APPG ON CYBER SECURITY MEETING

Topic - HOW THE BANKS PROTECT US AGAINST CYBER THREATS

24TH June 2019 Portcullis House

Present:

Chairman: James Morris MP

Secretariat: Andrew Henderson, Prof Keith Mayes, ISG, Royal Holloway

Apologies:

Admiral Lord West

Lord Arbuthnot

Baroness Finlay

Baroness Neville-Jones

Gerald Howarth MP

Richard Benyon MP

Speakers: Ray Irving, FS-ISAC

Sharon Barber, Lloyds Bank

Gary W, NCSC

1) Introduction: James Morris MP, APPG Chairman:

Role is to educate and to highlight cyber security issues to be raised with the Govt.

2) Speakers

i) Ray Irving, FS-ISAC

At a time when trust has become a vital asset for business, trade and commerce, the Financial Services Information Sharing and Analysis Center (FS-ISAC) is dedicated to reducing cyber-risk in the global financial system.

Serving financial institutions around the globe and in turn their customers, the organization leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate and respond to cyberthreats.

Think of FS-ISAC as a 'virtual neighborhood watch' where financial institutions help keep an eye out for each other.

FS-ISAC operates on 3 fundamental pillars:

Intelligence – FS-ISAC shares among its members and trusted sources critical cyber-intelligence that builds awareness through a robust offering of alerts, indicators, member insights, threat assessments and analysis.

Resilience – FS-ISAC leads multiple efforts to strengthen the financial system and aid in business restoration. This includes exercises, best practices, hands-on training and playbooks for rapid response.

Trust – Through summits, meetings, webinars and communities of interest, FS-ISAC convenes a global peer-to-peer network of experts and practitioners from the private and public sectors to share critical information and best practices in a trusting and collaborative environment. FS-ISAC has created and continues to build a strong community designed to secure and protect the financial services sector and the billions of people who rely on a stable, functioning system.

FS-ISAC was created in response to a US Presidential Directive in 1998. The consortium was founded with a mission: to help assure the resilience and continuity of the global financial services sector.

FS-ISAC is a non-profit organization funded by membership fees and sponsorship from the security vendor community.

In 2017, FS-ISAC expanded its geographical footprint by setting up regional hubs in London and, with support from the Monetary Authority of Singapore, in Singapore. We also have staff in Toronto, Tokyo, Melbourne and Central Europe.

Threat Environment

The current cyber threat environment continues to be very dynamic. Malicious cyber actors vary in terms of motivations and capabilities, from nation-states through cyber criminals, to political hacktivists. Tactics include:

1. Spear-phishing campaigns that can result in the theft of online credentials
2. Ransomware attacks in which malware is downloaded that restricts access to infected computers,
3. Distributed denial of service (DDoS) attacks which can impede access to services for extended periods of time,
4. Business email compromise which involves the compromise of legitimate business email accounts in order to initiate unauthorized fund transfers.
5. Destructive malware attacks that impact integrity and availability of data.
6. Supply chain threats on third parties.
7. Insider threats.

Core Activities of FS-ISAC

1. Public Private Partnerships

As already mentioned, FS-ISAC shares members intelligence amongst their peers. This is supplemented by co-operation with public-private partnerships. This includes facilitating information sharing from government partners to the FS-ISAC community and assisting members in engaging with government and law enforcement when required. To preserve it's trust model FS-ISAC never shares intelligence with government and law enforcement without the permission of the originating member.

In the UK FS-ISAC analysts are embedded with the NCSC, helping represent the sector and collaborating with the British Government. In the United States FS-ISAC staff sit in the National Cybersecurity and Communications Integration Center (NCCIC) where they can work with the FBI, The Secret Service and other government organisations and ISACs. Similar arrangements are planned for elsewhere and FS-ISAC has close relations with Interpol and Europol.

2. Incident Response

With offices in London, Singapore and Washington the lights are always on in an FS-ISAC office somewhere. In the event of an incident FS-ISAC can respond quickly by forming closed groups of members who are facing that incident - issuing alerts to the sector and running emergency calls with all the experts required to appraise members of the threat. For example after the Wannacry ransomware outbreak 3000 members joined the FS-ISAC emergency briefing call on this topic.

