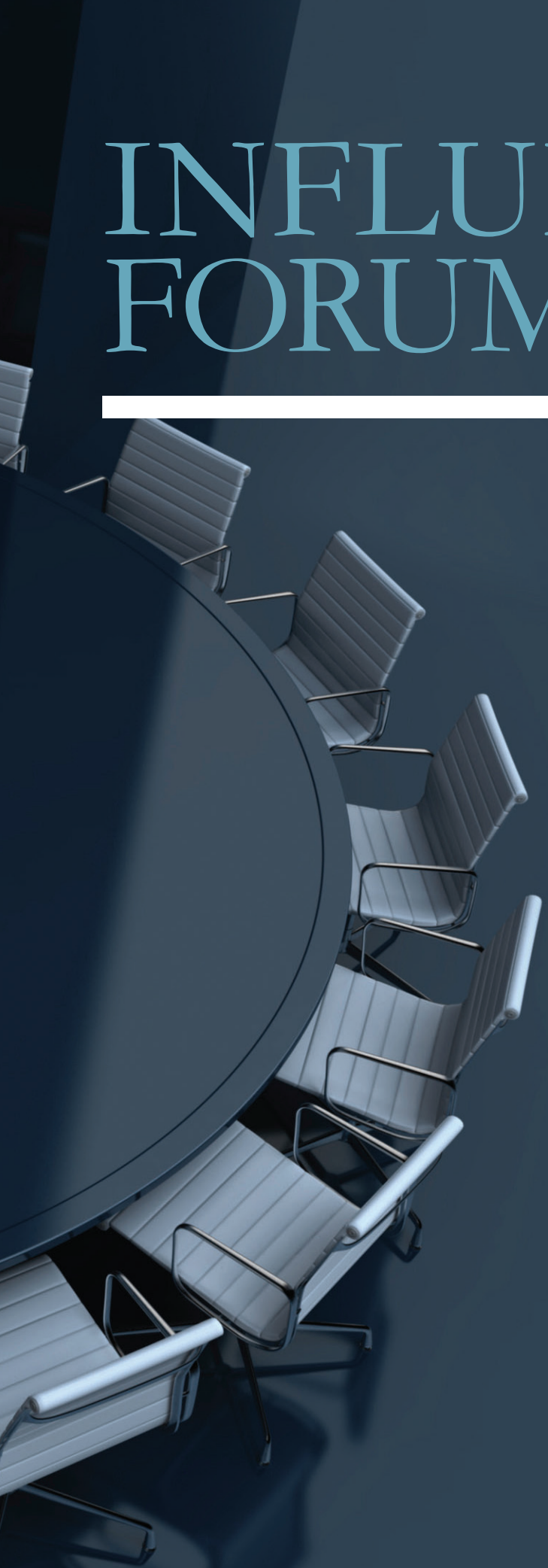
INFLUENCERS FORUM



The volume of cyber security incidents are on the rise across the board, and misconceptions continue to persist. Cyber security is the practice of protecting critical systems and sensitive information from attacks. Cyber security is designed to combat threats from across a range of systems of applications, whether those threats come from within or outside an organisation. In 2020 alone the average cost of a data breach was £3.86 million globally, and $8.6 million in the United States. These costs include discovering and repairing the breach, the cost of downtime, and the long term reputation of the business and its brand. Cyber attacks target personal identifying information (PII), names, addresses, National identification numbers, credit card information and then sell these in underground digital marketplaces. Compromised PII often leads to a loss of trust, regulatory firings, and legal action. Today we have a group of experts around the table who advise on what we can do to protect ourselves. I'd like to introduce Martin Briggs, MD of Hands On IT Services, Scott Nurston, CEO of ITHQ, Kieran Johnston, CTO of Red River, Chris White, head of cyber innovation from Cyber Resilience Centre for the South East, and Mike Perks from TVision Technology.

MAARTEN HOFFMANN

The Platinum Publisher

Maarten Hoffmann is the facilitator for the Platinum Influencer Forums

MARTIN BRIGGS

Managing Director,
Hands On IT Services

Martin started Hands On IT in 1995 which specialises in providing straight forward jargon-free outsourced IT support to small and medium-sized businesses. During those 26 years, the IT industry has changed dramatically with proactive managed support, cloud-based computing, and Cyber security now being pivotal to everything that he and his team of engineers delivers to their customers.

martin@hoc.co.uk
www.hoc.co.uk

KIEREN JOHNSTONE

CTO, Red River

Kieren Johnstone is the CTO and co-founder of Red River, a 13-year-old technology consulting business focussed on building industry-leading and innovative products, systems and apps for high-growth businesses and entrepreneurs. He heads up the Technical Steering team, which oversees tech strategy, appraisal of emerging technologies and R&D activities for the business.

k@river.red
www.river.red

CHRIS WHITE

Head of Cyber & Innovation,
Cyber Resilience Centre for the South East

Chris joined the South East Regional Organised Crime Unit as a Police Cyber Security Advisor and Prevent Sgt. Though he is now at the Cyber Resilience Centre for the South East, where he is Head of Cyber & Innovation, delivering as a speaker, presenter, technologist, and police officer working with the private sector and academia to protect business from cybercrime.

chris.white@secrc.co.uk
www.secrc.co.uk

SCOTT NURSTEN

CEO, ITHQ

Scott launched ITHQ in 2019 to support businesses with their cyber resilience, hybrid cloud infrastructure and data analytics journeys. In response to customer needs during lockdown, ITHQ developed new strategy-led solutions, which helped them beat growth targets and win their first awards. With 25 years of cyber experience, Scott has been running tech businesses in the UK for 21 years. As well as acting as an investor and non-executive director in several companies, he formerly owned Cisco partner s2s before it was sold to NG Bailey in 2008.

transform@ithq.pro
www.ithq.pro

MIKE PERKS

Contractor, TVision Technology

Mike Perks is attending this event on behalf of TVision. He has worked closely with our clients for many years, providing IT Consultancy, IT Implementation, Project Management and Business systems support to organisations who use the Microsoft stack. Mike has extensive knowledge of all things Azure, O365, licensing and business systems, including cyber security.

mike@tvisiontech.co.uk
www.tvisiontech.co.uk

LESLEY ALCOCK

Commercial Director,
Platinum Media Group

Lesley is a marketing professional, having spent many years with Capital Radio in London and the Observer Newspaper, and was instrumental in the launch of the Observer Magazine.

