TECH REIMAGINED
AN ENDAVA PODCAST

Portrait of a Hacker with Greg Van Der Gaast

00:00:01
Speaker 1: Tech Reimagined, redefining the relationship between people and technology. Brought to you by Endava, this is Tech Reimagined.

00:00:12
Bradley Howard: Hello, and welcome back. I'm Bradley Howard. I'm glad to welcome you to a new episode of Tech Reimagined. We're now in our third season and we aim to explore how technology is influencing the fabric of our society, how we live, the way we work and how we do business.

Follow us on your favorite podcast platform and listen to the interesting stories that all of our inspirational guests share with us. And speaking of great guests, it's an absolute delight to introduce you to today's guests, a man that has the ability to find weaknesses in systems and then help fix those bigger issues, Greg Van der Gaast, an information security expert, author, and all around people enthusiast.
Hello, Greg. How are you?

00:00:50
Greg: Hi, Bradley. I am very well. Thanks for having me. How are you?

00:00:53
Bradley Howard: Very good. Thank you. And welcome to the show again. Can you give us a bit of an introduction into yourself, please?

00:00:59
Greg: I'm Greg Van der Gaast. I am a massive petrolhead who also moonlights as a CISO and security expert. I've been doing this for about 25 years, currently CISO for a company called Scoutbee GmbH in the procurement space, helping some very, very large household names with their supply chains. And I think that's about it for now. We'll keep the rest for later.

00:01:23
Bradley Howard: Great. And just want to check CISO is chief information security officer, that's right?

00:01:29
Greg: That is correct. Yeah.

00:01:30
Bradley Howard: Excellent. So the subject of today's episode is about corporate information security in a digitally accelerated world. So let's start right to the beginning with the Big Global News Story all in capitals. Can you tell us what happened?

00:01:45
Greg: The one, if we go back about 20, 25 years. So there was a little thing with a nuclear weapons facility that may have been exploited by a certain teenage Greg at the time. No biggie, really. Some WIRED, some CNN, some United Nation Security Council stuff, nothing too dramatic.

00:02:06
Bradley Howard: And my first thought when I hear that, is what did your parents say?

00:02:09
Greg: I didn't tell my mom. And I was actually living on my own when the gentlemen from the various law enforcement agencies showed up at the door. So yeah, I was actually living by myself in the States and I just remember four gentlemen in suits showing up at the door and they were from the Defense Department and FBI.

And I was like, " I know why you're here, but I don't think you can prove anything." So I invited them in for a coffee and I, at some point told them, I was, "I don't think you can prove anything. I was actually worried you guys were from Immigration." And that's when suit number four in the back of the room, raised his hand and went, " I'm from Immigration." And I was quickly put into a van and taken away. But yeah, good times.

00:02:57
Bradley Howard: Wow. How did you get into hacking and what computer did you use at the time?

00:03:01
Greg: At the time, quite bizarrely I was very into Silicon Graphics machine. So I had an old SGI machine and just a PC running Linux. This is back in like 1997, 1998.
How I got into hacking is when I was 15 years old, my sister brought home a VHS copy of the movie Hackers, Angelina Jolie was in it. So obviously I was highly motivated. After hacking the Nuclear Weapons Facility, still no girls. I blame... Still no, Angie, I blame Brad Pitt for getting in the way.

Yeah, that was the about it. So that ended up with me being collected by the DoD and the FBI who made me a job offer, I couldn't refuse. I jokingly kid that they were quite adamant about the couldn't refuse part.

Then about three years doing some very unusual, undercover stuff for them, not all behind the computer. Being wired up for microphones, aerial surveillance, some pretty fancy stuff.

We were, I believe at the time, the largest and the only centrally funded, so out of Washington, cyber crime operation in the country. And that led to some more regular private public sector stuff over the years. And I actually had a pause where it was really fed up with IT and security, got very bored of it.

I tried to get into the automotive industry. I was actually a close protection officer for a few years, doing bodyguard work. And I eventually kind of returned to IT about five, six years ago, out of a financial necessity.

