Introduction to Cyber Security – Full Transcript

Our panelists were:

- Dr. Nicholas Ryder, Professor in Financial Crime, UWE Bristol, UK
- Ruslan Yusufov, Director of Special Projects, Group IB, Russia

Introductory Remarks

MODERATOR: Welcome to Taxlinked's latest webinar. Today we're looking at a pretty trendy issue. We're looking at cyber security and some of its main threats and we're going to provide you with some tips on how to best mitigate cyber attacks. We have a great set of panelists for us, both from academia and from the industry itself. So we should have a good combination of information provided to all of you today.

Just before we get started with the questions, we have about nine questions to cover, let me get some admin issues out of the way. This webinar is being recorded. We're going to have an audio recording available shortly after the webinar is over. We'll also have a full transcript that we will share with everyone via social media and via our community. We'll also share it with the panelists for them to distribute accordingly. If you have any questions as you listen to our panelists speak, make sure you submit them using the Go to Webinar control panel. Just submit them and I will try to work them into discussion since I'll be moderating.

Also, there's a handout offered by Ruslan and Group-IB. It is on private intelligence data and it has some of the services they provide. So make sure if you're listening in to download that. I have also added it onto the Taxlinked community's resource library, so it's available to all those of you there too. I'll make sure when the transcript is out, we will also attach it to the transcript, and the blog post, and so forth.

So without further ado I'm going to ask each one of our panelists to introduce themselves and then we'll just run straight into the question-and-answer portion of this session. Nick, how about getting us started with a short introduction.

NICHOLAS RYDER: Good morning, everybody. My name is Professor Nicholas Ryder. I'm a professor in Financial Crime from the University West of England in Bristol and my expertise is financial crime.

MODERATOR: Excellent. Ruslan.

RUSLAN YUSUFOV: Hello, ladies and gentlemen. It's my pleasure to be here and thank you very much for taking me onboard. My name is Ruslan Yusufov. I'm a director for Special Projects at Group-IB, a global cyber security company. We do invest in cyber threat response and we provide threat intelligence solutions.

MODERATOR: Excellent. Thank you very much, gentlemen. So let's get started with the questions. As I said we have about nine questions here. We'll try to work by each one, step by step, and I'll incorporate questions from our audience members as they come. So, let's start off with a kind of more theoretical, more I guess, philosophical question, just to get the discussion

started. Should hacking be forbidden in the absolute sense? This comes, I guess, in light of the Panama Papers, Paradise Papers in which, you know, a lot of crime has been revealed through the work of hackers. So Professor Ryder, how about getting us started there. What is your opinion on this philosophical issue?

Question 1: Should hacking be forbidden in the absolute sense?

NICHOLAS RYDER: Good question. I could probably write a paper on this. Should it be forbidden? I think it's one of those questions that really has no right or wrong answer. I think there are benefits to hacking and also weaknesses.

In terms of it being forbidden, as we've seen in the last 4 to 5 years with the growth of online banking, mobile banking, the growth of social media platforms like Twitter, Facebook, Instagram, and so on. In terms of it being forbidden, if you look at some of the attacks on some of the world's largest financial institutions like for example the USBC, NatWest, instances in America were ATM machines are being overtaken by organized criminal gangs. In that sense, it should be clearly prohibited. Obviously, it's a big if with cybersecurity, as Ruslan will know probably a little bit more than I will. It has to be prohibited and prosecuted.

Conversely, of course, you can have, well, what response do we have to hacking, for instance. There'll be new countermeasures and should nation states be involved in deliberately attempting to target the hackers. Well, that then begs the question, is that hacking illegal? Is it ethical? There are a whole raft of legal issues regarding jurisdictions. So hypothetically, let's say that a hacker in country A attempts to hack into Barclays or HSBC in London and the bank goes after the individuals, or law enforcement does, not question whether it has jurisdiction rights. So that would be dependent on links with the European Union, Europol, links with other nation states. You might find that some nations might not be cooperative with the investigation.