The Platinum Media Group is the largest circulation business publishing group in the UK, reaching up to 720,000 readers each month across three titles.

www.platinummediagroup.co.uk
07767 613707
lesley@platinummediagroup.co.uk

I turn to you first Chris, you deal with a lot of companies but mainly the police. Is this wave of attacks set to continue and are the villains going to get better?

CW: Cybercrime accounts for just under 49% of all recorded crime, which is an astonishing amount, and it will likely get worse. I often compare cyber security to day to day life, today I came into this building and there was a locked door, so I couldn't get any further, someone then came out to greet me, they vetted me, and then I was allowed in, they don't let strangers in the building. If we adopt those processes with cyber security then we will stay safe. However, small businesses are very willing to open up to the technology that they are being presented with, and that's without the proper risk assessments and security measures in place. One certificate that they should get access to is Cyber Essentials, it has a base of security controls within, and with those at your disposal you will be able to protect yourself from most of what is thrown at you. A lot of cyber crime is basic, so you don't always need the biggest and best security, but enough to protect you from these common yet smaller threats. So long as Windows Defender is updating every day it will likely be ok.

SN: I see this in the same way, stakes are high for business owners, the prize is huge for criminals. With this in mind, there is a huge disconnect between the costs of protecting yourself as a business, which are relatively low, compared to the costs of a major breach that may occur. In my experience businesses aren't doing enough to counter the crime, many aren't putting basic controls in place as, Chris has mentioned. Further up the scale people are in the same situation, which is even more concerning as they are held to the CIS (Center for Internet Security) which has 18 controls in place. When we are auditing businesses at that level we are finding that many of those controls are not in place, and with that being the case, we are inevitably going to see an uptick in crime. I wouldn't be surprised if 49% will rise much higher, it's a much easier crime than other traditional crime, especially with the rise of cryptocurrencies which provide a near untraceable outlet for the profits of cyber crime. Because of this, so much of the crime, even when we are dealing with millions of pounds worth of money in single transactions, isn't being followed up on by the police, because they are so complex.

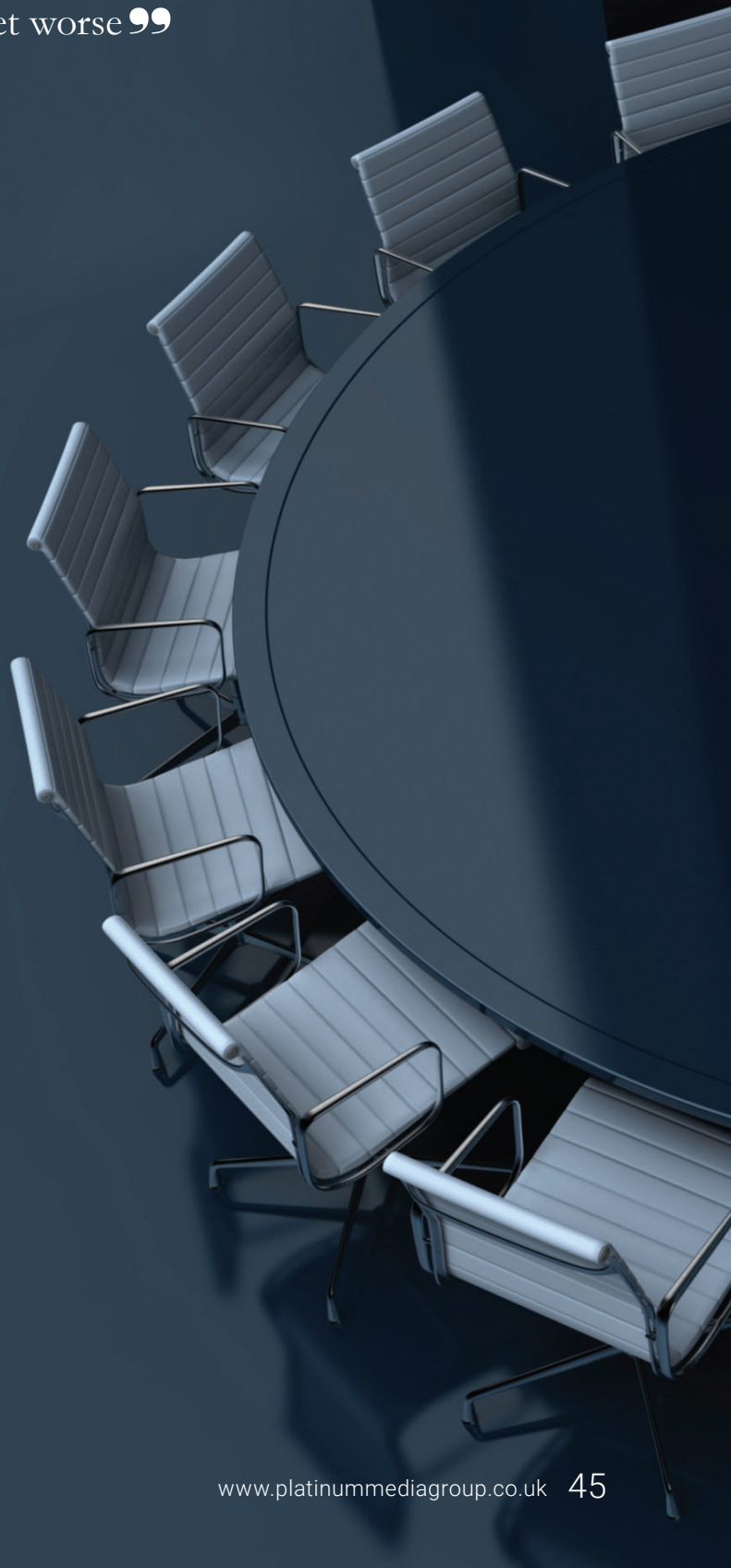
Is that not part of the problem? Discovering cybercrime is so difficult, let alone tracing it back to the source.

