Magellan – In The Know: Episode 31

Cyber security – The new world order

Announcement (00:00):

The information contained in this podcast is for general information purposes and does not constitute investment advice. You should seek investment advice tailored to your circumstances before making any investment decision. Opinions stated as Suzette Kent's own and not to be considered reflective of any of the organisations with whom she's affiliated.

Host (00:22):

This is In The Know, a Monthly Investment Podcast brought to you by Magellan Asset Management.

Suzette Kent (00:28):

The thing that concerns me the most is the bad actors that are after disruption. They're after business disruption. Some of those other things, identity, financial information, those have been happening. We know ways to stop it. We know ways to remediate that impact. But when you disrupt a business, when you create distrust between the two parties, those have profound effects that are beyond the actual event itself.

Host (00:56):

That's Suzette Kent, a former US Federal Chief Information Officer and a global business transformation executive, speaking about the greatest cybersecurity threats businesses and governments face. Welcome to Magellan, In The Know. In this episode, Suzette Kent is joined by Magellan head of Macro and Portfolio Manager, Arvid Streimann, to explore the data and cybersecurity landscape and how potential pitfalls can be avoided.

(01:29):

They cover the need for internal as well as external security maintenance, what to do if you have a breach, whether to pay a ransom and the sectors that are at most risk. And there's a surprise in store for anyone who suspects that the cloud lacks security. But first, here's a warm welcome from Arvid Streimann.

Arvid Streimann (01:47):

Well, welcome everyone to the latest episode of Magellan's In The Know. I'm Arvid Streimann, a Portfolio Manager at Magellan and also the Head of Macro. And we are very lucky today to have a very special guest, her name is Suzette Kent. She previously served as the Federal Chief Information Officer for the United States, and she's also held senior leadership roles at EY, Accenture and JP Morgan.

(02:14):

She's an expert on technology transformation, cybersecurity, digital enablement, workforce development, and also ways that technology can be leveraged to solve challenges that businesses and governments face. She's currently the CEO of Kent Advisory Services, which helps clients right around the world with strategic technology transformation projects. So, welcome Suzette.

Suzette Kent (02:35):

Thank you Arvid, I'm really glad to be here.

Arvid Streimann (02:37):

Okay, so it's great to have you here, Suzette, and I thought we might start today's discussion by talking a little bit about you. And perhaps you can talk us through a little bit of what you did as Chief Information Officer for the US government.

Suzette Kent (02:47):

I'd be happy to. It's an interesting role. Well, the Federal Chief Information Officer for the United States is the individual that the President appoints to coordinate a couple of things for all the federal agencies across the US government. So, policy oversight for how agencies use technology to deliver on their mission and services, oversight about how that technology is used. Is it used in the ways that we intend in following policies?

(03:16):

Managing the resources. So, that's both the workforce and the budget. The role actually is aligned with the Office of Management and Budget, so how we plan for on the budget side. Managing the councils, which is the leadership of all of our CISO organisations and the CIOs of every agency and lots of things in workforce development. And some of the things I was most excited about was that we updated the national cyber strategy for the first time in 15 years.

(03:45):

We put out the first ever federal data strategy for the United States. I had the opportunity to work with other governments, the fantastic team there in Australia, Canada, Singapore, and the UK. And the most important is to be an advocate for the priorities of the administration and the key things that need to get done across the government, inside and outside with our vendors. So, that's a little bit of all the things rolled into the job.

Arvid Streimann (04:15):

That sounds like quite a lot. And you mentioned something about a cyber strategy, first one in 15 years. So, that is something that rolls around every now and again, right?

Suzette Kent (04:23):

Absolutely. And we're looking forward to a new one coming out hopefully sometime very soon.

Arvid Streimann (04:27):

Okay, great. And how often do they come out? Is it a regular thing, or is it something that whenever someone asks for it?

Suzette Kent (04:33):

No, this will actually only be our third. Like I said, the first one under the Bush administration, we had the one that we put out on the Trump administration, so that had been a 15 year. And then they're going to, sometime in the near future, put out another one. And the great thing is regardless of administration, the principles have continued to be the same. And our overall goal is to uplift both the expectations and behaviours around cybersecurity, not only inside our government, but how it affects businesses in the United States and how we interact with the rest of the world.

