INTERVIEWS

Interview: Why World Leaders Must Invest In Open Source Technology

Amanda Brock, CEO at OpenUK and Andrew Martin, pro bono CISO at Open UK and CEO at ControlPlane, discuss the benefits of using open technology, the challenges of growing the open source community, and how government support is needed to overcome those challenges.

By Caitlin Jones
Updated Nov 25, 2022

Amanda Brock, CEO at OpenUK and Andrew Martin, pro bono CISO at Open UK and CEO at ControlPlane, discuss the benefits of using open technology, the challenges

of growing the open source community, and how government support is needed to overcome those challenges.

Amanda Brock is CEO at OpenUK, a UK non-profit advocacy organization with a goal to develop and sustain UK leadership and global collaboration in open technologies, including open source software, open hardware, and open data. Brock is a frequent and sought-after speaker at technology events, and was included in Computer Weekly's *Most Influential Women* and *The UK Leaders in Tech* long lists for 2021 and 2022.

Andrew Martin is pro bono CISO at OpenUK and CEO at ControlPlane, a cloud-native security provider that specializes in protecting Kubernetes from supply chain and runtime attacks. Martin is a supply chain security advocate with a wealth of experience in developing, testing, and hacking systems, giving him a deep understanding of how to secure enterprise and government cloud environments.

At OpenUK's thought leadership day, "Open Source Software Infrastructure, Curation and Security" in collaboration with OpenSSF, we spoke with Brock and Martin to discuss the benefits of open technology, the challenges associated with growing the open technology community globally, and the steps that world leaders and businesses can take to overcome those challenges.

OpenUK works to develop and sustain UK leadership in open technology. What are some of the main drivers for using open technology?

Brock: At OpenUK, we undertake an annual survey each May and, when we ask people why they use open source software, almost without exception they say the economics and savings —the value. They get software which is more economically viable by it being open source.

But they also get *better* software. Your team can develop skills on the job by collaborating around that open source software. You can avoid lock-in to a particular company's tool or product too. If you're working on a particular kind of open source software or a particular package, you can put some of your team into that software community where they'll actually learn about the software over time and develop skills in it. They get to engage, to learn and potentially make contributions and input into decisions, which may influence development through that engagement.

Martin: Financially, there's also the question of staff retention. Many engineers today develop their software credentials in public or are publicly accountable for the quality of their code. People want to work in the open, creative, communal internet space. If you as an employer are not amenable to an open approach, then you simply limit the number of potential candidates that you can hire.

You see this in lots of regulated industries: some people are used to a lifetime of working behind the firewall—hidden, perhaps—and just being presented with a subset of technologies they are permitted to use by virtue of the security and vulnerability assessment, and risk management. Others are not used to that, and simply won't consider roles that are not open. To attract and retain the best people, it is incumbent upon organizations to play in open source. The skill levels, and technology sets are considered highly desirable for many people.

Security is also an interesting case in open source. Historically, we would perhaps apportion more trust to a large vendor, that would essentially assure the provided software. But that's changing. The source code for the closed source Windows operating system, for example, has been given over to customers and third parties, so it can be independently assured. That's because compiled code can be difficult to reverse and understand. So, as long as there is a guarantee that the code you see in GitHub is the same code that's built into the compiled software artifact—you also need to make sure that that's cryptographically proven—it can be *easier* to assure a piece of open source code than it is to reverse engineer closed source. And that's a

balance, it's not a silver bullet but it makes a defender's live much easier and more efficient.

Brock: Picking up what you just said about Microsoft—Microsoft were historically the biggest source of friction between proprietary software and open source. Steve Ballmer, their former CEO, once described open source as cancer. But today they've been on a journey. Microsoft is now, if not *the* biggest, then *one* of the biggest contributors to open source by the number of developers working on it and by lines of code contributed. They explain that shift is based on three reasons—and none of them are economic.

The first is skills. Developers who've learned to code in the last 20 years or more use open source as their methodology, their way of coding.

The second is that Microsoft has a cloud product, Azure. So much of the cloud environment is built on open source software that they have to engage with it. Not just use it, but actually engage with communities.

Then the third is that the customers actually ask for open source software because a lot of technologies are developed open source-first these days. For some technologies, there are no options that are not open source.

What are some of the main challenges associated with open technology, and growing the open technology community globally?

Brock: Frequently people don't know they're using open source software. I've spent years training people where you've got lawyers and engineers in the same room, and the lawyers would say that open source is against their company policy, but the engineers will say, "No, it's not, we all use it all the time!"

Within the last five years, we've seen a shift in mindset creating an acceptance and an engagement, even an acknowledgement that it's simply the best code. You don't see many companies saying they don't want to use open source software today. Again, in our OpenUKsurvey, it was notable that companies that were under three years old, without exception, said that they are using open source.

Martin: I strongly agree. By virtue of the way open source software can be consumed—the licensing, permitting, use and reuse, sometimes people don't understand that they are using particular code depending on their internal processes. You may see very large security vulnerability events like Shellshock or Heartbleed, physical boxes racked and stacked in data centers all of a sudden require a new set of patches. In many cases it wasn't clear that they were using the particular software, but the contemporaneous timing perhaps indicated that they were. From that perspective, many organizations have no real appreciation for the full spectrum of open source software that they're using and that creates risk.

