Monday, January 11, 2021

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,

According to Benoît Cœuré, head of the BIS Innovation Hub, the swift response to Covid-19 of governments, central banks, and supervisors to mitigate the immediate impact on the real economy has stabilized what could have been catastrophic for global markets.

With mass vaccinations in sight, the policy focus is now shifting from liquidity provision and stabilization to addressing the long-term scars of the crisis: enabling capital and labor reallocation across industries, and avoiding permanent output losses.

He said: "Spurred by regulators, banks have built capital and liquidity buffers, improved risk management practices and internalised the social cost of risk-taking. Thanks to these efforts, they were better prepared to cope with a shock in 2020 than they were in 2008.

The jury is still out as to whether all this will suffice to prevent the initial liquidity crisis from morphing into a solvency one. While the scale is unclear at this stage, economic growth and forward-looking indicators of default risk already suggest that bankruptcies will rise significantly by the end of 2021.

On the other hand, credit spreads are fairly tight, raising concerns about a possible disconnect with fundamentals.

Looking ahead, it will be essential that banks make use of the available capital buffers to absorb losses without excessive deleveraging. As Carolyn Rogers, the Secretary-General of the Basel Committee on Banking

Supervision, recently emphasised, it is too early for banks to take a victory lap over their response to Covid-19.

Holding back on their discretionary distributions of capital makes sense."

This is what I find particularly interesting in the presentation:

" The pandemic's immediate consequence has been a change in the way we work. We are experiencing, at first hand, global collaboration through technology and platforms.

Covid-19 has also accelerated trends in digital innovation that were already well under way.

Consumers in many countries have stepped up their use of contactless payments, and as physical stores temporarily closed, e-commerce activity surged.

Yet, the pandemic has highlighted both progress and shortcomings in areas such as payments.

There is certainly no silver bullet, but what is clear is that international collaboration is essential – to underpin technological capabilities, ensure interoperability between national systems, enhance cross border payments and remittances, support financial inclusion, and prevent geographical and social fragmentation.

This is the essence of the roadmap from the FSB and the Committee on Payments and Market Infrastructures (CPMI) for enhancing cross-border payments, as endorsed by G20 finance ministers and central bank governors in October and actively supported by the BIS.

In the past few years, some big techs have entered credit markets, either directly or in partnership with financial institutions.

The expanded use of digital payments brought about by Covid-19 could fuel a rise in digital lending as companies accumulate consumer data and enhance credit analytics.

This in turn presents new and complex trade-offs between financial stability, competition and data protection.

To identify these trade-offs, design sound regulatory answers and continue to fulfil their mission in a rapidly changing environment, central banks need to be at the cutting edge of technology."

This was an interesting presentation. I remember the recent speech from Randal K. Quarles, vice chair for supervision of the Federal Reserve Board of Governors (since October 2017). He has said:

"In March of this year, customers of U.S. banks drew down nearly $480 billion on existing lines of credit to cover cash needs during the severe disruption in revenues in the early days of the COVID event—by far the largest monthly increase in history.

Banks were able to fund these loans without notable problems in part by drawing on liquidity buffers created by the new regulatory system. They have not only maintained, but actually increased their capital during this time—notwithstanding the large provisions taken earlier in the year.

And they have continued to extend credit throughout the protracted evolution of the COVID event, to this point largely satisfying the demand for credit in the economy."

