FT BOARD DIRECTOR

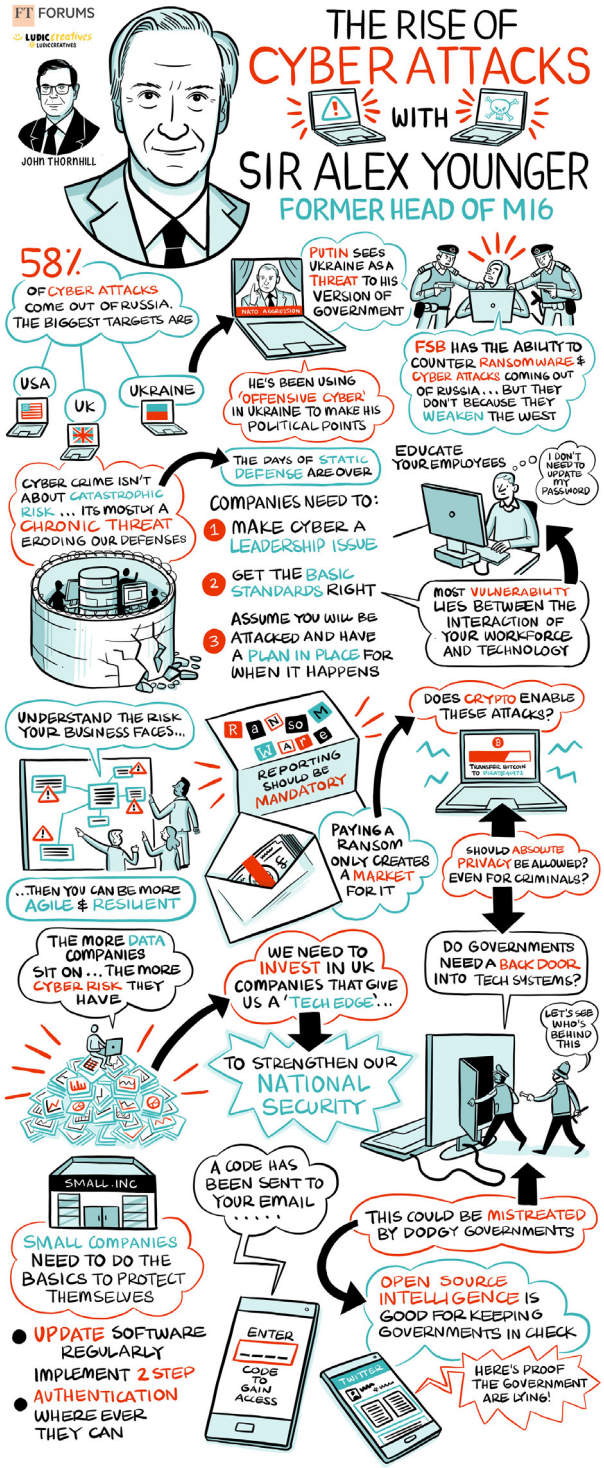
EVENT SUMMARY

THE RISE OF CYBER ATTACKS

23 FEBRUARY

SPEAKERS

John Thornhill, innovation editor, Financial Times
Sir Alex Younger, founding partner, Vega Cyber Associates



In this FT Board Director event, John Thornhill, the innovation editor of the Financial Times, talked with Sir Alex Younger, a former chief (or "C") of the British secret intelligence service, better known as MI6, and a founding partner of Vega Cyber Associates, a consultancy that focuses on digital resilience. Here are the highlights.

Here, below, are some selected highlights.

HOW THE CONFLICT IN UKRAINE MAY UNFOLD: THE PREDICTION OF A FORMER SPY

Speaking after Vladimir Putin, the Russian president, had recognised the breakaway republics in the east of Ukraine and a day before Russia invaded its neighbour, Sir Alex Younger said Putin's actions could have been predicted: "You don't need access to secrets to know that he's been very, very clear, including an essay he wrote last year, about his conviction that Ukrainian independence represents an aberration and, indeed, a threat to Russia."

Offering what John Thornhill called "a chilling analysis", Younger said that the recognition given to the republics was only the start of something bigger. "This has got all the makings of an escalatory environment," he said. "If you asked me to rank the probabilities, I'd say the most likely thing is that this is merely a preliminary move, and I'm afraid it's not the end of the story.

"I've always thought that he would break the taboo – and the taboo is the forcible change of borders in eastern Europe." He warned that "we should be under no illusion: he's gone through the looking glass and this is a different type of world that we are entering."

Asked about what Putin's endgame was likely to be, Younger said: "I think one of the things we don't do enough is listen to him. I think he's been pretty clear. It seems to me that in the short term the endgame is to rob Ukraine of an independent foreign policy … so the Finlandisation of Ukraine. And if he achieved that, then things would calm down pretty quickly – but not permanently because I'm sure his long-term aim is to unwind the eastward expansion of Nato."

WHAT NATO AND THE WEST SHOULD DO NEXT

"I think the imperative for the west is to try to defend the norm – defend the taboo against the movement of borders," Younger said. He added: "It is incredibly important that we attach a cost to this transgression or it will happen again." Asked about the likely effect of sanctions, he said they were an important tool although he had "limited expectation that they will change [Putin's] behaviour in the short term".

