Monday, July 16, 2018

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

The Financial Stability Board (FSB) has published a draft Cyber Lexicon for public consultation. It comprises a set of 50 core terms related to cyber security and cyber resilience in the financial sector. The Cyber Lexicon is intended to support the work of the FSB, standard-setting bodies, authorities and private sector participants, e.g. financial institutions, and international standards organisations.

In my opinion, the draft lexicon, as it is today, does not meet the expectations of the industry. I will give some examples.

According to the draft Cyber Lexicon:

- Cyber Risk is "the combination of the probability of cyber events occurring and their consequences."

- Cyber Event is "any observable occurrence in an information system. Events sometimes provide indication that a cyber incident is occurring."

- Cyber Security is the "preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved."

The National Institute of Standards and Technology (NIST) gives a very different definition: Cyber Security is the "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and

electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

Having many different definitions of the same term is not going to help governments, standard setting bodies, firms and organizations.

The FSB developed the lexicon in response to a request from G20 Finance Ministers and Central Bank Governors at their October 2017 meeting. The FSB delivered a stocktake report to that meeting on existing publicly available regulations and supervisory practices with respect to cyber security in the financial sector.

Ministers and Governors asked that the FSB continue its work to protect financial stability against the malicious use of Information and Communication Technologies, noting that this work could be supported by a common lexicon of terms that are important in the work.

After considering the responses to this consultation, the FSB will finalise the lexicon for delivery to the G20 Leaders' Summit in Buenos Aires in November 2018.

Welcome to the Top 10 list.

Best Regards,

George Lekatis
President of the IARCP
General Manager, Compliance LLC
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828

Number 1 (Page 8)

Global systemically important banks

The Basel Committee issues revised G-SIB framework

The Basel Committee on Banking Supervision released Global systemically important banks: revised assessment methodology and the higher loss absorbency requirement.

When the Basel Committee first published the global systemically important bank (G-SIB) framework in 2011, it agreed to review the framework every three years to allow for the opportunity to enhance the framework, as needed.

Number 2 (Page 10)

Identity and travel document fraud

Counterfeit – a document that constitutes an unauthorized reproduction of a genuine document. These documents are not legitimately manufactured, nor issued or recognized by an official authority.

Forgery – these are typically based on a genuine document, a part of which has been added or altered in order to give misleading information about the person who presents it.

Number 3 (Page 12)

Building the UK financial sector's operational resilience discussion paper

The Bank of England, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) have published a joint discussion paper (DP) on an approach to improve the operational resilience of firms and financial market infrastructures (FMI's).

It envisages that boards and senior management can achieve better standards of operational resilience through increased focus on setting, monitoring and testing specific impact tolerances for key business services, which define the amount of disruption that could be tolerated.

Number 4 (Page 14)

Proportionality in banking regulation

Fernando Restoy, Chairman, Financial Stability Institute, Bank for International Settlements, at the Westminster Business Forum Keynote Seminar: Building a resilient UK financial sector - next steps for prudential regulation, structural reform and mitigating risks , London, United Kingdom.

"I think that there is a general sense that the post-crisis regulatory reforms have already made substantial progress in meeting their objectives. While it would be a mistake to claim "mission accomplished", the time has certainly come to shift the emphasis from standard setting to ensuring an effective implementation of the agreed reforms."

Number 5 (Page 21)

VPNFilter, a Nation State Operation

enisa European Union Agency for Network and Information Security

The recent disclosure of a sophisticated malware affecting 500,000 networking devices is making headlines around the world.

It followed several warnings made by manufacturers, security researchers and law enforcement concerning a malicious operation classified as a state sponsored. The malware dubbed VPNFilter - initially affecting Ukrainian hosts - is now spreading over 54 countries at an alarming rate.

Number 6 (Page 26)

Legal Working Paper Series

The Eurosystem and the Single Supervisory Mechanism: institutional continuity under constitutional constraints

EUROPEAN CENTRAL BANK
EUROSYSTEM

This paper analyses regulatory solutions that have been adopted to address constitutional constraints imposed on the functioning of the Single Supervisory Mechanism (SSM), in which the ECB's exclusive supervisory competence is carried out.

Number 7 (Page 27)

Clipboard hijacking malware

National Cyber Security Centre
a part of GCHQ

A newly-discovered clipboard hijacking malware sample has been seen monitoring over 2.3 million cryptocurrency addresses.

The malware scans the Windows Clipboard for cryptocurrency addresses, switching legitimate ones for addresses owned by the attacker. The malware runs in the background and as processes look genuine there are no tell-tale signs of infection.

Clipboard hijacking, however, is not a new threat. Historically, earlier versions of web browsers would allow websites to silently read the data stored on the Windows Clipboard. Today, updated browsers prompt the user on screen to allow access to the clipboard.

Number 8 (Page 29)

Financial stability implications of a prolonged period of low interest rates

Report submitted by a Working Group established by the Committee on the Global Financial System. The Group was co-chaired by Ulrich Bindseil (European Central Bank) and Steven B Kamin (Board of Governors of the Federal Reserve System), July 2018

> *While a low-for-long scenario presents considerable solvency risk for insurance companies and pension funds and limited risk for banks, a snapback would alter the balance of vulnerabilities.*
>
> Philip Lowe, Chair of the Committee on the Global Financial System

"Interest rates have been low in the aftermath of the Global Financial Crisis, raising concerns about financial stability.

In particular, the profitability and strength of financial firms may suffer in an environment of prolonged low interest rates.

Additional vulnerabilities may arise if financial firms respond to "low-for-long" interest rates by increasing risk-taking."

Number 9 (Page 31)

Justice Department

Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices

Additional action necessary worldwide to remediate the botnet.

