Top cyber risk and compliance related news stories and world events, that (for better or for worse) shaped the month's agenda, and what is next

March 2018, cyber risk and compliance in Switzerland

Mark Branson, FINMA’s Chief Executive Officer since April 2014, gave a great presentation (Title: ‘Technology and the financial industry – opportunity or risk?’, Annual Media Conference, 27 March 2018).

This is part of what he said:

‘The subject of hacking leads us to the topic of cyber-risk for financial institutions. Financial institutions are a target much favoured by hackers and the perpetrators of cyber-attacks.

MELANI, the Swiss Reporting and Analysis Centre for Information Assurance, reports that two-thirds of the incidents targeting critical infrastructure in 2017 occurred in the financial sector.

The risks connected with these attacks are growing in sync with the pace of global digitalisation.

Cyber-attacks are now the most serious operational hazard facing the financial system, and both the private sector and public authorities should take them extremely seriously.

On the whole, the institutions we supervise are aware of the risks and seem well-equipped to deal with them. A large number of attacks are successfully repelled every day, for example, the roughly 100 attacks per day on e-banking systems by so-called "Retefe" malware.

Of course, the best defence is only as strong as the weakest link. For instance, hackers broke into the SWIFT international payments system through successfully targeting the central bank of Bangladesh.

In Switzerland, a large volume of customer data was recently stolen from a health insurer.

In light of these risks, what are FINMA's expectations?

First, it is essential that financial institutions understand where they are vulnerable. Here penetration tests are an essential instrument.

Equally important in the event of a cyber attack is crisis response. Speedy re-establishment of operational functionality is vital. Each institution must develop and test a crisis contingency plan.

However, the risks involve more than simply the theft of money or data. Targeted attacks, perhaps even perpetrated by terrorist, state or state-related sources, could assume systemic dimensions.

Although Swiss financial institutions appear individually well-prepared by international comparison, we are doing less than other countries to protect the system as a whole.

Other countries with important financial centres do more, for example by setting up cybersecurity competence centres or imposing system-wide penetration tests.

Switzerland should follow suit by enhancing its system-wide monitoring and response processes.

Here FINMA is ready to play its role. We have recruited specialists in this area and are prepared to make further investments.

In this connection the Advisory Board for the Future of the Financial Centre, chaired by Professor Aymo Brunetti, made three key recommendations that received little attention – wrongly so.

These were, firstly, that access to MELANI should be extended, also to small financial institutions in Switzerland.

Secondly, that cooperation between financial sector experts and the authorities should be institutionalised and reinforced.

Cyber-risk prevention is one area where the interests of the industry and the supervisor certainly coincide.

And thirdly, a cybersecurity crisis response plan for the financial sector needs to be designed and tested.

FINMA welcomes and supports these recommendations. Working together achieves more than going it alone.

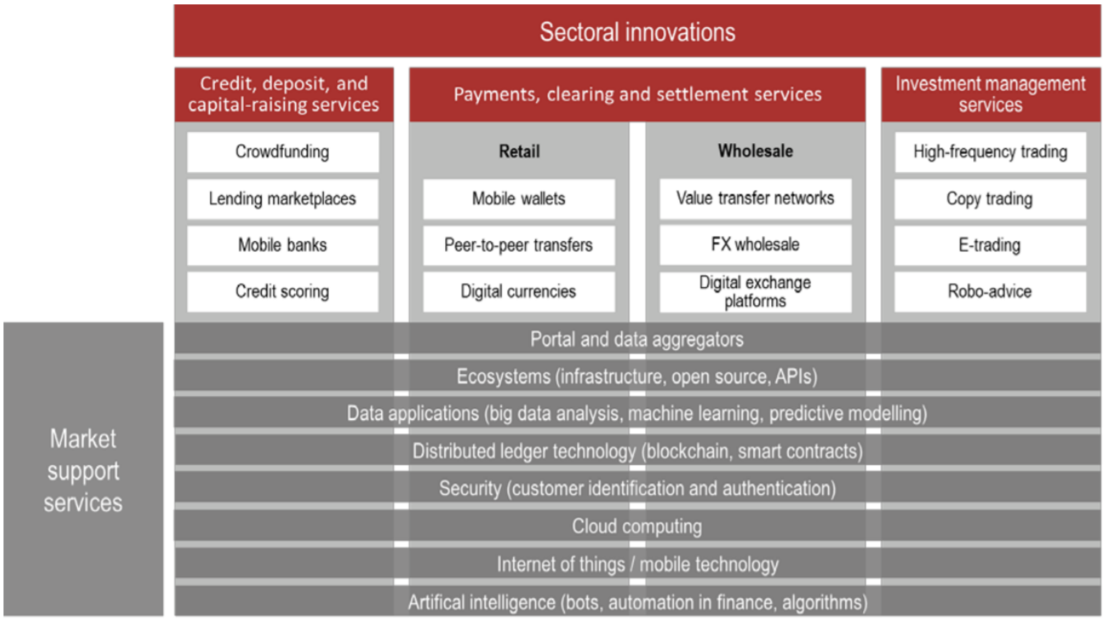
Switzerland is responding to the threat – but other countries are doing more.'