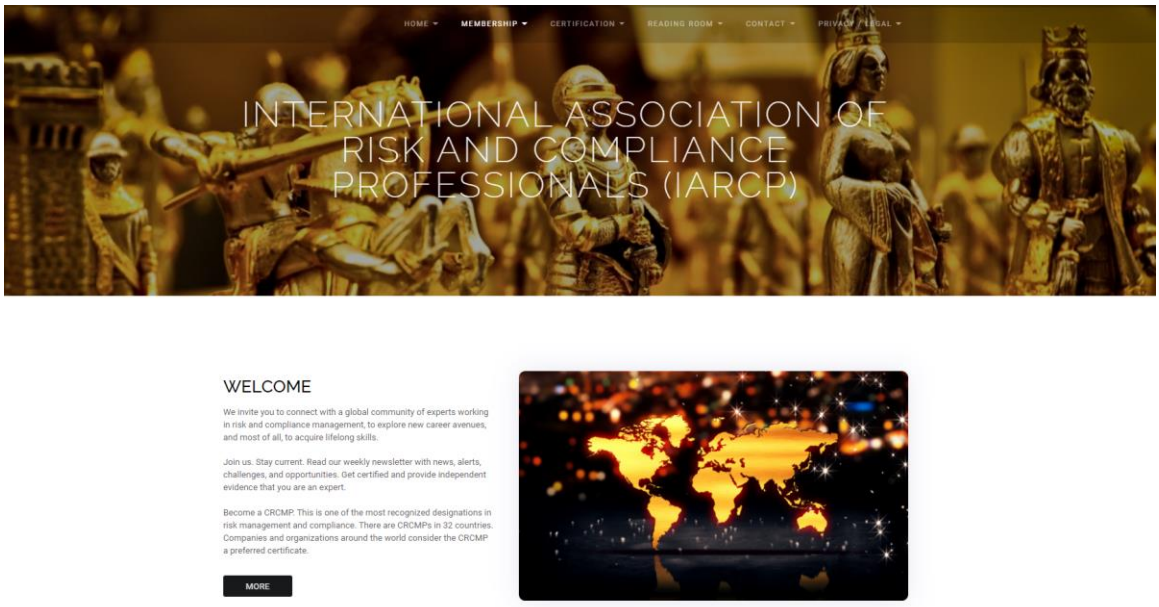
Read more at number 1 below. Welcome to the top 10 list.

Best regards,

George Lekatis

George Lekatis
President of the IARCP
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

Visit our updated website: https://www.risk-compliance-association.com



Number 1 (Page 7)

The financial system after Covid-19

Keynote speech by Mr Benoît Cœuré, Head of the BIS Innovation Hub, at the European Stability Mechanism fourth research seminar of the Regional Financing Arrangements.

Number 2 (Page 10)

NIST Releases Draft Guidance on Internet of Things Device Cybersecurity

Four new documents will help align manufacture and federal procurement of secure IoT devices.

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

Number 3 (Page 13)

Cloud Certification Scheme: Building Trusted Cloud Services Across Europe

ENISA launches a public consultation on a new draft candidate cybersecurity certification scheme in a move to enhance trust in cloud services across Europe.

enisa
European Network and Information Security Agency

Number 4 (Page 16)

Climate-related Financial Disclosures (TCFD)

FSB encourages the IFRS Foundation and authorities to use TCFD's recommendations as the basis for climate-related financial risk disclosures

FSB FINANCIAL STABILITY BOARD

Number 5 (Page 18)

EBA updates reporting framework 3.0 and technical standards on Pillar 3 disclosure

Number 6 (Page 20)

Consumer guide: What should you do if you have a life insurance policy or pension from the UK?

Number 7 (Page 22)

Guidance issued as SolarWinds compromised

Number 8 (Page 24)

Law enforcement wiretapped the very service used by criminals to evade interception

CYBERCRIMINALS' FAVOURITE VPN TAKEN DOWN IN GLOBAL ACTION

Number 9 (Page 26)

21 arrests in nationwide cyber crackdown

Number 10 (Page 28)

NIST Software Tool Improves Your Doctor's Vaccination Advice

Agency's testing tools have increased the correctness and consistency of computerized vaccination recommendations.

Number 1

The financial system after Covid-19

Keynote speech by Mr Benoît Cœuré, Head of the BIS Innovation Hub, at the European Stability Mechanism fourth research seminar of the Regional Financing Arrangements.

Introduction

Distinguished guests, ladies, and gentlemen,

Thank you for inviting me. It is a pleasure to join you virtually today at the fourth research seminar of the Regional Financing Arrangements. And, as a topic, the financial sector landscape post-Covid-19 could not be more timely.

The year 2020 will go down in history as one of the last century's most serious health crises and global economic contractions. The swift response of governments, central banks, and supervisors to mitigate the immediate impact on the real economy has stabilised what could have been catastrophic for global markets.

With mass vaccinations in sight, the policy focus is now shifting from liquidity provision and stabilisation to addressing the long-term scars of the crisis: enabling capital and labour reallocation across industries, and avoiding permanent output losses.

For such reallocation to happen, and to address longerterm sustainability challenges, we need a financial system which is fit for purpose. Could Covid-19 give us the chance to strengthen it?

