Martin Hinton (00:06)

Hi, and welcome to the next episode of the Cyber Insurance News and Information Podcast. I'm the executive editor of Cyber Insurance News and your host today, Martin Hinton. Joining me today is Craig Ramsey. He is with Omada and we're here today to talk about their most recent report on identity governance. What does that mean? What does Craig do? How does he come to this? I could tell you all that I know already, but what I'm going to do is let Craig tell you a little bit about himself, how he got to this moment in his career, and then launch into this identity governance report. ~

so that we can understand the importance of this, why it matters to companies of all size, and some of the challenges that the industry faces, ~ large and small, in that space. So Craig, first, thanks so much for joining us.

tell me a little about your career, how you got to this space, a little bit of Omada, and yeah, go ahead.

Craig (00:55)

Absolutely, and thank you for having me Martin. Pleasure to be here and hello to everyone who's listening. So Craig Ramsey from Omada. As you can hear, I am originally from Edinburgh in Scotland, now based out of Nashville, Tennessee. Moved here in January with Omada. I've been with Omada for about five years, so very happy for them to support me on that move. I've been an identity since I graduated from computer science in 2008.

apart from a small three years where I was a police officer. That's maybe a whole other story for whole other podcast.

But yes, I started in an operational IT graduate scheme, working in an identity team for a financial services organization in the UK. At that point, identity was a project. It wasn't a pillar of cybersecurity. I moved around to a couple of different organizations, eventually moved into the vendor world as a delivery consultant with RSA security. And then, as I said, I've been with Omada now in the pre-sales organization for the last five years currently in Nashville, Tennessee.

And OMADA themselves, they're actually celebrating their 25th anniversary this year. were in our head of operations in the US in Richmond, Virginia last week celebrating that. And yeah, we are a leader in identity governance and administration. And as you said, our report, the state of identity governance in 2025 was released at the start of this year.

There's a whole myriad of statistics, facts, findings that we can pull from that. think the two that jump out at me, given that we did a webinar about efficiency and security and IGA earlier this week is that 40 % of organizations still haven't modernized their IGA capabilities and nearly three quarters of them still think they've got users that are over permissive. So given that we've been around for 25

identity has been around for that long, there's still a lot of challenges that need to be tackled with organizations of any shape and

Martin Hinton (02:44)

So one of the things that I think I've mentioned to you is that this industry is full of acronyms. So identity governance and administration or IGA, not the supermarket. Explain to me what that

Craig (02:57)

Sure, so there's a mantra for identity governance administration that's been around for quite a while and it's giving the right access to the right people at the right time for the right reasons. And when you think about that, it's making sure that whenever you join an organization and what your job is, you could be a learning and development administrator, you could be a help desk operator.

when you log in from day one, one, you can log in, two, you've got the tools to do your job immediately. And then from an overall organizational perspective, you want to make sure that's done in a secure manner. If your job title changes, those accesses change with you. When you leave the organization, your access is disabled in a timely manner to make sure that you're not putting your organization to risks.

Martin Hinton (03:37)

so from a ~ putting it in a physical sort of security perspective, this is a bit like having a warehouse in an office. And if someone in the legal

or the accounting department has no reason to be in the warehouse where the televisions this company's shipping are sold, then using their ID card, it wouldn't work. There'd be no reason for them to go into that part of the company. And in a digital sense, that's the same idea that within the...

digital office space, the reality of all the things that occur in the digital world, contracts, invoices, that your permissions to gain access to these places are designed to make your job possible, but also limit your ability to wander the halls, if you will, the digital halls of the company's files. Is that oversimplifying it,

Craig (04:23)

No,

as oversimplifying at all. I think you're right. I think the challenge that we often have is that we do talk in complex language. And I think that's a good analogy. There's often talk about authentication and authorization and identity and authentication is, do I have the ability to log in? So to your point, can I go in the front door of that building, you know, of the house? Yes, I can. But then the authorizations are what you can do once you're authenticated. So making sure that's the concept of least privilege. I only have what I do.

only have access to what I need to do my job and nothing more. And I think that, kind of to your point, you can't just wander around freely in the building once you're in is a fair analogy.