More proactively we host regular threat information sharing conference calls for members and invite subject matter expert guests to discuss the latest threats. We organize and coordinate numerous conferences, member meetings and round tables that allow face-to-face exchange between members.

3. Cyber Exercises, Trainings, and Best Practices

Exercises are a proactive step to practice plans, find and close gaps, better protect systems and mature information sharing communities. Regularly practicing plans for cyber attacks is a necessity. FS-ISAC began conducting exercises in 2010 with what is today known as the Cyber-Attack Against Payments Systems (CAPS) exercises – tabletop exercises written together with members with over 2000 participants every year. We have since added what are know as "ranged-based exercises" for technical, hands-on-keyboard practice where security practitioners defend a real network from attackers. In the US FS-ISAC runs the Hamilton Series exercises which simulate a variety of plausible cybersecurity incidents or attacks on the financial sector. In the UK FS-ISAC staff sit on the Bank of England Sector Exercising Group and participate in planning the SIMEX exercises.

Conclusion

Financial institutions recognize that customers trust them to protect their investments. The sector has historically led the way in making substantial investments in security infrastructure and expertise. FS-ISAC is responding directly by expanding our capabilities to share information, conduct deeper analysis, provide exercises and cyber ranges, build stronger partnerships within the financial sector, with other sectors, with government agencies and with global partners.

ii) <u>Sharon Barber, Lloyds Bank:</u>

A quick bit of background on Lloyds Banking Group; we are the largest UK retail financial services provider with around 26 million customers. The Group's main business activities are retail and commercial banking, general insurance and long-term savings, provided under well recognised brands including Lloyds Bank, Halifax, Bank of Scotland and Scottish Widows.

The customer transactions we complete are c.£15 trillion of payments processed in 2018 (7 x UK GDP), £64 billion SME & Mid Markets lending portfolio, and c.£290 billion mortgage portfolio, so pretty significant to the UK community.

As Ray has stated, the Finance Sector is now the top target of cyber criminals; 2018 saw more cyber-enabled heists from Financial Institutions than ever before. The sector is targeted by the best in the world: hostile states, organised crime groups, as well as hacktivists, and also insiders.

This means that our focus on Security and Resilience also needs to continue to increase. The protection of customer data is paramount to the UK economic stability as well as retaining customer trust ourselves

We have a strategy that aligns to the UK Government cyber strategy – and we think of ours in 4 parts –

- Operational Excellence – getting the basics right, do the hygiene well like patching, automate as much as possible so we are not reliant on manual activity

- Business and People – to educate our colleagues and businesses so they understand their cyber risks, ensure they are prepared and ready to take action – so this is where documenting playbooks and scenario testing is important
- Customer is our third quadrant – how do we help our customers better understand security and how they can help themselves in their everyday life – we keep their online journeys secure of course but we have also provided an online secure zone for customer awareness, we provide branch brochures and we do many presentations to Businesses (small, medium and large) to help them understand the cyber risk
- Our last quadrant is Disruptive Security – this is where we recognise we can't do this alone. The threat is fast-paced, and both the Government and ourselves need to find new ways to adapt more quickly.

We recognise we need to change and innovation is critical to this:

- We have sponsored LORCA – London Cyber Innovation Centre – to help guide and support UK Innovation – which helps UK jobs and the economy, as well as create a more secure digital cyberspace
- We also work with a number of Israeli start-ups as they are exceptional in Cyber
- We are championing a number of women in cyber initiatives
- and we are also working with Auticon – a small company that only employ people with Autism as they have skills we really need in the industry

The second part is Collaboration and intelligence – it is critical that we get this right across the industry, our peers and law enforcement.

Sharing intelligence on cyber-threats is well established in the Finance Sector. It is viewed as a non-competitive issue: By sharing intelligence and information about cyber threats, we can help to protect our businesses and communities from criminals and other adversaries. Collaboration makes the whole sector more secure.