SN: Exactly. I was speaking to someone in the police the other day and they were saying that there is a two-year backlog of confiscated resources that still needs to be examined, but they don't have the equipment to do so. It is up to the businesses to defend themselves as it stands.

Kieren, what is Red River's involvement in this area?

KJ: We have seen both suppliers and customers who have been victims of automated attacks where they find out that their financial director's email has been hacked, contacting their clients with modified bank details to scam them – it's simple but very effective. Red River has seen the effects of cyber crime very clearly and we develop software that is bespoke for businesses. We want to make sure that this software is secure. Often that guarantee of security comes at an extra cost and we have to advise our clients of that and to be prepared for it, but it's a very low cost compared to being hacked.

> “Cybercrime accounts for just under 49% of all recorded crime, and it will likely get worse”

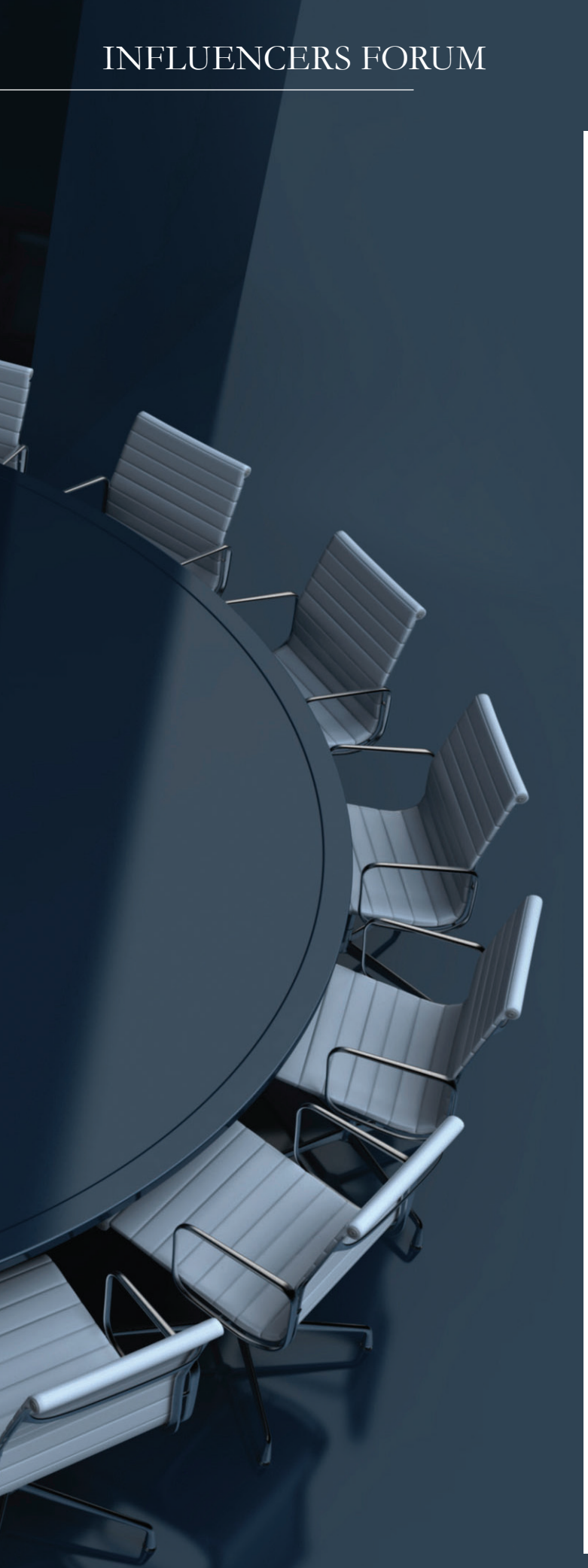


Is the cost the issue then?

KJ: We have always recommended penetration testing, just because its good practice and provides data for updates, and whilst that used to be harder to convince businesses of, the constant headline news has made it much easier. Cost isn't a huge barrier, though we would always suggest an extra budget for these things; it's important to be focussed when looking for bespoke software.

Mike, do you find it difficult to convince your customers to protect themselves?

MP: Yes, we have quite a range of customers that have 10 user systems without any form of protection, or very limited protection. Then we have the other end of the scale, 200 user systems that have a large IT investment; between the two, it is the larger organisations that struggle the most with security. They often have all the technical expertise to prevent attacks, but what often is lacking is the users who aren't fully clued up. Unless you are educating your users it all goes out the window. The two malware attacks that we have seen recently were due to users, not poor security practices of the company as a whole. Unless businesses spend the money on educating users, I don't see an end to this rise in crime.



It seems extremely simple, but Martin, do you have the same problem with getting your clients to teach their staff?

MB: Absolutely. We deal with smaller businesses and many of them don't have the budget to put time aside to train their staff or pick up on the updates we give them on cyber security, they don't have the time or money to take a step outside the running of the business to learn and understand these issues. Unfortunately, it's often only after an attack that people wish to speak with us about why something happened, again not understanding that protection is a more involved process. On our part, this is frustrating and poses a problem of how we are able to get people to truly engage with the information we provide before it is too late.

You can't force people to pay attention to this, even when its about an incident that may destroy their whole company. How do we educate people about this?

CW: It is difficult. We do countless presentations to companies to highlight the current trends and problems facing the cyber and business worlds. One example I use is if a company has 140 offices around the world, and their office in Australia gets compromised, if their London office doesn't respond within four minutes it will be offline. Putting that into perspective for smaller businesses, in the South East alone ransomware is on the increase in the last quarter, that's when your data is held hostage and is ransomed back to you, you ultimately make the choice as to whether you want to pay the ransomer lose the data. We recommend you report the attack, as it's estimated that only 30% of businesses actually report cybercrime in the first place. The reason for that is that some people don't realise it is against the law to ransom your information, others don't want to tell the police because then their share prices might dip. If you do pay the ransom for your data, there is only a 50/50 chance that you will receive your information back, and you have now highlighted yourself as someone who is willing to pay in that situation: they are likely to return. If they do return, they are likely to do what is called exposure, meaning that they have a copy of your data and will demand another ransom for them not to publish it. It will never end.