What's really developed my, and I think this is important to say, what's really developed my current position and what makes me a bit different is my hacking days. It's not what most people think. It's not the actual hacking. It's the competitiveness and the needing to defend your own system and to build things right.

And this is something I only realized like 15 years later, that I seem to be one of the very few people doing this in information security, caring more about how we build things to make them impervious, rather than constantly responding to threats and events and situations.

00:05:21
Bradley Howard: It's not really about impervious, because you know, we've had bank robberies for hundreds of years now and still people can still get into banks. It's about trying to slow down the criminals, isn't it?

00:05:31
Greg: Yeah, there's no 100%, but banks have vaults, they have security systems, they have laws, they have locks, they have all kinds of stuff going on. We don't just put 500 security guards in front of a big pile of money in the middle of the street, which is unfortunately a closer analogy to what we currently do in IT.

There's very little thought into how we actually build stuff to make it as secure as possible. And then we try to layer a bunch of stuff on it. It's a bit like having a house with a great security cameras and alarms and lots of doors and locks, but all the walls are made of paper you can just punch through.

00:06:11
Bradley Howard: You talked about your first set of equipment, the Silicon Graphics machine, which must have been worth quite a lot of money back in those days. I remember having them at university, admittedly more than 20 years ago, but they were pretty top end machines.

But remember that was probably just at the very start of the Internet, so how were you learning how to do some of the hacking at that time? Probably not from hackers either, from Angelina Jolie.

00:06:36
Greg: No, no. Although bizarrely, that movie was actually quite historically accurate to a lot of stuff that happened in the early '90s, down to the character names. I think I picked it up just learning about hacking. This is a thing, and I would go on the Internet with your dial up modem. And there was no Yahoo!, or there was no Google, so you couldn't Google anything.

So you had to Yahoo! things back then and just kind of hacking. And then by that, I stumbled upon this thing called Unix and Linux and Usenet and you start researching, researching, researching, and you add vulnerability feeds, you learn coding languages, you learn what buffer overflows are.

You start coding stuff, you start building up to the finding the IRC channels with the people in it, that you just kind of build up from there. And it's a much, much larger ecosystem nowadays than it was back then.

00:07:24
Bradley Howard: When you hacked into the nuclear facility, how serious and sensitive were the final devices that you'd got onto? I'm not obviously expecting you to say the big red button, but were you bouncing around from router to router at that time? Or, was it a bit more serious than that?

00:07:39
Greg: So, I mean, first of all things were, I'm not going to say we had any capability of launching weapons, this was a research facility where they actually developed and enriched and that kind of stuff. But the funny thing is I didn't actually know what I was hacking into at the time.

It was only after I hacked into it by tricking a mail server to mail itself an entry for an account that we got access. I think there were like, I want to say eight servers, for memory, in there. So that was the whole network, eight machines.

But once, once I hacked it to it, I punched the IP address into Netscape, the premier web browser at the time and up loads this page. And I'm like, " Ah." So yeah, went back in and started downloading all the emails, which made their way to WIRED magazine, to the CIA to all kinds of stuff.

So, there's an article out there, I think on CNET that talks about the NSA being involved, the CIA being involved, the DIA being involved. Everyone's involved. Yeah, good times.

00:08:45
Bradley Howard: Right. And would you mind sharing, was there anything that went through your mind at that time that was, " I probably shouldn't be doing this. I'm going to get the hell out of here."? Or was it just your inquisitive personality at that time?

00:08:55
Greg: I was 16 years old. So no. I think I went back to the kitchen and got some more crisps was the level of thought involved here, with some more Coca- Cola.

00:09:10
Bradley Howard: And then bring it up to present day in and maybe even to the future as well. How much has hacking changed from then to now?

00:09:18
Greg: Well, this is my gripe with things because I don't think it's changed much at all. It really, really hasn't. And we keep talking about this fast evolving threat landscape, blah, blah, blah. And yeah, the players change and the methods of capitalizing on breaches. So you have to think, " Everyone knows about ransomware nowadays," but ransomware is merely a way of capitalizing on a breach.

You used to breach stuff because you wanted to face the Spice Girls website and Photoshop their hair off because you couldn't stand them as a teenager. Not that I did that, but that used to be it. And then it used to be a bit, " Okay, we can maybe blackmail this company. We can maybe do this. We can steal some card data."

