Cyber security in the era of quantum computing

Duncan Blaikie	Well welcome everyone to the second in a series of podcasts where we will be delving into the world of Quantum Computing. In this podcast Rob Sumroy speaks to Dr. Ali Kaafarani and Robert Hannagan about cybersecurity in the area of Quantum Computing. Rob is a Partner in our IP and tech group and head of our Technology Data Privacy and Cyber Practices. Dr. Kaafarani is a Research Fellow at Oxfords Mathematical Institute and the Founder and CEO of PQShield a British cybersecurity start up specialising in Quantum Secure Solutions. Robert Hannagan is Chairman of Bluevoyant International a Global Cyber Security Services Company and a Senior Adviser to McKinsey.
Rob Sumroy	Welcome to the second in our quantum series where we explore Quantum Computing and look for answers to the big questions of what Quantum Computers can offer to our organisations, the threats and opportunities they pose and whether there are steps we should be taking now to be prepared for a Quantum Computing future. I am Rob Sumroy, Partner and Head of the Technology Group at Slaughter and May, thank you for joining us. This week I am looking at cyber, the risks that Quantum Computing poses to the security of our organisations and the data and other valuable assets we own. From what I understand Quantum Computers could pose an existential risk to how the now ubiquitous encryption algorithms that we have greater rely on to stay one step ahead of the cyber criminals are threatened by Quantum Computers. I want to understand how this is and whether there's a solution that we should be investing in now to stay quantum secure. I am going to rely on the views and insights of two experts in this area to help us to get to grips with it all but for now just a little bit of background. So cybersecurity is of course not a new concept by any means, our clients are well use to planning for cybersecurity threats as are we as a major global law firm. Organisations across different industries hold lots of sensitive data and information. Not to mention all of the highly confidential and valuable trade secrets and business process information that would be gold dust in the hands of an unscrupulous competitor. This data has eye watering valuations. In 2019, Ernst & Young reported that data held by the NHS has an annual value to the NHS of £10 billion, that's definitely worth protecting. But the data is also a value to the cyber criminals, if stolen and illegally resold on the dark web, the average email address is reportedly worth £84.50 over time. Another report indicates that the average October 2020 dark web price for stolen online banking logins with a minimum of US$2,000 in the account was $65. And it's not just the opportunity cost and reputational damage, regulators are increasing their enforcement activity around cyber. You only need to look at the ICO in the UK with fines for Ticket Master of £1.25 million, British Airways have a £20 million fine and Marriott an £18.4 million fine and you just see the risk of regulatory fines for cyber breaches. The facts of

	each of these may be different but each had at its route a cyberattack. So in the face of all of this risk, companies invest for security and deployment of powerful encryption solutions tends to keep the potential targets one step ahead of the criminals, at least for much of the time. As many will know encryption uses algorithms to scramble data and limit access to that data to those who have the unscrambling decryption key. These algorithms are based on mathematical functions, so they're easy to compute in one direction but hard to invert. Computing the product of two numbers is easy but factoring large prime numbers is difficult, especially when you are into numbers of say three or four hundred digits, you just don't have the methods to efficiently solve that problem and as I understand it with my basic maths understanding, encryption relies on that hardness. So that's why organisations look to implement security technology based on powerful encryption tools. Ok, so why are we talking about cyber today because as I understand it over the past year or so and longer there's been a growing level of concern that this encryption base comfort may be misplaced. All of these security tools can be undone by powerful Quantum Computers and the computer with the necessary quantum power is only a few years away. This threatens a huge change, or if you forgive the pun a quantum leap in the threat and risk that cyber poses to all of our organisations. So I am really pleased to be able to turn to two industry experts on Quantum Computing to help understand more about this and what we can do or should be doing. So Robert Hannagan is Chairman of Bluevoyant International a global cybersecurity services company and Senior Adviser to McKinsey & Co. During Robert's career in the UK Government he was Prime Ministers Security Adviser and Director of GCHQ the UK's largest intelligence and cyber agency. He established The National Cyber Security Centre in 2016. Robert writes regularly for the FT and other publications on cyber and technology and is a senior fellow at Harvard's Belfer Center, so it's great to have Robert with us and Ali El Kaafarani is a Research Fellow at Oxford Mathematical Institute and the Founder and CEO of PQShield a British cybersecurity start-up specialising in Quantum Secure Solutions, a University of Oxford spinout PQShield is pioneering the commercial rollout of a new generation of standards compliant cryptography solutions that are designed to protect organisations from the biggest threats of today and tomorrow. Ali is a former engineer at Hewlett-Packard Labs with over a decade of academic and industrial experience. So thank you to both of you and welcome. I feel that the questions I've posed will hopefully be answered today for all of us. Can I start and maybe Robert I'll turn to you first to ask you what, if anything, is particularly new or concerning about the threat that Quantum Computers pose to data held by our clients?
Robert Hannagan	Well thanks Robert, I mean I thought you summed it up nicely and cryptography and encryption are scary subjects for most people but I think the concepts are really quite straight forward