The Justice Department has announced an effort to disrupt a global botnet of hundreds of thousands of infected home and office (SOHO) routers and other networked devices under the control of a group of actors known as the

"Sofacy Group" (also known as "apt28," "sandworm," "x-agent," "pawn storm," "fancy bear" and "sednit").

The group, which has been operating since at least in or about 2007, targets government, military, security organizations, and other targets of perceived intelligence value.

Number 10 (Page 34)

SP 800-71 (DRAFT) Recommendation for Key Establishment Using Symmetric Block Ciphers

Draft NIST Special Publication (SP) 800-71, Recommendations for Key Establishment Using Symmetric Block Ciphers, addresses key establishment techniques that use symmetric key cryptography algorithms to protect symmetric keying material.

The objective is to provide recommendations for reducing exposure to the unauthorized disclosure of the keying material and detecting its unauthorized modification, substitution, insertion or deletion.

Number 1

Global systemically important banks

The Basel Committee issues revised G-SIB framework

The Basel Committee on Banking Supervision released Global systemically important banks: revised assessment methodology and the higher loss absorbency requirement.

When the Basel Committee first published the global systemically important bank (G-SIB) framework in 2011, it agreed to review the framework every three years to allow for the opportunity to enhance the framework, as needed.

	Timetable for implementation	
2018	Jan:	HLA requirement applied to banks designated as G-SIBs in Nov 2016
	Mar:	Collection of end-2017 data
	Nov:	Publish updated list of G-SIBs to be subject to HLA requirement from 1 Jan 2020, and updated denominators and G-SIB indicators of all banks
2019	Jan:	HLA requirement applied to banks designated as G-SIBs in Nov 2017
	Mar:	Collection of end-2018 data
	Nov:	Publish updated list of G-SIBs to be subject to HLA requirement from 1 Jan 2021, and updated denominators and G-SIB indicators of all banks
2020	Jan:	HLA requirement applied to banks designated as G-SIBs in Nov 2018
	Mar:	Collection of end-2019 data
	Nov:	Publish updated list of G-SIBs to be subject to HLA requirement from 1 Jan 2022, and updated denominators and G-SIB indicators of all banks
2021	Jan:	HLA requirement applied to banks designated as G-SIBs published in Nov 2019
	Mar:	Collection of end-2020 data according to the revised methodology published in July 2018
	Nov:	Publish updated list of G-SIBs to be subject to HLA requirement from 1 Jan 2023, and updated denominators and G-SIB indicators of all banks according to the revised methodology
		Complete next methodology review and announce changes

The Committee has concluded the first review of the G-SIB framework. Building on member jurisdictions' experience and the feedback received during last year's public consultation, the Committee has reconfirmed the fundamental structure of the G-SIB framework.

There is general recognition that the framework is meeting its primary objective of requiring G-SIBs to hold higher capital buffers and providing incentives for such firms to reduce their systemic importance.

The decision to maintain the core elements of the G-SIB framework also contributes to the stability of the regulatory environment following the end-2017 finalisation of the Basel III post-crisis reforms.

Based on the review, a number of enhancements to the G-SIB framework have been agreed, including the extension of the scope of consolidation to insurance subsidiaries and the introduction of a trading volume indicator in the substitutability category.

The revised G-SIB assessment methodology is expected to be implemented in member jurisdictions by 2021.

The Committee will complete the next review of the G-SIB framework by 2021.

To read more:
https://www.bis.org/bcbs/publ/d445.pdf

Number 2

Identity and travel document fraud

The different types of document fraud

Criminals and terrorists often make fraudulent use of identity and travel documents in order to carry out their illegal activities.

Both false and genuine documents are used to perpetrate a variety of frauds, which can be classified as follows:

False documents

Counterfeit – a document that constitutes an unauthorized reproduction of a genuine document. These documents are not legitimately manufactured, nor issued or recognized by an official authority.

Forgery – these are typically based on a genuine document, a part of which has been added or altered in order to give misleading information about the person who presents it.

Pseudo document – a document produced with no authority and which is not officially recognized. They can occur in various forms and may have the physical appearance of a passport or an ID card.

Genuine documents

Fraudulently obtained genuine document – an authentic identity or travel document obtained through deception by submission of either false or counterfeit documents, cooperation of a corrupt official or impersonation of the rightful holder of a genuine document.

Misuse of a genuine document through deception by a person who knowingly misrepresents him or herself by using someone else's identity or travel document.

Often, the biographical details and photograph resemble the impostor, helping him or her to pass as the rightful bearer.

To read more:
https://www.interpol.int/News-and-media/Publications2/Fact-sheets2

Number 3

Building the UK financial sector's operational resilience discussion paper

The Bank of England, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) have published a joint discussion paper (DP) on an approach to improve the operational resilience of firms and financial market infrastructures (FMI's).

It envisages that boards and senior management can achieve better standards of operational resilience through increased focus on setting, monitoring and testing specific impact tolerances for key business services, which define the amount of disruption that could be tolerated.

The challenges for operational resilience have become even more demanding given a hostile cyber-environment and large scale technological changes. As recent disruptive events illustrate, operational resilience is a vital part of protecting the UK's financial system, institutions and consumers.

An operational disruption such as one caused by a cyber-attack, failed outsourcing or technological change could impact financial stability by posing a risk to the supply of vital services on which the real economy depends, threaten the viability of individual firms and FMIs, and cause harm to consumers and other market participants in the financial system.

This DP focuses on how the provision of these products and services can be maintained within reasonable tolerances regardless of the cause of disruption. It reinforces the need for firms and FMIs to develop and improve response capabilities so that any wider impact of disruptive events is contained. The speed and effectiveness of communication with the people and institutions most affected, in particular customers, should be at the forefront of every firm's response.