And now we realize, or the criminals out there have realized, " Well, holding their data to ransom, holding their ability to operate as a business to ransom is much more lucrative," but that's all it is.

The actual ways in have not changed in 25 years. They are basic vulnerabilities that are found, that are known, that are announced, that companies do not act on, or they are engineering and design and architectural principles that have been known for 20, 30 years. But people are now implementing them.
And unfortunately we've developed a security industry, which is all about fixing all this stuff or detecting and responding to all this stuff very, very late in the game before all this stuff has already been built in such a way that it is vulnerable. And this is a fantastic business model, because you have endless recurring revenue.

But there are very, very few people in the security industry who actually endeavor on engaging the business and building things properly so that they are less likely to have issues and too, so that they are more easily maintained and fixed when they do have issues.

00:11:13
Bradley Howard: So before we start talking about corporate security, I've just got one more question. So if you could give your 16- year old, some advice, any advice, what would it be?

00:11:24
Greg: Even just life advice?

00:11:26

Bradley Howard: Yeah.

00:11:27
Greg: I'm going to make it very, very simple. Don't marry that woman. Someone needed to tell me that one. I'll just move on from there.

00:11:37

Bradley Howard: Definitely move on. Right. So let's talk about some corporate security. So we are now talking post pandemic or it's July 2022, so who knows what's in store around the corner?

So earlier this year, we at Endava commissioned a survey of 1, 000 IT leaders and 57% of them said that security was in their top three priorities. Yet every year, there's new records of security breaches, cyber attacks and data leaks.

So what do you think decision- makers should be doing better to protect their organizations?

00:12:13

Greg: So I think they, and this is the crux to what I was talking about before, I still in 25 years, I've not come across an organization that is actually focusing on building things right. There are some out there, but they're extremely rare. You know, basic patching, asset management, healthy processes, integration of security into the business, but also integration of the business into security.

These are all either terrible or nonexistent. And this is where we really need to start focalizing. I have this parking lot analogy, I call it, for the industry and it's basically, it's a car factory where cars are being built on the assembly line. And then they're eventually being pushed out into this parking lot or car park, as you would call it here in the UK to be sold.

The problem is they're being lobbed from the third floor. So each one of these cars ends up damaged and someone has to take it somewhere and build a workshop around it. And try to figure out what's wrong with it, what tools will be needed, what parts needed, what the processes to get to that part, how to change it? And you need a lot of technical expertise to do this. You need people to manage the workflow. You need to figure out what your minimal acceptable standard is. And these cars keep coming. So this workload just keeps increasing, increasing, increasing.

And next thing you know, you need thousands of highly skilled people to do all this work, and you need consultants and you need bodies to give ways of working and you need vendors to sell you better tools to do it a little bit faster. But no one is taking a step back and saying, " Why are we lobbing the cars off the third floor?"

And the security industry is so focalized on this parking lot mentality, the focus of work, that we completely ignore it. In fact, we dismiss the very people who would look at it. Now, the cars aren't actually being dropped from the third floor. Issues are being introduced throughout the assembly line. But what we should be doing is finding those issues in the parking lot, going into the business, the assembly line, and addressing those issues there so we stop this flow.

And that is the fundamental paradigm shift that we need to start doing. Start building right? Start insisting on quality, documentation, oversight, a culture of care and engagement. And I don't just mean in IT, but in all senses of the word.

To give you an example of that, I did an onboarding session with a new employee this morning. It was supposed to be a meet year manager, and it was the entire team. Everyone talked about what they did, their weekends, their passions. Everyone's making fun of each other. We were talking about what dates we've been on. You know, funny stories in the past just to get this person hugely comfortable, happy, feel open, trusting, we're mocking ourselves in front of them.

We want that maximum engagement from that person. We want to show that we're very aware about the impact that we have for each other. No one is just doing a job. We think about all the connection points, all the impacts. What if I do something, if I cut this corner, how will that impact somebody else? And that's very rare.