On the flipside, you then have, I suppose, the ethical benefits of hacking with the Paradise Papers, the Panama Papers, clearly exposing a very controversial, some would argue unethical, illegal link between tax evasion and obviously tax avoidance. Now, under UK law, tax avoidance is not illegal, but tax evasion is illegal. Where do you draw the line? So, you can argue that indirectly, maybe, that if a country has a rather flexible tax and legal framework and enforcement procedure, does that actually indirectly encourage tax avoidance?

So, I think that both sides of the argument have some very favorable points, so I don't think there is a definitive answer, I'm afraid, for that one.

MODERATOR: Right. Exactly. Ruslan, what is your take on this question, coming from the industry that is looking to prevent this?

RUSLAN YUSUFOV: Yeah. I'm not in the position to speak of all issues related to hacking. Well, we can think about hacking as a tool to achieve other goals. For example, theft of money. So theft of money is definitely a crime and it is prohibited nowadays. Illegal access to data is also a crime, so it is prohibited. Hacking per se, well, it could be used for good or bad. For example, penetration testers, they use the same schemes and they use the same instruments to

understand the vulnerabilities of an organization or a business, for example, to understand whether the threats are there and they help to fix those vulnerabilities.

But if we started speaking about hacking, I would like to stress that recently, the world has dramatically changed. We have now everything in the digital world. Probably, there is no more offline world anymore. Just imagine for a second we don't have Internet. How will we communicate? How will businesses work? Whether it is possible to survive in the world without Internet?

So just imagine a Wild West 150 years ago. There were different crimes like robbing a train and many people rode trains because they were delivering financial goods like money, and diamonds, and gold bars, whatever. You can barely hear about a train robbery nowadays because the world has changed. And the same happens with the banks, nobody steals banks from banks in a physical sense anymore. I mean they do, but it is becoming less and less. It occurs less often, but if you, for example, think about the organized crime involved in bank robberies that steal from the storages of banks that are already digital. We can think about, let's say, Cobalt organized group which Europol says have stolen over 1 billion US dollars robbing banks globally. So, of course, organized crime moved to the Internet and that should be forbidden and that is forbidden and it is prosecuted.

But hacking, I wouldn't think that anything related to technology should be forbidden. Technologies are not good or bad, they are neutral. The people of knowledge that utilize them to commit crimes, that is what we should fight against.

MODERATOR: Perfect. So, that gets us off on a good foot here with the discussion. We'll jump now into the more, I guess, look at some definitions and look at some of the ways in which, I guess, cyber security has changed for financial service providers and what not. So, just to provide a general understanding of cyber threats. Could you provide a definition for us, Nick, want to get us started there?

Question 2: What is a cyber threat or attack?

NICHOLAS RYDER: Yes, I suppose in terms of what a cyber threat is. I suppose again with any legal definition, it's open to loose interpretation case law. So, I think it is any attempt at illegality, criminality that seeks to circumvent security mechanisms of an electronic or a computer nature.

So, for example, one of the things we see in the UK with the Fraud Act of 2006 is now fraud can be committed by a computer. There is recognition within the UK legal framework from a financial crime perspective that there is an increase in threat posed by cyber threat or cybercrime. You have a broad range of European initiatives in terms of cybercrime prevention.

The UK has an extensive array of legislation that tries to protect the people's use of the Internet. But I suppose the intriguing thing, I think, as the point that Ruslan mentioned in his answer to your first question. If you just look at the evolution of banking and how people now communicate, it's via Skype or via WhatsApp or text or even conduct financial transactions. I

mean, now there was a study by the Office of National Statistics in 2017 and they said that 90 percent of UK households now has Internet access and, of course, 70 percent of those people have purchased goods via laptop, iPads or their phone. So I think in terms of security or cyber threats, you also have to look at your handheld device as well.

So, I think it is certainly broader than looking at attacking a computer structure that's there for a company to prevent information being stolen, the data. So, I think to me, it's a very broad definition that can mean just a broad range of activities.

MODERATOR: Excellent. Ruslan, anything you can add to that?

RUSLAN YUSUFOV: I totally agree with that. Basically, we can think about not computer crimes that are committed on the Internet like drug trade or different fraud schemes that just involve communications like Skype as a means of communication. But at the end of the day, it's just another fraud that you can find, you know, walking somewhere down the street and there is a guy coming to and trying to scam you. The same guy is sitting in front of the computer trying to scam you…those all are cyber threats.