We have some other interesting developments this month.

What is fintech?

The Basel Committee has opted to use the Financial Stability Board's working definition for fintech as "technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services".

Graph 1: Sectors of innovative services



Sectoral innovations

Credit, deposit, and capital-raising services
Crowdfunding
Lending marketplaces
Mobile banks
Credit scoring

Payments, clearing and settlement services
Retail
Mobile wallets
Peer-to-peer transfers
Digital currencies
Wholesale
Value transfer networks
FX wholesale
Digital exchange platforms

Investment management services
High-frequency trading
Copy trading
E-trading
Robo-advice

Market support services
Portal and data aggregators
Ecosystems (infrastructure, open source, APIs)
Data applications (big data analysis, machine learning, predictive modelling)
Distributed ledger technology (blockchain, smart contracts)
Security (customer identification and authentication)
Cloud computing
Internet of things / mobile technology
Artifical intelligence (bots, automation in finance, algorithms)

Source: BCBS.

The Basel Committee also used a categorisation of fintech innovations.

Graph 1 depicts three product sectors, as well as market support services.

The three sectors relate directly to core banking services, while the market support services relate to innovations and new technologies that are not specific to the financial sector but also play a significant role in fintech developments.

The results of a comparative survey on supervisory approaches indicate that most surveyed agencies have not formally defined fintech, innovation or other similar terms.

Some of the reasoning provided for this lack of formal definitions was that other definitions already exist, or that it would be premature to more narrowly define a field that is rapidly evolving.

To read more:
www.bis.org/bcbs/publ/d431.pdf

Do you believe that Artificial intelligence (AI) is enhancing the power of the human brain in the *same way* that electricity enhanced the power of the body 150 years ago?

Prof Joachim Wuermeling, Member of the Executive Board of the Deutsche Bundesbank, gave a very interesting presentation at the 2nd Annual FinTech Conference. He said:

"Artificial intelligence and big data are currently the strongest and most vivid innovation factors in the financial sector.

Using AI in finance may trigger dramatic improvements in many businesses. AI elevates the role of data as a key commodity.

Used wisely, big data make outcomes more reliable and may improve financial mediation.

Process chains can be organised in new ways. "The scope and nature of banks' risks and activities are rapidly changing," as a recent Basel Committee analysis puts it.

This evolution towards increased use of non-human intelligence is not something that has just occurred in the last few years.

The first invention of neural networks, a central pillar of most AI systems, dates back to the year 1943.

Until a few years ago, the main users of big data and AI in the area of finance were certain hedge funds and high-frequency trading firms.

In recent times, the application of AI in finance has begun to spread widely, via "normal" banks, FinTechs and other financial service providers, to the general public."

But, Prof Joachim Wuermeling continued:

"But opportunities are always accompanied by risks. As regards the financial system, if too much trust is put in "intelligent" systems, the stability of financial markets may be at stake.

The workings of AI can be a mystery; it can trigger loss of control, make fatal errors, and have a procyclical effect due to its mechanistic functions.

Pattern recognition has its limits. This can be dangerous particularly in crisis scenarios. An autopilot would never have been able to land a jet on the Hudson River. Nor can algorithms stabilise in periods of financial stress.

Looking at the recent turbulence in equities and the market for VIX-related financial products, it can be concluded that the events of 5 February share many similarities with a "flash crash".

Unfortunately, as with the original flash crash of May 2010, we have only limited knowledge about the direct drivers that triggered the event.

It can be assumed that algorithmic market participants were quite active during the relevant period. But as to which strategies were applied and to what effect, we have no knowledge so far.

The rise in volatility in the S&P 500 then nearly instantly affected the VIX industry, making it not the cause but more the first victim of this market event, with losses up to 95 % on assets.

We do not expect this phenomenon to disappear in the future. On the contrary, more of these flash events are to come. AI is still in its infancy. Continuous processes for the entire AI lifecycle still have to be defined and scaled for business needs.

That means that AI must be embedded in the process of acquiring and organising data, modelling, analysis and delivering analytics.

The skills gap, particularly with regard to data science and machine learning expertise, is the foremost challenge.
At this stage, non-human intelligence is far from replacing the human brain in any respect."

This is a very interesting presentation.

I understand that, like Heraclitus has said, there is nothing permanent except change. Perhaps it is too early to feel confident that AI will not create new major vulnerabilities.

Albert Einstein believed that the true sign of intelligence is not knowledge but imagination. Is this possible with artificial intelligence?

Aristotle has said that there is no great genius without some touch of madness. Edgar Allan Poe added that science has not yet taught us if madness is or is not the sublimity of the intelligence. As you see, I try to be positive, and I try to ignore that, according to Plutarch, the mind is not a vessel to be filled but a fire to be kindled.

Welcome to our monthly newsletter.