Motivating the approach are a number of important concepts, which include:

- focusing on the continuity of the most important business services as an essential component of managing operational resilience

- setting board-approved impact tolerances which quantify the level of disruption that could be tolerated

- planning on the assumption that disruption will occur as well as seeking to prevent it

The approach to operational resilience set out in this DP is consistent with the Financial Protection Committee's (FPC) recent plans to establish its tolerance for disruption to financial services from cyber incidents, with both focusing on continuity of business services. The supervisory authorities may expect some firms and FMIs to consider the FPC's impact tolerance when they set their own tolerances.

The supervisory authorities are encouraging responses to questions posed in the DP from all types of firms and FMIs, trade associations, consumer bodies, individuals and businesses as users of financial services, and especially those who have suffered harm from disruptive events.

The discussion period ends on 5 October 2018.

To read more:
https://www.fca.org.uk/publications/discussion-papers/dp-18-4-building-uk-financial-sector-operational-resilience

Number 4

Proportionality in banking regulation

Fernando Restoy, Chairman, Financial Stability Institute, Bank for International Settlements, at the Westminster Business Forum Keynote Seminar: Building a resilient UK financial sector - next steps for prudential regulation, structural reform and mitigating risks , London, United Kingdom.

Introduction

Many thanks for the invitation to participate in this prestigious forum.

I am very happy in this distinguished company to have the chance to discuss issues relating to financial regulation. Working for the BIS in Basel, I see my role as providing a global perspective on current policy challenges in the financial domain.

I think that there is a general sense that the post-crisis regulatory reforms have already made substantial progress in meeting their objectives. While it would be a mistake to claim "mission accomplished", the time has certainly come to shift the emphasis from standard setting to ensuring an effective implementation of the agreed reforms.

Within the broad topic of implementation, an area that has attracted much attention worldwide is the question of which institutions should be subject to the new prudential standards.

Or, to put the question differently, what scope do we have to tailor the requirements to a specific subset of institutions that lie outside the perimeter where the Basel standards normally apply. This issue is often referred to as the application of proportionality to banking regulation.

In my remarks I will review the concept, motivation and the constraints associated with the proportionality principle, and I will compare the different approaches in various jurisdictions.

To this end, I will make use of some work we've recently done at the BIS's Financial Stability Institute (FSI).

The concept

The concept of proportionality, embedded in all legal systems, stems from the need to keep the level of public intervention - in the form of rules, restrictions or sanctions - appropriate to what is actually needed to achieve the desired social objectives.

In the field of financial regulation, authorities tend to use the concept of proportionality to justify adjusting the rules imposed on a subsector of regulated institutions in order to lighten their regulatory burden.

In some domains, such as insurance regulation, proportionality aims at promoting the diversity of market participants, the development of the industry and even financial inclusion.

In this domain, therefore, proportionality is effectively a formula for weighing different, and potentially conflicting objectives.

In banking regulation, the concept of proportionality is more frequently used to justify the application of simplified prudential requirements for small or non-complex institutions to avoid excessive compliance costs.

This concept of proportionality entails, in principle, only an adjustment to the complexity of the rules but not necessarily a lower degree of stringency. We will come back to this issue later.

It is interesting to note that the concept of proportionality, when applied to banking regulation, is different to the one used when referring to banking supervision. The latter is roughly a synonym for risk-based oversight and focuses on the adjustment of supervisory intensity to the risk profile of each institution.

Proportionality in supervision thus relates to the objective of employing authorities' scarce resources efficiently while proportionality in regulation refers to reducing the costs faced by the institutions themselves. These two concepts should not be conflated.

The aims

In the debate on the role of proportionality in banking regulation, as a way of reducing compliance costs for small and unsophisticated institutions,

three types of argument are often heard.

First, a political argument: regulation should recognise the social role that small institutions play in facilitating access to credit - and financial services more generally - by households and small firms and their contribution to the development of local and regional economies.

Second, a financial stability argument: concentrated and undiversified banking systems in which a few large institutions prevail are more exposed to systemic crisis and to the too-big-to-fail problem.

And, finally, an economic argument: excessively burdensome regulation for small firms - if not sufficiently justified on prudential grounds - may damage their competitiveness, thereby undermining the level playing field and potentially harming the interest of consumers of banking services (Joosen et al (2018)).

Arguably, not all the above arguments are equally convincing. In particular, the political argument is based on the assumption that large institutions are less able or willing than smaller banks to offer credit and other services to retail customers or small businesses in local communities.

However, to my knowledge, there is no compelling evidence that access to credit in concentrated banking systems (like those of France, Canada or the Netherlands) is generally more cumbersome than in countries with a more diversified banking industry (such as that of Germany).

Some caveats could also be raised in relation to the financial stability argument. In fact, small institutions typically run less diversified business models and are therefore more exposed to adverse developments in specific regions or economic sectors.

Moreover, a proliferation of small institutions does not always imply a more diversified banking sector. Indeed, in the recent past, systemic crisis have occurred as a consequence of the simultaneous failure of several small or medium-sized institutions running similar business models, which were all jointly exposed to the same type of shock, such as the collapse of the housing market.

Finally, recent work by the Financial Stability Board to tackle the too-big-to-fail-problem suggests that this issue can be addressed with an adequate resolution framework for larger firms.

The economic arguments are probably more solid. Basel standards are, in principle, meant to be applied to internationally active groups.

Those banks have complex business models that are subject to a variety of risks, including the ones posed by their own operational complexity. As a consequence, in order to achieve sufficient risk sensitivity, the regulation of large banking groups requires more intricate methods to properly measure those risks in order to determine their coverage.

Yet the Basel standards are often applied to a wider set of banks which may or may not be internationally active. The desire to widen the application of Basel in the domestic markets, even in jurisdictions with no internationally active banks, may be driven by the goal of achieving sufficient homogeneity of the domestic prudential rules as well as promoting the international recognition of their national regulatory framework.

The complexity of the rules implies costs which may be disproportionately higher for smaller - and typically less complex - institutions, as these have less scope for exploiting the economies of scale associated with the compliance function. This is precisely the group of institutions for which risk-sensitive regulation does not need to be excessively complex.

