as a scalable challenge, engage.
That would be my big feedback.

James -
Brilliant again, Kevin, I really appreciate the time. It's been great to chat to you again and hear about this challenge that you've put forward.

KEY POINTS

Introduction:

- The conversation is part of the Alliances projects, in partnership with Cyber25, a part of the Cyber Innovation Hub at Cardiff University.
- Dr. Kevin Jones, Global CISO for Bauer Sciences, is the guest, focusing on pharmaceuticals, life sciences, crop science, and consumer health.

Organizational Overview:

- Bauer Sciences is involved in pharmaceuticals, life sciences, crop science, and consumer health.
- Kevin emphasizes that cybersecurity is crucial across all domains, including business conversations, data protection, safety-critical product manufacturing, and OT systems.

Current Cybersecurity Challenges:

- Challenges include cloud transformation, implementing SASE and Zero Trust architecture.
- Handling legacy systems and environments, especially in the OT environment.
- Increasingly complex global regulatory landscapes, including GDPR, US cybersecurity laws, China's cybersecurity law, etc.
- Specific challenges related to AI security, especially generative AI (Gen AI).

AI Security Challenges:

- Gen AI becoming widely available in the last six months, leading to concerns about data protection and potential misuse.
- Adversaries using Gen AI for advanced phishing and social engineering attacks.
- The challenge of using Gen AI to improve security practices, creating an AI battle with defense and attack strategies.
- Operational Roles and Internal Initiatives:
- Cybersecurity is a team sport, involving developers, data custodians, data scientists, and end-users.
- Internally, they are developing Gen AI platforms, focusing on good coding practices, security monitoring, and data tagging.

Procuring Solutions:

- Kevin acknowledges the need for a multi-faceted solution, including design principles, cultural aspects, and multiple technologies throughout the stack.
- Caution against considering any solution as a silver bullet.

Innovation Hub Contribution:

- The Cyber Innovation Hub can contribute by addressing challenges like Gen AI, focusing on entrepreneurship and scalability.
- Kevin emphasizes the need to identify problems not already in a saturated market and finding solutions that add unique value.

Success Metrics:

- Success is measured by customer feedback, growth through onboarding new customers, and interest from investors or VC's.
- Entrepreneurship-related KPIs are crucial for the sustainability of the Innovation Hub.

KEY POINTS

Closing Thoughts:

- Kevin encourages others to get involved with the Cyber Innovation Hub, pose challenges, and invite the team into their organizations for a better understanding of real-world problems.

Future Outlook:

- The future of cybersecurity involves AI, with challenges like Gen AI requiring proactive solutions, combining technology and innovative practices.