Best regards,

George Lekatis

George Lekatis
General Manager
Cyber Risk GmbH
Rebackerstrasse 7,
8810 Horgen
Phone: +41 43 810 43 61
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

Cyber Risk GmbH, Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341

Our catalog, *in-house* instructor-led training in Switzerland, Liechtenstein, and Germany:
www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2018.pdf

Number 1 (Page 12)

A Euro Cyber Resilience Board for pan-European Financial Infrastructures

Benoît Cœuré, Member of the Executive Board of the European Central Bank, at the first meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt am Main.

‘Recent technological advances have enabled cybercriminals to conduct ever more sophisticated, precise and powerful attacks.

And nobody is immune to cyber risks, including businesses, financial infrastructures and public administrations. So we should avoid a "blame and shame" culture and work together.’

Number 2 (Page 15)

The European Cyber Security Challenge: Lessons Learned report

Both the growing need for IT security professionals and skills shortage are widely acknowledged.

To help solve this, multiple countries have initiated national cybersecurity competitions for students, security professionals and even non-IT professionals, all with a common goal: find cyber talents and encourage all of them to pursue a career in cybersecurity.

Number 3 (Page 17)

Brief thoughts on the financial regulatory system and *cybersecurity*

Randal K Quarles, Vice Chairman for Supervision of the Board of Governors of the Federal Reserve System, at the Financial Services Roundtable 2018 Spring Conference, Washington DC.

'Let me now turn from regulation to supervision, and more specifically, to the topic of cybersecurity, which continues to be a high priority for the Federal Reserve.

The Federal Reserve is committed to strategies that will result in measureable enhancements to the cyber resiliency of the financial sector.

Given the dynamic and highly sophisticated nature of cyber risks, collaboration between the public sector and private sector toward identifying and managing these risks is imperative.'

Number 4 (Page 20)

Largest reported DDoS attacks mitigated

National Cyber Security Centre
a part of GCHQ

The largest ever reported Distributed Denial of Service (DDoS) occurred in early March 2018, according to Netscout Arbor.

A peak of 1.7 Terabits per second (Tbps) was recorded, although the attack was mitigated.

This followed a recent attack against GitHub on 28 February, with a peak of 1.35 Tbps. The largest known attack previously took place in 2016 against the US DNS provider DYN, which peaked at 1.2 Tbps.

Number 5 (Page 22)

Call for experts for TRANSSEC - Transport Resilience and Security Expert Group

ENISA launches this call for participation to invite experts in security of different sections of the transport sector to participate in its expert group

enisa
European Network
and Information
Security Agency

ENISA has established this expert group to cover security and resilience of transport systems as they undergo a digital transformation built around a plethora of interconnected devices and systems that facilitate automation and intelligent decision-making.

The threats and risks associated with the digital transformation of the transport sector are manifold and have a potential impact on citizens' safety, health and privacy, in addition to the availability of the critical transport services themselves.

Number 6 (Page 24)

Former employee jailed for intentionally damaging computer network

National Cyber
Security Centre
a part of GCHQ

A disgruntled former Canadian Pacific Railway (CPR) employee was sentenced last week to a year in prison for intentionally causing damage to CPR's computer network.

Number 7 (Page 25)

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Ronald S. Ross, Patrick Viscuso, Gary Guissanie, Kelley L. Dempsey, Mark Riddle

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations.

Number 8 (Page 26)

Making Gray-Zone Activity more Black and White

New program aims to lift the fog obscuring an adversary's intentions in slow, simmering non-traditional conflicts

DARPA
DEFENSE ADVANCED
RESEARCH PROJECTS AGENCY

An emergent type of conflict in recent years has been coined "gray zone," because it sits in a nebulous area between peace and conventional warfare.

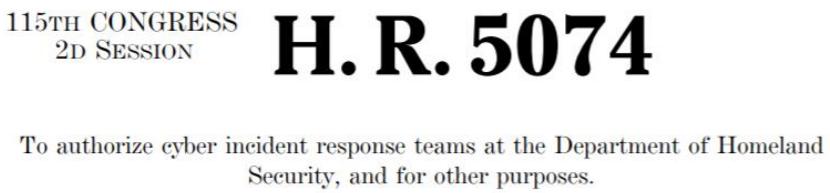
Gray-zone action is not openly declared or defined, it's slower, and is prosecuted more subtly—using social, psychological, religious, information, cyber and other means to achieve physical or cognitive objectives with or without violence.

The lack of clarity of intent—the grayness—makes it challenging to detect, characterize, and counter an enemy fighting this way.

Number 9 (Page 29)

DHS Cyber Incident Response Teams Act of 2018

A BILL To authorize cyber incident response teams at the Department of Homeland Security, and for other purposes.



115TH CONGRESS
2D SESSION

H. R. 5074

To authorize cyber incident response teams at the Department of Homeland Security, and for other purposes.

'CYBERSECURITY SPECIALISTS. — The Secretary may include cybersecurity specialists from the private sector on cyber hunt and incident response teams.'

Note: House lawmakers have passed legislation that would codify into law the cyber incident response teams that help protect federal networks and critical infrastructure from cyberattacks.

The bill is sponsored by House Homeland Security Committee Chairman Michael McCaul (R-Texas).