But talking about typology, I would probably give the following: theft of money could be one possible type of fraud or a type of cyberattack. Another one is a whole combination of crimes related to illegal access to data and possibly illegal data. And the whole variety of different frauds and scams probably could be the third one. And I would say the fourth one would be a combination of our so-called denial of service attacks that the purpose of which would be just turning off some computer system or twerk or it has many purposes. For example, usually a DDoS attack is accompanying the thefts from bank because the cyber security guys they are switching in, you know, fighting against DDoS attacks. But there is a backdoor somewhere and the money is being stolen at the same time.

I think the biggest issue here is the word cyber. So we utilize cyber, the computer networks to commit those crimes. So, it can be a broad definition, can be a narrow definition, but they all involve networks.

MODERATOR: Excellent. Thank you, Ruslan and Nick. Okay. And who are the main threat actors and what do they do? I know we've touched upon some of this a little bit, but who would be the main threat actors? Ruslan, how about getting us started with that one.

Question 3: Who are the main threat actors and what do they do?

RUSLAN YUSUFOV: Well, it's very easy. We usually read about different types of hackers in the newspapers, but it is very important to understand that, I would say 90, maybe 94 percent of all cyber threat actors are financially motivated criminals. Those are people who want to steal money and who want to, for example, steal information and then sell it for money.

Of course there are other experts like state-sponsored groups, there are cyber terrorists, there are cyber activists and some others have different motivations. And it's very important as not only they have different motivation, they have different targets.

For example, cyber terrorists, well, they're just normal terrorists which want to do as much damage as possible, but they use new methods and they use new instruments and they hire hackers to commit the attack, their target would be like, probably, a plant and a disaster on this plant would be achieving their goals.

For cyber activists, using a cybercrime to achieve their, let's say, geopolitical or probably to bring attention to some issue would be their goal, that's why they commit the crime. But most of the people—and those people would be starting from just the guy trying to rob $10 from a credit card of some stranger and the other end of this line there would be this crime which is transnational. Those people are motivated by financial gains.

MODERATOR: Excellent, Ruslan. Nick, anything to add to Ruslan's answer?

NICHOLAS RYDER: Yeah, I think I support what you just mentioned. In terms of what my research concentrates on and obviously looks at the terrorist financing perspective and money laundering. But, I think, yeah, it's organized from the gangs in relation to malware, identity theft and how that identity will be sold on.

We've seen Barclays most recently and they're very concerned about what's called sharing on Facebook where parents would put up images of their children in a family picture at some sort of event and then how identity thieves can use that in the future. The biggest concern for me in relation to terrorists is the apparent ease at which they were able to launch their propaganda via a broad range of social media platforms, Facebook, Twitter, and other forms as well. But also now it's beginning to use these platforms as a funding stream.

We've done some research in Bristol where we are currently investigating whether or not any payments made via social media platform fall within the 2017 money laundering regulations. Well, that question hasn't appeared to be answered yet…But also you can argue that anybody with access to a laptop, a mobile phone, cellphone can fund terrorism. I think gone are the days of, you know, depositing large sums of cash or even money mules taking money from country A to country B to support Al Qaeda.

And I think, as Ruslan has mentioned, you've also got the state sponsors and I think that probably is the biggest threat. And I have no doubt that many nation states have been hacked. We might see that with banks, with the National Health Services in the UK. And also, I have no doubt, the countries have then retaliated in turn.

Of course it would be intriguing to see what is the ultimate goal of a cyberterrorist. Is it, for example, to steal money from a bank or your or my identity, or is it maybe to attack the infrastructure within a nation state? So, what happens if the Internet goes down? Are people then going to be prepared to pay for goods and services via a card or via a mobile phone? I think that would be the biggest threat posed by cyber terrorist if that actually happens.

MODERATOR: Moving to the next question now to kind of take a look at where cyber security stands these days. So, you know, I mean, what shifts have there been in cyber security currently

happening these days? Ruslan, you want to get us started with that one since you're in the industry?

Question 4: What shifts have there been in cyber security these days?