And I think that the leadership skills to enable that kind of connection and want to bring out that really play hard, work hard, but also care mentality is really rare in general. It's especially rare in IT and security in particular. We've got very low kind of EQ and soft skills.

But that connection between people that enables that kind of tightness of connection between the processes and technologies they use together is essential, to have that holistic way of thinking that resolves these issues. I know it seems very disconnected from what people think is security, but that mindset of really caring and looking at how things fit together and addressing the human needs behind that is hugely important.
And people need to do that. People need to stop building, just trading security as building big SOCs, which are basically burnout factories, which are so far down the chain where you're just constantly just repeating finding an issue, fixing an issue, finding an issue, fixing an issue. You're never actually... You don't have the power or the reach to actually fix what's sending all these things your way in the first place. That needs to change.

00:16:25
Bradley Howard: Yeah. I mean, I would definitely challenge there are no companies doing that because at Endava, we produce some financial systems for a variety of different companies. I've worked on some of the, let's say the payment clients, where security is absolutely front and foremost of some of the requirements.

What I would say is that often companies want something delivered much more quickly. So therefore some of the quality elements, not just security, become much harder to deliver on and

not just security. But do you think that security is part of overall quality? Or do you think that it should be separated?

00:17:04
Greg: First of all, I believe you, my expression was I have not. Obviously you're in a sector where it's very, very critical and you understand the importance of it. A lot of businesses don't, they don't understand and they've been sold this idea that security is the silo. And that really needs to stop. Whereas you, I think in your line of business, you understand it's fundamentally important for your business success.

If you didn't have that, I mean, your transaction volumes are so high that if there's an issue, it's very quickly a very big issue and you lose business, and no one wants to trust you to build their payment systems, right? I think security is a quality function.
What was your question? Exactly? Can you reword it?

00:17:42
Bradley Howard: So do you think that security is part of the nonfunctional requirements of building a platform along with many other quality factors from automated testing, et cetera?

00:17:53
Greg: I think it is. I think it's definitely a quality function, but I think the mindset you need to have in security is to look at how everything works together, which I think actually makes it tremendously powerful. So just to give you, for me security, you need to get involved into everything. You have to look across silos.

It can be strange things. It can be like if your sales team is rewarded to just land deals, but there are no controls around, they're allowed to overpromise. And then that puts huge pressures on your engineering team and quality suffers as a result and security issues tend to be quality issues, then your sales remuneration process is a security issue.

So you really have to look at things very holistically, like what causes the root impacts? You know, Boeing's a great example. The issues that led them to build planes that they knew could crash and try to cover it up are cultural issues. They're not technical software issues, or defects in a sensor. They are ultimately cultural issues.

And I think you need to treat security that way. And the beauty of doing it that way is you help bring, it's not just security awareness, it's caring. So you really help develop a culture of transparency, a culture of accountability. But also you tend to be, if you're doing this in security and you really want to see how all the pieces fit together... I read an article a couple of weeks ago that most security teams are unaware of about 40% of business platforms inside their own business, because they don't necessarily think about them.

They're thinking about servers, this and that, but I'll give you an example at Scoutbee, there's customer data, like very sensitive customer data, schematics, that sort of thing, maybe stored in Salesforce. So if you're not thinking about securing your Salesforce, because you think it's just contracts and sales stuff, you don't know about it.

But we go through that. And this is a great example as well because we re- architected how we use Salesforce to make sure that we could have the controls over this. And by doing that, we actually optimized how operations used Salesforce. So they actually like it a bit better and we shaved 48,000 a year on licensing costs by re-architecting it.

So we did a security effort, initiative that improved productivity, as well as security and saved us money.

00:20:26
Bradley Howard: That comes back to your car production line analogy, doesn't it? That not only are you improving some of the output quality, but you're likely to reduce some of the cost as well?

00:20:36
Greg: Yeah, exactly. Because most security, the way it's done now is cleanup. I mean, I genuinely think 90% of the Sec Op stuff, so the SOC based activities we do nowadays can be completely eliminated if you spent 10% of that funding and resource being more proactive elsewhere.

00:20:55
Bradley Howard: So as a CISO, chief information security officer, what's the first thing that you do when you go into a new organization? What's the first thing you look at?