Number 10 (Page 31)

Progress Update on Cyber Lexicon

FSB FINANCIAL STABILITY BOARD

This note, delivered to G20 Finance Ministers and Central Bank Governors for their meeting in March 2018 in Buenos Aires, provides a progress update on the FSB's work to develop a cyber lexicon.

G20 Finance Ministers and Central Bank Governors, in their March 2017 Baden-Baden Communiqué, noted that the malicious use of Information and Communication Technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability.

Number I

A Euro Cyber Resilience Board for pan-European Financial Infrastructures

Benoît Cœuré, Member of the Executive Board of the European Central Bank, at the first meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt am Main.

It is a pleasure to welcome you back to Frankfurt. Our last meeting was in June last year.

Today, we will discuss the future course of the high-level cyber resilience forum for pan-European financial market infrastructures, critical service providers and competent authorities.

Establishment of the Euro Cyber Resilience Board for pan-European Financial Infrastructures

Recent technological advances have enabled cybercriminals to conduct ever more sophisticated, precise and powerful attacks.

And nobody is immune to cyber risks, including businesses, financial infrastructures and public administrations. So we should avoid a "blame and shame" culture and work together.

The ECB and the Eurosystem are striving to lead by example. At the ECB, overseers, operators, supervisors and IT security services are working together more closely on cyber issues.

Within the Eurosystem, there has been close collaboration on implementing the Eurosystem oversight cyber resilience strategy for financial market infrastructures that we presented at our last meeting, in line with CPMI-IOSCO's guidance on this topic.

The Market Infrastructure Board, which is in charge of Eurosystem financial market infrastructures, has also scaled up its activities to ensure the continued cyber resilience of its systems and platforms.

Eurosystem initiatives are part of a growing international effort to combat cyber threats. The CPMI-IOSCO guidance is being implemented.

In October 2017, the Financial Stability Board (FSB) delivered a stocktake report of relevant regulations and supervisory practices to G20 finance ministers and governors, and G7 ministers and governors published the "Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector".

The FSB will produce a common lexicon of important terms, while the G7 Cyber Expert Group continues to work on third-party risks, cross-sector coordination and threat-led penetration testing, and will make proposals for G7 cross-border cyber crisis simulation exercises.

In this context, the Eurosystem aims at coordinating its own activities in the field of cyber risks with that of market participants and other public authorities to succeed in protecting the financial system from cyber threats. I therefore invite you today to become part of the Euro Cyber Resilience Board (ECRB) for pan-European Financial Infrastructures - a regular forum where we can work together in a trusted environment.

The ECRB's objective is to enhance the cyber resilience of financial market infrastructures and their critical service providers, as well as that of the wider EU financial sector, in line with international standards.

This will be achieved by fostering trust and collaboration and facilitating joint initiatives - whether among market players or between market players and authorities. The ECRB will thus contribute to the overall stability of the EU financial system.

The ECRB will have no formal powers to impose binding measures and will not make supervisory judgements. Its legitimacy will stem from the voluntary commitment of its members to abide by its common positions, statements and strategic views.

The ECRB will be chaired by the ECB, which will be closely involved together with national central banks and observers from the relevant European public authorities. This will ensure that the ECRB acts in the interest of Europe as a whole. Its common positions, statements and strategic views will be adopted by consensus.

To kick off the work of the ECRB, we would like to reflect with you on possible work items which we could address collectively. As part of this, we will also report on two of our most recent activities.

First, a cyber resilience survey, developed under the Eurosystem oversight cyber resilience strategy, was conducted across more than 75 payment systems, central securities depositories and central counterparties throughout Europe.

As you will see, the survey highlighted a number of very pertinent issues for discussion, such as cyber governance, training and awareness, and cyber incident response.

Second, the Eurosystem is currently finalising the main elements of the European Threat Intelligence-Based Ethical Red-Teaming (TIBER-EU) Framework.

This is an interesting concept which we hope will raise the level of cyber resilience in Europe and enable cross-border, cross-authority testing, which has not been done before.

We look forward to hearing your feedback on these two initiatives. We will also update you on the forthcoming market-wide exercise, which will explore the challenges of a specific cyber scenario and see how we can work closer together in times of crisis.

I am confident that we will have a fruitful discussion. I will now hand over to my colleague Sabine Lautenschläger, who will make some introductory remarks from the supervisory perspective.

After that, I would like to invite the European Commission representative to briefly introduce the very recently published "FinTech Action plan", which presents some interesting points to be considered with regard to the cyber resilience of the financial sector. Thank you.

Number 2

The European Cyber Security Challenge: Lessons Learned report

Both the growing need for IT security professionals and skills shortage are widely acknowledged.

To help solve this, multiple countries have initiated national cybersecurity competitions for students, security professionals and even non-IT professionals, all with a common goal: find cyber talents and encourage all of them to pursue a career in cybersecurity.

The European Cyber Security Challenge (ECSC) builds upon these competitions adding a pan-European layer.

The ECSC is an initiative of multiple European countries supported by the European Union Agency for Network and Information Security (ENISA) that aims at engaging cybersecurity talent across Europe and connecting high potentials.