In my remarks today, I will argue that we first need to draw the lessons of the crisis, and I will focus on two dimensions.

First, there are the known challenges. The reforms after the Great Financial Crisis (GFC) had the effect of pushing risks outside the banking system, as non-bank financial intermediaries (NBFIs) started to fill in the gaps.

We knew it before Covid-19 and the crisis has confirmed it. What does this tell us about the resilience of this new system? Second, there are the unknown challenges.

The crisis has speeded the digitalisation of our economies, accelerating shifts in how companies and individuals work, save and spend. How can technology support the digitalisation of the financial sector post-Covid-19, and can it help regulators make the sector safe and sustainable?

The lessons of Covid-19 for financial sector resilience

Spurred by regulators, banks have built capital and liquidity buffers, improved risk management practices and internalised the social cost of risk-taking. Thanks to these efforts, they were better prepared to cope with a shock in 2020 than they were in 2008.

The jury is still out as to whether all this will suffice to prevent the initial liquidity crisis from morphing into a solvency one. While the scale is unclear at this stage, economic growth and forwardlooking indicators of default risk already suggest that bankruptcies will rise significantly by the end of 2021.

On the other hand, credit spreads are fairly tight, raising concerns about a possible disconnect with fundamentals.

Looking ahead, it will be essential that banks make use of the available capital buffers to absorb losses without excessive deleveraging.

As Carolyn Rogers, the Secretary-General of the Basel Committee on Banking Supervision, recently emphasised, it is too early for banks to take a victory lap over their response to Covid-19.

Holding back on their discretionary distributions of capital makes sense.

Even though the banking sector was not at the epicentre, the turmoil highlighted structural vulnerabilities in the NBFIs sector and the market structures supporting them.

These vulnerabilities have become more important post-GFC, as the footprint of NBFIs has grown – accounting for almost 50% of total financial intermediation globally – and as banks have retreated from certain activities, such as market-making, to preserve balance sheet capacity.

The first weeks of the Covid-1 crisis revealed that the matching and price discovery mechanisms were impaired in large swathes of the capital

markets. As conditions worsened, demand soared for cash and near-cash, or short-dated assets. In such circumstances, market liquidity can be as crucial to financial stability as bank solvency or bank liquidity.

As events unfolded, central banks had to intervene to ensure financial stability.

To read more: https://www.bis.org/speeches/sp201217.pdf

Number 2

NIST Releases Draft Guidance on Internet of Things Device Cybersecurity

Four new documents will help align manufacture and federal procurement of secure IoT devices.

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

As the Internet of Things (IoT) grows to connect an amazing diversity of devices to electronic networks, four new publications from the National Institute of Standards and Technology (NIST) offer recommendations to federal agencies and manufacturers alike concerning effective cybersecurity for these devices.

The four related publications will help address challenges raised in the recently signed IoT Cybersecurity Improvement Act of 2020 and begin to provide the guidance that law mandates.

Together, the four documents — NIST Special Publication (SP) 800-213 and NIST Interagency Reports (NISTIRs) 8259B, 8259C and 8259D — form a unit intended to help ensure the government and IoT device designers are on the same page with regard to cybersecurity for IoT devices used by federal agencies.

The four documents:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213-draft.pdf

Draft NIST Special Publication 800-213

IoT Device Cybersecurity Guidance for the Federal Government:

Establishing IoT Device Cybersecurity Requirements

https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259B-draft.pdf

Draft NISTIR 8259B

IoT Non-Technical Supporting Capability Core Baseline

https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259C-draft.pdf

Draft NISTIR 8259C

Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline

https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259D-draft.pdf

Draft NISTIR 8259D

Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government

"The three NISTIRs offer a suggested starting point for manufacturers who are building IoT devices for the federal government market, while the SP provides guidance to federal agencies on what they should ask for when they acquire these devices," said NIST's Katerina Megas, program manager for NIST's Cybersecurity for IoT Program. "We look forward to the community's feedback on these drafts as we work to provide IoT cybersecurity guidance that aids both vendors and customers."

As is the case with all NIST publications, the guidance itself is not regulatory. However, NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal systems.

Because companies that do business with government agencies will need to interact with technology the government finds acceptable, the guidance is likely to have far-reaching influence.

SP 800-213 provides overall guidance for federal agencies, extending NIST's risk-based cybersecurity approach to include integration of IoT devices into federal information systems and infrastructure.