Martin Hinton (05:04)

In the scheme of cybersecurity issues, ransomware, phishing, malware, all this sort of thing, where does IGA or identity governance fit and how does it matter to the audience? Why should a small business owner or a medium-sized business owner or anyone watching this care

Craig (05:23)

So I mean, if you think about all of those attack vectors you were just talking about in terms of ransomware, et cetera, I think what's central to nearly all breaches, maybe not all, but a very, very high percentage of breaches we see just now, the common factor in it is identity. an identity has been compromised, a user account has been compromised in some way or form. So you've got the two things of a breach. You've got the likelihood and you've got the impact.

All those controls with anti-ransomware and all that are reducing the likelihood of that happening. And then IGA has some capabilities to reduce the likelihood, but then if you have that least privileged access, et cetera, you're reducing the blast radius, so to speak. You're reducing the impact of a potential breach by ensuring that your identities are properly managed.

Martin Hinton (06:12)

So when it comes to managing this at companies, one of the things that I gleaned from the report is that 60 % of companies that you talk to for this cite the cost of it all ~ as a barrier, is the word I've got in front of me. ~ Is that really the case, or are there reasonable solutions here? How do you rate that as a real reason for things to be not what they could be?

Craig (06:37)

Yeah, and I think, and I'll put my hands up working in the pre-sales organization, it's a challenge we have in the industry that we maybe do not explain the value of identity governance.

~ as effective as we can do. So as much as it has value and security and compliance, there are big cost savings that can be made. There is a huge return of value, return of investment. Your end users can have a better experience. There can be improved productivity. So making that compelling business case about the value IGA can bring, I think is important.

It's not always seen necessarily as the most sexy of technologies. People view user recertifications as something not core to their job. I mean, until there's a breach, everyone, it's kind of, why would we fix the roof while the sun's shining a little bit?

Martin Hinton (07:31)

Yeah.

One of the things the report gets into is sort of the nature of the way these systems work and that there's some outdated sort of a, what's the right word to use, know, manual process for how it all works. And I wonder whether you could touch on what that means and cite some examples of where a that can go cause problems.

Craig (07:53)

Sure, mean focusing purely in the manual part of it, mean one thing that IGA can do and has done for a while is automate the provisioning ~ of access. That's why initially when sort of identity was looked as an operational IT piece, it was an efficiency project or something.

of those natures. You've got a baseline of the effort involved to do all these things. You can look at the amount of tickets that are raised with the service desk to grant access for a joiner, grant access for a mover, remove access for a lever, provision access as a result of access requests. So mean, if you can automate all of those things, as well as put intelligence around them to make sure people are making informed decisions, you're making a huge saving on the administrative side. ~

I said, you're starting to provide insight into the decisions that people should make, you start to do role insights to create role-based access control for people so there's less

access requests, less decision points and user access reviews. You're massively reducing the manual effort not only to actually implement the processes, but interact with the processes so they become less cumbersome to the end users that have to do them because they have those responsibilities.

Martin Hinton (09:06)

So that's an important thing about making it a manageable thing for the user, right? so they don't get worn out by the, you know, having to unlock five locks to get in the door. You're like, Lord, this is, you know, like, there needs to be a wisdom around the human element of all this so that it becomes manageable. Is that something that people need to keep in mind?

Craig (09:26)

Yeah, and I think to give a very clear example of that and an example of how we actually help solve that, recertification or user access review fatigue is definitely a thing.

If you have, say, 50 people reporting to you, all of those people have 150, 200 individual pieces of access, which is not unrealistic. That's maybe a quite low estimate. You're talking, you know, 1,000 plus decision points for that user to make. If you were presented with a user access review without any insight on saying how often it was used, when it was requested, et cetera, then it just, you're gonna go for the path of least resistance. You're gonna select all and keep.

if you couple the intelligence and start making smart recommendations to users, as well as make role-based access control a thing where you've got...

~ bundles of common access grouped up based on business function or technical function, you're then dealing with a much smaller number of items. And the real life example we did have was an organization that had their user access review had nearly a million ~ access decisions that needed to made. We cut that down to 130,000, which is still a lot, but the average for a manager went down from.

around 750 to 1000 down to below 100. So, you it makes it much more manageable and you're identifying true risk and allowing them to make those informed decisions.

Martin Hinton (10:52)

When you consider this environment, when it's less than ideal, when there's IGA or identity governance weakness within an organization, particularly now, I think that one of the things that the audience needs to know is that the organization around cybercrime now, and cybercrime as a service and that sort of thing, and all this sort of thing, it's highly, highly organized, international, state-sponsored. When you're looking at how professionalized cybercrime can exploit

IGA weaknesses. What kinds of things do you see?