00:21:04
Greg: So first thing as a CISO, management support. Is their management support? Because I don't want to go in there without it.

00:21:11
Bradley Howard: And who are you looking for the support from in the management team?

00:21:15
Greg: I am looking at basically CEO, COO, CFO level. I'm looking for support, but I'm not looking for the support that most people think, which is give us a bunch of budget. It's not necessarily about budget headcount. I think in most cases, these executive teams, so that real upper C- level, they've never been communicated, the real/ commercial value of security. Even by the industry, by most CIOs and by most CSOs even.

I'll use another car analogy. I take my car to a garage and I don't know what they're doing to it. My car's my pride and joy, but I just get a bill saying they changed the oil and some filters after five hours. And I assume they did it. And this is about the level of scrutiny you get with most security questionnaires.

But then if I go to a different garage and it's completely transparent, and I can see them work on my car in the background, because there's a glass behind the reception. And if I have questions, they answer me and I'm invited in and I can see that they're putting brand name fluids in. And if I have any questions, I can walk right up to it. And they're putting blankets on it to not scratch at all the stuff.

Then I know that they're doing it and that makes me feel much better about it. And if I have a choice of garages, I'm going to go back to that one next time. Even if it costs me 10 or 20% more, and that's the crux. And if you were in a very sensitive area in terms of data protection and value to your customer sensitivity, that is a competitive top line differentiator.

And it's not just something that makes revenues, but it's something like we've had tenders where there's no mention of security on tenders, but you talk about it and what you do about it and you demonstrate, you make some very interesting points and you show that you've done market research. And " that's why we do this, da, da, da." And you reply to the tender offer, including that. And the next thing you know, they're going to your competitors and asking them tough security questions, because they've just realized, " Our data is actually quite important to us."

Normally, this is relegated to after we signed a deal, we'll get your security team to our security team and hash it out. And no one from the commercial side cares, but you've now used it to actually rule out some of your competitors because you've brought it to the fore.

Things like the cost efficiencies, like we just mentioned with the optimizing SAS platforms and internal tools and all that stuff. These are all things that bring you, that build support. There are also things that, which you're going to need that support.
And they are things that bring you closer to the business, which it's not just the support, it's the visibility. Because most significant breaches are not highly sophisticated cyber tech. They are brain dead, simple things happening in areas where the IT or security team wasn't aware existed.

The closer you are to the business, the more you can see, the more you can influence. And the more you can protect. It's a bit like having a 13- year old daughter and all the things she wants to do you say, " No, no, no, no." And then she asks you if she wants to go to the festival and you say " No," and she goes anyway without you.

Whereas if instead you builds a relationship to empower her, do the things she likes, develop her talents. Then the question is, " Do you want to come to the festival with me?" And you are there and able to protect, even though the whole time, because you have such a great relationship and great things come out of it, protection is never even in her awareness, but you have been able to be there to protect because you had that level of involvement. So that's very important. So that's one.

The second thing is to really understand the business, the culture, the value, the revenue and cost centers, the dependencies. Again, that's your business quality function, not an IT function. So you have to do that before you can think of anything.

Third is get into details, question everything, because questionnaires are absolute BS. I don't know why we use questionnaires. I've done due diligence for cyber insurance companies and been able to show negligence to avoid doing insurance payouts within three hours.

I know CISOs hate me because I get them their insurance money withheld, but you should have done a better job, sorry. And I think when doing, this is actually relatively easy because what I call the cultural effect. I once walked into a place and they showed me this maturity assessment that they'd done. And it was a bar graph showing me about 10 different areas of IT. And they're like, " Oh, well here, our maturity is a 10. Here our maturity is a six, here's a seven. Here it's a two, here's a four, here's a six, five, seven, eight, whatever. So we're about a six on average. We'd really like you to look into these areas where we're a two and a four."

And I turned around and was like, " Well, no. Because this is BS. I'm going to put your maturity at about 1. 5." And they're like, " What? That's impossible. Like can't you do basic math because our average is a six and our lowest score is a two. So it's impossible that it's a 1. 5."