As a consequence, the universal and complete application of the Basel standards within a banking system may generate market distortions as it may unduly penalise the competitive position of a group of entities, without any strong prudential justification.

The constraints

From my vantage point, it may make sense to adjust the regulatory requirements applied to smaller and/or less complex institutions in order to alleviate the excessive regulatory burden that they would otherwise face.

Yet, to be unambiguously positive from a social point of view, the design of such a proportionality regime will need to meet a number of conditions.

First, it should not water down institutions' capacity to absorb losses or face liquidity shocks. Any proportionality regime must focus on reducing complexity without undermining the fundamental prudential safeguards in order to avoid compromising financial stability.

And second, the proportionality regime should not overprotect small or medium-sized institutions against competitive forces.

In particular, proportionality should not generate spurious incentives for banks to remain small or simple if there are competitive forces that promote consolidation, potentially leading to a more efficient banking industry.

Technological developments and overcapacity in some jurisdictions are examples of competitive forces that help to shape market structure.

The modalities

Naturally, different proportionality regimes can work towards the desired objectives in various ways, while meeting the relevant constraints.

In a recent FSI study (Castro Carvalho et al (2017)), we looked at how proportionality is applied in several jurisdictions. The first relevant observation made in the study is that the scope of application of the Basel standards is quite diverse, ranging from a limited application to a few large international banks in the United States to a much wider perimeter in the European Union.

The approaches to tailoring regulatory requirements to different classes of institutions also vary markedly across jurisdictions.

Nevertheless, they could be broadly classified into two main types: what we call a categorisation approach - followed for instance in Switzerland and Brazil - under which banks are classified into a few categories according to their size, or complexity, and a specific set of rules is applied for all banks within each category; and a specific standard approach - now used notably in the European Union and to some extent the United States - for which exceptions are applied to each relevant regulatory obligation (eg liquidity, market risk or reporting requirements) for banks meeting specific criteria.

While the former approach is certainly simpler and more transparent, the latter permits a finer adjustment of the requirements to the characteristics of the supervised institutions. In particular, it allows exemptions or simpler versions of specific requirements to be adopted only for banks for which the original rules are considered unnecessarily complex from a prudential point of view.

The study also shows that, in most jurisdictions, the proportionality regime affects a variety of regulatory requirements. In particular, within Pillar 1, the standards on market and liquidity risk are the ones most often tailored to specific institutions.

Within Pillar 2, proportionality often affects stress testing requirements and procedures for the supervisory review process. Proportionality regimes also typically include simpler reporting and disclosure requirements for small firms.

The analysis shows that proportionality does not normally imply reduced

minimum capital ratios for smaller or less complex institutions. Yet the application of some simplified approaches to assess the solvency, liquidity and risk profile of the institutions and the reduced reporting and disclosure requirements may collectively have prudential relevance.

In particular, the reduced frequency of reporting requirements for small institutions - as is already allowed in some jurisdictions and a subject of discussion in the European Union - may hamper the ability of supervisors to properly monitor emerging risks (Angeloni (2018)).

In view of these prudential considerations, some jurisdictions are considering the possibility of accompanying the application of simplified requirements to some institutions with the introduction of a more demanding coverage of risks.

A case in point is the recent legislation passed by the US Congress in which institutions with a balance sheet below US$ 10 billion may be exempted from meeting standard minimum risk-based capital ratios - which must be calculated in terms of risk-weighted assets - if they keep their leverage ratios - whose calculation is simpler - substantially above the ones required under the Basel standards.

This combination of simplicity with additional stringency would seem to be a promising formula for the calibration of proportionality regimes and one that might be well worth exploring in other jurisdictions.

Some final considerations

To conclude, the increased complexity of the Basel standards strengthens the case for moderating the requirements in some cases - in particular, for institutions where the desired resilience can be ensured without invoking the framework's full complexity.

Yet, there is always a risk that the principle of proportionality could be misused to give a significant regulatory advantage to small institutions. As we have seen, this may not only be unwarranted from a prudential point of view but could also distort competition and prevent a necessary restructuring of the industry.

Arguably, the latter effect may become particularly relevant when technological innovation is likely to disrupt the market, as this will most likely modify the competitive position of traditional banks in varying ways depending on each institution's size, business model, adaptability and other characteristics.

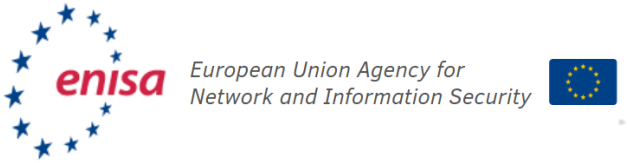
In order to exploit all potential social benefits associated with this innovation, regulation should aim to address emerging risks while minimising the impact on market dynamics and removing obstacles to an efficient restructuring of the sector.

In that context, the European banking sector faces specific challenges. In addition to the disruption that technology is likely to unleash on market structure, the sector may need to enter a phase of consolidation in order to gradually correct the current overcapacity.

For those reasons, the ongoing review of the European prudential legislation should ideally deliver a measured application of the principle of proportionality that is consistent with an orderly reorganisation of the industry.

Number 5

VPNFilter, a Nation State Operation



Introduction

The recent disclosure of a sophisticated malware affecting 500,000 networking devices is making headlines around the world.

It followed several warnings made by manufacturers, security researchers and law enforcement concerning a malicious operation classified as a state sponsored. The malware dubbed VPNFilter - initially affecting Ukrainian hosts - is now spreading over 54 countries at an alarming rate.

Researchers attributed this malware to a Russian state-sponsored hacking group Sofacy (also known as Fancy Bear and APT28) just weeks after the discovery of "Lojack" attack, attributed to the same group.

