ALLIANCES
PROJECTS

UNITING STRENGTHS
EXPANDING OPPORTUNITIES

CyberSight25

Problem 2

Visibility into your data security

KEVIN FIELDER

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

Kevin -
I'm Kevin fielder. I'm currently chief information security at Natwest Boxed
it's genuinely one of the most exciting roles I've ever had, and and it's a really good culture as well as kind of cool tech. And I guess very quickly, historically I've been around security for quite a while. I got my first break in security Probably 20 plus years ago now. Getting rid of the virus before we had a fix from Symantec back in the day I've done. I've had some really lucky roles.
There I did a chunk of time with the ocado from when they were 45 people up to 1800 people before they even lived through the whole go live. So I've yeah. And then I've got this role. And so I've been, I've had quite a few roles in my career where I've been really lucky to be.
I've done a variety of things in and out of financial service through my career as well, so I've just been, I think well reflected. We're doing a series of talks at work currently about some of the kind of senior folks in our company just kind of career journeys people to see how we got to where we got to and kind of advice on what we've learned during that journey and things and it may.

James -
Could you Touch your objectives in the context of cybersecurity, within the role that you're in?

Kevin -
Broadly, what are the key things working on so pretty standard stuff for a lot of roles, really visibility. So if I don't know about something, I can't protect it. So I make sure we understand the environment, understand all the things we've got, what they are, what they're doing with those baselines and behaviour, that kind of stuff. So make sure security operations and my team have really good visibility.
This is the tool you've got to use, right? For example in the DLC for those who are new to security software development, life cycles are basically how you build things. Devs will have ways of working so a bit of engineering flow. You might have pipelines, it might be water for whatever it is, right?
But they'll have a way of working, a set of tools that use security and go oh, but use this tool of code scanning and this tool for 3rd party library scanning and another tool for automated testing and another tool for this. And you've got to log into like 20 different dashboards and it's gonna go now mate.
So one of the things you actually have to learn is how do we integrate our tooling into their ways of working and how do we automate things? Much possible. Yeah. A great example of, you know, you know, if you're in an organisation.
Fixing vulnerabilities might be not because the people don't wanna fix them, but it's right because they just it's not in their flow in the way they work. So how do you surface things? So a lot of stuff.
But then we also surface the results to the right people via the tools here which use messaging slack or we use I think all backstage where we basically have all the components and various things not just security scores of those components how currently are.
Pulls up into tools that the devs were using so they can go to one place. Everyone needs to understand what they need to do to fix their components so it's not just the automation and the speed, it's how you surface it to people.
So you don't give them 20 different things to look at. Yeah. What else? We're looking at. Data security was huge everywhere. So a bit like what? You know what you've got, but what data? You got to say, most organisations are quite good at understanding what's structured in inverted commas data they've got right. So what's in their data lake or their database? Or you know, production systems? They'll know that fairly well because it's, you know, you've got a table structure of some sort and things are labelled everything else but then.
You've got emails and docs and spreadsheets and slap. People using it, should they be emailing that pretty about all those things, right? And that's so that's really hard and I can't you know depending on which company you ask for anything from 60 to 80% of all your data.
Is unstructured in piles of stuff everywhere, right, and now matter, how to actually try not to have it. It's going to be there. So understanding exactly what data we've got where make sure it's labelled, make sure people understand how they should be using it, and then putting controls around that well. So yes, automating all kinds of software stuff, building processes, so things like the SDLC, make sure people understand.

TRANSCRIPT

When they need to engage us for threat modeling and any manual stuff like pen tests and code reviews and things work on culture, culture I think is usually overlooked.
I brought use NIST generally for my kind of security programme because it covers everything quite nicely off you tailor it for every organisation.
It's a really.
Good baseline of you know, understand what you've got. Protect it, detect what's happening, protect it, respond. Recover. But I squish, respond and recover together so that I can have a culture pillar. Cause apparently I don't. Where I come from, you should have more Than five pillars in the strategy.

James -
On that note, what specific cyber security challenges is your organisation currently facing or do you see the sector facing?

Kevin -
I'd say how you do data protection for things like data lakes and stuff and developing things into data lakes and things. But that's a whole other one. But this might be one for someone to think about as well.
Yeah. So I think in terms of where I've seen the most fun stuff happening, it's probably the whole what's happening in my environment and and is, is it what's running and what's it doing and what should it be doing. But there are quite a few players in that space already and the one I think probably is the most ripe for some real innovation. It's probably data security, right.