This report contains a detailed list of the lessons learned from previous ECSCs, of which the key takeaways are:

- The quality of the ECSC is crucial in meeting the participants' expectations. The scenario, stability and complexity of the platform used during the ECSC are key success factors in order to provide a challenging competition that attracts top cyber talent from all over Europe.

- Public relations and communication activities are key in order to meet the objectives on participation and sponsorship.

- The event agenda should be tailored to the participants needs and expectations, and include activities that relate to their interests and subject matter expertise.

- Given the current growth objectives of the ECSC (plus five countries per year), solid back-office processes regarding the organisation of the event are necessary to meet the rising quality expectations from stakeholders. This includes, amongst others, a proper governance structure with clear roles, responsibilities, decision-making, agreed-upon principles and rules with regard to fair play and transparency.

- Sharing lessons learned and recommendations between organisers and participating states is crucial in order to improve the quality of the event and implement best practices.

To read more:
https://www.enisa.europa.eu/publications/the-european-cyber-security-challenge-lessons-learned-report

Number 3

Brief thoughts on the financial regulatory system and *cybersecurity*

Randal K Quarles, Vice Chairman for Supervision of the Board of Governors of the Federal Reserve System, at the Financial Services Roundtable 2018 Spring Conference, Washington DC.

Thank you very much for having me here at the Financial Services Roundtable's spring meeting. I am pleased to speak with you all about our financial regulatory system: both the broad principles that have been directing my approach to evaluating the regulatory system, as well as cybersecurity, which is a topic of great import to financial system participants and their regulators.

Efficiency, Transparency, and Simplicity of Regulation

As I have said before, we have an opportunity to improve the efficiency, transparency, and simplicity of regulation. We have spent the past decade building out and standing up the post-crisis regulatory regime, and as a result we have made critical gains. The financial system is undoubtedly stronger and safer. We have robust capital and liquidity levels, an effective stress testing regime, and improved resolvability of our largest firms.

But at the same time, it is our responsibility to ensure that those rules are effective. And if we identify rules that are not working as intended, we should make the necessary changes. With the benefit of hindsight and with the bulk of our work behind us, now is a natural and expected time to evaluate the effectiveness of that regime.

Our efforts toward implementing those principles are underway. Federal Reserve Board staff members continue the review that I have previously outlined. The goal is to consider the effect of past regulatory initiatives on the resiliency of our financial system, on credit availability and economic growth, and more broadly, their costs and benefits. I am confident that that review will reveal some clear ways that we can improve the core post-crisis reforms.

Cybersecurity

Let me now turn from regulation to supervision, and more specifically, to the topic of cybersecurity, which continues to be a high priority for the Federal Reserve.

The Federal Reserve is committed to strategies that will result in measureable enhancements to the cyber resiliency of the financial sector.

Given the dynamic and highly sophisticated nature of cyber risks, collaboration between the public sector and private sector toward identifying and managing these risks is imperative.

While we know that successful cyber attacks are often connected to poor basic information technology hygiene, and firms must continue to devote resources to these basics, we also know that attackers always work to be a step ahead, and we need to prepare for cyber events.

Many of you provide services that are critical to maintaining the functionality of the financial system. Those critical services should be highly resilient. But at the same time, some of the solutions in place to improve the resiliency of those critical services may actually contribute to a cyber event.

One example would be the replication of bad data across data centers. As the Federal Reserve thinks about its financial stability mandate, this concern will be a particular focus. Solutions will not come easily, but I am confident that with strong public and private efforts, solutions will emerge.

The Federal Reserve also focuses on the sharing of threat information and collaborates with a number of partners toward protective mechanisms. We work with other domestic agencies as well as international authorities, and we have partnerships between the public and private sectors to introduce and participate in programs that combat the increasingly frequent and sophisticated cyber threats.

Specifically, we collaborate with government and industry partners to plan and execute cybersecurity tabletop exercises focused on identifying areas where sector resilience and information sharing can be enhanced. We also participate in community and industry outreach forums and actively share threat intelligence with sector partners including the Financial Services Information Sharing and Analysis Center (FS-ISAC). And we encourage financial institutions to work collectively through arrangements such as FS-ISAC so that threat information can be shared promptly and effectively.

Collaboration among many stakeholders on cybersecurity is critical to progress. The Federal Reserve has been working with, and will continue to work with, other financial regulatory agencies on harmonizing cyber risk-management standards and regulatory expectations across the financial services sector.

Specifically, we are focused on aligning our expectations with existing best practices, such as the National Institute of Standards and Technology's Cybersecurity Framework, and identifying opportunities to further coordinate cyber risk supervisory activities for firms subject to the authority of multiple regulators.

We support industry efforts to improve harmonization across the sector, which are complementary to achieving our regulatory safety and soundness goals.

Conclusion

The Federal Reserve continues to work toward improving both post-crisis regulation and our approach to cybersecurity.

I hope that my intention to lay out the broad principles guiding us as we move forward was helpful. And while many of the areas will require additional work and may not have fast results, the Federal Reserve is committed to getting it right, and I look forward to those efforts.

Number 4

Largest reported DDoS attacks mitigated

National Cyber Security Centre
a part of GCHQ

The largest ever reported Distributed Denial of Service (DDoS) occurred in early March 2018, according to Netscout Arbor.