To help facilitate this collaboration, we are a leading member of a number of international intelligence sharing forums like FS-ISAC, we sit on the Board of FS-ISAC and we chair various technical UK working groups.

These forums hold regular touch points, ranging from daily cyber threat calls which enable members to share tactical intelligence about emerging threats and incidents, to quarterly meetings that are more focussed on the threat landscape and strategic intelligence sharing.

A lot of the intelligence we share is technical in nature and is used by recipients to adjust existing defences or create new ones. We also have regular discussions about the nature of the attacks and threats we are facing. When sharing intelligence externally we are careful to comply with legislation such as GDPR and competition law - we do not share customer information with external partners and we are careful not to share information that could be commercially sensitive, either to ourselves or to our suppliers and clients.

This sharing is particularly effective when we are responding to incidents that have an impact across the whole sector, from third party data breaches, physical and cyber-attacks on ATMs or industry-wide denial of service attacks.

The one area which change would help is Privacy Legislation:

In its current format it hinders the ability for the finance sector to share customer information for the purposes of identifying criminal activity that could ultimately protect customers and support law enforcement.

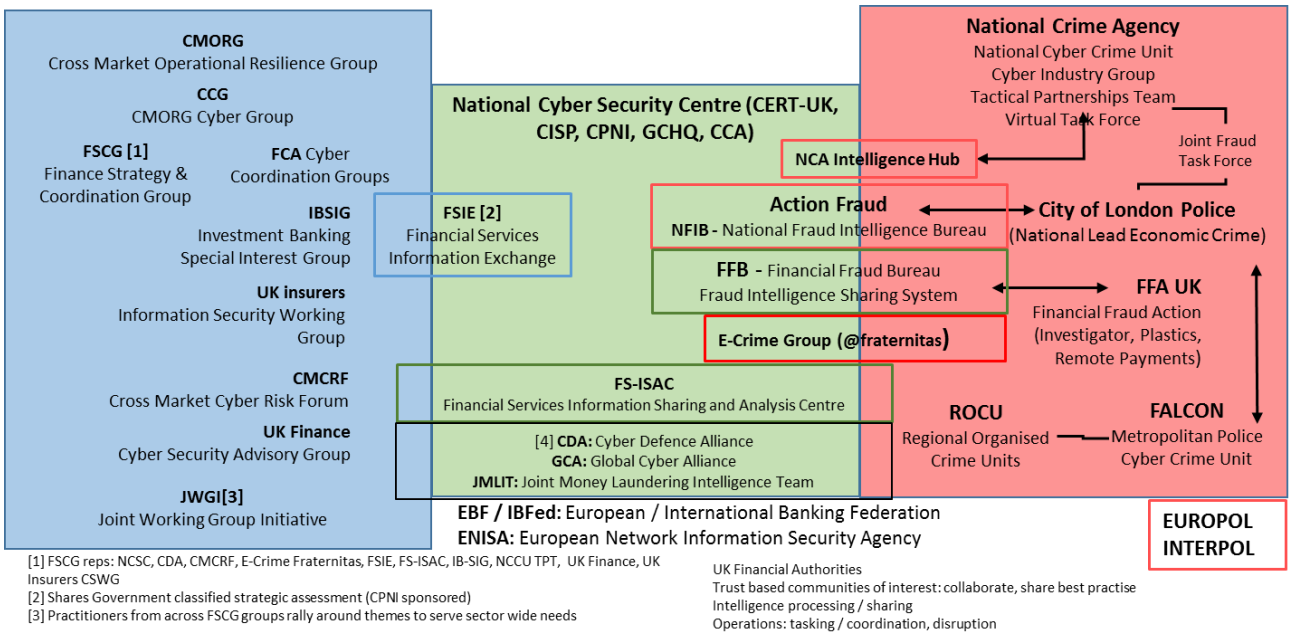
In response, we are evaluating and investing in innovative solutions that maintain privacy, however adjustment of this legislation would help customers.