RUSLAN YUSUFOV: Yeah. Well, I would be happy to discuss, for example, how banks and how businesses started utilizing threat actions to prevent and to predict crimes and we know such cases when banks use some prediction models to understand what's happening. But frankly speaking, well, you know, what we saw last year was the WannaCry and the Petya virus epidemics.

People and businesses are negligent and still they don't understand that those threats are related to them. They think it is not of their concern. So, we had the Panama Papers, we had the Paradise Papers, we had huge thefts from banks. There was an attempt to steal one billion dollars from the Central Bank of Bangladesh, Sony Pictures was hacked, LinkedIn, Yahoo, every big guy out there was probably hacked and some information leaked. There was Equifax, every second a U.S. citizen has a Social Security number out there in the Internet nowadays.

And probably with, you know, observing this, you should be totally paranoid because it looks like, well, if the big guys are hacked and for some of them the businesses are over, probably when they come to me and to my smaller business or not that secure business, I will be totally destroyed. But, probably you know, it's changed so fast that or maybe businessmen have other issues to solve.

Unfortunately, well, this topic of cybersecurity doesn't have as much attention as it should be. Nowadays, well, I read a recent PWC paper, they said that banking and capital markets are at risk. Cyber threats are number one risk for banking and capital markets. It is in second or third place for all corporate risks out there. So, it's not a geek issue, it's not the IT issue anymore. It's the biggest risk for business. But when we see this WannaCry attack, it is very easy from the technical point of view and it's infected like 200,000 computer networks globally and such big companies like FedEx or Mayersk, and many others. They become victims, then they will announce, let's say 300 million US dollars damage to their business.

So, from the company being really deep into developing technologies to protect services to prevent and so on, I see a lot is happening. AI is coming, different tools to understand who the hackers are. How to catch them and, from the technological perspective, a lot is going on. But from the business sides and from the society part, I think still we generally think it's not our concern and it will not be our issue.

You know, there is a story, one enthusiast connected a toaster to the Internet and during the first 12 hours this toaster was attacked 300 times and the first attack came after 40 minutes this toaster was online. If you're on the Internet, if your device is connected to the Internet, you are at once becoming a potential victim because you are on the Internet and they scan everything they can. So, I think that's what we need to change, not in cyber security. But in understanding that cyber security is our number one priority in the broad sense as a society, as a country, as a business, as an individual and so on.

MODERATOR: Excellent. Thank you, Ruslan. Nick, anything to add on what shifts you've seen?

NICHOLAS RYDER: I would wholeheartedly support what Ruslan just said and I can't really paint a pretty picture. I'm afraid it is the number one threat to, I think, companies, financial institutions, individuals. I mean, you know, we're all online. Most of us on social media profiles. Most of us might use various devices like Alexa to play music or to order things. The more and more things that we have connected to the Internet, the bigger threat it's going to be.

So I think from a personal security perspective, personal data, this is the biggest threat. But of course it's another example of the organized criminal gang, the terrorist evolving quicker than maybe how the legislation can catch up with that. And I think it's an example of, you know, from a financial crime perspective, it's always going to be 20 steps ahead and the laws are always going to be reactionary as our system is put in place to prevent them. So, I think the key thing for your listeners obviously is to be aware of current trends.

I still get at least three e-mails a week that I've won the Yahoo lottery or somebody wants to give me 80 billion dollars, which is a lovely thought. But still the old scams, even the Nigerian 419 scam, I get those emails frequently. Of course, I delete them, but even if you look at the e-mails, the old e-mails that you might get, they're still very sophisticated that, you know, from HMRC, from my bank and of course I would delete them, but most people who might be new to the Internet and what we tend to find is that criminals will target the older generation, might be a little bit more susceptible perhaps. "Oh, I have an email from my bank, I will reply, I will send them my personal details…" So, I think yeah. So, this is the number one threat to nation state security, it is the cyber threat.

MODERATOR: Excellent. Thank you, Nick. Now, let's move on to a different section of the webinar. We still have about half an hour left. Let's look more at the kind of practical aspects, how a business or a financial service provider can actually prevent cyber attacks or what they should be doing to enhance their cyber security, let's say. So, the first question in that area is can we predict cyber crime rather than simply respond to it. Ruslan?

Question 5: Can we predict cyber crime rather than simply respond to it?