And I was like, " Well, this is all your IT operations team. And there is simply no way that a team that is so dedicated and detail oriented to score a perfect 10 in one area, scores a two for being sloppy and messy in another. Which means that whoever gave this a 10 and a two, whoever gave this a 10, probably missed some stuff in the two. So I'm going to downgrade your two as a 1. 5 and I'm going to say, that's your benchmark."

They thought I was crazy. And then we spent the next year digging stuff up and we did a much more detailed assessment a year later. And the average was 1. 6 and it was incredibly consistent. It was all between like 1.4 and 1. 8, in every area. And that just shows to show the consistency of culture.

So if you see even a handful of small things that stand out, you start digging and you will find stuff everywhere. So it's very important to have that accurate, honest baseline, and then build a program to figure out what the issues are, where things need to be fixed and then build a program.

And I always create a multilayered or multi pillared program with executives. So capture executive support and actual security strategy teams, roles, that kind of stuff. A program management layer, where we actually manage, update, keep, integrate, all the integration of everything we're going to do in the program apart for our legal and HR. How we're going to integrate with that? Onboarding, off- boarding, also training, disciplinary processes, compliance layer, which I think is really important, because it's like a huge mistake that people do is they try to build security programs around ISO in this SOC 2 cyber essentials.

It's so important to not do that and to align it to what your actual business is, does, what matters to it, how your processes work, the skillset of your people, your own capabilities. Build something that works for you and cover every aspect of your business. And then map that to the various standards.

And the beauty of doing this is you have something that really works for you. So it's going to be more effective, more sustainable, cheaper, and it makes it very easy for you to map it to other standards very quickly. So you can enter a new market that has a different set of requirements, different standard. Can be a market, it can be a region, it can be an industry and you can do a mapping exercise in two or three weeks instead of having an 18 month project every time.

Other things, product security. Like if you're a product company like we are at Scoutbee, document the hell out of your infrastructure, your products, your development. The internal business platforms, they're often forgotten as well.

So things like your Salesforce, your NetSuite, your Google workspace, your Mirror Board. All these things tend to be really, really neglected. Then all the operational IT processes. Review absolutely everything IT and engineering does from a security perspective. Then you get your SIC Ops, which is the only security most people do.

You know that's your SOC, your forensics. And the human factors, hugely important, hugely underrated. Have a person dedicated to human factors. That's not just awareness training, but role specific training and fostering a culture of openness and communication. And the amount of stuff that you find from a humans factors person who's good at talking to people and going through their jobs and their like their day- to- day is incredible. Because you can have Mark who, if you're looking at logs and Mark looks really, really busy, top employee. " God, we've got some great people here." Yeah. Mark actually left the company two years ago, and there's 25 people using his admin account to do a bunch of stuff.

But the logs don't tell you that. The tech doesn't tell you that. You only find out when people trust you enough to actually tell you what's going on in their department.

And the final layer is commercial. That's everything from make security part of our brand value, do marketing, do blogs about security, raise awareness. The more awareness you raise of it to your customers, the more traction you get internally as well, because it becomes more of a commercial concern. But also things like contract review and RFIs and SLAs.

It's amazing how many people, companies, MSPs sign contracts. And two years later have absolutely no idea what's in them and what they're supposed to be delivering against. So this is my approach to building something that's a bit holistic and works and actually does what it's supposed to do.

And you can by all means alter it any way you want to, whatever works best for you, simplify it.

00:30:58
Bradley Howard: And what do you think is the highest threat to most businesses on the cloud today? Is it an edge attack through the website or a mobile app or basically something which users can interface with? Or do you worry about a centralized attack? Let's say at the server level or the cloud level?

00:31:15
Greg: I think both of those things are quite interrelated because one could lead to the other, for starters. I'm actually going to simplify it and say, " I think the biggest threat to any cloud- based business is themselves." The threats themselves don't necessarily matter. I don't think people realize how constant attacks are. There are groups with botnets of hundreds of thousands of computers currently scanning, probing everything.

If there's a vulnerability somewhere, it gets picked up, it gets put in a queue and eventually someone will get to it. And I mean, the attackers. It's like filling a container with water, it doesn't matter where, if there's a crack somewhere, it's going to come out.