	actually and it goes back a couple of thousand years and people have been trying to protect their information from the wrong people and make sure it gets only to the right people and up to about a hundred years ago that was all about languages and linguistics and in the last hundred years it's now about maths as things became recognised and this really is the age of mathematics which is why it's great to have Ali here to answer the questions. And essentially what has happened is that in order to protect information you're setting very very tough mathematical problems which are not necessarily insoluble but will take a very very long time to solve unless you have the keys. That's the founding principle of modern cryptography I would say and that's a really important lead into your question because it's all about time in a way. No cryptographer sets out to have encryption that can never ever be cracked in the fullness of the time. It's about making it completely impractical to decrypt it in any useful timescale. So I am sure Ali will talk about RSA and how you measure that difficulty but essentially we talk about, we measure the difficulty in bits, so the length of those prime numbers you were talking about for example and mathematicians love prime numbers for reasons you touched on but in current standards, for example, your Gmail is encrypted to a level which most researchers and I guess Google themselves would say would take sort of 8400 years to decrypt with usual computing power. So if you can suddenly shrink that time limit that becomes a real problem and if you saw the headlines about what Google, for example, were claiming that their breakthrough in Quantum Computing could do, reducing a process that took ten thousand years for a standard computers to two hundred seconds, whether or not you believe that and there's lots of academic debate about that, that's the scale of the problem, you're shrinking that time that is key to the cryptographers art if you like. And maybe that's the point at which it's best to hand over to Ali because I think that is the challenge for me, is how do you get around that?
Dr. Ali El Kaafarani	Yeah, thanks Robert I think that beautifully answered the question, I'm not sure what to add here but, I guess I will go back to how we introduce the history of cryptography and how it started right. So yes it is as old as humans, like trying to hide information and at the very beginning, thousands of years ago until recently, what people used to do is to hide the method that they are using to hide the information, so they were hiding both of them and it wasn't until like 1883 or something around where Kerckhoff's principle, you know happened which says that you shouldn't hide the method you only need to hide the information and if you hide the method then it's breakable at a high level and then of course Claude Shannon the father of information security or information of theory also said that you know you should expect the method to fall into the enemy's hand right, so this is how it started. So now we moved from hiding the method, hiding the information to just hiding the cryptographic key, so now it's time when maths started being used. Now you are using mathematics to scramble the data

	like you said, how you do it, basically you use the mathematical you know method permutations substitutions etc. in symmetrical style to encrypt data and use the same key to decrypt the data. Then comes the next problem, how can you distribute this key? This key distribution problem was only solved in 1970s when RSA became a reality and GCHQ was also working on a similar problem and developed something similar to RSA perhaps before RSA and also one time when Diffie-Hellman which is the main key exchange port of call that be used in you know over of the internet and cyber security nowadays was developed. So that the second problem was how to distribute the cryptographic keys. And this is the exact problem that we will be focusing on today because now you want to, you want to send Robert the key but he can use it to encrypt data to you and you are the only the one who can actually decrypt it. So now from the concept of having one key, we're moving to a concept where we have two keys. One that is a public key that you can, you feel confident safely taking, you know, sending it to Robert over insecure channels and one that you keep for yourself so that you can decrypt. And here's the mathematical function that you mentioned yourself in the introduction which is the one way function, we call the one way function. It is easy to compute how to invert so you apply the one way function on your secret key and you get the result as a public key. You send it over the insecure channels and because you're sure that nobody can invert this function in any reasonable time, then people cannot get your secret key back from the public key. That's the problem that we're solving today. Now you have to define the complexity of these mathematical problems. When you want to say how difficult it is to solve a certain problem you have to define the computing model that you have, which computing model are using, you know, your brain and pen and paper or are using a mechanical machine or a digital machine or a quantum computing because these are different things right. So how can these very mathematical problems that we rely on these days or we've been relying on since 1970s which are namely integer-factorisation which is the factorisation of a big composite number into prime factors and the problem, the discrete logarithm problem these are the main problems that RSA and Diffie-Hellman key exchange rely on. They are very difficult to solve, very time consuming to solve on conventional computers on Turing machine like computers but they happen to be easily solvable on a quantum machine because it's a different computing paradigm, it works differently, it's got this spooky effect throughout how it stores data, it's different how it processes the data, its different from you know super-position to entanglement to quantum interference, this whole concept of quantum computing makes you know solving these problems a lot easier problem for quantum computing. How to solve it we're going to talk about it I guess later on but the other points are yes, they are widely used, RSA and Diffie-Hellman. These are the main algorithms that we rely on every time you know you visit your bank account over the internet, you open web