Arvid Streimann (05:09):

And cyber strategy, I think we'll maybe talk about this a little bit later, but obviously cyber as a risk to businesses, investors, society, governments is something that's getting an additional press all the time. So, we can drill into that a little bit later. But I was interested in how that role that you had with the government differs from what you do with the private sector? You mentioned that obviously the private sector is someone who's interested in cyber and technology as well.

Suzette Kent (05:32):

The work had a lot of similarities. It's mission focused, development of policy, understanding performance, matching. I often said the magic is matching the technology capability to the problem that we're trying to solve, because there's so many technologies that are out there, but they uniquely can have impact depending on the problem. But the biggest difference that I found was sometimes, or most of the time, in how the funding happens and prioritisation.

(06:03):

Coming out of a private sector background, the majority of almost three decades in private sector, the company sets a directive, you get the resources, the team goes after. It is that clear. The key stakeholder setting the priorities and awarding the money are incredibly well aligned. It's not the same thing, at least in the US federal government. Sometimes you have priorities coming from say the executive office and executive order from the President or the head of an agency, but Congress awards the money.

(06:32):

And the way that that happens is a very slow process and technology is not slow. So, those were some of the things that a lot of similarities in what kind of outcomes you want to affect, a lot of differences in the process that you have to go through to get there.

Arvid Streimann (06:46):

Yeah, technology certainly isn't slow. I think even if we look across the past five or 10 years or even your lifetime, there's certainly a lot that's changed. And I think the threat profile of course has changed as well when you're thinking about companies and governments, national security, that type of thing.

Suzette Kent (07:02):

It certainly changed.

Arvid Streimann (07:03):

So, maybe let's start on that track, let's start with talking about cyber risks. And maybe as a bit of a scene setter here, we can talk a little bit about who the main actors are behind these cyber risks that companies face. We'll get to the government later. And when we're thinking about those actors, maybe we can talk about what are their goals and which areas do you think there's the most concern or the most risk.

Suzette Kent (07:24):

For your listeners and how they're thinking, I'm going to kind of frame it as maybe two pieces, like who's inside and poses threat and risk and who's outside.

Arvid Streimann (07:33):

Okay.

Suzette Kent (07:34):

Start with the outside first, because that's the most obvious. There are many different groups that are after a thing, and that thing is an identity. Credential information, financial information, intellectual property. But we also know that two thirds of cyber events that happen are bad actors exploiting known vulnerabilities. So, they're looking for weakness, they're looking for people who have not acted quickly. And that may sound simple to fix, but it isn't a small task looking at the proliferation of technologies that many companies use, staying up to date on all those vulnerabilities and applying patches to all the various sets of tools and never disrupting your business.

(08:14):

The thing that sometimes concerns me the most is the bad actors that are after disruption. They're after business disruption. Some of those other things, identity, financial information, those have been happening. We know ways to stop it. We know ways to remediate that impact. But when you disrupt a business, when you create distrust between the two parties, those have profound effects that are beyond the actual event itself.

(08:43):

And those are the ones where when I look at dedicating resources and actions, those are the ones that are most concerning. But for companies, they have to think about what goes on inside. And we also know that behaviour is a huge component of managing your risk. So, they have to keep their employee base at the edge of the best behaviours, the most secure behaviours, and understand what information leakage looks like and have tools that prevent ransomware. They have to have a good resiliency programme.

(09:19):

And from my technology experiences inside companies, there was often that positive friction, but it's something we always have to manage around ease of bringing new products to market and how easy they are to use and being secure by design. Because sometimes ensuring something as secure means you have a few more steps, or the process may feel a little bit different. So, when companies look at that big landscape, they're facing challenges outside, but they also have a to-do list inside that never stops.

Arvid Streimann (09:51):

So, what was really interesting in your answer just then, Suzette, was the two-thirds number, which I presume is when your iPhone says that you need a data update or Windows says you've got to restart your computer and download an update. It's basically that, right?

Suzette Kent (10:04):

It's that on steroids. But yes, we see devices that have updates, we see software that have updates, we see all types of things. And when that action isn't taken, you're creating an opportunity for someone to exploit that vulnerability. And even when companies consider their resource needs, that takes a lot of resources. Like you use the iPhone as a great example, you don't know when that update's coming and you don't know how long it's going to take. And for large, very sophisticated companies, you also don't know what other things that might affect. So, it's a very important part of maintaining your business continuity every single day.