A peak of 1.7 Terabits per second (Tbps) was recorded, although the attack was mitigated.

This followed a recent attack against GitHub on 28 February, with a peak of 1.35 Tbps. The largest known attack previously took place in 2016 against the US DNS provider DYN, which peaked at 1.2 Tbps.

The method used for these attacks is known as a 'memcached server DDoS'. Memcached servers store data in memory that applications may need access to on external databases.

Large companies often use memcached servers to help speed up and assist in dealing with large demands on their services. When memcached servers are openly accessible over the internet via User Data Protocol (UDP), they can be utilised to significantly amplify data.

The attackers 'ping' a server with a small packet of data in order that memcached servers reply with a response to the victim which is up to fifty thousand times the original packet size.

If there are no mitigations such as filtering or management of networks, this could easily cause a service to go offline.

Whilst the vectors were different in the 2016 DYN attack, the incident demonstrates the potential ramifications if other services are dependent on the targeted service; for more information, see the NCSC Weekly Threat Report 24 October 2016 at https://www.ncsc.gov.uk/report/weekly-threat-report-24-october-2016

In the attack against GitHub, there has since been reporting of a ransom made in the data payload, demanding a payment of 50 Monero (worth approx. $15 000).

There are also suspicions among various mitigation service providers that this method of amplification has now been adopted by DDoS-as-a-Service providers.

These latest DDoS attacks were mitigated, but further attacks may occur. The NCSC has previously provided DDoS advice regarding understanding the threat of attacks and also response and recovery planning. There is also a detailed catalogue of NCSC DDoS guidance.

To read more:
https://www.ncsc.gov.uk/guidance/denial-service-dos-guidance-collection

https://www.ncsc.gov.uk/guidance/understanding-denial-service-dos-attacks

Number 5

Call for experts for TRANSSEC - Transport Resilience and Security Expert Group

ENISA launches this call for participation to invite experts in security of different sections of the transport sector to participate in its expert group

ENISA has established this expert group to cover security and resilience of transport systems as they undergo a digital transformation built around a plethora of interconnected devices and systems that facilitate automation and intelligent decision-making.

The threats and risks associated with the digital transformation of the transport sector are manifold and have a potential impact on citizens' safety, health and privacy, in addition to the availability of the critical transport services themselves.

TRANSSEC is an information exchange platform that brings together experts to ensure security and resilience of the Transport sector in Europe.

It is the intent of ENISA for this group to produce specialised work streams focusing on specific sub-sectors of transport, namely Air, Rail and Water Transport with the possibility of eventually establishing one or more specialised individual Expert Groups.

Experts of the TRANSSEC shall have technical background expertise and direct exposure on one or more of the following:

1. Operators and infrastructure owners of Transports systems with an interest in cybersecurity in one or more of the following sub-sectors:

- air transport e.g. air carriers, airports, traffic management control operators etc.

- rail transport e.g. infrastructure managers, service facilities etc.

- water transport e.g. water transport companies, ports, vessel traffic services etc.;

2. Manufacturers or integrators of transport systems with a focus on cybersecurity;

3. Suppliers and developers of transport hardware and/or software with a focus on cybersecurity;

4. Associations and not-for-profit organisations involved in transport security;

5. Relevant authorities, academia, standardisation bodies and policy makers directly involved in the above topics.

For details and registration, please visit:
https://resilience.enisa.europa.eu/transport-security

Number 6

Former employee jailed for intentionally damaging computer network

National Cyber
Security Centre
a part of GCHQ

A disgruntled former Canadian Pacific Railway (CPR) employee was sentenced last week to a year in prison for intentionally causing damage to CPR's computer network.

It is unclear whether train services were affected, but the incident is reported to have cost the organisation approximately $30,000.

In December 2015, the employee resigned from CPR after being informed that he would be fired for insubordinate behaviour.

However, before returning his laptop and remote access authentication token to the organisation, the disgruntled individual accessed CPR's core computer network switches, through which critical data flows.

He strategically deleted files, removed admin accounts or changed their passwords, returning the laptop after wiping its hard drive of any evidence of his actions.

This meant IT staff were unable to access the switches, forcing them to reboot the network, causing a system outage.

Forensic investigations of systems allowed the damage to be traced back to the individual concerned.

This case is a good example of how disgruntled, former employees can pose a cyber threat to organisations.

Such insider threats are not unique to the rail sector. Public and private organisations in every sector need to be vigilant to such threats.

It highlights the importance of ensuring IT privileges and account access is suspended when a staff member's employment is due to be terminated, preventing malicious cyber activity from being conducted.

Number 7

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Ronald S. Ross, Patrick Viscuso, Gary Guissanie, Kelley L. Dempsey, Mark Riddle

The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations.

This publication provides federal agencies with recommended requirements for protecting the confidentiality of CUI:

(i) when the CUI is resident in nonfederal information systems and organizations;

(ii) when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and

(iii) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry.

The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components.