	browser, you are actually using RSA and/or Diffie-Hellman, every single time you're doing it, every single time you are using you know your bank card, putting it in an ATM machine, you're authenticating yourself, you're using some forms of those cryptographic operations.
Rob Sumroy	So that's really fascinating background both but particularly Ali, it's interesting what you're saying that these two methods or the algorithms which are ubiquitous so every time we're using systems that we trust and in the global banking system is an example of that we're relying on these and yet what we're hearing is that new technology through quantum computing could put those at risk and you know with my sort of legal and regulatory hat on, I know that you know regulations that organisations have to comply with like the privacy regulation, the NIS regulations around infra-structure security all require that organisations put in place technical and organisational measures to protect the data in the systems and if these methods that we are relying on like RSA and others are now vulnerable then actually our organisation is not actually doing enough to implement so that's I think what we need to move on now which is to ask the question, which is you know, what, well I think actually first I'll ask, before we talk about what organisations should be doing let me just ask one other thing for both of you, which is you know we've got clients across all different sectors, is the threat the same across them all or are some people more vulnerable than others would you say? Or you know is this something that applies really regardless of whether you're financial institution, utility company, retail company or the like.
Robert Hannigan	I would say that of course any serious company or organisation is using a form of RSA and using high grade encryption. There are something other things available but I mean as Ali has set out here, this underpins everything we do, all commerce and all business and it is why the public key cryptography break through which as you said first happened in GCHQ, a good shout out for the UK. It's so fundamental it's changed really 2000 years of cryptography because you don't have to kind of get a key to the other person physically. But I would answer your question by saying it depends what data they've got. So assuming everybody's got a high level of encryption and RSA has got better over the years so it's not that its static, we've improved it, we've made it tougher. But it really matters what kind of data you've got so some data is ephemeral and frankly doesn't really much matter if somebody can read it next year or the year after. Some data is not ephemeral at all and it will really matter if somebody can read it, in 5, 10 years' time. So one of the reasons why governments are so concerned about this is that if you intercept data at the moment it's going to be unreadable very often, it's going to be a line of dots and ones, ones and zeros but you can store it away until quantum arrives and then decrypt it, so in that sense this is a current problem and I guess the answer to your question is, if you're a business you need to think through the data you hold, as you should be

	anyway for cyber security or GDPR or all the other things you've mentioned including NIS directive. Think through with this and with encryption in mind or decryption in mind, and think well what is the data that we would really worry about if it is taken now and decrypted in who knows, 3, 4 or 5 years' time, that's the worry and for governments especially there's a lot of that data but also aspects of financial services, health care for example, anything to do with safety, you know there are plenty of sectors where they would not want data from now to be decrypted in 5 years' time.
Rob Sumroy	So that underlines as you're saying Robert, the point that this is a here and now thing, even though we hear that quantum computers or the powerful computers we need to I suppose decrypt are not going to be available yet, the point is it's a current threat because the data will still be valuable in the future.
Robert Hannigan	Exactly. Exactly. So probably worrying about how to use a quantum machine in your business is some way off and in practice you'll be contracting that out anyway. Most businesses will never have a quantum computer themselves but they will use the service from one of the big providers but that's something you can worry about you know in the medium to the long-term. The encryption problems for the reasons Ali set, you have to worry about now really.
Rob Sumroy	So should we look at then what companies can be doing, I mean both from a sort of a practical perspective in terms of services that are out there, tools that are out there. I know Ali, you know that's what PQ Shield are working on and Robert you advise on. So you know, practical suggestions as to what we should be doing at the moment.
Dr Ali El Kaafarani	So I took the view with Robert, he touched on very important points and I think that the problem that is now defined for all known as harvest now decrypt later. It is a well-known problem now right so this is one of the huge impacts of quantum computing on our, kind of, public key and cyber security infrastructure. So the quantum attack works retrospectively in the sense that yes we don't have access to a quantum computer now but we have access to encrypted data. Anyone can intercept any connection and download any encrypted data and if someone is really interested in your data for any reason whether you're a government, whether you're a healthcare provider whether you are you are a OEM who holds lots of IPs and who wants to protects their IPs. A lot of angles that can be looked at people will be interested in downloading and storing your intricate data and decrypting them once they have access to a quantum computer. So that's one angle and the other angle, because they are relevant to who should care now and the other angle is that you know life time of your products. It's often the case that cryptography is embedded and hotwired inside your product and or deployed in fields or in a space where you cannot actually go and update the hardware so it's actually hardware crypto, then you should