> "Unfortunately, it's often only after an attack do people wish to speak with us about why something happened; protection is a more involved process"

What do we do about this - is this down to tech giants to fix this, is this down to after market software to fix it, or is this down to forcing business to fix this themselves?

SN: There are several answers to that. Some of the things we have already touched on are really important. As we have said, much of this crime is automated, nobody is targeting you, you are simply picked up in an automated spree if you have a weakness. It's only when they are in your system that you become actively targeted, they investigate you, find out what you are able to pay and what would be too much, and then they ransom everything back. That's really important to understand. It's not up to tech companies at all, if we were to say that then it would be the equivalent of saying that it is the government's job to stop you from getting conned in the streets, it's never going to happen. The main thing is awareness training as Mike said. It is software, it is training, it is budget; it is all of these things combined, there is no silver bullet. What Chris was saying about Windows Defender stopping most crimes is really interesting, at the moment we have just over 5000 global businesses that are registered as cyber security businesses, every one of these businesses claims that they are able to stop breaches: who do you trust? In the stand-up tests that MITRE do, Windows Defender doesn't do that well, it will still stop most attempts as Chris says, but it's not fool-proof. This again comes back to user understanding of what is safe and what is not safe.

Is that not the problem though, are we not sold security that is not secure? We lose the ability to trust anybody. Would it be sensible to have a group of people who passively hacked companies systems to show weaknesses in their business?

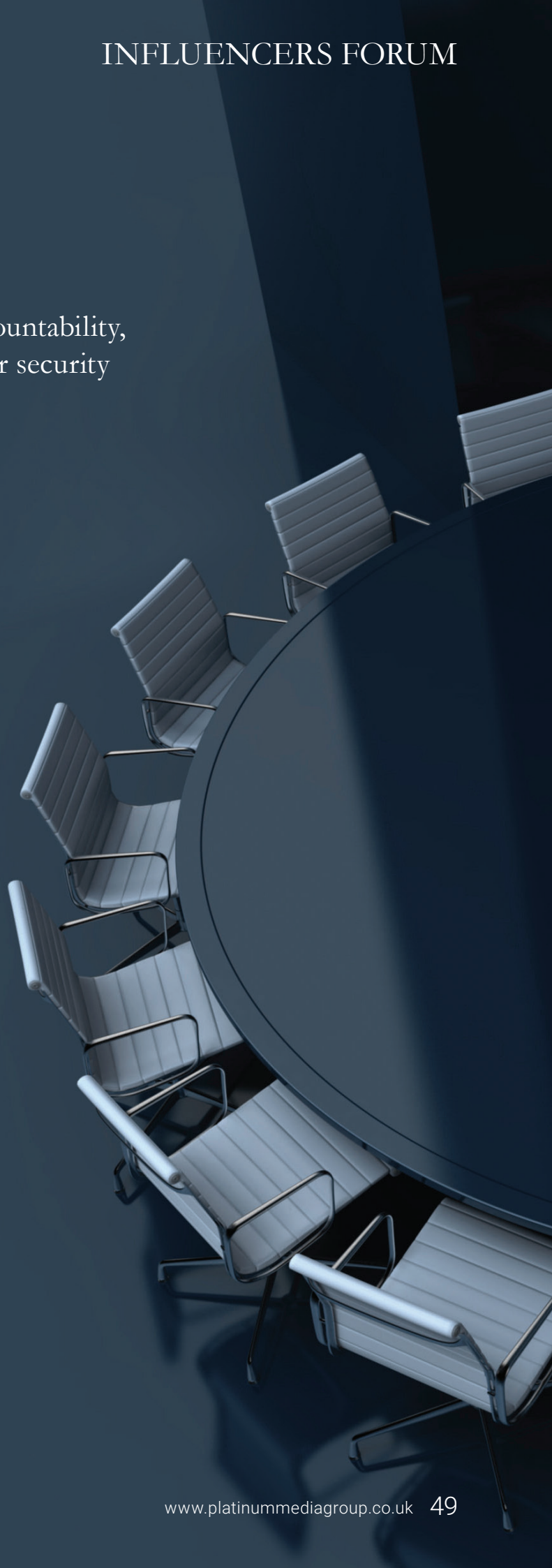
KJ: I think that there are many who do this, but not out of the goodness of their hearts. They will look to eventually be employed or contracted, so it definitely doesn't benefit everybody, especially smaller businesses. There are security researchers who find bugs in what is known as a bug bounty programme. Most large tech and software firms will be using this, this looks for vulnerabilities, reporting them to the vendor, judging the impact of these vulnerabilities, but these are still working to make money from finding these issues. That's slightly known as white hat hacking, black hats are the bad guys. It works to an extent, but in a smaller business, you will need to commission this service.

SN: There is also a problem with what you have said Maarten in that you can't go around breaking into peoples things and then leaving a business card, that's illegal. It would be a very poor choice of the government's if they were suddenly to make that legal, any criminal could just say that they were simply testing if it was secure.

Are we not far from that already though? With a backlog of two years the police can't keep up with this.

SN: Businesses have to protect themselves, they need to take their head out of the sand, no matter your level of business. We often deal with quite large businesses, from 100 - 2000 desks, and the first question we ask is who is in charge of your security management system; we are yet to have anybody be pointed out as being responsible for that area. This is not the case for anything else, finance, physical security, all of these areas have people who are in leading roles, but cyber security is bizarrely seen a different way. You need proper accountability, make someone own that area within your company.