To read more:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

Number 8

Making Gray-Zone Activity more Black and White

New program aims to lift the fog obscuring an adversary's intentions in slow, simmering non-traditional conflicts

DARPA
DEFENSE ADVANCED
RESEARCH PROJECTS AGENCY

An emergent type of conflict in recent years has been coined "gray zone," because it sits in a nebulous area between peace and conventional warfare.

Gray-zone action is not openly declared or defined, it's slower, and is prosecuted more subtly—using social, psychological, religious, information, cyber and other means to achieve physical or cognitive objectives with or without violence.

The lack of clarity of intent—the grayness—makes it challenging to detect, characterize, and counter an enemy fighting this way.

To better understand and respond to an adversary's gray-zone engagement, DARPA's Strategic Technology Office today announced a new program called COMPASS, which stands for Collection and Monitoring via Planning for Active Situational Scenarios.

The program aims to develop software that would help clarify enemy intent by gauging an adversary's responses to various stimuli.

COMPASS will leverage advanced artificial intelligence technologies, game theory, and modeling and estimation to both identify stimuli that yield the most information about an adversary's intentions, and provide decision makers high-fidelity intelligence on how to respond–-with positive and negative tradeoffs for each course of action.

"The ultimate goal of the program is to provide theater-level operations and planning staffs with robust analytics and decision-support tools that reduce ambiguity of adversarial actors and their objectives," said Fotis Barlos, DARPA program manager.

"As we see increasingly more sophistication in gray-zone activity around the world, we need to leverage advanced AI and other technologies to help commanders make more effective decisions to thwart an enemy's complex, multi-layered disruptive activity."

Current military decision-making follows a well-understood and effective OODA loop—Observe, Orient, Decide and Act. This is how planning is done in various geographic areas around the world, which works for traditional kinetic scenarios, Barlos said.

This process, however, is not effective in gray zone warfare. Signals in the environment are typically not rich enough to draw any conclusions, and, just as often, adversaries could implant these signals to induce ambiguity. COMPASS aims to add a dynamic, adaptive element to the OODA loop for complex, gray-zone environments.

The COMPASS program will leverage game theory for developing simulations to test and understand various potential actions and possible reactions by an adversary employing gray-zone activity.

Barlos quickly noted, however, that the program is not about developing new sensory technologies, virtual reality systems or other advanced hardware.

The program focuses rather on advanced software that would quickly present options to decision makers by assimilating a large amount of intelligence collected using existing, state of the art systems (such as standard video exploitation, or textual analysis tools) related to rapidly changing scenarios.

"We're looking at the problem from two perspectives: Trying to determine what the adversary is trying to do, his intent; and once we understand that or have a better understanding of it, then identify how he's going to carry out his plans—what the timing will be, and what actors will be used," Barlos said. "The first is the what, and second is the where, when, and how.

"But in order to decide which of those actions is important you need to analyze the data, and you need to understand what different implications are and build a model of what you think the adversary will do," he said. "That's where game theory comes in.

If I do this, what will the adversary do? If I do that, what might he do? So it is using artificial intelligence in a repeated game theory process to try to decide what the most effective action is based on what the adversary cares about."

The COMPASS program seeks experts in AI, machine learning, game theory, modeling and simulation, control systems, estimation and other related fields. A Proposers Day is scheduled for March 30, 2018, in Arlington, Virginia.

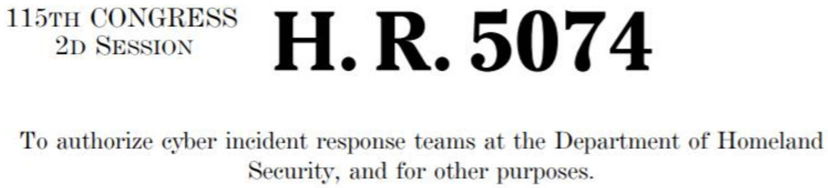
Registration instructions and more details are available on FedBizOpps (FBO): https://go.usa.gov/xQqjt

A Broad Agency Announcement (BAA) solicitation is expected to be posted on FBO prior to the Proposers Day and will be available on DARPA's FBO solicitation page: http://go.usa.gov/3W53j

Number 9

DHS Cyber Incident Response Teams Act of 2018

A BILL To authorize cyber incident response teams at the Department of Homeland Security, and for other purposes.



115TH CONGRESS
2D SESSION

H. R. 5074

To authorize cyber incident response teams at the Department of Homeland Security, and for other purposes.

The Center shall maintain cyber hunt and incident response teams for the purpose of providing, as appropriate and upon request, assistance, including the following:

(A) Assistance to asset owners and operators in restoring services following a cyber incident.

(B) The identification of cybersecurity risk and unauthorized cyber activity.

(C) Mitigation strategies to prevent, deter, and protect against cybersecurity risks.

(D) Recommendations to asset owners and operators for improving overall network and control systems security to lower cybersecurity risks, and other recommendations, as appropriate.

(E) Such other capabilities as the Under Secretary appointed under section 103(a)(1)(H) determines appropriate.

CYBERSECURITY SPECIALISTS. — The Secretary may include cybersecurity specialists from the private sector on cyber hunt and incident response teams.