There's a lot of companies that do some bits like they'll do that data discovery.
Monitoring of access to things or they'll do DLP on the endpoint or whatever, but I think something that combines a bunch of those capabilities and some easy to manage.
You know key based or other based kind of DRM controls that don't get out of hand with having you know impossible key management and stuff would be really interesting. So if I can guarantee to my exec all the data they care about is labelled and controlled. And even if it does get accidentally sent out of the business, it doesn't matter because all the bits we care about are redacted.
Unless you've got our walls on, I think that would be a really cool thing to look at and I've seen a few people in that space, but not.

James -
What would be the risks and the the consequences of of that challenge then?

Kevin -
Well, just data breaches, right? Look at all the data breaches to see every day, both accidental or malicious. Because lots of people have to have access to data and there's very few businesses that don't have some processes where someone has to e-mail something sensitive to someone else or to third parties or to HR companies or to other bits of your company or whatever else.
Right. So I think, yeah, the fundamental thing is we, you, we there's an expectation especially in kind of regulated industries but also from.
Every customer right to think that you're looking after data and they're all. I imagine most people assume that as a business we know what data we've got where it is and how.
And the reality is most businesses don't. It's a cold like fact, right? Most businesses like touched on. They'll be pretty strong on databases and whatever other data stores they've got where they might have a data team managing it, whatever else. But as soon as it's outside of that.

TRANSCRIPT

You know, it's not awesome. Well, they have here, or they might have like, hey, we got DLP everywhere and it's really good at finding card.
How good is it? Everything else? How many forces? Yeah. How many? How is it? If you get 1000 false positives in a week? Does your security team check them all or is it just in all of them? Cause it knows most of the false positives, so the, the and even places where they do it quite well. I think they do it quite well because they've got a ginormous team, which is why I kind of touched on the efficiency piece, right. So it's not just.
Can you? If you've got like an entire data security team of people who spend their entire life doing data labelling, data discovery, managing DLP tool and dealing with alerts chasing people out when they might do something wrong, can you do that without a massive team?
And even when you've got that massive and I don't know many places that have it buttoned down to point that, if I'm allowed to send out the business, then I know what's going on with it. So I don't right, it's then gone and you assume the person you sent it to is gonna treat it appropriately, which is great if they do. But I think if you had.
Those kind of access controls that travelled with the files for sensitive files, right?
I know when I sent it to Jim's company, who in Jim's company tried to. Open it, yeah.
And who's accessed it and who's tried to put their password in, who's tried to see their reactive parts and everything else right. So you then get some visibility of how it's being used when it's not even your environment. And you know, right, OK, there's these three bits in that file that no one should see outside of our CFO or whoever.
You know they haven't cause it's just they just get a redacted bit of encryption until they put in an auth key that they haven't got because they're not on our SSO system. So yeah, so that kind of stuff I think has a huge bit of value for sensitive data.
And you have to look at, like, the amount of work people put into protecting sensitive information, especially when it's money involved. Look at the work they put into protecting, like, you know.
When there's live streams of sports events and stuff, you know, they send a different key to every single person watching it. That's embedded in the screens. If I film it and share it and you know, it's a thing where people, when they've got direct money on the line, put huge work into it. But the rest of us don't have the luxury to do as much in that space. So yeah, I think.

Protecting you. See, I mean, you see data breaches every day, right? And some of them are. Yeah, someone hacked. But if you were even with phishing or whatever else, right. If you've got this kind of like cryptographic controls around your data. Even if I get finished and the file gets out to you, it's useless to you because the stuff I don't want To get out Is redacted without the right stuff. So I think that would be a really cool space to be in terms of managing genuine risk of data breach because it makes it much harder to get access to things we really need.

James -
Would be the operational roles of the individuals impacted by that risk or by that problem?

Kevin -
Everyone! So unless you literally have access to no data that we that is not public, you have access to data that's internal or sensitive or whatever your your classification is, right and even internal data, you might not apply every single control to it, but it still shouldn't get out the office without approval or access internal.
Genuinely probably 90% of most organisations, certainly in terms of people who have access to computers.

TRANSCRIPT

James -
Have you tried to solve the problem internally? Or have you heard of anyone that's tried to solve that issue and if so why hasn't it worked?