Secondarily, the reluctance to use open source—from legal departments not being well aligned with understanding—has tipped over the past few years. We're now into a time of full embracing of open source.

Brock: Ten years ago, you generally had to persuade risk professionals to agree a contract around open source software. But since GitHub and GitLab have really escalated, engineers having gained the power to just take the open source code that they want and bring it into their organizations. That's going to mean a lot of open source, because it doesn't make sense for them to go out and recreate things that already exist that they can take for free. It's just a waste of time. And most of the younger engineers in particular have grown up with those open source practices being the norm.

We've heard people talk today about how security is starting to become more of a consideration in the open source space. How do you see the two

continuing to evolve together over the next five years, both at a national and commercial level?

Brock: From a policy perspective, the UK is a little bit behind in that we haven't delivered a policy around this yet. I suspect that the UK will take a broader approach. We've seen in the US the Biden Ordinance from 2021 and there's the EU Cyber Act, which lifts and shifts that. UK organizations are going to have to comply with those so it makes sense that we will follow with something along those lines.

But I'd be really pleased if we could see the UK, which has so much talent around open source engineering, taking a leadership position and a broader approach from a policy perspective. Sometimes being first mover isn't the most advantageous. We have an opportunity to not only pick up security issues but to sweep up the things beyond security that need to be managed as part of "curation" – the broader term for good technical hygiene and governace as well.

Martin: Very much so. The most recent proposed regulation from US was generally highly competent. They were reacting to the SolarWinds issue, but covered off technologies and ways and means in a future leaning manner. It's a good example of second mover advantage because though the European Union is not in lockstep, it's certainly in the footsteps of those proposals.

Thinking about the UK, my mission is to get UK government and the private sector to start to pay open source maintainers for their toil, and directionally security patching and hardening, and of course to prevent the risk of bad legislation.

Brock: Andrew [Martin] was a big part of OpenUK's Summer of Open Source Software Security. It was designed to create an engagement with the public and private sectors, so people who are not familiar with some of the issues that exist around security and open source software can watch videos and listen to the podcast. Today's Thought Leadership event is a culmination of that activity.

Martin: The Kubernetes and the Cloud Native Computing Foundation's KubeCon is a great example of community collaboration. It's gone from being a three-day conference with security as a small "day zero" event for a few interested people, to now having two dedicated security days as part of the main conference. The Linux Foundation has now spun this out into its own dedicated event in Seattle during February, and it's looking to be in the same realm eventually as established conferences like RSA or Black Hat. It's very much self-propelled by the renewed scrutiny that's on open source security.

What changes will we have to make to support that evolution, both within the open source community and outside of it?

Martin: Remuneration is key. For many people, intellectual pursuit and fun are their key motivations to be involved in open source. But there is a disparity between open source and the proprietary software that goes into Britain's national infrastructure.

Who assures its quality? Who makes sure software is always moving, and that it never stands still? We want this constant evolution, and any software that doesn't move forward will die because the APIs that it integrates with will advance. Eventually, a lot of software becomes obsolete just by virtue of not being recent. And all these things cost money.

People will often build open source software, place it into the commons, and allow it to grow. It has to be supported and kept up to date, and that takes time and money to do properly. Without remuneration for those activities, the code risks atrophying and becoming independently useless.

Brock: Just to add to that—any obligations around security and curation sit with the end user, not the distributor or creator of code. The users must make sure the code they select is suitable for the use case it's being used for. They are accountable for

ensuring its well delivered. There's no responsibility on the part of the developer or distributor and this is specifically called out in open source licenses.

Understanding that is critical to security.

The remuneration Andrew is alluding to is to my mind going to come in two ways: it's going to come from direct contracting for services from skilled developers, but also governments are going to have no choice but to look at how they collectively fund the work of open source communities.

Not only can you not realistically expect people to continuously work for free and then ask them to maintain things, or do more to support any requirements of your use cases without remuneration, but we also need to recognize the imbalance. Also, it's not just this need for sharing funding but there is a need to support maintainers with resource too.

On the other hand, the fundamental premise of open source software is that it is usable by anybody and for any purpose. There can be no restriction on third party usage including commercial usage. So you can use the code to profit with no obligation to give back. Nobody who shares their code open source can stop that. It's the choice you make by sharing your code on an open source licence.

But as we increasingly see end users without the skills to manage their usage appropriately needing support with their implementation and ongoing curation of the software, that's where we are going to see the need for contracting for services and money changing hands. I think we're going to see a lot more of that over the next few years.

Thank you to Amanda Brock and Andrew Martin for taking part in this interview. You can find out more about how OpenUK supports the open technology community via their website.

Expert Insights provides leading research, reviews, and interviews to help organizations make the right IT purchasing decisions with confidence.

Caitlin Jones

Deputy Head Of Content

Caitlin Jones is Deputy Head of Content at Expert Insights. Before joining Expert Insights, Caitlin spent three years producing award-winning technical training materials and journalistic content. Caitlin holds a First Class BA in English Literature and German, and currently provides our content team with strategic editorial guidance as well as carrying out detailed research to create articles that are accurate, engaging and relevant.

Cloud Back-Up and Recovery

Zero Trust Security

All Categories

Contact Us

Careers

News

For Vendors

Lead Generation

Get Listed

 Review Guidelines

Privacy Policy Terms Of Use

Advertiser Disclosure FAQs