Craig (11:25)

Yeah, I mean, that's a very good point. When you look at cybercrime taken in its totality, it's actually, I think, the third biggest economy in the world when you look at the money it's making. And these groups are seriously organized. They have recruitment, they have training, they have everything you'd expect to see in a typical enterprise-sized organization. It's not this lone person in a hoodie behind a laptop that we've seen from movies in the 90s and that you see when you ask ChatGPT to generate an image of a hacker.

So you know when you see how seriously organized these people are you need to be seriously organized in your defense as well to make sure that as I said earlier you're one of the tenets of zero trust is to assume breach. So you know if you have that mentality and you're constantly trying to reduce the likelihood and impact of a

you're in a far better position against these very organized foes.

Martin Hinton (12:16)

So take me through what like a typical breach path might look like when an attacker exploits an identity management environment. What goes on?

Craig (12:26)

Yeah, I mean, there are many different routes you can get to. I mentioned early Britain identity being compromised. And I think one thing we see or we have seen is where people are socially engineered. So depending on how much information is publicly available about you via LinkedIn, Facebook, Instagram, et cetera, people can then phone up the help desk of your organization, pretend to be you, say they've been locked out of whatever account and you know, they'll look for somebody that's maybe ~ that they think would have those elevated

permissions and then you know they're not hacking it and they're logging it because they've done this social engineering they've been able to convince the person without and if you've not got multi-factor authentication ~ to protect you they've been able to log in and then you can switch off your critical controls deploy around somewhere and you know I mean that's just one potential path into the organization which stresses the importance of strong identity controls

Martin Hinton (13:19)

There

are reports that that's how the Marks and Spencer hack initiated. I don't know if it's been confirmed by Marks and Spencer, but what's interesting about it is that we have this presumption that it's all high tech. And some of it in the case of calling a help desk and being able to pretend to be someone so effectively because of their social media footprint, for example, that's a reminder that there's a street level sort of three card Monte reality

some of this still that exists. isn't all, you know,

hackers with, like you said, keyboards and writing code and all that sort of thing, there is still a very human element to how this can unfold from an identity management point of view. Is that something that you see?

Craig (14:02)

Yeah, and I mean, you've got these deep fakes and stuff as well now where people will potentially be able to mimic high ranking people in your organization. And I think there's technology out there that's starting to be able to identify those fakes, et cetera. But I hate to say, and I don't say, it's said a lot, that humans are the weak chain. And I don't think that is the case because people don't do things maliciously. They don't act in such ways. So there's a responsibility in people in the information security, cybersecurity industry.

departments to make sure that there is a good culture, education etc to try and avoid these pitfalls that people can fall into.

Martin Hinton (14:41)

Yeah. So I want to move on now because it's the ~ million dollar phrase or two words, AI, automation, and then also this, you know, the specter of agentic AI. And for the audience, agentic AI means it has agency over itself. has ~ the ability to adapt once prompted in a way that a human might change a plan once contact is made with the enemy on a battlefield, right?

It can think for itself in a way that the AI we may be using nowadays doesn't, which is, you know, well, let's start with artificial intelligence and automation, and then we can get into agentic AI, how realistic it is a concern as it is now, and that sort of thing. But start with AI in this space. What opportunities, ~ in practical terms, does AI ~ create to reduce friction in identity

Craig (15:36)

I mean, AI is awesome. It's the biggest technological leaps that I can remember certainly in my lifetime. And the opportunities that he presents are massive. There are massive

considerations around privacy, how to use it with, you know, morally as well. But if we think about it from an identity perspective,

I mentioned earlier about recommendations when people are trying to make decisions in user access requests or reviews. AI can take a huge amount of information and present to the user, you know, based on information about how often this is used, how many of this person's peers have this access, maybe you should approve or reject this. I still think the important thing about AI, that's a phrase that I've coined a little bit, is that AI needs AI. Artificial intelligence needs an accountable individual.

Ultimately, the decision for this kind of stuff, when you think about data being one of the most critical assets of a company, the decision still needs to be made by the person that has the accountability over that. ~ And not to creep onto the next point, I think that's where there's a conversation between assistive agents and fully agentic AI agents comes into play as well.