The document has background and recommendations to help agencies consider what security capabilities an IoT device needs to provide for the agency to integrate it into its federal information system.

The NISTIR 8259 series provides guidance that IoT device manufacturers can use to help organizations implement SP 800-213's guidance. Two

publications in this series, NISTIR 8259 and NISTIR 8259A, were released previously, bringing the current total in the series to five.

Megas describes these two earlier publications as a set of foundational activities to help manufacturers meet their customers' cybersecurity needs.

"These two previous publications outline a process and starting point for manufacturers to identify the capabilities a customer will expect," she said. "If you buy a device, you would want to be sure you can see and identify the device on your network and change its password, for example. It articulates those kinds of features on a high level."

The three new publications extend the landscape of the first two. NISTIR 8259B complements 8259A with guidance on nontechnical processes manufacturers should implement that support cybersecurity, such as documenting updates and informing customers of how to implement them.

NISTIR 8259D begins to get more particular, helping manufacturers consider the needs of a specific market sector — in this case, the U.S. federal government.

NISTIR 8259C describes the process NIST followed to develop 8259D, so that manufacturers in other markets — such as medical devices that would have to meet health information privacy requirements — can use that same process if they desire to do so.

"We help a manufacturer start with a baseline set of capabilities and then tailor it to their market needs," Megas said. "Whoever they are, we want to help them improve their security in a world where things are still developing."

More details about how the publications relate to one another are available in a NIST blog post:
https://www.nist.gov/blogs/cybersecurity-insights/rounding-your-iot-security-requirements-draft-nist-guidance-federal

Number 3

Cloud Certification Scheme: Building Trusted Cloud Services Across Europe

ENISA launches a public consultation on a new draft candidate cybersecurity certification scheme in a move to enhance trust in cloud services across Europe.

The European Union Agency for Cybersecurity (ENISA) launched a public consultation, which runs until 7 February 2021, on its draft of the candidate European Union Cybersecurity Certification Scheme on Cloud Services (EUCS).

The scheme aims to further improve the Union's internal market conditions for cloud services by enhancing and streamlining the services' cybersecurity guarantees.

The draft EUCS candidate scheme intends to harmonise the security of cloud services with EU regulations, international standards, industry best practices, as well as with existing certifications in EU Member States.

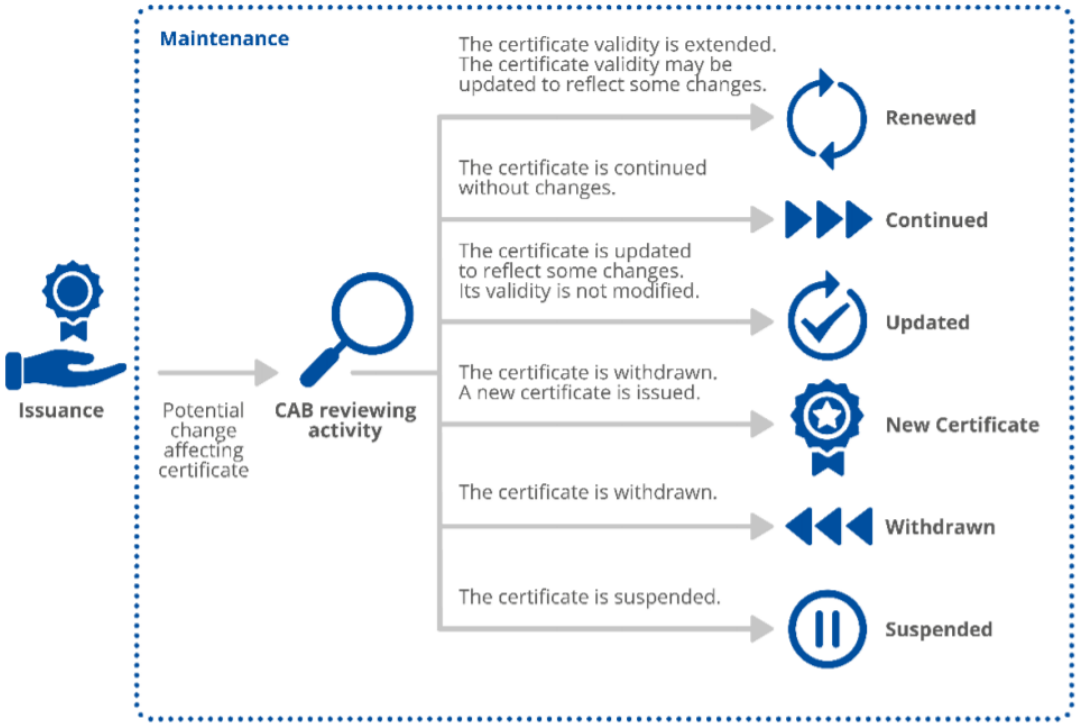
EU Agency for Cybersecurity Executive Director Juhan Lepassaar said: "Cloud services play an increasing role in the life of European citizens and businesses under lockdown; and their security is essential to the functioning of the Digital Single Market. A single European cloud certification is critical for enabling the free flow of data across Europe, and is an important factor in fostering innovation and competitiveness in Europe."