RUSLAN YUSUFOV: Yes, definitely we can, and that's what threat intelligence is for. For example, our threat intelligence system is intended to predict and to prevent crimes, part of which is human intelligence, and we see it in many different marketplaces and forums and we read what hackers write. And we see how their malicious software evolves and we understand how they are interconnected with each other. And some attacks we can predict before they happen because, for example, somebody is trying to understand how SWIFT works. And they sit and they discuss it together so we can think that probably that would be an attack on SWIFT and that's what actually happened.

Then, let's say before WannaCry happened, there was a leak and it was publicly a leak of malicious software. It was publicly announced and everybody could come on WikiLeaks and

open the Vault 7 archive and download it. So WannaCry epidemics happened two months after there was a leak. So, you can just, less cybercrimes will happen because, first of all, there is some vulnerability or there are some threat experts that are trying to commit this crime and then it happens. So, if you catch them at that very stage, you can predict and prevent.

And also the artificial intelligence comes in place. Machine learning helps to predict because print connections, they have connections on social media, they have those connections with their Darknet avatars and probably there are some technologies that are already connecting the cryptocurrency wallets to specific people.

So if you trace cryptocurrency wallets and that crypto money is somehow related to drug trade, to committing cybercrimes, you can probably build a formula to understand who the people are and what they are planning to do. But I think AI is the goal of our next years. Today it's about building networks and understanding how the malware, the infrastructure, the threat actors, how they are interconnected, and what their plans are.

MODERATOR: Excellent. So, I mean, kind of as a follow up. I'll tag this question to the previous one and Nick can give us his opinion. What does the future look like for AI in the cyber security sector, Nick?

Question 6: What does the future look like for AI in the cyber security sector?

NICHOLAS RYDER: I think as Ruslan says it's a natural progression. I'm not specific expert on AI, but from what I've read various reports that have been published by think tanks and professional bodies, it is going to be, you know, the next stage in terms of attempting to prevent or predict when the next cyberattack might come.

But of course the opposite side is: when will AI be used to attack a network? I think it's welcomed the developments from a law enforcement and a prevention perspective. But again you always have the flipside, will it be used against the network?

MODERATOR: Ruslan, on the future of AI. I just want to get your thoughts a bit more.

RUSLAN YUSUFOV: Well, yeah. Unfortunately, the hackers, they also know what machine learning is. They also will use AI and, what's more important nowadays, they have stolen that much amount of money. They can invest in R&D, they can invest in lawyers, they can invest in accountants, they can invest in services for themselves, so those are not geeks sitting, you know, building AI with their home machine in their garage. They are organized criminals. It is organized business and they can invest, in some cases, they can invest more than antivirus companies can invest.

NICHOLAS RYDER: Can I just pick at one of Ruslan really interesting points there, if you don't mind, I think that you're suggesting that criminals are using the corporate model, which I wholeheartedly agree with and, of course, that's how terrorists now appear to be operating as well. So, if you look at the funding models that were used by the IRA before the peace accord in

the UK, they were essentially run like a company, so they would have accountants, they would have research and development officers, which is similar to how ISIS were financed.

So, there is a common theme I think between all these criminal gangs and how terrorists operate. And obviously with the demise of ISIS and the geographic area that they controlled in the Middle East. We're now seeing that there's a second wave of ISIS, but also the Boko Haram and Al Shabaab. So they will form that corporate structure which does make it—and obviously to prevent that is extremely difficult and so that might be a useful comparison for some of your listeners.

MODERATOR: So now basically we'll look at financial service providers and we'll provide them with tips as to how they could mitigate the risk of hacking. So just to start us off, Ruslan, how can an organization mitigate the risk of hacking? What should they be doing? I mean, do you have some tips, you have a step-by-step plan? You will have, you know, some suggestions, that'd be great I think, for our listeners and our members of course.

Question 7: How can an organization mitigate the risk of hacking? What should they be doing?

RUSLAN YUSUFOV: You know, if you look at 1998 recommendations about how to mitigate cybercrimes, probably the first one would be change your password to a long and strong one. Well, today I would say it's the number two step because the first step would be changing your attitude. So any organization today needs to understand that's the real threat. If the attitude and the mindset changes, then changing your passwords, because otherwise it wouldn't work at all. You'll have those policies full of instructions and the security officers will be the ones who are pushing and the rest of the team will be, you know, no, no, no, that doesn't help.