Martin Hinton (16:52)

So imagine a future for me where there is this agentic adaptive AI. I mean, how close is that to being real? how would it manifest itself if you can put on your see over the horizon goggles? What do you imagine it being able to do, assuming it comes to fruition and lives up to the of the blue sky kind of ideas that are put out about what it can do now, which seems realistic, it

Craig (17:19)

I think it is realistic. How far away it is, I don't know, but we are absolutely moving in that direction. We have at Omada our own generative AI assistant, Javi, which is a natural language interface where people are able to start talking to it and request access, approve access, ask questions about IGA and how to deploy and how to configure Omada.

And I think getting to that fully agentic state will be where you log in in the morning and it'll say overnight, I identified these risks, I mitigated them for you. Here's some stuff you have to approve. Here's recommended actions you should take. These new systems or accesses

have been detected. Maybe you should update these roles. Maybe this policy should be updated. It's taking a holistic view across your entire estate, all your identities, all your system, all the data, and then making recommendations, potentially taking action.

and making those suggestions on what should be updated and what action should be taken. The comparison I make it though is, if you think about agent-ic AI, and you can do this with chat GPT already today, you're going on a two week vacation to a country you've never visited before. And you can prompt AI to say, I'm going here, here's my interests, put an itinerary together for me.

you still want to validate, and this is just, this is your holiday, this is your vacation. I want to validate that before any bookings are made. If you give that to a fully agentic AI, it will go and make all the bookings on your behalf for you. And that's where I think assistive agents are maybe a better way because you're augmenting the human element rather than replacing.

Martin Hinton (18:53)

One of the things that I've thought about, and this is a little off topic, so if you don't have much to say about it, don't worry. But one of the things I've seen in a number of reports is how many attacks occur during, say, the holidays or at times when staffing is cut because it's a vacation period, like the Christmas holiday season or summertime, where you have people preoccupied by Christmas shopping or holiday shopping or summer planning or vacation planning coming into the summertime.

The thought I've had is that those are perfect opportunities where at Agentic.ai, to what you're pointing out, to really augment the human thought process can be there sort of as a backstop against someone being on vacation or the, if you will, to keep it very simply, the 10 person cybersecurity team having two or three people out on vacation or sick or something like that. It bolsters them in a way that provides that sort of, I don't know,

clarity of thought, I guess, about what needs to be

Craig (19:53)

Yeah, and I think being on the vendor side is slightly different, but I think any organization that are considering that, I AIs must have their own AI strategy manifest that goes beyond just identity. I think there needs to be a very strong direction in any organization about what they want to use AI for, the risks they're willing to accept that goes

with it. Because in the example you gave there, during these periods of vacation or whatever where...

If things are coming and it need to be approved, if you give AI agency over that and a decision it makes leads to a breach, who's responsible for that in terms of once that investigation, AI is not going to take the stand and say, I made this decision because of X, Y, Z. The accountable person that should make the decision is still the person that's going to be accountable for whatever goes wrong when they start doing that investigation.

Martin Hinton (20:45)

That's a very, very good point. Thank you for making it. moving on now, we want to get into cloud-based IGA versus old school legacy setups. Explain to me what those two things are and a little bit about what the benefits are for the cloud base.

Craig (21:01)

Sure, legacy solutions tend to have been deployed to fix a very specific problem. They tend to be on premise. They tend to be highly customized, quite costly to maintain, and they carry a large amount of tech debt. think when you then look at the advances we've made in cloud computing, the technology there, the explosion of cloud services as well, and the computational powers needed to start taking advantage of some of these AI things we've been talking about, I think that's where...

legacy, we're not trying to change the processes. Those processes are deeply embedded. IGA is a technical translation of your business processes, but what you want to be able to move towards is having ~ identity architecture that is scalable. And that's not only from a performance perspective for your elastic scalability on periods of high demand, but

scalable to the number of types of identities you have, scalable to the number of types of resources and systems that you have. It needs to be ~ simplified. So as I said, removing all that

you want to align things with best practice, you want to be able to grow at that speed, and you want to lower the overall total cost of ownership, which cloud enables you to do. And then finally, it needs to be agile. I'm not talking the project management methodology there. I think it needs to be able to respond at speed to the change in the organization, to the risks that it can detect, and utilizing cloud technology that can interact far quicker with other cloud solutions, and using things like the shared signal framework that's being worked on by the OpenID Foundation.

To be able to adopt and start making use of that, you need to have a modern SAS IGA solution in place.