	think from now and if you're taking you know security by design then you should actually take into consideration the upcoming standards and develop your products that can be, can actually use and perform and compute the upcoming standards. So these are the two angles that you want look at where you know in terms of hardware and in terms of confidentiality problem and the problem you said that who should, you know, which companies or which corporates, which categories of companies should, are more vulnerable and the answer will be the problem is a lot of those companies don't know where they're using their cryptography and why. They take it for granted because things happen, you go to your ATM and you just put your card there and you get money or you pay or etc. but you don't know when you're using crypto. Inside big corporates, all corporates, it's a lot bigger the problem because they have lots of legacy crypto that they need to replace. So the first thing that we advise as a company specialised in post quantum crypto and you know involved in the new standards that are being written by NIST within the US government is to have this cryptography inventory to understand what crypto you have and why you're using them. What are the regulations that you are complying with?
Robert Hannagan	Yes I think that is a great point and Ali's too modest to mentioned that he's involved in some of these standard developments for the US and UK so and that will have a huge impact because quite soon governments and big corporations will be choosing the standards they want to follow and in practice everybody is going to follow particularly NIST in the US. And regulators will follow that. So at the moment we are encouraging everyone to improve the standards of their crypto in new devices as Ali says, to build in security by design, that's a new buzz phrase in cybersecurity for governments and to regulate that and we're seeing more and more regulation in nearly every major jurisdiction. But minimum standards of security and crypto and there's the slight danger that we completely missed the boat here and that we end up with a good move towards better regulation of minimum standards but we adopt the wrong standards. So it's almost inevitable that regulators will start to insist on Quantum safe encryption standards because, particularly for anybody any sector that is serving governments, I think that would be critical and that's most sectors frankly for the US and the UK and even I think people like the information and commissioner's office for GDPR will start to say you should be using this standard and you should be using it now and not in five or ten years' time, so that's I think a key point that is difficult because as Ali says people don't always know what crypto they've already got and trying to get you head round that is difficult and all I'd say is you need to do both, you kind of need to think about now cybersecurity you need to do all the minimum things we've been telling people to do for years and not everybody is doing but you also need somebody in the organisation to be thinking about the five, ten year timescale.