> “You need proper accountability, make someone own cyber security within your company”

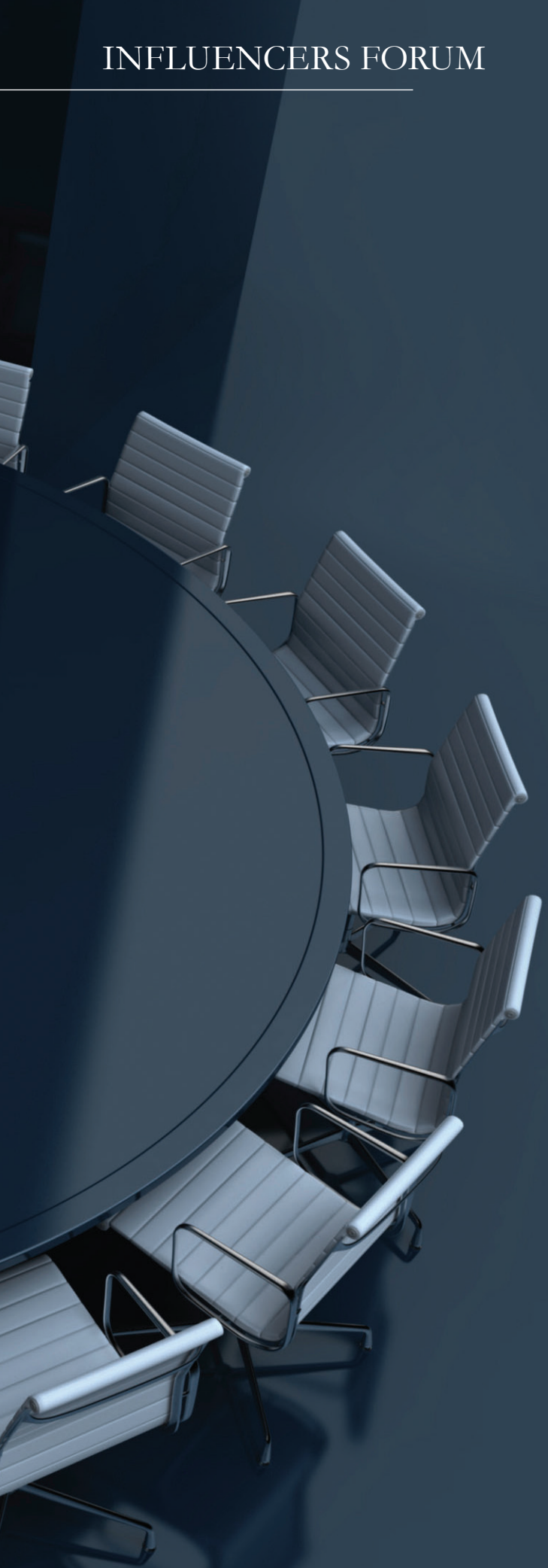


Martin, do you think that white hat hacking will be an answer?

MB: It was mentioned earlier, but Cyber Essentials is an MOT for your security, your system goes through that much like a car, it checks an array of basic points and then when your system drives out the other side you know that it is roadworthy. That, however, doesn't mean that it will remain roadworthy for the next 12 months, but it does mean that you know that it is fit for purpose at that moment in time. Doing that puts the responsibility back onto the company, and that is where it has to go.

MP: I have a view that Cyber Essentials might not be the way to go. I have customers who have gone through it, and I'm confident that if it is done via a third party who has collected the data from the company and then answered the questions, then it's a good start. Often people are producing this MOT internally, and at that point we see people fabricating the truth about their systems just to get the tick at the end.

SN: The concept is right as you say, and if you do it properly it does make sense. ISO 27001 is the stamp that everybody goes for, many of the large companies stamps are of that standard, but none of their processes are. We ask them to evidence the quality of their processes and to show a log of the process from months ago, they simply don't have it, they can't evidence it at all. That means that they have lied to quality auditors and don't have the level of security that they are stamped for. This gold standard of ISO 27001 hasn't been shown to us in any of the companies that have been awarded it. There is no penalty to this if they are found out, and many don't remove the stamp on their site that states they are ISO 27001 standard either.



I suppose the idea about a car MOT is that it's legally mandated, otherwise I doubt that 10% would go and get one done.

SN: That's right, but an MOT also has to be done under a third party, you can't produce your own MOT, as that would defeat the point.

Is there a way to legally mandate these checks though? For some companies or institutions, the risk is enormous, especially if we look at the topic of pension funds etc. which affects a lot of people.

CW: In relation to cyber security, we can self mandate it all. That means that if you are in a supply chain you can say that you are only able to compete for the contract if you are able to prove that you reach a certain standard. When you look at the mandatory controls within business, for example, first aid, most of us have done mandatory first aid training so that if someone in here has a heart attack we can do CPR etc. Another example is fire drills, we have done these from a young age, we know how that works, it's mandatory. When I go into a business and ask them when the last time their business was burnt down the reply is always in the context of years, but when I ask about cyber security attacks to the IT people, the context is in minutes. Today's threat is cyber, but nobody does cyber drills in the same way we do fire drills. We need to limit the damage, it's not a case of if, but when.

> “Todays threat is cyber, but nobody does cyber drills in the same way we do fire drills. We need to limit the damage, it’s not a case of if, but when”

SN: We have done drills with companies that we work with, and thrown many of the threats that we expect to see into those drills. Not only have the results been promising, but the companies have actually quite enjoyed doing them. It doesn’t take long, just a couple of times to cement it in your mind. Also, legal mandate is coming. Every government organisation has to mandate companies that supply goods to them to this standard, ranging from 1 to 5 depending on the level of security that is required. If you want the government as a customer they are going to start mandating your security levels.

MP: I agree with what is being said here. What I should say is that I think it should be removed from the user’s responsibility to accept a patch: why do we need to be consulted before our safety is increased, that should just happen.

CW: I see what you say, but there are systems that need to be consulted before we are updated, specifically with things like laser cutting machines, there’s a risk of loss of life in that area which we don’t want to see. That said, there is certainly a huge amount of areas that can have their systems forcibly rebooted with no real loss.

Is there a potential that AI could be the answer to solve this problem in the long run? Why can’t we have an AI walking through the system, looking for vulnerabilities?