Researchers were conclusive determining this as a global, broadly deployed threat that is actively seeking to increase its footprint.

Contextual Information

The research of the VPNFilter threat has been ongoing since 2016 leading to a stage where researchers agreed to disclose before concluding it.

The versatile and persistent behaviour of this malware on networking devices is generating great concern among security professionals and authorities around the world.

In its multi-stage and modular capabilities is able to support the collection of intelligence, misattribution and destructive cyberattack operations.

Moreover, it has a range of capabilities including data exfiltration, spying on traffic and ultimately rendering the infected device unbootable.

According to the researcher, the malware code overlaps with versions of the BlackEnergy malware, which was responsible for multiple large-scale attacks that targeted devices in Ukraine.

Known VPNFilter capabilities

- Adopts a multi-stage architecture, in which some of the more complex functionality runs only in the memory of the infected devices;

- Contains a payload capable of self-destructing by overwriting critical portions of the device's firmware and rendering the infected device unbootable. This capability can be triggered individually or en masse, and has the potential of cutting off internet access for hundreds of thousands of victims worldwide;

- Allows C2 anonymous communication over TOR network or SSL-encrypted connections, meaning it will be hard to notice on regular network traffic checks.

- Include typical workhorse intelligence-collection capabilities such as traffic monitoring, file collection, command execution, data exfiltration and device management.

- Modify non-volatile configuration memory (NVRAM) values to add itself to the device crontab (Linux job scheduler) to achieve persistence.

- Downloads images from a gallery (Photobucket) to extract the download server IP address from the GPS six-integer value stored in the EXIF information, to achieve persistence.

- Use the infected device as a hop point before connecting to a final victim obfuscating the true point of origin.

VPNFilter attack vector

VPNFilter attack vector is based on the exploitation of SOHO/NAS network devices vulnerabilities to gain initial access to the targets.

Once the malware gains control over the device, is capable of executing a variety of malicious actions and deploy additional payload in a persistent way.

Researchers were not able to confirm if the exploit of zero-day vulnerabilities is involved in spreading this threat.

VPNFilter Kill-Chain

Installation – The attacker injects malware into devices running firmware version based on Busybox and Linux.

The main purpose is to gain a persistent foothold and enable the download and deployment of additional malware in a persistent way.

Command & Control - Utilizes multiple redundant C2 mechanisms to discover the IP address of deployment servers, making this malware extremely robust and capable of dealing with unpredictable C2 infrastructure changes.

Actions on Objectives – The attack is executed using a variety of capabilities such file collection, command execution, data exfiltration, device management and firmware overwrite among others. Additionally, the malware introduce multiple modules serving as plugins providing additional functionality.

The researcher identified two plugin modules: a packet sniffer for collecting traffic that passes through the device including theft of website credentials and monitoring of Modbus SCADA protocols, and a communications module over the TOR network.

Affected devices

While the research is still ongoing, the current estimated number of infected devices is ca. 500,000 spread over 54 countries. The known device models affected by VPNFilter range from different manufacturers naming Linksys, MikroTik, NETGEAR and TP-Link in the small and home office (SOHO) space, as well at QNAP network-attached storage (NAS) devices. An updated list of affected devices can be found at the researcher's web site.

Mitigation challenges

The targeted devices are frequently found on network perimeters, with no intrusion protection system (IPS) in place, and typically have no available host-based protection system making it more difficult to protect.

Furthermore, affected manufacturers published recommendations to device owners but failed to provide assurance for older versions that have known public exploits and default credentials making the compromise relatively easy. To mitigate this risk, victims are required to hold technical knowledge that in most cases they do not have.

Internet service providers (ISP) play an important role in mitigating this threat. Service providers typically supply these type of devices as part of an internet subscription package, and in some cases, remotely manage them. In this case, ISPs are required to assess which customers are using affected devices and advise on a course of action.

Recent reports reveal that law enforcement agencies such as the FBI, are seizing domains such as “toknowall.com” and “photobucket.com” used by the malware. Researchers and authorities believe that these domains are linked to the Russian group Sofacy, also known by the names “APT28,” “Sandworm,” “X-agent,” “Pawn storm,” “Fancy bear” and “Sednit”. These actions will help containing the incident temporarily, but will not resolve the underlying problem.

Recommendations

- Users of SOHO routers and/or NAS devices to reset them to factory defaults and reboot them in order to remove the potentially destructive, non-persistent malware.

- Ensure that the device is up to date with the most recent firmware/software version by contacting manufacturer.

- Avoid using the default password for the administrator account.

- If possible, install a malware remover tool and run a full scan.

- If the device is not maintain by a service provider, access the device admin page and turn off the remote management option in the advanced settings.

- Internet service providers that remotely maintain SOHO routers to reboot and update the firmware on their customers' behalf.

- ISPs and/or device owners to replace the equipment, if in the list of affected devices.

Closing Remarks

Several factors are determining the seriousness of the VPNFilter threat: the different capabilities that this malware presents, its fast and wide spread and the difficulties in mitigating the risks due to technical and human challenges.

Much is still to uncover while researchers investigate the threat, assess the impact and better understand the malicious actor motivations.

Users, industry, ISPs and law enforcement have a critical role in providing adequate response to this incident, that if not properly contained, may

configure a similar or even higher scale to what was observed last year with the WannaCry and NotPetya aggressive outbreaks.

Number 6

Legal Working Paper Series

The Eurosystem and the Single Supervisory Mechanism: institutional continuity under constitutional constraints

This paper analyses regulatory solutions that have been adopted to address constitutional constraints imposed on the functioning of the Single Supervisory Mechanism (SSM), in which the ECB's exclusive supervisory competence is carried out.

It argues that the operational framework governing the functioning of the SSM has assimilated, to a certain extent, three specific regulatory solutions underpinning the workings of the ESCB/Eurosystem:

1) the (legislative) allocation of certain tasks and responsibilities between ECB internal administrative bodies and structures;

2) the possibility of internal delegation of decision-making powers; and

3) the decentralised exercise of certain of the Union's tasks.