Rob Sumroy	Thanks Robert I'm glad you mentioned and introduced the concept of the new regulation and the regulators because, you know from my perspective scanning the horizons for what we're seeing from governments, for example, you know the UK data strategy which is you know out for consultation mentions the importance of having secure infrastructure for data and similar messages coming out or the EU but there is no specific reference in any of that to Quantum and so it's interesting to hear what you're saying and I think good news that the governments and the regulators will follow the science and the technology, so the standards will be improved and the regulation will be developed from those standards. I know Ali that you've got some involvement with the World Economic Forum and obviously their sense of the cybersecurity published a report at the end of last year which looked at the issues arising from Quantum technology in this area and identified a number of major challenges. I think as solutions clearly, you know the publication of principles and standards to promote better use of Quantum but also to get better standards around Quantum security I think was one of the key areas there. I don't know if you can give us an insight Ali on some of the work in that area which might lead to regulation in the future?
Dr. Ali El Kaafarani	Absolutely, yes and I will actually give you a little bit of an update on what's happening within NIST when it comes to standardisation process. So this started in 2016, following an announcement from NSA where they said Quantum risk is a real risk and we need to mitigate against this risk and NIST shall follow with a standardisation process of what we call post-Quantum cryptography. I think basically, rely on different mathematical problems because this is going to be also a question related to how can we use Quantum Computing in a constructive way, and the answer would be like, Quantum Computer does not do magic and cannot solve every, you know difficult problem it can solve some problems a lot faster than conventional computers but not every single problem that we have today. So what we do with the new standard is that we rely on different mathematics, that is not easy to solve on Quantum Computers, that is just as difficult to solve on a conventional and on a Quantum Computer and that's why it's called, that's the field in cryptography that is called post-Quantum cryptography and this is being standardised by NIST. It started in 2016 we are now in the final phase it was announced back in August 2020. Yes they were still working during Covid, NIST, and so they have done an amazing job and now we're like a year away from announcing the result. So a year from now, now we've been talking about RSA and Diffie-Hellman and elliptic-curve cryptography. In a year from now there will be new acronyms that we would have to get used to. There might be NTRU or Falcon or dilithium or Kyber, there will be new acronyms and the thing is with post-Quantum cryptography there are five different mathematical fields so we're moving to a slight, I wouldn't say slight it is a more difficult field in cryptography because its more diverse, relies on different mathematical problems namely five different

	mathematical problems and they are not as trivial as discrete logarithm problem and integer-factorisation. So we are moving to a more engineering challenging problems and security problems that we're tackling there. And now you think about it so there will be standards that would rely on different mathematics and not only you need to know what crypto you're using and why then there will be new standards and you will need to understand so which algorithm should I use for this use case or for that use case and so that's the problem and these other things that were mentioned in the report. The point that we touched on that I wanted to say and its very relevant to Robert is that governments, maybe the governments in some sections are not aware of this but the likes of NCSE and BSI and NSA are very well aware of the quantum threat and post quantum and Robert can tell as more about this.
Robert Hannagan	Well absolutely and I think governments are not always the first off the block in technology but in this case they are for the obvious reason that you raised earlier Rob which is criticality, so if you're encrypting nuclear submarines on a nuclear firing chain it really really matters if this can be decrypted in any reasonable time and space. And there is a whole other range of government sensitive data that including health data that people don't want to be available in five years' time. I think the interesting follow on from Ali's point is that the supply chain is also going to be at risk, so it's all very well for the maker of a nuclear submarine which itself has a massive supply chain, say "well I'm going to change my crypto to the new standard" but actually what about the whole ecosystem around it? So this does effect pretty much everybody because they either have data they really really care about and don't want to fall into the bracket we talked about earlier as being available or they're part of the supply chain which does and governments are going to have to become increasingly careful and frankly paranoid about what crypto they allow into their network.
Rob Sumroy	Fantastic. Well, I'm really sad to say that we're running out of time. I would definitely carry on this conversation for a lot longer but I think I probably just need to pause us there and say thank you very much for your time. We've probably got chance for each of you if you've got a sort of a final thought in this area for thirty seconds or so, I don't know if you want to, you know certainly a message to leave with people listening about Quantum. We've heard obviously that it's a present threat not one in the future and that governments are working with the mathematicians by the sound of it to find the right solution but Ali, Robert any sort of last thoughts before we have to finish?
Dr. Ali El Kaafarani	I would just say don't leave it to the last minute. It's really important to get ready for the new standards now because it's happening now.
Robert Hannagan	Yeah I agree and clever maths, even clever maths is the answer to this and there is an answer which is the good news, so we have a kind of vaccine here and it's a good time to get

	consultancy on it for somebody in the organisation to start thinking about the practical implications.
Rob Sumroy	Brilliant, well thank you both and I know we had planned if we had time to talk about some of the more positive use cases that maybe Quantum Computing will be put to within organisations although I'm happy to say that's the theme of our third podcast which we're going to be recording shortly. So just to both of you to Robert Hannagan and to Dr. Ali El Kaafarani thank you so much for your time, it's been great and hopefully we'll get together again in months to come to develop these thoughts further. Thank you to those who've been listening and joining us. If you would like to hear more on the subject of Quantum and other technology and digital topics in our horizon scanning series, please do visit the Slaughter and May website at slaughterandmay.com/insights but from all of us for now, thank you very much and goodbye.
Duncan Blaikie	So tune into our next podcast where we will be speaking to Alexei Kondratyev from Standard Chartered Bank about some of the vast opportunities presented by Quantum Computing.