MB: Whilst it might seem like a solution at first glance, the problem will then become what happens when the security AI gets hacked? It would be a great tool for the hackers. There have to be very good checks and measures in place for me to turn and say that the AI system will be the way forward. Hackers will move and attack that AI, giving them even more control and reach.

Is there anything that cannot be hacked?

CW: There was a US casino that claimed it was the safest casino in the world. Not the smartest boast as it's just a challenge to hackers. Within days someone had hacked the temperature regulator in the fish tank at reception that was connected to the internet, gaining access to the casino's information. It just shows how vulnerable we are from almost all angles. To protect from these areas, you need an external hard drive as a backup that is not connected to the internet after your backup is completed, only there is it safe.

SN: When we do an audit, we do asset management, we check that everything is up to date and backed up. However, most of the time we find that many businesses don't have their asset registers up to date or they don't have effective maintenance on all of their registers. We start at the bare minimum before we get into anything else and yet we still find problems there. The basic cyber hygiene is not being taken care of, and if that isn't being taken care of then there is no chance that your system is safe, especially as this is the cheapest stage. We have one client that was spending £7 million a year on AWS (Amazon Web Service) believing that they were protecting their security, yet it specifically stated in the terms and conditions that AWS wasn't responsible: people need to be more careful.

That's good to hear following the announcement that the UK security services, MI5 and MI6, are using AWS to store all our secrets? I presume remote working is confusing the issue even further?

CW: With remote working comes remote desktop protocol, which enables you to log into the office and see everything you would be able to there but from home. 15% of the successful attacks we see are because of incorrectly configured computers that allow anybody to log in. Whilst it is understandable for many smaller businesses to have these problems, it's shocking how many larger businesses have them as well when the resources are out there for them and the risks are as immense as they are. You have to either outsource your cyber security or have an expert in house, there is not one business today that is not reliant on technology and defence from cyber attacks.

Are we not being cheated by tech companies? If I were to buy a car with faulty brakes and crash it would be the car companies liability, but if I buy a computer it's my responsibility? If I then buy a security product, it is still my responsibility it it fails and I get hacked. There is no comeback. Why do we accept this when on everything else we simply hold the manufacturer to account?

KJ: I think that often tech companies are actually doing quite a lot. The invention of the computer and internet was a sudden and meteoric increase in our technological abilities, and one that is available to a huge part of the world. With that comes an equal amount of new adverse problems which arise at the same speed but very slightly behind the initial spike. We need to catch up and be responsible with this newfound ability and power so that we are less susceptible to the negatives of the tech boom.

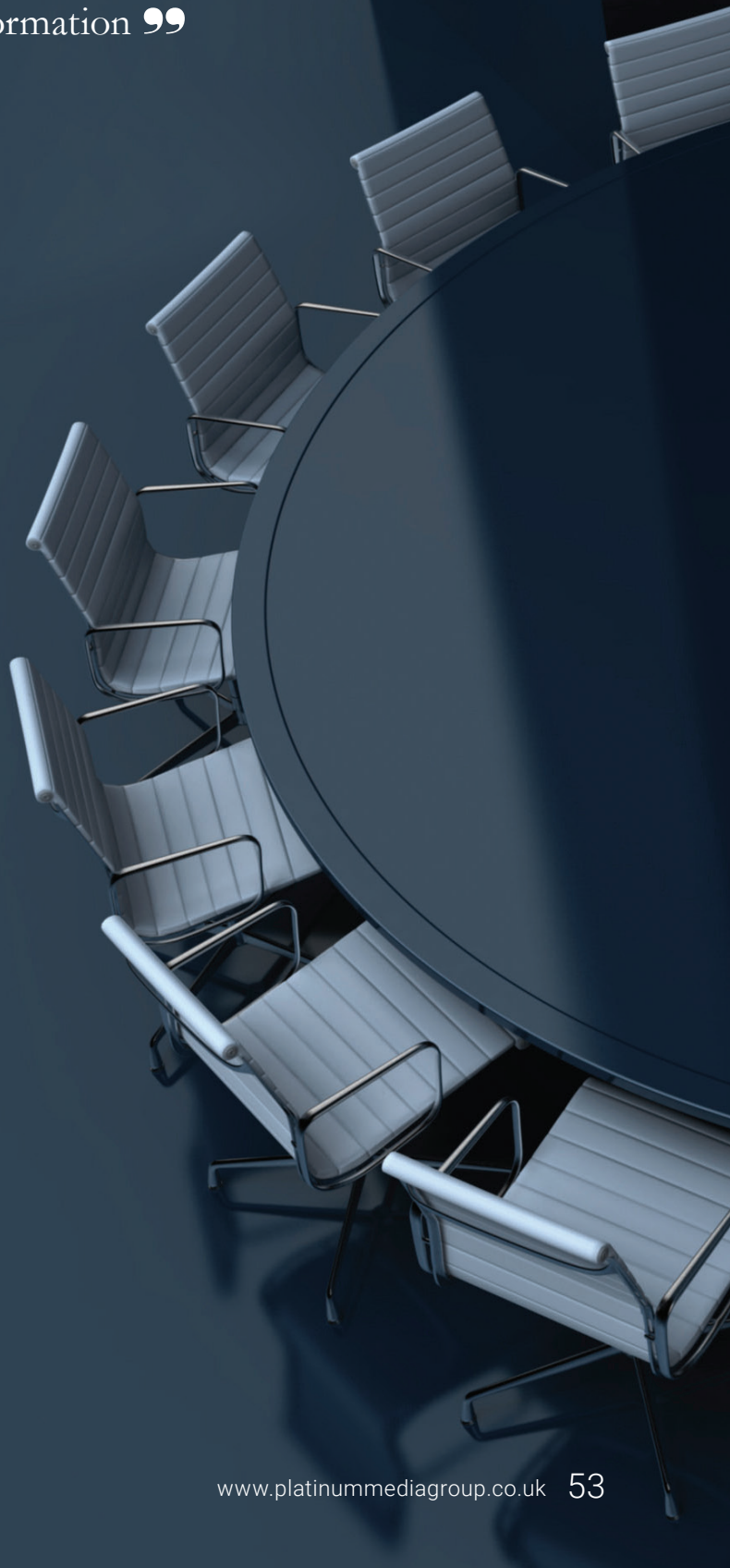
SN: I think you are right to a point, but I think that the initial question is still at large. Microsoft makes a huge amount of money, the past year has been their highest recorded profit margin ever, yet at the same time they have also had the highest number of recorded security bugs: they have the ability to invest to stop this. If Ford is not allowed to put out a car that kills people, but Microsoft is allowed to put out an operating system that gets deployed in hospitals and results in the deaths of people after a security breach, what is the difference? Why are they not held accountable? Deaths from security breaches have happened in the past, this isn't hypothetical.