I'd like to finish by assuring you that Lloyds Banking Group recognise the cyber threats that can impact the whole of our society, and as well as pursuing our own cyber security strategy to keep our business and customers safe, we recognise the need for us to continue to play a leadership role in the private sector and work closely with Government to help make sure the UK is in the vanguard of the digital revolution. Thank you for listening.

iii) Gary W NCSC

Gary introduced the work of the NCSC and how the collaboration around cyber security and financial services fits into the bigger picture. NCSC have set up the Financial Services Cyber Coordination Centre – FSCCC in conjunction with UK Finance to enable a co-ordinated response to the "clear and present danger" posed by hack attempts and large scale cyber attacks.

Gary explained how the FSCCC fits into the broader framework of NCSC and other Government activity to combat cyber attacks:



The Project STRIDER Working Group was introduced to make recommendations to enhance cyber response across the sector and better support the UK national cyber defence effort. The group Proposed a Concept of Operations that involved

- An integrated operational construct using existing entities
- Coordination node in UK National Cyber Security Centre
- Alignment with regulatory communication channels and government national response process

This led to the formation of the FSCCC in 2017 when the Bank of England's Cross Market Operational Resilience Group (CMORG) concluded its Project Strider diagnostic, a report that examined the cyber defence capability of the UK financial sector and made a series of recommendations. In 2018 UK Finance was invited to co-chair CMORG and to coordinate the UK financial sector in delivering the recommendations made in the Strider diagnostic.

FSCCC is the evolution of CMORG's Strider initiative and aims to adhere to its principles:

- Accessible for all in the UK financial sector.
- Complement existing structures / avoid duplication.
- Be technology agnostic.
- A cooperative approach putting defence ahead of regulation or competition.
- Aim at operational actions.
- Support all levels of cyber maturity / affordability.
- Seek to identify systemic issues.
- Inform risk management strategies.
- Solution to allow for continual improvement.

"The FSCCC's mission is to support collaboration across the UK financial sector in order to strengthen the resilience of the UK financial sector. The FSCCC aims to enable proactive identification, investigation and mitigation of large-scale cyber attacks with systemic consequences through

effective coordination of activities and focused operations across financial services organisations, industry partners, and UK and international authorities."

Operationally, the model is envisaged as one of mutual self help and collaboration delivered by and for the benefit of its members. The FSCCC will complement existing cyber capabilities and services currently available whether in the UK or overseas. A future state operating model will be developed in line with the services, to ensure it meets member needs & is fit for purpose moving forward.

3) Open discussion

Khalid Rashid DTCC – couple of weeks ago received an email stating his password and asking for him to transfer money in bitcoins. Probably came through his 14 year old child installing some dodgy software. As a member of the public it was not clear where to go to report the crime.

SB – Lloyds reports all its phishing software and advises colleagues not to respond. Advised contacting your ISP. Challenge is how do you educate customers to do that?

Chris Jamieson, Novacoast – report it to Action Fraud.

Peter Drissell CAA – not heard regulators mentioned, what role do they play?

RI – from a trust perspective it is difficult to get people to share if they think that the regulator is listening. BoE Operations staff can participate in sharing activities but not the regulatory staff. There is a separate forum for regulators.

Talks to regulators globally and FCA and BoE have an enlightened attitude.

SB – in incident mode do not work with regulators. Have a trilateral meeting every quarter and share warts and all with the regulator. Try to do what we can do and are challenged. Working on operational resilience right now, proactive sessions.

GW – NCSC work closely with Treasury and the Regulators. FCA bring in sub-groups in Finance and allow for conversations to happen.

James Morris MP – as the CEO of a bank to whom am I accountable for cyber risk?

SB – All Banks have someone allocated. Accountabilities are written down and signed off

Keith Mayes – homomorphic encryption is very resource intense, seems wrong that privacy regulations are forcing this sort of behaviour when criminals have an easier route.

SB – working with Govt as to how legislation can be changed. Some information that we do need to share and sometimes we do not know if there is criminal activity or not.

RI – Cross border sharing of information is very tricky. GDPR is believed to provide for sharing but no case law to support it

Mike Hurst – What about vulnerable customers who are more open to fraud and too many things mitigate against older people who do not understand technology. How aware are systems about excluding people. Family are a big threat.