Such a design of the SSM reflects institutional continuity concerning a political choice on how to achieve stage one of a genuine Economic and Monetary Union.

It concludes that the Union operates at its best when centralised decision-making on substantial policy issues is combined with a decentralised operational framework allowing for the meaningful involvement of national administrations in the exercise of Union exclusive competences.

To read more:
https://www.ecb.europa.eu/pub/pdf/scplps/ecb.lwp17.en.pdf?b39bee753107db68032c7238e711ae91

Number 7

Clipboard hijacking malware

National Cyber Security Centre
a part of GCHQ

A newly-discovered clipboard hijacking malware sample has been seen monitoring over 2.3 million cryptocurrency addresses.

The malware scans the Windows Clipboard for cryptocurrency addresses, switching legitimate ones for addresses owned by the attacker. The malware runs in the background and as processes look genuine there are no tell-tale signs of infection.

Clipboard hijacking, however, is not a new threat. Historically, earlier versions of web browsers would allow websites to silently read the data stored on the Windows Clipboard. Today, updated browsers prompt the user on screen to allow access to the clipboard.

In June, a cyber security company identified a clipboard hijacking malware campaign targeting Bitcoin and Ethereum users, infecting over 300,000 computers.

Due to the complex nature of cryptocurrency addresses, transferring funds requires users to copy a destination address from one application into memory and then paste it into the program they are using to send money. Attackers are likely to have noticed this behaviour and created the malware to take advantage of this.

There is no evidence to suggest that any other information is being taken as a result of this clipboard hijacking but, since the clipboard is often used as a place to hold passwords and other sensitive information, users should be vigilant. If you are sending cryptocurrency it is recommended that the destination address is double checked to make sure it has not been replaced with a different one.

As the price and popularity of cryptocurrencies continues to grow, we assess that illicit actors will increase efforts to obtain and profit from them, including through theft, speculation, fraud, illicit mining, and abuse of new cryptocurrency offerings.

It is recommended that devices and software, including antivirus, is kept up-to-date and patched where necessary.

The NCSC has also issued mitigating malware guidance at:
https://www.ncsc.gov.uk/guidance/mitigating-malware

Number 8

Financial stability implications of a prolonged period of low interest rates

Report submitted by a Working Group established by the Committee on the Global Financial System. The Group was co-chaired by Ulrich Bindseil (European Central Bank) and Steven B Kamin (Board of Governors of the Federal Reserve System), July 2018

> *While a low-for-long scenario presents considerable solvency risk for insurance companies and pension funds and limited risk for banks, a snapback would alter the balance of vulnerabilities.*
>
> Philip Lowe, Chair of the Committee on the Global Financial System

Preface

Interest rates have been low in the aftermath of the Global Financial Crisis, raising concerns about financial stability.

In particular, the profitability and strength of financial firms may suffer in an environment of prolonged low interest rates.

Additional vulnerabilities may arise if financial firms respond to "low-for-long" interest rates by increasing risk-taking.

In light of these concerns, the Committee on the Global Financial System (CGFS) mandated a Working Group co-chaired by Ulrich Bindseil (European Central Bank) and Steven B Kamin (Federal Reserve Board of Governors) to identify and provide evidence for the channels through which a "low-for-long" scenario might affect financial stability, focusing on the impact of low rates on banks and on insurance companies and private pension funds (ICPFs).

The following report presents the Group's conclusions about whether prolonged low rates induce fragility in the financial system because of repercussions on banks and ICPFs.

The first message is that while banks should generally be able to cope with solvency challenges in a low-for-long scenario, ICPFs would do less well.

Banks can undertake a number of adjustments to shield profitability from low rates, whereas ICPFs are characterised by negative duration gaps that make them vulnerable to falling interest rates.

The second message is that even though the Working Group identified only a relatively limited amount of additional risk-taking by banks and ICPFs in response to low rates, a low-for-long scenario could still engender material risks to financial stability.

For example, even in the absence of greater risk-taking, a future snapback in interest rates could be challenging for financial institutions.

Banks without sufficient capital buffers could face solvency issues, driven by both valuation and credit losses.

ICPFs, instead, could face liquidity problems, driven either by additional collateral demands linked to losses on derivative positions or by spikes in early liquidations.

The adjustment of financial firms to a low interest rate environment warrants further investigation, especially when low rates are associated with a generalized overvaluation of risky assets.

I hope that this reports provides both a sound rationale for ongoing monitoring efforts and a useful starting point for future analysis.

Philip Lowe
Chair, Committee on the Global Financial System
Governor, Reserve Bank of Australia

To read the report:
https://www.bis.org/publ/cgfs61.pdf

Number 9

Justice Department

Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices

Additional action necessary worldwide to remediate the botnet.

The Justice Department has announced an effort to disrupt a global botnet of hundreds of thousands of infected home and office (SOHO) routers and other networked devices under the control of a group of actors known as the "Sofacy Group" (also known as "apt28," "sandworm," "x-agent," "pawn storm," "fancy bear" and "sednit").

The group, which has been operating since at least in or about 2007, targets government, military, security organizations, and other targets of perceived intelligence value.

Assistant Attorney General for National Security John C. Demers, U.S. Attorney Scott W. Brady for the Western District of Pennsylvania, Assistant Director Scott Smith for the FBI's Cyber Division, FBI Special Agent in Charge Robert Johnson of the Pittsburgh Division and FBI Special Agent in Charge David J. LeValley of the Atlanta Division made the announcement.

"The Department of Justice is committed to disrupting, not just watching, national security cyber threats using every tool at our disposal, and today's effort is another example of our commitment to do that," said Assistant Attorney General Demers. "This operation is the first step in the disruption of a botnet that provides the Sofacy actors with an array of capabilities that could be used for a variety of malicious purposes, including intelligence gathering, theft of valuable information, destructive or disruptive attacks, and the misattribution of such activities."