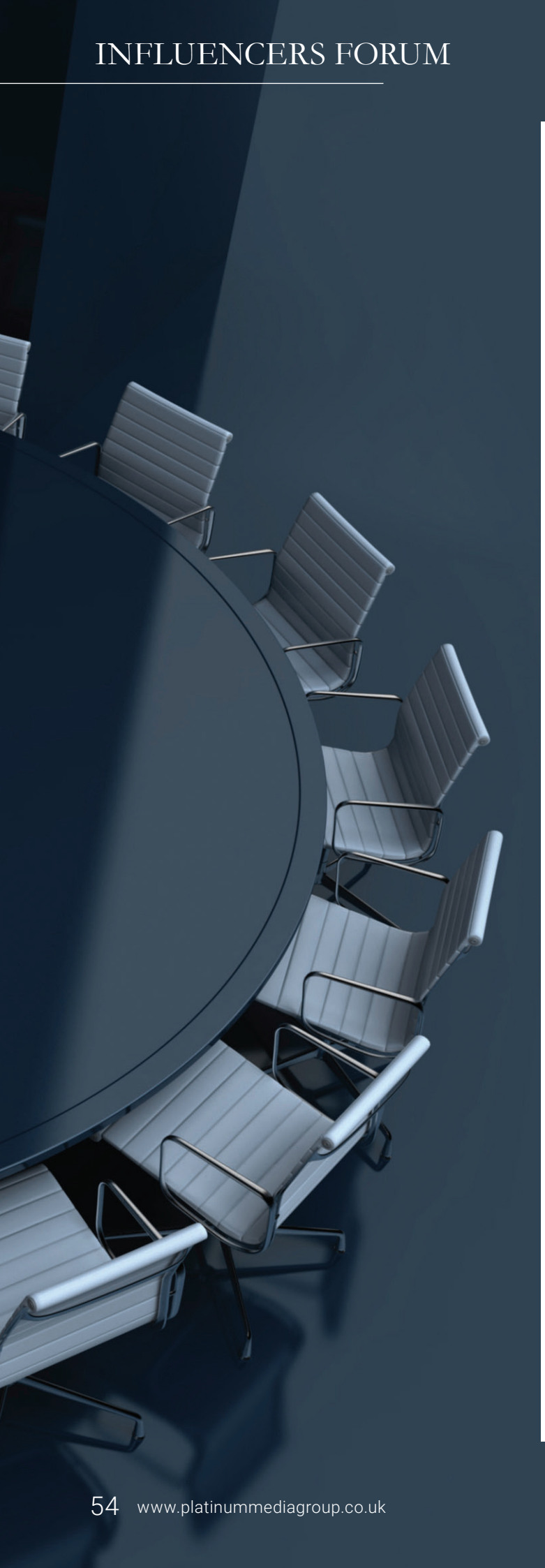
> “A US casino claimed it was the safest casino in the world, within days someone hacked the fish tanks temperature regulator, gaining access to the casino’s information”

MB: I suppose the difference is that Microsoft is innovating very effectively at the front of the market, and in their extensive lines of code there will be inevitable weaknesses but to find them they have to release them to a market. We also push for a new system to come out a lot, there is a large demand for the latest product.

MP: Though I think a big part of the drive is because we aren’t looking at security as the focal point of something new that is coming out, there is still that lack of sensitivity when it comes to our tech security, as if it isn’t an issue. Do we just need a mentality change in the industry that pushes manufacturers to do something different, much like we need a shift in user mentality?

CW: Though there are a lot of things out there that come with the product to begin with, most obvious is two-factor authentication; the problem is that we are in an opt-in opt-out culture, where many people are currently opting out of those security breaks because it’s easier and faster to begin your workday.





The internet of things, is that not going to make this entire issue explode?

MB: Something that we have seen with one of our clients is them using a programme to hack their own system, sending a spoof email to a number of their employees, and the users who click on the email and open the link will be given more training and awareness. I think that is quite a good way to test, but also to educate. This is what we were speaking about earlier with penetration testing.

SN: This is a very serious problem, especially with devices like Alexa. I have a friend that recently installed smart locks in his home, but he also has an Alexa device in the house, meaning that if you were to go up to the post box and shout at it to open the door, you could get in no problem. This kind of security risk obviously also applies to hacking as well: now your whole house can literally be walked into.

CW: Similar to what we were saying earlier, there is a human issue here, people aren't following what is suggested to them. The information commission office suggests that when a new employee enters your business they should adhere to awareness training within a month, and they should do a refresher every year. Sadly, most businesses don't do this. We need to change our culture around this, especially in terms of going to IT and asking if something is safe or potentially dangerous.

SN: Something that we do is send out a 10-minute a week exercise to do which is a little refresher to your understanding of cyber security, if you don't do that refresher then it will notify your management. However, rather than disciplinary action, we advise creating a competition out of it, a leader-board type system, where the top person who has done the most of these refreshers receives a benefit of some kind. There needs to be some kind of recognition for people trying to be cyber safe within the workplace.

MP: Something that we have seen in one of our clients is them using a program to hack their own system, sending a spoof email to a number of their employees, and the users who click on the email and open the link will be given more training and awareness. I think that is quite a good way to test, but also to educate. This is what we were speaking about earlier with penetration testing.