Speaking at the ENISA Cybersecurity Certification Conference on 18 December 2020, Director of Digital Society, Trust and Cybersecurity at the European Commission Directorate-General for Communications Networks, Content and Technology (DG CONNECT) Lorena Boix Alonso said: "We must ensure that cybersecurity certification strikes the right balance, following a sensible risk-based approach, with flexible solutions and certification schemes designed to avoid being outdated quickly. And we need a clear roadmap to allow industry, national authorities and standardisation bodies to prepare in advance."

There are challenges to the certification of cloud services, such as a diverse set of market players, complex systems and a constantly evolving landscape of cloud services, as well as the existence of different schemes in Member

States. The draft EUCS candidate scheme tackles these challenges by calling for cybersecurity best practices across three levels of assurance and by allowing for a transition from current national schemes in the EU.

Figure 2: Processes related to the issuance and maintenance of a certificate



The draft EUCS candidate scheme is a horizontal and technological scheme that intends to provide cybersecurity assurance throughout the cloud supply chain, and form a sound basis for sectoral schemes.

More specifically, the draft EUCS candidate scheme:

- Is a voluntary scheme;
- The scheme's certificates will be applicable across the EU Member States;
- Is applicable for all kinds of cloud services – from infrastructure to applications;
- Boosts trust in cloud services by defining a reference set of security requirements;
- Covers three assurance levels: 'Basic', 'Substantial' and 'High';
- Proposes a new approach inspired by existing national schemes and international standards;
- Defines a transition path from national schemes in the EU;
- Grants a three-year certification that can be renewed;

- Includes transparency requirements such as the location of data processing and storage.

To read more:
https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/

Number 4

Climate-related Financial Disclosures (TCFD)

FSB encourages the IFRS Foundation and authorities to use TCFD's recommendations as the basis for climate-related financial risk disclosures

Globally consistent and comparable disclosures by companies of their climate-related financial risks are increasingly important to market participants and financial authorities as a means to give financial markets the information they need to manage risks, and seize opportunities, stemming from climate change.

The FSB created the Task Force on *Climate-related Financial Disclosures (TCFD)* in 2015 to develop a set of voluntary disclosure recommendations for use by companies in providing decision-useful information to investors, lenders and insurance underwriters about the climate-related financial risks that companies face.

The TCFD published its disclosure recommendations in 2017.

Since then, nearly 1,700 organisations have expressed their support for the TCFD recommendations.

Nearly 60% of the world's 100 largest public companies support the TCFD, report in line with the TCFD recommendations, or both.

The TCFD continues to promote and monitor adoption of its recommendations worldwide and issued supplementary guidance to support implementation.

Alongside this industry-led progress in promoting consistent voluntary climate-related disclosures, a growing number of official sector initiatives are developing requirements or guidance at the national or regional level, or considering the development of international standards.

It is important that steps by the official sector and private sector are well aligned in promoting globally consistent disclosures and avoiding fragmentation.

The FSB therefore welcomes the recommended approach by the Trustees of the IFRS Foundation to initially focus on standards for climate-related financial disclosures, as set out in the September 2020 IFRS Consultation Paper on Sustainability Reporting.

The initial focus on climate-related information would be appropriate given the growing interest of investors in the topic for financial risk management and the importance of global consistency in the actions that are already beginning to be taken by national and regional authorities to develop requirements and guidance in this area.

Such internationally agreed minimum standards for disclosures would, as usual, not preclude individual authorities from going further if they wish.