But as soon as the whole company understands that that's the case, probably something will change. And in order for every single person in the company to understand that it is actually related to them. I would recommend doing cyber security trainings because most of the attacks, even those first targeted attacks on banks in 80 percent, they start from a phishing e-mail.

So each and every individual, each and every employee in the company should understand what a phishing email is, what they should do step by step after they click the phishing link. How they should open or not open any attachments to the email and so on and so forth. So, after that, from the technical perspective, I would recommend running a security audit probably in the form of penetration testing or some source code audit.

So, your goal is to understand what is the current stage, where you are. Are you vulnerable or not? After that you will fetch and fix those issues and only after that we can start talking about rebuilding the infrastructure because we need to understand how the infrastructure looks like. If its current state is relevant to what we have now on the dark side, right? And then you can rebuild the infrastructure, then you can install some specific APT solutions or intrusion detection systems or intrusion prevention systems. Or you can even connect yourself to some outsourced providers that will be 24/7 monitoring your activity. You can dig into threat intelligence solutions, but the first step would be understanding.

It is of your concern then training employees and then doing a penetration test to understand where you are currently. I would say that is required for 9 of 10 companies nowadays that has never treated cyber security as the issue for them. Although the GDPR would force these issues.

MODERATOR: Excellent. Nick, anything to add to Ruslan's tips, suggestions, et cetera?

NICHOLAS RYDER: Yeah, I think I'd endorse it is about common sense. Obviously, from a legal perspective, compliance is important under UK legislation, you know, all authorised entities for the Financial Conduct Authority must have in place a system to prevent its being abused by financial crime, which obviously would include cyber crime. We have seen several examples of where, you know, well-documented UK financial institutions that are hacked or a data breach and they've been fined by the City Regulator. But you know, banks are spending probably in excess of a billion pounds a year on cyber security. So, I think they're not taking this lightly, you know, the authorities, government employees and former military intelligence officers in some attempt to boost their cyber security systems.We've also been appointing geopolitical analysts to monitor global security threats.

But I think it is about common sense and it's about making consumers aware and I think as Ruslan said, it's about training every member of staff. You know, if you do get an email that contains the Love Bug virus for example, then don't open it. I mean that was 2015, 50 million people were hacked by it. So, it's about common sense and not automatically clicking open an email, though that might be important, but just look at who the e-mail is from.

The Bank of England did a resilience test on the UK banks a couple of years ago, they found that there were no immediate shortcomings. I would suggest probably that those figures would now be significantly in doubt. Obviously we've seen with TSB recently and their online mobile applications. With between 10 to 15 million people using a banking app in the UK every day, you can see how that can cause an open door to a savvy cybercriminal who can hack in your account.

MODERATOR: Excellent. Thank you. So, as a follow up question I guess now looking more at how an organization can structure itself or how a business, I mean, can basically have some sort of organizational structure that will actually help it maintain a proper cybersecurity program? How do you go about organizing yourself to do this, Ruslan? Are we going to need like a cyber security officer eventually or something along those lines?

Question 8: How can an organization structure itself or how can a business basically have some sort of organizational structure that will actually help it maintain a proper cybersecurity program?

RUSLAN YUSUFOV: I think it's a topic that probably requires a few hours' discussion and a flipchart to draw. Well, today every organization needs this cybersecurity function. It could be the guy, it could be the division. But this is not the IT guys, so cybersecurity and IT, they are different guys. I think that's the most important for us to understand nowadays because usually the owner or the CEO, they say, "Okay. You are the IT, so give us the functions. Give us the

opportunities and give us more to use the digital technologies." But, on the other hand, you should secure them.

But philosophically, the more you open, the more vulnerabilities you have, so those guys they're usually balancing, you know, between the opportunities and cutting them in order to become secure. So, you definitely need the other guy who will be balancing these kind of issues.

Well, it is a big topic whom this guy should report to. One opinion that this guy should report to the board itself not the CEO, but I think it's arguable, there can be different organizational structures according to the needs of different organizations. Definitely you need this guy or this function inside your company.