Arvid Streimann (10:44):

And it's almost an advertisement when the iPhone says, "We need to do an update." So, is that something which criminals or bad actors or foreign adversaries look at and go, "Hey, we didn't know about this, but now we do, we'd better get onto it and start using it," or did they already know about it?

Suzette Kent (10:59):

Sometimes some of both. Unfortunately the bad actors communicate with each other as well. And when something new occurs, there is a creativity applied in how to gain something of value from another entity. So, if you leave your front door open, eventually someone's going to walk in.

Arvid Streimann (11:18):

And particularly if you advertise that it's open as well.

Suzette Kent (11:20):

Yes. That house, the second house on the left, right?

Arvid Streimann (11:24):

Yeah, the porch light's on. Okay. So, in Australia, and I'm sure it's the same in the US, we've seen many companies that have seen their cyber defences breached. In Australia we've had a couple of big ones recently, Medibank and also Optus, very different businesses, but I would say still at the end of the day, they've had a data breach and there's maybe that trust thing that you were talking about. That's been a little bit of breach, and I guess this goes to brand damage when you're thinking about a business, maybe their brand with customers has been a little bit damaged there.

(11:51):

Now when a breach occurs and we hear about it, people on the street or people that read the financial press, we see that and there's a lot of uncertainty, there's a lot of people discussing about how much they should worry, but that seems to fade over time. And maybe that's because these cyber incidents are becoming more common. We are becoming used to them and it's normal. Maybe there's nothing else that can be breached, I don't know. Or maybe it's because they don't do much damage. I was wondering if you had any thoughts on that sort of response that people have and whether it is becoming normalised.

Suzette Kent (12:21):

First of all, for many businesses, the trust of their customers is a core element of their business. I came out of financial services and it's an example of an industry where the trust and the security of your information is core to the product that the company is delivering. I think that any type of breach is something that ought to be communicated. I'm kind of the proponent of information sharing. We know globally, as we've seen events occur, that sometimes they start really small.

(12:52):

They start really small with somebody trying something, whether it's an intrusion or whether they kind of poke and see, "Wait, is this going to work? Can I get at that?" And they actually get better. And so if we connect and communicate on small incidents, we have a better opportunity of stopping big ones. And that's really important. And sharing that information with your industry, with your government sources, maybe law enforcement, are ways that we can make a bigger impact.

(13:20):

Some of the biggest ransomware issues globally had different effects in different regions because they shared the information government to government. And I look at how impactful an event is based on the level of business disruption, based on the volume and type of information that was potentially exfiltrated, and then really are there visible signs of doing something with that information? For example, did somebody try to use your identity for something else?

(13:48):

Did someone try to use your financial information to misdirect a payment or to use money in a way that was not authorised? Did intellectual property end up in a place it should not be? So, those are the ways that I judge both what should we do, as well as how big of an impact a particular thing is.

Arvid Streimann (14:07):

And let's just talk about when a cyber breach occurs. So, let's just say it's occurred. Does it have to be reported in the US or not?

Suzette Kent (14:15):

It depends on the industry. There's a lot of things. Overall, like I said, I very much lean towards information sharing, but there are rules and some of the newest guidance that you've seen on our side in the US coming from the banking industry side and the regulators coming from CISA, our Cybersecurity Infrastructure Agency actually coming, I expect, in other forms and groups, there are some requirements for reporting incidents. Now the discussion continues because if something occurs, what you want to do is catch the bad actors, right?

(14:52):

And to your point of if you advertise a vulnerability, if you also advertise what happened and you're public about that, you may miss opportunities to trace down who did it and what happened. So, there's a partnership with law enforcement. So, at the government level, there are very specific timelines and reporting requirements. For industries there are reporting requirements and levels of impact. But assessing that level of impact and understanding that is still very much at the discretion of the company or the entity that was impacted.

Arvid Streimann (15:27):

Okay, that's interesting. So, as an investor, we don't know whether the company that we've been investing in has actually been breached. It may be non-disclosed or it may be disclosed to the government authorities but not to the public.