Martin Hinton (22:38)

to move on to the next topic. We were going to discuss quantum computing and the next threat horizon is the heading of this section. ~ if quantum computing breaks today's encryption, how does identity governance respond?

computing, maybe you could explain a little bit about what that means for the audience, because I think a lot of people don't quite understand how this is a leap in the capacity of computer to do things in a way that is, you know, sometimes a bit hard to comprehend. It's about a bit like looking into the night sky and imagining that these stars are all actually galaxies with a thousand planets around them and that sort of thing. it's, it's for me, at least that's how I kind of

Is that too much? Tell me a bit about this space.

Craig (23:21)

No, I mean to try to simplify it, the leap to quantum computing is to do with the amount of calculations or processes that can be done in a short period of time. if you think about the advance of mathematics, gone from counting on your fingers and toes to an abacus to a calculator to a computer.

the next jump would be to quantum computing. In terms of those kind of leaps, in terms of how many things can be processed at once, that would be how I would explain the leap. the sheer number of ~ calculations it can do in...

nanosecs, pardon, not parsecs, that's Star Wars. ~ But in a tiny amount of time, it's huge. And as you said, it's trying to wrap your head around the number of stars and grains of sand on a beach, et cetera. it's that kind of advanced computer we're talking about.

Martin Hinton (24:12)

And are companies like yours and is the security side of it, obviously you're paralleling the progress and the growth so that there's like anything, any evolution, any development, the ability to adapt to new threats and utilize new tools like quantum computing to protect the IGA space.

Craig (24:36)

certainly keeping an eye on it. think the main concern people do have is that quantum computing will then be able to break modern encryption techniques.

to your point, cybersecurity criminals are already looking at AI. The ability for them to start to use those kind of things to agentically start you doing denial of service attacks is there already. And I think even if that quantum decryption does arrive in the next 10 years, everything else we're talking about from, I think, an identity first security perspective, we should be working on that today anyway. Because even if they do manage to break in the front door, if they get in and they can't do anything, then

we've kind of we've seen off that challenge. What that'll look like in terms of how quantum computing will affect IGA, I genuinely don't know at this point in time. It's

Martin Hinton (25:27)

Yeah. Well, I

Craig (25:29)

early in the pack.

Martin Hinton (25:31)

I think what I'm hearing you say is that there's old adages in this new world. And one of them is that you have to be constantly adapting and moving forward and looking for ways to improve. And quantum computing is just another thing that has to be reacted to like AI was, or I mean, even from putting it in a very historical space, right? You know, we didn't have banks for a long time and vaults.

art as old as you think or as common as you think even 150 or so years ago. The idea is that, you know, once upon a time you didn't need a police car to chase a getaway car. We just have to be in that mindset where if there's something valuable in a space, in this case a digital space, there are always going to be people who are motivated to try and steal it and they're going to use the tools available to them. that just a, you need to have that kind of persistent kind of

Craig (26:25)

yeah, there's always going to be a job in the cyberspace. I don't think that's going to become agentic. think the human nature of that is still absolutely needed. you're right, I think keeping up with the pace of technology and innovation, there's always going to be people using it for good or bad, to really simplify it. And just keeping an eye and making sure that you keep yourself aware of the most modern. ~

attack vectors people are trying to compromise, trying to keep on top of that, trying to keep educating and you know, the whole purpose of this, trying to simplify this and get the message out to as many people as possible with the importance of being, know, risk aware and aware of, you know, your identity footprint out there and what you can do to help protect your own identity and not just your enterprise stuff when you're at work is important.

Martin Hinton (27:09)

I want to move on to wrapping up. And a couple of questions that we kicked around when we first talked were what kind of myths exist around identity governments that you wish you could, I think the phrase in the question we talked about was delete from the internet forever, as impossible as that might be. What's something you think people need to realize isn't true?

Craig (27:30)

What do I want to put in Room 101? I think identity security being a barrier, I think, is the thing to me. It's seen as a barrier to the business. People look to circumvent it, it'll slow them down, it's inefficient. And when it's done properly, it's a business enabler. It enables cloud adoption, digital transformation, and it can improve your end user experience and productivity. I think identity being seen as a barrier is something I would very much like to banish from the internet or into Room 101.