MODERATOR: Excellent. Thank you. Nick, any opinions on that?

NICHOLAS RYDER: I think, yeah. I think both the IT chap and the cyber security definitely need to be a different person. I think, to me, that there probably is a call to maybe mirror the money laundering reporting system that we have. Which of course is one of the major tools used against money laundering and terrorist financing and other forms of white collar crime so there's a compliance system in place. So you have a team, whether you have a cybersecurity team, a compliance officer that has obligations and those obligations then extend all the way up to the CEO or CFO of the company.

I think what would be a possible weakness in the financial services sector is that when the financial crime reports goes across the CEO's desk, it's how much attention do you pay to it. And of course, if it's a cyber crime threat maybe they've picked something, a possible attempted hack, they're not quite sure. How much attention and priority does the company give to that potential threat.

So I think that it is important, obviously, for consumers to be aware of products, but also people working within the sector to be aware, as Ruslan said, this probably is the biggest threat. National security, our personal data and companies. So I think that maybe there's an argument here for a compliance system to come in place and if that compliance system isn't adhered to or followed, then, you know, people are fined, companies are fined, people are prosecuted, which in theory should happen to the money laundering regime but of course in the UK that doesn't happen in relation to prosecution.

MODERATOR: Excellent. Are there major institutions who have been looking into cyber security compliance? Are there any cases at the local level?

Question 9: Are there major institutions who have been looking into cyber security compliance? Or at a local level?

NICHOLAS RYDER: I mean, I know that if you looked at, for example, virtual currencies, Bitcoin and so on. I know that the US anti-money laundering legislation now incorporates virtual currencies. So if there is a suspicious transaction under US law that has to be filed by the deposit-taking institutions of the American FIU but also I believe is the case coming in Australia

soon. The UK doesn't appear to be ready yet, so it's obviously, a gradual step, but I'm not aware if there any system or specifically of cybersecurity reporting systems in place.

MODERATOR: Okay. Perfect. So, since Nick brought up crypto currencies, and Bitcoin, and so forth. I have a question here was actually this question was submitted by Ruslan for you, Nick. So, I'll let you tackle it first. So, according to the recent Europol analysis, criminals in Europe have laundered at least 5.5 billion dollars of illegal cash through crypto currency. What do you think about money laundering with regards to the crypto industry and the trans boundary movement of capital? What are the main challenges in this sector? That's all yours.

Question 10: According to the recent Europol analysis, criminals in Europe have laundered at least 5.5 billion dollars of illegal cash through crypto currency. What do you think about money laundering with regards to the crypto industry and the trans boundary movement of capital? What are the main challenges in this sector?

NICHOLAS RYDER: I think that the use of crypto currencies is a natural evolution in money laundering. I think what we are seeing is—one of my colleagues actually at UWE is doing his PHD on the regulation of crypto currencies and he's hoping to finish early next year. And from my understanding of crypto currencies, of course, it is the anonymity which causes a particular significant threat, that's one point.

I think the second point is that because the current UK AML regime doesn't appear to impose any reporting obligations on the use of the crypto currency, through Bitcoin or other forms of currency, I think that's a major concern. And what we're seeing is an extension of the terrorist financing model, especially with ISIS where they may appear to be using Bitcoin, to mine Bitcoin, and obviously to gain access to finances.

And what we've seen in America now is a number of prosecutions and convictions of people who have been convicted of assisting a known terrorist group to actually mine Bitcoin, so in 2015 or 2016, a 17-year-old student in America was found guilty of providing material support to ISIS and sentenced to 17 years imprisonment for advising them on Twitter how to mine Bitcoin.

I think before Christmas last year a person in New York was also charged with attempting to support a terrorist group by the mining of Bitcoin. So, I think it does cause a significant threat. I think you mentioned 5 billion Euros or 5.5 billion, I believe, of cash. I'd probably argue it's more than that because every attempt to quantify the amount of money laundered globally by economists, accountants, lawyers are all inaccurate because there is no precise figure for the amount of money laundered anywhere in the world. The Financial Action Task Force says it could be up to 2.5 percent of global GDP, in excess of trillions of dollars.