The FSB strongly encourages the IFRS Foundation to build on the work of the TCFD, by using the TCFD's recommendations as the basis for standards for climate-related financial disclosures.

The TCFD recommendations set out a comprehensive framework that has been developed by, and is directly responsive to the needs of, users and preparers of financial filings across a range of financial and non-financial sectors around the world.

The TCFD's recommendations have attracted widespread support from users and preparers.

The FSB strongly encourages national or regional authorities that are developing requirements or guidance for climate-related disclosures to consider using the TCFD recommendations as the basis.

Such consistency in approach would help to avoid the risk of market fragmentation, both across jurisdictions, and between requirements and guidance being developed today and international standards that may be introduced in the future.

To further promote global coordination, the FSB will explore with standard-setters and other international bodies ways to promote globally comparable, high-quality and auditable standards of disclosure based on the TCFD recommendations.

The FSB will report to the G20 Finance Ministers and Central Bank Governors meeting on progress in this area in July 2021.

Number 5

EBA updates reporting framework 3.0 and technical standards on Pillar 3 disclosure

The European Banking Authority (EBA) published an update to the reporting framework 3.0 and the Implementing Technical Standards (ITS) on institutions' Pillar 3 public disclosures.

These updates are the result of the European Commission's adoption of the ITS on Supervisory Reporting (v3.0) on 17 December, the EBA publication of the revised version of the mapping between disclosures and reporting, and the EBA release of phase 1 of its technical package on the reporting framework v3.0.

EC adoption of ITS on Supervisory Reporting (v3.0)

The EBA updated its website to reflect the European Commission's adoption of the Supervisory Reporting Implementing Act and its Annexes, which included changes introduced by the revised Capital Requirements Regulations (CRR2) and the Prudential Backstop Regulation.

Mapping between Pillar 3 ITS on Disclosures and ITS on Supervisory Reporting (v3.0)

The Pillar 3 ITS on institutions' public disclosures have been developed to foster consistency across supervisory reporting.

The EBA has updated the mapping of quantitative disclosure data and supervisory reporting, which aims at facilitating institutions' compliance and improving the consistency and quality of the information disclosed.

The EBA also published a file summarizing the frequency at which each type of institution should disclose each template and table, in accordance with the CRR2.

Phase 1 of technical package of reporting framework (v3.0)

The technical package of the reporting framework provides the standard specifications for the implementation of the EBA reporting requirements.

The package includes the validation rules, the Data Point Model (DPM) data dictionary and the XBRL taxonomies for v3.0.

The EBA also updated the DPM query tool. Finally, the technical package includes reporting requirements on FINREP, COREP, own funds (including the Fundamental Review of the Trading Book - FRTB), COREP liquidity, asset encumbrance, large exposures, leverage ratio and G-SII data.

To read more:
https://eba.europa.eu/eba-updates-reporting-framework-30-and-technical-standards-pillar-3-disclosure

Number 6

Consumer guide: What should you do if you have a life insurance policy or pension from the UK?

This consumer guide provides practical information for consumers with a life insurance policy or pension from the UK and living in the European Union or considering moving residence from the UK to the EU.

You may visit:
https://www.eiopa.europa.eu/sites/default/files/publications/consumer_guide_brexit_final.pdf

Number 7

Guidance issued as SolarWinds compromised

National Cyber Security Centre

SolarWinds, a popular IT system management platform has been compromised and could be used for further attacks on connected systems.

As a result of a cyber attack of their systems, an attacker was able to add a malicious modification to SolarWinds Orion products which allows them to send administrator-level commands to any affected installation. This modification causes the Orion products to connect to an attacker-controlled server to request instructions and does not rely on the attacker being able to directly connect from the internet to the Orion server.

Not all customers who have an installation with the unauthorised, malicious modification will have been seriously affected, but all should take immediate action.