Suzette Kent (15:40):

That is true. But, again, if investors are following where some of this is going, there are proposed rules that would change that. What I would say to investors to think about is though, how do we make that rule? How do we create transparency and not diminish trust? And what I mean by that is, let me give you an example. If I told you, if you think something happened, you have to tell me within 48 hours and I'm going to disclose that to the street about what happened in my entity, what's the first thing the customer's going to say? What happened? Was I impacted? What are you going to do about it? You might not be able to answer that in 48 hours. So, where is the right point of actionable knowledge that you can do something about that is meaningful? I would also say to investors, when you see certain companies who have had repeated security breaches, that's a concern.

Arvid Streimann (16:33):

Well, that's an interesting observation, because I wanted to get onto that, which is when you do see a breach occur and you sort of reference the case where you see multiple occur for the same company, what sign posts or can you make any judgement at all as to whether it's a serious breach or not? Is that possible to do, or you find out when you find out?

Suzette Kent (16:51):

There can be different indicators like we just talked about in the other point. Do you see active action with what was taken? Again, someone's identity, money that has moved inappropriately, intellectual property or information that has been shared, somebody that has now taken over as directing activities or significant business disruption. That matters, right? That the breach mattered. I also look to see if companies have taken action with the individuals impacted to remediate that. Whether that's identity protection, whether that is giving them other controls around their data, other things like that. So, again, I look at are there signs in the ecosystem? And then also what is the company doing in its relationship with whomever was impacted and how quick are they on that and how intentional are they on correcting the situation?

Arvid Streimann (17:51):

And I guess that reaction that you see when a cyber breach occurs sort of goes to forward planning and their cyber strategies within the organisation. But is there a way that you can tell whether a company has a good cyber defence network or defences set up at all, or you find out when it doesn't occur?

Suzette Kent (18:10):

Sometimes it is hard to tell from the outside. You can think about things like older technologies. Is it visible that somebody has been slower to patch? Maybe do they have a less sophisticated technical staff. That might lead you to making some assumptions. I judge it sometimes when I'm interacting with a company based on the identity protocols and information sharing permissions and the security measures that they have with different types of activities, whether it's a payment, whether it's an inquiry, whether it's an ordering a good or service, whether I'm requesting information or accessing information, those types of things. When you see high standards met, when you see digital health, and every one of our countries has a set of standards, when you see those very clearly met, that's a great indication that security is a priority.

Arvid Streimann (19:05):

And just on this, there's a variety of different companies in the world and industries in which they operate. Who would you say are the companies or industries that are at most risk of, well, maybe at most interest to bad people?

Suzette Kent (19:18):

Go back to what we were talking about. If you see consistent, slow to patch different things, to be really blunt, we see more impact in small businesses, sometimes law enforcement, definitely territory type governments. And when you ask yourself why, many of the security solutions are exceptional, but they're very complicated to use. That may also translate into very expensive. And some of the types of things that I hope to see as we go forward, and it's becoming a little more prevalent as security capabilities are delivered as a service, is that they're more approachable, they're more consumable by businesses at all levels.

(20:02):

And that security is not only for those who can afford it. That security tools are available for all those who intend to use them in the right way. So, you can look at the incidents and you can see them around the world. They fall into many of the same categories, those that may have lesser resources and those that may not have as much personal identifiable information or financials, a non-regulated industry. So, they don't have measures that are already defined by the nature of their industry that they need to follow.

Arvid Streimann (20:39):

Now we've talked a lot about the cyber risk facing companies, but of course it's also government as we mentioned. How worried should we be about those cyber risks that the government's facing?

Suzette Kent (20:48):

It's funny you asked. I'm worried about every cyber incident, right? [inaudible 00:20:53] private sector.

Arvid Streimann (20:54):

Yeah, I can imagine.

Suzette Kent (20:55):

Because in a way all of those create distrust. Our entire world is so much more technology dependent and as we saw during COVID, extremely dependent on digital delivery and digital services, any of those events has an impact on how we perceive what is to come. I think on the government, when we see cyber activities against a government, every single government has the richest information about its citizens and they are in a central position to provide critical services to citizens. So, disruptions of those have mass impact and more wide-reaching impact. So, again, the issue could actually be very similar between a government and a private sector client, but the level of the impact or the disruption be more significant.