> “I have a friend that recently installed smart locks in his home, but he also has an Alexa device in the house, meaning that if you were to go up to the post box and shout at it to open the door, you could get in no problem”

That must be the answer then, continual penetration testing which can be carried out in house and regularly throughout the year. What does that cost though?

MP: Well that will depend on the number of systems, but for a company that has 50 computers internally, if those were externally facing computers, it would cost you several thousand pounds per month. I have customers that have pen testing at £150 a month, and that's through a third party, twice a week.

SN: Ultimately that is a very difficult question to answer, it's like asking how long is a piece of string, it entirely depends on the situation of your business. Depending on how exposed your business is naturally, and what is happening inside your business, it might be very expensive or relatively cheap, as Mike mentioned. At a base level, we generally say that to cover the costs of your security you should be looking at £20-£40 per person per month if there is no security already in place.

KJ: I'd like to impress that that really isn't a large amount of money, it's simply that it is currently un-budgeted, but so is a security breach and a ransom.

CW: The Home Office recognises that SMEs are the backbone of the UK's finance, and these people have a big impact on our supply chain. Whilst the larger companies can afford and handle cyber security, smaller companies might not be able to, and because of that, there have been cyber resilience centres that are giving small businesses the chance to get access to security. There is support out there.

Who do I know who to trust outside of the usual methods of referrals and reviews?

MB: We have to have certified individuals who have done the training to get accreditation from vendors. There are also areas like ISO, though as we said earlier there may be some problems with that, so ask a few more questions about that. Though at the end of it all, word of mouth is still the best thing to go to.

KJ: Another thing you can do is to look at the write ups of companies who have just gone through a major security alert. If the company that is handling their cyber security is immensely transparent then they would be a good bet to learn from. Also, make sure that the person who was responsible for this didn't get fired, if they did then that's more likely to be a poor culture around security and one you don't want to be working with.

The conversation has been enlightening, but unfortunately we have reached the end of the discussion. Does anybody have any final statements?

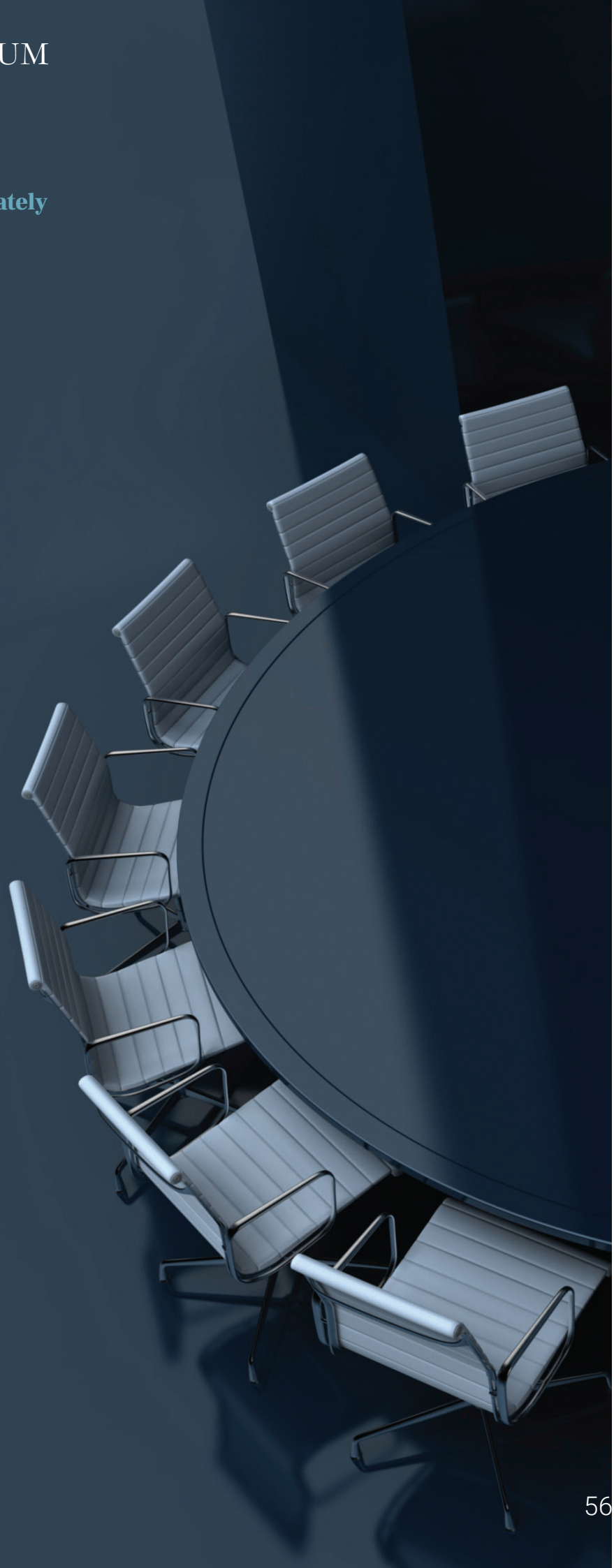
MB: If there is one thing that I would take away after having read this is if you don't have two-factor authentication on your Office 365, stop reading now, put this aside and go and do it.

MP: My take away would probably be that the onus of security needs to shift towards the manufacturers and the vendors. I ultimately believe that there is a huge amount of power that resides in those companies and they could do so much more for our safety.

KJ: I would like everybody to be pretty alarmed by the nature of everybody being a target, and how much that could affect us all. I would say that the biggest 'bang for your buck' would be to look at Cyber Essentials Plus, and if possible, to mandate that where you can when looking at contracts with suppliers and customers. I hope that this will push through and have a ripple effect, if you today go and mandate it, then hopefully someone else will who works with you, and so on.

SN: My take away, if you're slightly larger as a business, would be that you have to have someone at the board level who deals with cybersecurity: make somebody accountable right now. To an extent, that can go to every business, get someone to report on it, why it happened and what you are doing to stop it from happening again.

CW: Mine would be the cyber resilience centres that are across the country, you can access trusted resources and products, we are providing services to SMEs that currently find them unaffordable to access. www.secrc.co.uk



56