SB – vulnerable customers are a hot topic as there are millions. Give them special attention and have a number of indicators. Important not to share identities.

Graham Mann – FSCCC encompasses a number of smaller bodies, with a lot of the challenger banks, AI systems and FinTech firms, they don't have the deep pockets to invest in cyber security. Are they included?

GW – yes intention is to ensure that anyone from a one man band upwards can participate. Cited example of a mortgage broker, look at how you change behaviour and work through large FIs who have the reach.

SB – how do we start to look at intelligence sharing to larger and larger groups? Needs to be done in an actionable way.

RI – Regulator decreed that it would be a good idea to join FSISAC in the US. This meant a lot of new, but budget members. Very active community of smaller banks. Put out a separate newsletter to this sector raising issues. Looking after the small guys is a challenge.

Also need to work with MSPs.

GM – Do you give more than advice?

GW – FSCCC is about intelligence sharing. NCSC has a wide range of advice and guidance. They struggle to reach this large audience. Push info. Out via Lloyds and other big banks. You invariably find that the new banks take a service and buy turn key solutions. FinTech firms use Open banking to get to information.

GM – probably two Cloud providers who most go to which means an (almost) single point of failure.

GW – Difficult to hedge against.

SB – looking at Cloud strategy.

Duncan Haines – do yu just rely on FISAC or do you have internal readiness exercises.

SB – yes, we have reactive and proactive teams. Also exercise with the Board and all their businesses.

James Morris – Geopolitical factors at play, to what extent do you do geo-political analysis. Is that a formalised dashboard of risks that the CEO can view?

SB – We do it every day. Not risk in real-time though. We look at the threat landscape which does not change daily. 3 hour session with the Board per quarter.

Brad Collier – recent events in Hong Kong, do you have a specific working group on China.

SB – Lloyds tracks all the actors. Look at skill sets, capabilities, motivation and level of risk of attack.

RI – We run a threat call every 2 weeks with members. This includes a vote on threat levels by members. If something starts to go hot, we will stand up a particular briefing call. Also run emergency incident calls.

PD – Getting good intel from Govt is very hard. How does information travel from the Govt to the banking world?

GW – it is improving and we recognise the need to get information out quickly. Need to be timely and not to compromise the source.

SB – it is improving. Always a view that the NCSC has more information to give us than it does. I100 and FSCCC will help industry to get the comfort that they are getting everything that they need.

GW – important to make sure that the sharing of information is useable. Difficult balance.

RI – very useful to have conversations with NCSC to highlight worries that members have.

Ollie Bone, Technation – Good to see what the FSCCC is doing, has seen how hard it is for entrepreneurs to understand the challenges. Hard for small firms to access, understand the challenges and putting this forward. FSCCC – what are you doing to bring matters together to have a single point of contact with the wider UK eco-system. Has it got an innovation element?

RI – more about formalising what is going on with different groups.

SB – this is one of the reasons that Lloyds sponsors LoRCA. Also trying to do a lightweight contract with FinTechs. Got to be more agile with FinTechs.

KR – is there a link back into 3rd party risk management such as Cloud service providers?

SB – We have a significant work programme about securing the supply chain.

KR – do you have plans to cater for service disruption?

SB – yes, we include 3rd Parties in testing.

Brad Collier – would you do that with soMe of your NHS customers?

SB – we would do that, get more support from NCSC.

GW – NCSC undertake the role.

Duncan Hayes, BoA – do you find lack of budget in the NHS a challenge?

GW – across any IT estate you are always running vulnerabilities or risk.

CJ – big believer in the engineering philosophy, is it a conscious strategy to engineer more controls in?

SB – we call it evergreening and are looking at evergreening processes. Engineer it to work like that in the first place.

GM – At the meeting about the NHS, it was raised that IOT systems use old technology and it is hard for customers to make changes.

4) <u>Conclusion:</u>

JM – the main policy point is that of privacy issues- we will pick that up as an APPG.

Thanked the speakers.