"The United States Attorney's Office will continue to aggressively fight against threats to our national security by criminals, no matter who they work for" said U.S. Attorney Brady. "This court-ordered seizure will assist in the identification of victim devices and disrupts the ability of these

hackers to steal personal and other sensitive information and carry out disruptive cyber attacks. We will be relentless in protecting the people of Western Pennsylvania - from international corporations to local businesses to the elderly - from these threats."

"Today's announcement highlights the FBI's ability to take swift action in the fight against cybercrime and our commitment to protecting the American people and their devices," said Assistant Director Scott Smith. "By seizing a domain used by malicious cyber actors in their botnet campaign, the FBI has taken a critical step in minimizing the impact of the malware attack. While this is an important first step, the FBI's work is not done. The FBI, along with our domestic and international partners, will continue our efforts to identify and expose those responsible for this wave of malware."

"The FBI will not allow malicious cyber actors, regardless of whether they are state-sponsored, to operate freely," said FBI Special Agent in Charge Bob Johnson. "These hackers are exploiting vulnerabilities and putting every American's privacy and network security at risk. Although there is still much to be learned about how this particular threat initially compromises infected routers and other devices, we encourage citizens and businesses to keep their network equipment updated and to change default passwords."

"This action by the FBI, DOJ, and our partners should send a clear message to our adversaries that the U.S. Government will take action to mitigate the threats posed by them and to protect our citizens and our allies even when the possibility of arrest and prosecution may not be readily available," said FBI Special Agent in Charge David J. LeValley. "As our adversaries' technical capabilities evolve, the FBI and its partners will continue to rise to the challenge, placing themselves between the adversaries and their intended victims."

The botnet, referred to by the FBI and cyber security researchers as "VPNFilter," targets SOHO routers and network-access storage (NAS) devices, which are hardware devices made up of several hard drives used to store data in a single location that can be accessed by multiple users. The VPNFilter botnet uses several stages of malware. Although the second stage of malware, which has the malicious capabilities described above, can be cleared from a device by rebooting it, the first stage of malware persists through a reboot, making it difficult to prevent reinfection by the second stage.

In order to identify infected devices and facilitate their remediation, the U.S. Attorney's Office for the Western District of Pennsylvania applied for

and obtained court orders, authorizing the FBI to seize a domain that is part of the malware's command-and-control infrastructure. This will redirect attempts by stage one of the malware to reinfect the device to an FBI-controlled server, which will capture the Internet Protocol (IP) address of infected devices, pursuant to legal process. A non-profit partner organization, The Shadowserver Foundation, will disseminate the IP addresses to those who can assist with remediating the VPNFilter botnet, including foreign CERTs and internet service providers (ISPs).

Owners of SOHO and NAS devices that may be infected should reboot their devices as soon as possible, temporarily eliminating the second stage malware and causing the first stage malware on their device to call out for instructions. Although devices will remain vulnerable to reinfection with the second stage malware while connected to the Internet, these efforts maximize opportunities to identify and remediate the infection worldwide in the time available before Sofacy actors learn of the vulnerability in their command-and-control infrastructure.

The FBI and the Department of Homeland Security have also jointly notified trusted ISPs. The Department and the FBI also encourage users and administrators to review the Cisco blog post on VPNFilter, for recommendations and to ensure that their devices are updated with the latest patches.

The efforts to disrupt the VPNFilter botnet were led by the FBI's Pittsburgh and Atlanta Offices; FBI Cyber Division; Trial Attorney Matthew Chang of the National Security Division's Counterintelligence and Export Control Section; and Assistant U.S. Attorneys Charles Eberle and Soo C. Song of the Western District Pennsylvania. Critical assistance was also provided by Richard Green of the Criminal Division's Computer Crime and Intellectual Property Section and The Shadowserver Foundation.

Number 10

SP 800-71 (DRAFT)
Recommendation for Key Establishment Using Symmetric Block Ciphers

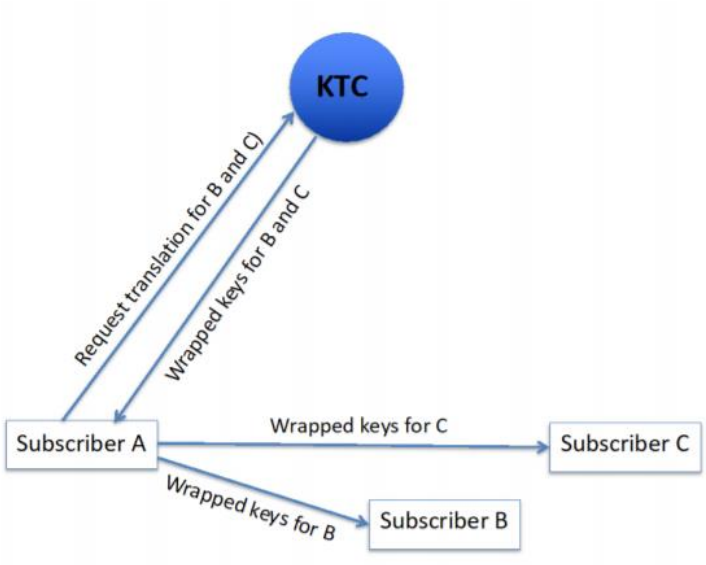
NIST
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

Draft NIST Special Publication (SP) 800-71, Recommendations for Key Establishment Using Symmetric Block Ciphers, addresses key establishment techniques that use symmetric key cryptography algorithms to protect symmetric keying material.

The objective is to provide recommendations for reducing exposure to the unauthorized disclosure of the keying material and detecting its unauthorized modification, substitution, insertion or deletion.