The problem with cloud- based companies is in how fast they themselves can create problems that will eventually be found and exploited. It's not like old school where you had to build a server. It took time and it was there in the office and people saw it and thought about it.

It's very easy for an engineering team without governance to just spin up all kinds of stuff that you are not aware of, that does not get maintained, that wasn't there this morning. And that is the single biggest threat. So I think cloud has hugely accelerated stuff, but you need to really double down on your governance to make sure that it doesn't get away from you.

00:32:47
Bradley Howard: At the start of the conversation, we talked about how hacking used to be about the kudos to say that someone has hacked into a system and maybe for a cause. I think of it a bit like graffiti, that you can kind of tag your ego to having hacked into something. For the records, Greg's now smiling. And nowadays it's become a bit more of a business to generate some income.

How do you think that will evolve in the future? Do you think it will become all business focused?

00:33:17
Greg: It's funny because yeah, we used to call it web defacement didn't we? We'd break into websites and defaced the website. And in fact, the hacking group I was in, I remember MTV actually mock defaced their own website, claiming one member of our group had done it, as a publicity stunt.

But I do think nowadays it's becoming a business. It is a business. We have hilarious presentations where we see ransomware groups have better tech support and customer service than our phone companies and our electrical, our utility companies.

It's incredibly well organized. And the support is actually very quick and very good. I mean, it sucks because they're extorting you, but they're surprisingly professional about it.
So I do think it's going to become more and more monetized. I think the scary part is it's also going to be more and more weaponized, as this problem continues to grow. As we continue to ignore what actually makes things difficult to break into in the first place. It's increasingly easy to use it to cause disruption.

You can potentially shut down infrastructure and funnily enough, part of what's really helping our infrastructure being resilient is just because it's so old. The stuff, the vulnerable things on it, haven't been commoditized yet. But both in terms of disruption and also influence, you can break into a website, you can break into an API and start feeding false information, causing all kinds of disruption. So it's actually quite scary.

00:35:01
Bradley Howard: And what's your view of companies that take out cyber insurance and then make a claim once they've been hacked. Does that become a self- monetized industry in itself?

00:35:12
Greg: Cyber insurance in general, I think for a lot of reasons you said is a bad idea because it tends to support the wrong behaviors. In a way it's self- regulating because the premiums are going up and up and up, and the scope of coverage is going down and down and down. And the requirements that they have is increasing. Which the requirements increasing is a good thing.

I'm actually surprised to hear how many CISOs are actually complaining about the increased requirements rather than celebrating that finally, I have some leverage to do my job. And I think one very good approach now, and part of this is because of the reason you mentioned, is to insure yourself.

Set money aside every year or reserve part of your capital or whatever for what you would normally be your insurance premium, and your needed payout. Because A, if nothing happens, you get that money back. If something does happen, you're guaranteed that it's there.
And you're also not on a list saying that you are insured, which if you are insured, you're actually more likely to be targeted. And if you pay out on insurance, you are far more likely to be targeted again. And again, because companies don't understand this. That the management team's making these decisions getting these policies are not informed about the quality issues and how they work in their processes, in their products, in their infrastructure.

So for them, it's just a, " these things happen" type scenario. They're not aware of the option of, " I could be investing here and making this a whole lot less likely." That is what needs to happen rather than just think, " Oh, acts of God. So I need insurance."

There's a lot you can do to minimize the risk of this. You know, if I drive everywhere with my eyes shut at 150 miles an hour, I'm a lot more likely to have an accident than if I drive 70 and pay attention. And we need to kind of refocus that and stop using the insurance as to kind of get out of jail free card.

00:37:12
Bradley Howard: Well, thank you so much, Greg, for sharing bits about yourself and your career with us. It was really interesting hearing those stories. To all of our listeners, I hope you enjoyed this edition of Tech Reimagined. Thanks for joining us today. And please look for next week's episode on all relevant podcast platforms.

Until next time, please like this podcast on your podcast app right away. And please don't forget to subscribe so that you don't miss any future episodes. Please share this episode with your friends and colleagues, if you've enjoyed it. Thank you very much.