Arvid Streimann (21:52):

Yeah, it's interesting, because whenever there's a breach at a company level, one of the first things that I think the press gravitates to is whether there's any personal identifiable information, maybe a social security number in the US, your date of birth, your tax file number here in Australia. But as you say, the government's got all of that plus more. So, that's probably a better target if you can get in. So, Suzette, we were talking earlier about the cyber strategy and you mentioned that there had been one under your watch and there's another one which is going to come soon or be released soon. Do you have any insights into what we might expect from that cyber strategy?

Suzette Kent (22:26):

Well, I'll tell you Arvid, what I am hoping that we're going to see, I'm hoping that we're going to see more around how we support those who are more vulnerable. As we talked about, what are ways that we can make proven tools and capabilities easier to use or more accessible to smaller businesses or those who may not have the resources. And when I say resources, I don't mean just money. Globally we know that we have tech talent gaps around the world and we've seen whether it's World Economic Forum or someone else, lots of other places have done the forecast of where we need to be by 2030 with technology talent, and every single nation has a gap.

(23:13):

So, I'm saying how we close that gap, we have to also have capabilities that are more approachable based on the talent pools that we have for every nation. I hope that we're going to continue to see more clarity on what's expected, not just standards, but some of the reporting and information sharing that we've talked about. There are lots of different proposed rules and things out there, we have to continue to advance those. And it is also my hope that we'll take more steps at addressing bad actors. And right now the economy and the businesses bear the brunt of the loss and the pain and we need to figure out a different balance for that.

Arvid Streimann (23:57):

It's really interesting that you mentioned almost the democratisation of these cyber tools or these cyber-defence tools, because we all know that if you are a bigger company, you have more resources and you can spend more on cyber as well as you can spend more on marketing and all those other things. So, it falls into that I would say economies of scale bucket. So, I think it's reassuring that that is maybe part of the strategy, of course, because it seems to me as that there's two parts here.

(24:21):

The first is the two-thirds that you talked about earlier, the two thirds that you referenced, which is please patch your computer as soon as possible. And maybe the other third is, well, if you have patched your computer and someone's still attacking you, then you need those tools. So, I think it's really interesting that those tools may be more widely available and not just for the institutions with more money.

Suzette Kent (24:42):

Yeah. Inside, and I'm going to use the US example because I know it, but like I said, I've had great conversations with the team there in Australia as they've built tools. CISA actually offers some of the tools for free. They are available for free on their website. That is a way to make things more accessible. Jen Easterly, the current director, has spoken outright asking industry to up their game, those weren't her words, those are my words, but up their game on security levels and to make some of these, why do I need to do 10 patches? Did I rush something to market? That could have used a little bit more time in security.

(25:21):

But to consider security more broadly in their path to delivering products and services. So, maybe we lower the level of effort to address all of those types of things. And I also think that many companies, they have a lot of tools but not necessarily as a service. And places where we don't have the technology staff, in the US I've talked to many of the state and local governments and they don't have a team with that breadth sometimes of skills or have access to it. But if they can buy the capability as a service, that's a really interesting business model.

(26:01):

And as your investors look at things that are coming in the future, making those different kind of tiers of services that are available are going to be more important, especially as rules, requirements and penalties get finalised and everyone has to meet that same base level.

Arvid Streimann (26:22):

So, as an investor, so we're sitting here and we go, "Okay, so there's going to be this cyber strategy which is going to be released in the shorter term." Who knows when it is exactly going to be released. But you sit here as a company, as an investor in a company and you go, "Okay, so what's the impact going to be?" And I presume it means better defences, whether that's because they're required or they're almost induced or influenced to have better defences. It sounds as though there's going to be more reporting requirements, I would guess, that kind of would make sense to me.

(26:51):

But these things here, I think they're reducing the risk. I think that's kind of reducing the risk. Are there any opportunities which this cyber strategy could create? Because I think there's the risk mitigation piece, but then there's also the opportunity piece as well. Is there something that might pop out that's more than risk mitigation?

Suzette Kent (27:08):

As I do work with companies and boards and technology companies around their service in all the different places, there are definitely interesting opportunities. A changing of rules at any point in time is going to create new dialogues. And particularly some of the rules that have been proposed, just like some of our financial rules in the past are requiring visibility of activities at a much higher level. And sharing of information within your industry, sometimes again with law enforcement or customers, that means we have to capture information in a consistent way and we have to talk about it in plain language. I love all folks in the technology industry, but sometimes it's speaking your own language.