The Recommendation also addresses recovery in the event of detectable errors during the key-distribution process. Wrapping mechanisms are specified for encrypting keys, binding key control information to the keys and protecting the integrity of this information.

To read the paper:
https://csrc.nist.gov/CSRC/media/Publications/sp/800-71/draft/documents/sp800-71-draft.pdf



Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

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 context of enforcement or similar regulatory action;

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

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- 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.

The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

International Association of Risk and Compliance Professionals

You can explore what we offer to our members:

1. Membership – Become a standard, premium or lifetime member.

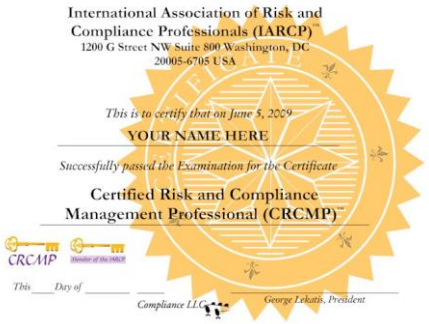
You may visit:
www.risk-compliance-association.com/How_to_become_member.htm

Become a lifetime member of the association, and to continue your journey without interruption and without renewal worries. You will get a lifetime of benefits as well.

You can check the benefits at:
www.risk-compliance-association.com/Lifetime_Membership.htm

2. Weekly Updates - Subscribe to receive every Monday, the Top 10 risk and compliance management related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next:
http://forms.aweber.com/form/02/1254213302.htm

3. Training and Certification - The Certified Risk and Compliance Management Professional (CRCMP) training and certification program has become one of the most recognized programs in risk management and compliance.



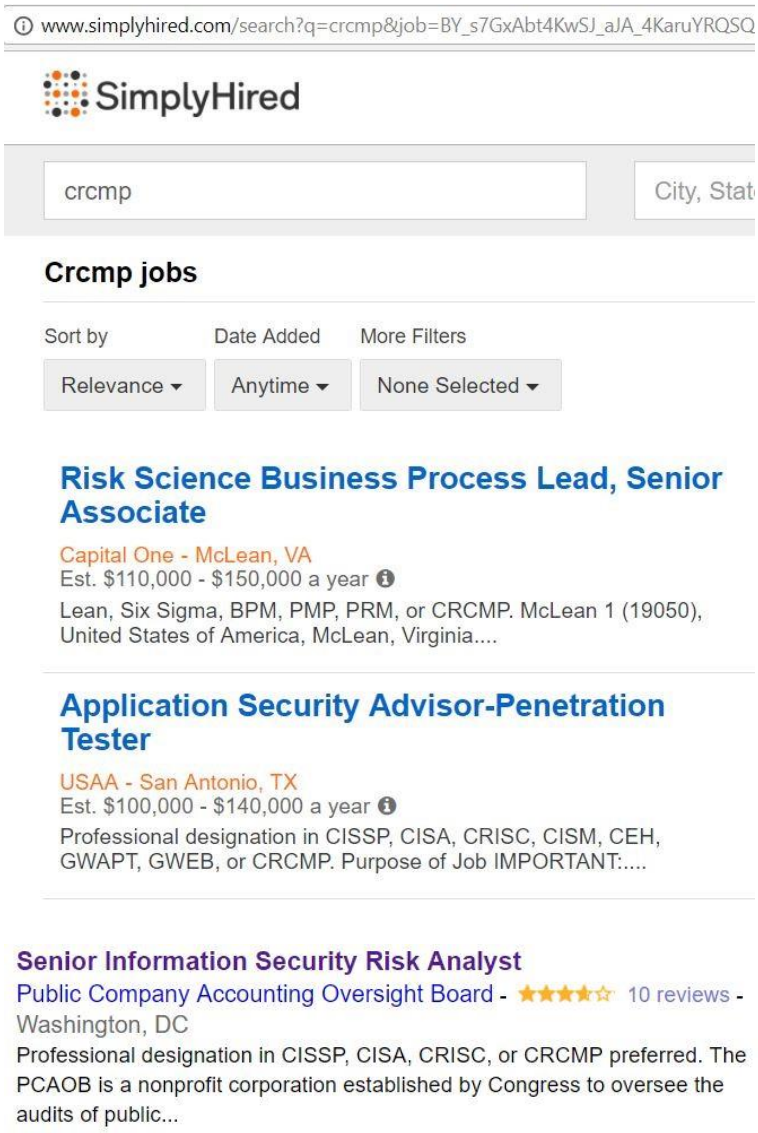
There are CRCMPs in 32 countries around the world. Companies and organizations like Accenture, American Express, USAA etc. consider the CRCMP a preferred certificate.

You can find more about the demand for CRCMPs at:
www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf

For the distance learning programs, you may visit:
www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For instructor-led training, you may contact us. We can tailor all programs to meet specific requirements. We tailor presentations, awareness and training programs for supervisors, boards of directors, service providers and consultants.

Some CRCMP jobs:



4. IARCP Authorized Certified Trainer (IARCP-ACT) Program - Become a Certified Risk and Compliance Management Professional Trainer (CRCMPT) or Certified Information Systems Risk and Compliance Professional Trainer (CISRCPT).

This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.
Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

To learn more, you may visit:

www.risk-compliance-association.com/IARCP_ACT.html

5. Approved Training and Certification Centers (IARCP-ATCCs) - In response to the increasing demand for CRCMP training, the International Association of Risk and Compliance Professionals is developing a world-wide network of Approved Training and Certification Centers (IARCP-ATCCs).

This will give the opportunity to risk and compliance managers, officers, and consultants to have access to instructor-led CRCMP and CISRCP training at convenient locations that meet international standards.

ATCCs use IARCP approved course materials and have access to IARCP Authorized Certified Trainers (IARCP-ACTs).

To learn more:
www.risk-compliance-association.com/Approved_Centers.html