Kevin -
So I think a lot of it's either because people will be too niche so they can do one little bit of it or I've said a lot of DLP tooling seems to Struggle with how you identify label files.
There's tools out there that are quite good at discovering and labelling data, but they don't do a deal. P piece, you have to implement a tool to discover, and that's fine. But then does it? How well is it linked with the tools that manage the data? Does it see all of your stuff? So you've got data in SAS tools, your data in E-mail spreadsheets. Yeah, whatever.
Slack or teams or whatever else you know what data are everywhere. So how do you know that you've got you've you've gone to all the places where you've got data. How confident are you've labelled it all? Or you understand who's?

And it is a complex issue right then who should access it? How should I behave with it, understanding all of those things and then? The DL DLP tooling does some stuff quite well in terms of on the endpoint of Things but, You know, does it capture everything? Does it rely on regex or does it rely on behaviour or? But both? Yeah like cause some companies did it quite well, but tends to have High overhead and once it's outside of your control, it's usually gone and you're assuming whoever you oh, we've done our due diligence, fire whatever else. But you don't really know what happened to it. As soon as it leaves your control. Right? So that piece is often, I think, very overlooked in terms of how important it is because it's, we just assume it's fine because we've done a little bit of D on someone or we're we're allowed to.

And I think as organisations you can do much better in terms of how you protect that most critical of data by knowing what happened to everywhere.

James -
With the tools that you mentioned that are out there, can i ask why these have not be precurred?

Kevin -
Most of the things out there that all do bits of it and it's gonna be a combination of budgets, resourcing like a lot of them have quite high Overhead, right? So it's not just, yeah.
Can I have the budget to do it? Have we got the resources and the people to manage it so much? Kind of thing the folks on with this is data secure everywhere, but also the ease of management of that piece, right. And I think you know, you could probably Look at a tool that did. If you came up with something that does Some really clever DLP stuff and the kind of protection of your data everywhere piece, not necessarily all discovering leading cause they are quite different capabilities, but managed to do effectively DLP better than we do now with controls around what happens to data once it's left. That would be awesome and I think that's the problem.
A lot of tools that do bits of it, a lot of them cost quite a lot and a lot of them cost quite a lot in terms of resourcing and it's like OK, so. What is enough? So it's like, OK, I can tick a box and say, hey, I've got the LP. I couldn't give evidence to someone who asked me here some screenshots with LP discovering things and here some labelling. So I get to a point where it's like it's OK.
And I might have other priorities, or I might not have the budget for the people to do it. So I think the more you can simplify it and the more you can kind of unify some capabilities into one, the better chance you have.

TRANSCRIPT

James -
If you identified that solution, is it something you would purchase?

Kevin -
Yes, absolutely. Yeah. Yes. Yeah, yeah.

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

Kevin -
So let's say they help kind of start-ups, get funding and and support their start. Yeah, so so.

Yeah. So you want to like, I guess, innovative individuals who are keen on some of these different areas of tech and going right, how do we best identify files and and and how what's being done with them on a computer, how do we look at their use, how do we?

Yeah, manage the encryption of bit parts of files or whole files. So you need certain things to access that kind of stuff. So looking at the problem space of files and data in use and identifying those files and data in use and the. It's basically the kind of.
Bit around, you know, encrypting parts of it or redacting parts for automatically that kind of stuff that were sensitive and then logging out into product, right or tested file. And that was something in the customers. So it'll be I guess help. I assume the innovations will do things like help with people finding funding, help people kind of have some space to work, help people like.
Talk to friendly customers, that kind of thing and and give them some advice and guidance and and and I think a lot of the stuff around this isn't necessarily The tech solution.
A lot of help you can Give people that are doing startups especially, they're Kind of first time.
The business side of things in terms of.
So it's things like, you know, budget cycles. So if you have an annual budget cycle, understand that, hey, I've got this really cool thing and it's like that's great, but I may already have a plan a year ahead and this your thing is so it's filling a gap that was so important.
I'm gonna drop something else.