The NCSC has been working closely with international partners as well as FireEye - a cyber security organisation who discovered the compromise. In a statement issued earlier this week, we recommended that organisations ensure any affected instances of SolarWinds Orion are installed behind firewalls disabling internet access (both outbound and inbound) for the instances.
The statement:
https://www.ncsc.gov.uk/news/ncsc-statement-on-fireeye-incident

The NCSC has now also published full guidance highlighting immediate actions for all organisations using the SolarWinds Orion suite of IT management tools. You may visit:
https://www.ncsc.gov.uk/guidance/dealing-with-the-solarwinds-orion-compromise

We would also recommend further reading:

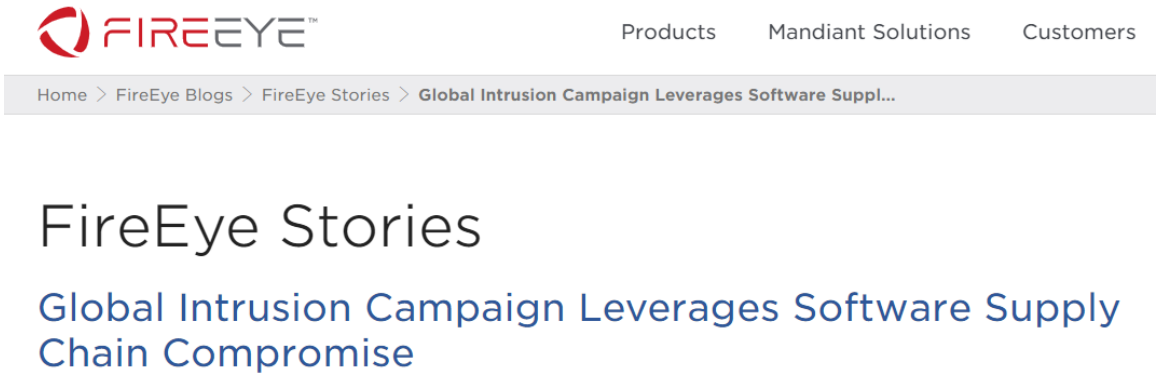
solarwinds

PRODUCTS › SOLUTIONS › SUPPORT › COMMUNITY › FREE TRIALS

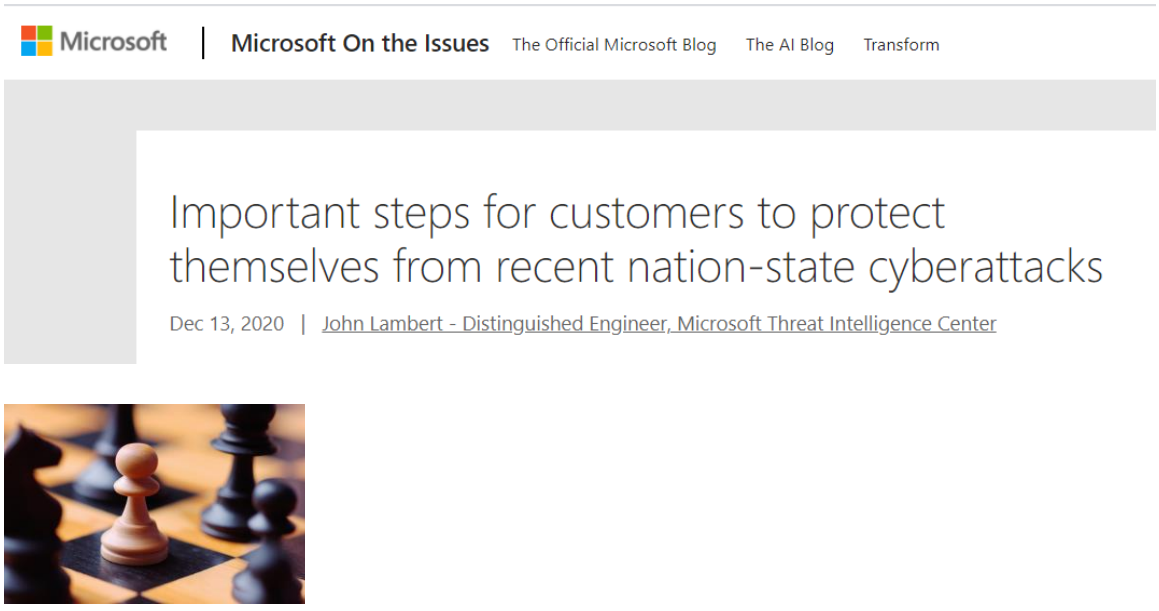
SolarWinds Security Advisory

1. SolarWinds have published a security advisory on this incident including details of affected software and the vendor's advice. You may visit: https://www.solarwinds.com/securityadvisory

2. FireEye has published a blog on its investigation. This includes extensive technical details which may help in investigation of a suspected server compromise. You may visit: https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html



3. Microsoft has also published a blog on this attack which includes other potential routes for investigation of compromise. You may visit: https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/



Number 8

Law enforcement wiretapped the very service used by criminals to evade interception

CYBERCRIMINALS' FAVOURITE VPN TAKEN DOWN IN GLOBAL ACTION

The virtual private network (VPN) Safe-Inet used by the world's foremost cybercriminals has been taken down yesterday in a coordinated law enforcement action led by the German Reutlingen Police Headquarters together with Europol and law enforcement agencies from around the world.