Martin Hinton (27:58)

That's a really good point. mean, I think that again, putting it in the physical security space, you need to get to the point where everyone having to swipe their ID to get by the stern style and not being able to wave to the guard who recognizes you and let you in. this is just, this actually makes the company more secure, more financially secure, know, resilient against risk and any kind of problem that might occur. And we need to adopt that for this digital space, which is sometimes a bit hard for

us to kind of contemplate because it is, for the most part, despite being able look at your computer and all the things you can do and your phone and all these other things, is invisible to us. I think that's a really good point that you need to just get over it to some

degree, maybe. ~ So, go ahead and get started. So just to wrap up, ~ one of the things that we talked about is if you could sit down with a CISO who's stuck

Craig (28:43)

It's so Sorry.

Martin Hinton (28:54)

a decade ago in this space and you had a 30 second or an elevator pitch moment with them to convince them to really rethink the need that they have to move into the current era of this space and IGA security. What would you say to them?

Craig (29:12)

I'm assuming I can't give them any spoilers like there's going to be a global pandemic that will accelerate digital transformation in a way that you can't possibly imagine. ~

Martin Hinton (29:20)

That's a good point.

mean, I you know, I mean, you think about remote work and the way that impacted this space now it's dramatic. I mean, I mean, there are a lot of companies that don't have the very basic stuff like, like what are the things that everyone should have in this space now, given the remote work and the hybrid workspace that's become a reality, no matter what anyone says, since COVID and undeniably in the future because of the

The fact that it's as efficient as everyone going to the office nine to five, four days, five days a week, pardon me.

Craig (29:55)

think to take your original question about the 2015 CISO, I there was a phrase that was going to do that identity is the new perimeter and you're moving away from traditional perimeter based ~ technology. And I think that's still the case. I think, ~ well, it's not only because of the identity is the control plane. I think we live in a pretty perimeter as world where you've got to your own identity, work from anywhere, et cetera.

And digital transformation was a theme back in 2015, but then cloud adoption was just starting. So I think, you know, as those journeys are beginning, you're going to start being faced with more modern challenges around managing your identities, managing the risks that come with identities, and therefore modernizing your identity architecture to keep up with that pace of change is important.

So that's how you would then start being able to meet those challenges. And then you're also, to the point I made earlier, if you're able to grow and scale with these cloud applications, with the number of different identities, you're be able to make a bigger case for the value you're able to add to the organization through those efficiency savings, productivity gains, cost savings. And I think that's how you would then make that case to multiple stakeholders in the organization. Not only from a risk perspective, cost saving, efficiency gains, productivity gains, modern IGA can really, really boost

your business in ways that is valuable to everyone in the organization.

Martin Hinton (31:16)

Is there anything about this space that we haven't touched on that you think is really important for people to know? mean, one of the things that you said that makes me think about it very simply, which is how I tend to approach things, is that identity governance and identity security for a company is as simple as knowing who's inside your base, who's inside the company.

And in order to be secure and confident that you know who's around and know who's in the home, if you will, or in the company, you've got to make sure that your system works. But what do people need to know about this that we haven't touched on? What haven't we discussed that you think is important?

Craig (31:52)

Yeah, so I think identity security strategies are becoming more and more prevalent. Identity governance to me is the control plane of that. know I'm shocking somebody that comes from an IGA vendor saying we're central to that, but it's part of a wider identity fabric. So we talked about AI in terms of how it can have an impact and positive impact on IGA. The things it can do around yet another acronym, UABBA, user endpoint behavior analytics. So baselining normal user behavior

to generate or detect indicators of compromise and take action and all these identity solutions talking to each other is maybe something that would be worth a further conversation. So governance and sort of centralized governance is very central to that, but there's far more in the identity security space beyond identity governance that is very important to take that holistic view to identity security.

Martin Hinton (32:49)

Well, I think that's a good spot to wrap up. So Craig Ramsey with OMADA, chatting about their most recent identity governance report from earlier in 2025. Thank you really so much for your time and your breaking down some of this complicated stuff in ways that I think that help people understand why it matters and why it's important. So again, thank you very much. We're going to have a link to the report and our coverage of it in the notes for this. So wherever you might be watching or listening, you can look for that to learn a little bit more.

First off, I'm Martin Hinton with Cyber Insurance News. Thank you so much for watching. If you enjoyed this, please leave us a comment. If you've got questions about this or you're wondering about something, we'll do our best to answer them and I can share them with Craig if I can't get an answer to you. And as always, subscribe, like and share. Your

is what we live with. So again, Martin Hinton with Cyber Insurance News. Thanks so much Enjoy the rest of your day.

then we just need to make sure it all