Note: House lawmakers have passed legislation that would codify into law the cyber incident response teams that help protect federal networks and critical infrastructure from cyberattacks.

The bill is sponsored by House Homeland Security Committee Chairman Michael McCaul (R-Texas).

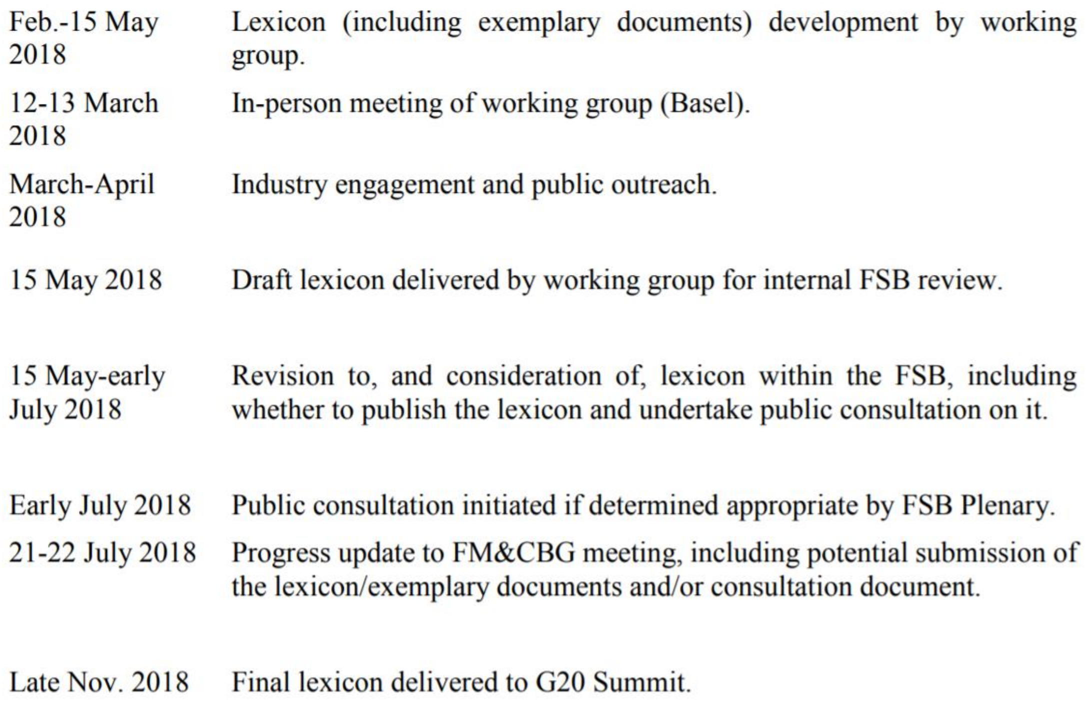
To read more:
http://docs.house.gov/billsthisweek/20180319/HR5074.pdf

Number 10

Progress Update on Cyber Lexicon

This note, delivered to G20 Finance Ministers and Central Bank Governors for their meeting in March 2018 in Buenos Aires, provides a progress update on the FSB's work to develop a cyber lexicon.

G20 Finance Ministers and Central Bank Governors, in their March 2017 Baden-Baden Communiqué, noted that the malicious use of Information and Communication Technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability.



Feb.-15 May 2018	Lexicon (including exemplary documents) development by working group.
12-13 March 2018	In-person meeting of working group (Basel).
March-April 2018	Industry engagement and public outreach.
15 May 2018	Draft lexicon delivered by working group for internal FSB review.
15 May-early July 2018	Revision to, and consideration of, lexicon within the FSB, including whether to publish the lexicon and undertake public consultation on it.
Early July 2018	Public consultation initiated if determined appropriate by FSB Plenary.
21-22 July 2018	Progress update to FM&CBG meeting, including potential submission of the lexicon/exemplary documents and/or consultation document.
Late Nov. 2018	Final lexicon delivered to G20 Summit.

With the aim of enhancing cross-border cooperation, the FSB was asked, as a first step, to perform a stocktake of existing relevant released regulations and supervisory practices in G20 jurisdictions, as well as of existing international guidance, including to identify effective practices.

The FSB published this stocktake on cybersecurity regulations, guidance and supervisory practices on 13 October 2017.

In October 2017, G20 Finance Ministers and Central Bank Governors at their Washington DC meeting welcomed the FSB stocktake report, asked the FSB to continue its work to protect financial stability against the malicious use of ICT and noted that this work could be supported by the creation of a common lexicon of terms that are important in the work being pursued.

This note provides a progress update on the FSB's lexicon work, including a description of the objective of the work, the process for creating the lexicon and a description of next steps with an indicative timeline in order to deliver the lexicon to the November 2018 Buenos Aires G20 Summit.

To read more:
http://www.fsb.org/wp-content/uploads/P200318.pdf

Disclaimer

Cyber Risk GmbH enhances public access to information about cyber risk and compliance in Switzerland.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which Cyber Risk GmbH has no control and for which Cyber Risk GmbH assumes no responsibility;

- is not professional or legal advice);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.