WHY THERE WON'T BE A CYBER EQUIVALENT OF PEARL HARBOR

The US entered the Second World War after Japan attacked the US fleet in Pearl Harbor in 1941. Thornhill wondered whether the world faced "a cyber Pearl Harbor". Younger does not think so. Nor does he think cyber is "the new nuclear" – another comparison sometimes made. He said that what he called "the catastrophisation" of cyber security was "not particularly helpful". "There are distinct features of offensive cyber conflict that don't make the comparison a ready one: it's cheaper, there are many more actors, and you can to some extent obscure attribution. So, it's not symmetrical," he said.

To sum up, a cyber attack will not necessarily prompt an escalation of conventional warfare. In fact, he said, the best response to a cyber attack might not be another cyber attack (or something worse) but rather the use of sanctions or the law.

RUSSIA: THE GLOBAL CAPITAL OF THE RANSOMWARE AGE

Younger said that companies faced serious damage from "the chronic problem that is cyber. We are having our IP removed, our strategic advantage eroded and we're being threatened by criminals through ransomware".

Much of the problem is rooted in Russia. Thornhill pointed to a report by Microsoft which suggested "that Russia is by far and away the biggest national state actor when it comes to cyber attacks, accounting for 58 per cent of the attacks. The three biggest targets are the US, Ukraine and the UK".

Asked for his opinion on this, Younger agreed that “the vast majority of ransomware operations are based in the former Soviet Union, and principally in Russia”. He explained that this “is not to say that the Russian state is behind them but it is to say that it suits them rather well”.

A FORMER SPY’S TOP TIPS FOR COMPANIES FIGHTING HOSTILE STATE ACTORS AND CYBER CRIMINALS

Younger said companies should “think carefully” about where they are positioned in what he called “the system of systems”. “You need the imagination and the intelligence to work out what your risk is – what you look like to any potential adversary,” he said.

Business leaders should ask themselves a series of questions:

- are you likely to be on Russia’s list of critical national infrastructure?
- are you likely to be a hostile state actor’s intelligence target?
- are you likely to face a greater threat of ransomware?
- could you be an accidental victim?

He said companies should attend to the basics of security. “One of my key messages is that the days of static defence are really over – even if basic standards still matter,” said Younger. The basics include regular software updates and two-factor authentication.

WHY CYBER SECURITY IS A LEADERSHIP ISSUE

Younger said that “the most vulnerable link in the chain” was not so much technology as people, and specifically leaders. He said some leaders thought they were “too posh for security”. In other words, they seem to think that it is a problem best addressed by their minions. But Younger warned that “there’s nothing a cyber adversary likes more than a leader who thinks that cyber isn’t their problem”.

So, what should leaders do? Younger said: “If I were in their position, the first thing I would do is to ostentatiously demonstrate my engagement with this issue. Your people need to know that you care and are willing to learn.”

THE CASE FOR MANDATORY REPORTING OF RANSOMWARE ATTACKS, AND THE PAYING OF RANSOMS

Younger said companies often stayed silent when they paid a ransom to cyber criminals because there is “still a stigma around getting attacked”. But he said mandatory reporting should become “a thing” so that law enforcement agencies could develop an effective response to criminals.

On the subject of legislation to ban the payment of ransoms, he was less concrete in his views. By way of background, he said that, at MI6, he was director of counterterrorism for 10 years. He “saw at first hand the terrible human dilemmas and costs” that the ban on payments to terrorists imposed. He eventually came round to the view that “it was the right policy because if you don’t have that you create a market and the problem gets worse”.

He did, however, acknowledge that the situation is “different in the ransomware space”, and observed that “we need to think harder about how we stop this market existing”.

QUESTIONS FROM THE AUDIENCE

How would you categorise cyber attacks in terms of business risks? How much of a priority should this be?

Younger said: “We’re manifestly underinvested in cyber risk.” Originally, the problem was loss of intellectual property – especially to China. Now, he said “ransomware represents the most pernicious and difficult close-in problem that firms face”. He warned that “it’s going to happen to just about everybody until a strategic solution is found”.

Do you have any advice on how you would test the efficiency of cyber security firms that offered solutions?

Younger said: “There is a lot of snake oil out there and I’m not just telling people to go out and buy more shiny technology.” He said: “If someone offers you 100 per cent resilience or security … that’s not going to be true.”

Which businesses have developed a successful cyber security plan? How did they do it?

Younger didn’t name any companies but he did say that “the ones that spring to mind are those that have been hit and have grown up as a result of that”. Also, he said there was “a correlation with the amount of money that a firm has to spend”.

Is this a bigger problem for small and medium-sized enterprises? Do you have any advice for them?

Younger agreed that cyber security was a big challenge for SMEs. His advice is: “If you do the basics, you will be harder to hit than 80 per cent of companies.”

Do you think we need a heavier hand to manage the internet?

Younger said: “It would be a total disaster if we fell into that trap.” He acknowledged that there are “huge problems associated with anonymity and encryption and all the sort of anarchy of the dark side of the web”. A more authoritarian approach would be unwelcome however. “That is not a country I want to live in,” he said. “God forbid that it’s up to the government to say what is true or not. That would be ridiculous.”