(27:55):

And the difference between someone who's deploying technology solutions and how we might think about business risk in a boardroom is a wide gap. And I think there's an opportunity to close those gaps. I also believe in the world that we are in right now with privacy as a concern, the ability to manipulate, whether it's data or images or have AI write your college paper, do to those types of things, it becomes much more important that we individually understand the controls that we have around our own information, be it any type of information, image, data or access credentials.

Arvid Streimann (28:42):

Yep, I agree. Now one thing I wanted to ask you, Suzette, has to do with the cloud. And we all know that a lot of data, instead of being stored on your personal computer at home or your personal computer at work, it's now in this thing called the cloud, which you can think of as a big data centre somewhere with loads of, let's call them computers. And people use those computers instead of using their own. And the reason why I think this is interesting is because I kind of think of it as a bit like Fort Knox, right? Where Fort Knox has all this gold and everyone knows that there's loads of gold in there.

(29:14):

And so I presume people who want the gold are thinking about breaking into Fort Knox. And of course there's a lot of razor wire and people with guns around Fort Knox. But I think you can see what I'm getting at here, which is that there's a concentration of really valuable stuff, in this case data on the cloud and maybe in some data centre or in the one spot virtually. How do you think that changes the cyber risk profile? Because I would've thought it makes a breach of that cloud facility or infrastructure a little bit more dangerous or risky.

Suzette Kent (29:43):

When we started this, you asked what are the things that were your responsibility, and one of those was policy. And one of the major policy updates that we did was cloud smart. And that particular policy was talking about just like any other technology, where is cloud the best fit? I am very positive on the cloud capabilities, because they let you make for scale, for modern capability, for the ability to have tools and services around how your data is used that are significantly more fungible and expandable in the future.

(30:20):

And the example that you gave, what's really cool about most of the cloud solutions is it's a conceptual web of Fort Knox's that have different protocols to get to information and all of it may not be in one place. So, there by design, by the architecture of these various cloud service providers, they are embedding security at the core of how the service is delivered. And that is their business, so they maintain it. So, what I see is I'm actually buying more security, I'm buying more scale, and I'm buying someone for whom keeping that current and updated and on top of it every minute, that is their core business.

(31:05):

And that allows me to go focus on my core business, whatever it may be, and know that that resource is available to contract and expand as my business contracts and expands.

Arvid Streimann (31:21):

So, when we are thinking about Fort Knox and the cloud, Fort Knox as far as I can recall, I don't think it's being broken into successfully, not even in the movies. Of course there was the movie Goldfinger, but those two thirds of cyber intrusions which are caused by people not doing the update, presumably that doesn't happen in the cloud infrastructure and presumably they've got the best cyber defence gear as well. And I think this is kind of your point, right? It's the safest place to be.

Suzette Kent (31:45):

Arvid, I will say, no one's immune. No one is immune.

Arvid Streimann (31:50):

Sure, sure.

Suzette Kent (31:50):

But when you are moving very quickly on all the known actions, you're at least reducing your risk surface. You're changing your risk, you're reducing your threat surface, you're reducing the potential impact of an incident. And for all companies, that is kind of the ideal goal of where you want to be. I want to address everything that I know and I want to have a plan to act and tools at my disposal for what I don't know.

Arvid Streimann (32:19):

So, Suzanne, I wanted to ask you about something in the technology space which has been getting a lot of press and a lot of interest and a lot of clicks, which is AI. And I think we've all had a play, or maybe most of us have had a play on ChatGPT. Among other things, it could disrupt the internet search industry and there's a company which kind of dominates that in the western world. But I think about AI and ChatGPT and I always go back to the dot-com boom, I'm sure you remember this very vividly.

(32:46):

There are a lot of technological inventions or steps which occurred at that time. And from an investor's perspective, I think a lot of them actually came true and were implemented. They just didn't get implemented as quickly and as profitably as people have thought. So, I'm interested in your view as someone who works in the technology space, what you think of AI and particularly in that lens of are people getting too excited too quickly with respect to the implementation of AI in a commercial aspect?