I might not be able to get a budget for it, so if you talk to me in Feb, it might be right. Yeah. This looks really cool. We can trial it Through a supplier on boarding, especially in a regulated industry where there's like loads of rules about what you can do about how you procure people and then checking out supplies and things they need to PO see it and trial it and then.
Oh yeah, it's very good, but a good test in October or September that can go to next year's budget year Q1Q2 next year. So it might be kind of a 612 plus month process getting on board with some companies. So I think helping startups or people with a cool idea not just execute the idea, but understand things like.
I don't. I can't assume funding coming in from people buying it for quite some period because it might be quite a long thing and then helping you with introducing to maybe companies that are a bit kind of a bit more fun and a bit looser about how they do things. So maybe you can get in there a bit more quickly than a A regulator and that kind of thing. So I think yeah, whether it's people like us.

TRANSCRIPT

James -
How would you measure The success of the solution, developed through a collaboration with the Innovation Hub?.

Kevin -
I guess if it's a trial or whatever, it would be all your data, but you would look at.
How easy is it to implement what the efficacy was? Did it genuinely mean I understood how my files and stuff were being used? If stuff was sent externally, could the people still see what they needed to see, but not what they shouldn't see? That kind of stuff, so it'd be a Bunch of tests You do as part of that and like I said, obviously part of that's gonna be ease of use.
Is an implementation right? If it's like an agent that sits on your computer and takes up 3/4 of your resource, that's a bad implementation.
Some stuff that's not technically security in terms of management roll out, ease of use. Could my business use it? So if my CFO or whoever in its equal Chief Risk Officer wanted to send some stuff out or wanted to you know contact someone and send some stuff that they wanted things redacted or whatever else could they use it easily? Did they understand how?

Could we break it as well, right? So you do the security testing off, right? I've sent a bunch of files everywhere. I've got this tool on my laptop. What crap can I send out? That isn't gonna be encrypted and it doesn't capture. Can I send stuff to file out and then get into the stuff I shouldn't get into? She does all the security testing of it as well. But the biggest not the biggest part of the big part of it would be.
Assuming they got the security stuff right, because that's what they're doing everything.

James -
Is There anything else you would like to add regarding the collaboration wit the innovation hub?

Kevin -
I don't think so. It'll Be really exciting to kind of look at some of this.

James -
I appreciate the time. Thank you for joining us Kevin, great to talk to you as always

Kevin -
No problem. Thank you. Cheers.

KEY POINTS

Introduction:

- Kevin Fielder is the Chief Information Security Officer at Natwest Boxed.
- He has over 20 years of experience in the security field and has held various roles, including at Ocado.
- Kevin is currently involved in a series of talks at work discussing the career journeys of senior individuals in the company.

Objectives in Cybersecurity Role:

- Focuses on visibility, understanding the environment, and establishing baselines and behavior to ensure security operations have good visibility.
- Discusses challenges in integrating security tools into software development life cycles (DLC) and the importance of automation.
- Emphasizes the need to surface security results to the right people effectively, avoiding information overload.

Cybersecurity Challenges:

- Highlights the challenge of data security, particularly in understanding unstructured data that constitutes a significant portion of most organizations' data.
- Discusses the difficulty in protecting sensitive information and the need for better controls, automation, and processes.

Risk and Consequences:

- Identifies data breaches as a significant risk, whether accidental or malicious.
- Stresses the importance of businesses understanding and managing their data, as customers expect organizations to safeguard their data.

Operational Roles Impacted:

- States that everyone in the organization is impacted by the challenge of data protection unless they have no access to non-public data.
- Highlights the need for controls and approvals for internal data access.

Internal Problem Solving:

- Acknowledges that solving the data security challenge internally is challenging due to the complexity of the issue and the limitations of existing tools.
- Discusses the need for more unified, simplified, and effective tools.

Procurement of Solutions:

- Mentions that budget constraints, resource requirements, and the complexity of existing tools can hinder the procurement of solutions.
- Expresses the need for simplified and unified tools that effectively address data security challenges.

KEY POINTS

Collaboration with Cyber Innovation Hub:

- Envisions the Cyber Innovation Hub supporting startups by providing funding, space to work, and guidance.
- Emphasizes the importance of business-related support, such as understanding budget cycles and supplier onboarding processes.
- Highlights the potential for the hub to connect startups with companies that are more flexible and faster in adopting innovative solutions.

Measuring Success:

- Suggests that the success of a solution developed through collaboration with the Innovation Hub would be measured by ease of implementation, efficacy, and security.
- Proposes tests to evaluate the solution's ability to understand and control file usage, as well as its ease of use and potential security vulnerabilities.