So, I think what we are seeing is the evolution of money laundering from money mules from cash-in-hand into the virtual world, if you like, and this is going to become an ever increasing problem. And we published a paper earlier this year on the funding streams of ISIS and one of the things that we're now looking at from our research is the threat posed, for example, by social media payments or social media platforms so that, again in itself, is another legal loophole that I

think needs to be carefully looked at by the international community, regional bodies, and also nation states as well.

MODERATOR: Okay. We've covered all of our questions. We set a good pace and we covered a lot of information. So, we'll wrap up the webinar a bit early. But, basically, do you have any concluding remarks, any last suggestions, last tips, any points you want to reaffirm for our listeners. Nick, you want to get started with some concluding comments.

Concluding Remarks

NICHOLAS RYDER: I think that cybercrime is such a broad term to define and legally speaking, you know, you could have webinars on that and maybe one for the next few months.

I don't think you can paint an optimistic picture. I think with relation to cybercrime and I think it is essential not just for corporations and banks, but also for individuals to become more savvy, to become more educated about the threat posed by cyber crime from hacking, from stealing money, from cyber terrorism, and so on. But I think it's probably more important for our nation state governments to realize the threat posed by cybercrime and to redouble their efforts and that could be more funding possibly, more training, but also I think more to make people aware of the threat posed by opening an e-mail, by maybe replying to a text, by maybe conducting transactions online.

And I think that the cybercriminal will always be one step ahead from a preventative policy that we've had in relation to other forms of financial crime.

MODERATOR: Excellent. Thank you, Nick. Ruslan, any final remarks as the industry's side, I guess?

RUSLAN YUSUFOV: Yeah, as we're now presenting for a community of lawyers, accountants, trustees, tax specialists, usually those are people who possess sensitive information. And as the Panama Papers, for example, told us, a breach could be the end of the business and it could be a trigger to transform the whole industry as we now see the current regulation changes...I just want to stress, well, you're absolutely right about the individuals and that each of us should be more technical savvy and we should start with our kids probably and we should train them as well.

For example, last year we started the special short master class and we're teaching people from 9 years old what the Internet is. Well, usually they speak about such severe cyber threats as stealing skins from Counter Strike Go and Minecraft, and that's the issue for them and then they try to understand how to…because it is of matter for them and these are some assets for them. So, I think the individuals that are listening now today, they should just spend an hour to secure themselves.

What they can do? They should change passwords right now. Today you should change your passwords because if you don't change your password regularly then there is a leak. For example, just recently there was a leak from 2,100 like cafes or bakery stores, I don't remember

specifically. There was a retail chain in the US and 2,100 retail stores, every data related to the customers is leaked, like log in, and password, and credit card, and billing address, and so forth.

So if you don't change your password and, moreover, if you use the same password at every service you use like Gmail and Facebook and so on, somewhere there will be a leak and this password will be automatically scanned across different services. So, not only you should have a strong and long password, you should change it regularly and also you should have different passwords on different services. So, that's what probably you should do, just take a piece of paper and write down all your services that you have. If you have Gmail make sure you change your password. Make sure you turn authentification on. You can use either SMS, you can use Google Authenticator, then write the second one. Okay. Here is a Facebook account to which Gmail account connects or whatever, and then you build the whole scheme of your assets. And you try to understand if you turn on the very basic security, I think that's the first step.

MODERATOR: Excellent. So, I'll get some admin issues out of the way and then we'll finalize the webinar. So, for all of you listening in, this webinar was recorded. We'll have an audio recording available to everyone shortly. We'll also have a full transcript of this event that will take us a few weeks to get out, but we will make sure to share it on the blog and social media and share it with our panelists.

There's also a handout that Ruslan kindly provided for us on private intelligence data with some of the services that Group IB offers and make sure to download that. Those of you who are members, it is on our resource library so you can find it there. I will also post it on the blog when the transcript is out, so it will be readily available for whoever is interested and wants to get in touch with Ruslan.

So, with that said, I want to thank Nick and Ruslan for this great discussion. I think we've learned a lot, we've got some good tips on how to go about securing our cyber world. So thank you very much, Nick. Thank you, Ruslan. And hope you guys have a great weekend.