Suzette Kent (33:18):

Well, it's always exciting to think about what's possible and to dream, and AI is a very powerful tool. And the tools are going to continue to advance, that is a fact. I could point to 10 other things in history where almost the same conversation occurred where the capability advanced maybe sometimes faster than the rules surrounding use of the thing. And I think this is today's instance of that. I work with a global group at OECD around AI and we looked very specifically at how AI advances, how it can be used for societies and governments and others and innovation, particularly innovation.

(34:06):

So, reflect just against our short few years back using AI in COVID situations, using AI to predict and pre-stage for weather impacts, transportation, some of those types of things. We're seeing great leaps and

bounds, but like many technologies, there are some who may use data with a bias or may not think through all of the unintended consequences. We have to continue to evolve. I have enjoyed following the ChatGPT conversation and here's why. Again, great capability, how do we manage that? We think about, rather than trying to find every single place someone might do something bad, how do we prove what's real? How do we stay focused on that trust equation?

(34:56):

So, some of the universities and publishers are not looking to say, how can we tell that it's used? How can we tell it wasn't used? And Microsoft and Adobe just had an announcement where they were promoting content credentials for deep fakes, which they can't tell you all the things that got faked, they could tell you if something was true. And there was a morning show on it, but I've seen examples of how that's being done. And back to what is the citizen responsibility and how do we react, we have to demand that source of authentication. And that's how we continue the trust equation, is I can use tools for all kinds of things.

(35:36):

If I want to make a dog dance on the moon, we all know that's not real, but I could make it look real, right? How do I get to the source of the real data of how that was produced? And I think as not just your investors think, but as all of us live as citizens, if that's our bar for demand, how do I know this is real? Then we're going to drive both technology companies and products in that direction through economies, through acceptance and through use. And that's a much better pathway.

Arvid Streimann (36:11):

Suzette, we're coming to the end of the podcast and I just want to ask you one last question. From your standpoint, is there anything else that you would highlight to our listeners that they should know about? For instance, maybe there's a risk that companies face or even an opportunity that they have, which is underappreciated. We've talked about a lot of things, a lot of risks and opportunities, but what are the things that we are not talking about, which could be quite important?

Suzette Kent (36:38):

Here's just kind of a couple of things as I look to the future. We already talked about prove the truth, right? Show me how I know something is true. We already talked about more consumable security products for companies at all levels. We talked about talent development and different creative ways of developing talent and aligning it. Visibility tools. So, when I say that, I don't just mean who's on my network. I mean what are they accessing, what are they doing with it? And advancing the identity tools. Every single nation, especially the things we do globally, everyone has a whole different identity protocol, and understanding and appreciating those, but ensuring that they are sophisticated against usable is going to be important.

(37:25):

I would also say think about some of the nation state actions and how those are going to affect global product roadmap developments and particularly where investments are made in interoperability and data sharing. There's some folks that will play here but not here, and I can do this but not with this device. And those may create some differences in the scope and scale of opportunities. And then we talked about AI and we talked about data, but the availability of commercial high performance compute or high performance compute assets becomes an underlying kind of scaling factor.

(38:03):

And it has some of the same characteristics of what we talked about with where are those capabilities right now. They sit at nation states, they sit in labs, they sit in universities, and they sit in the world's

largest companies. So, if we aspire to leverage AI, we aspire to be data driven, those are also the resources that are needed. So, access to those is going to become important as we continue to advance capabilities.

Arvid Streimann (38:30):

Yeah, I would say increasingly important and a lot of these technological advances really rely on those institutions that you talked about. And so I think it's really important that they continue to be supported. So, Suzette, thanks very much for your time. It's been a wonderful conversation and I think we've all learned a lot. So, thank you for your time.

Suzette Kent (38:47):

Well, thank you for inviting me. It was great talking to you.

Host (38:50):

That was Magellan Head of Macro and Portfolio Manager, Arvid Streimann, speaking with former US Federal Chief Information Officer and Global Business Transformation Executive, Suzette Kent. We trust you've enjoyed this episode of Magellan, In The Know. Join us in a month's time for the next episode. For more information on upcoming episodes, visit magellangroup.com.au/podcast where you can also sign up to receive our regular Investment Insights Programme. Thanks for listening.