The Safe-Inet service was shut down and its infrastructure seized in Germany, the Netherlands, Switzerland, France and the United States. The servers were taken down, and a splash page prepared by Europol was put up online after the domain seizures. This coordinated takedown was carried out in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT). You may visit:
https://www.europol.europa.eu/empact

Turning the table on the criminals

Active for over a decade, Safe-Inet was being used by some of the world's biggest cybercriminals, such as the ransomware operators responsible for ransomware, E-skimming breaches and other forms of serious cybercrime.

This VPN service was sold at a high price to the criminal underworld as one of the best tools available to avoid law enforcement interception, offering up to 5 layers of anonymous VPN connections.

Law enforcement were able to identify some 250 companies worldwide which were being spied on by the criminals using this VPN. These companies were subsequently warned of an imminent ransomware attack against their systems, allowing them to take measures to protect themselves against such an attack.

The service has now been rendered inaccessible.

Investigations are ongoing in a number of countries to identify and take action against some of Safe-Inet's users.

International cyber sweep

International police cooperation was central to the success of this investigation as the critical infrastructure was scattered across the world.

Europol's European Cybercrime Centre (EC3) supported the investigation from the onset, bringing together all the involved countries to establish a joint strategy and to organise the intensive exchange of information and evidence needed to prepare for the final phase of the takedown.

The Police President of the Reutlingen Police Headquarters, Udo Vogel, said:

"The investigation carried out by our cybercrime specialists has resulted in such a success thanks to the excellent international cooperation with partners worldwide. The results show that law enforcement authorities are equally as well connected as criminals."

The Head of Europol's European Cybercrime Centre, Edvardas Šileris, said:

"The strong working relationship fostered by Europol between the investigators involved in this case on either side of the world was central in bringing down this service. Criminals can run but they cannot hide from law enforcement, and we will continue working tirelessly together with our partners to outsmart them."

Participating agencies

Germany: Reutlingen Police Headquarters (Polizeipräsidium Reutlingen)
The Netherlands: National Police (Politie)
Switzerland: Cantonal Police of Argovia (Kantonspolizei Aargau)
United States: Federal Bureau of Investigation
France: Judicial Police (Direction Centrale de la Police Judiciaire)
Europol: European Cybercrime Centre (EC3)

Number 9

21 arrests in nationwide cyber crackdown

NCA
National Crime Agency

21 people have been arrested across the UK as part of an operation targeting customers of an online criminal marketplace that advertised stolen personal credentials.

The operation, which ran over the past five weeks, was coordinated by the National Crime Agency and involved cybercrime teams from across the Team Cyber UK network.

Those targeted were customers of WeLeakInfo, a site that hosted 12 billion stolen credentials from over 10,000 data breaches before it was taken down in January 2020 following an NCA investigation.

Cyber criminals paid for access to the site in order to download personal data for use in further criminality, including cyber attacks and fraud offences.

NCA investigators identified UK-based customers of WeLeakInfo and shared the intelligence with partners ahead of the coordinated period of activity launching on 16 November.

Of those 21 arrested - all men aged between 18-38 - nine were detained on suspicion of Computer Misuse Act offences, nine for Fraud offences and three are under investigation for both.

NCA officers conducted 11 of the arrests and seized over £41,000 in bitcoin.

As well as being customers of WeLeakInfo, evidence suggests that some had also purchased other cybercrime tools such as remote access Trojans (RATs) and crypters.

Additionally, three subjects have been found to be in possession of, or involved with, indecent images of children.

A further 69 individuals in England, Wales and Northern Ireland aged between 16-40 were visited by Cyber Prevent officers, warning them of their potentially criminal activity. 60 of those were served with cease and desist notices.

Many more of these visits are due to take place over the coming months.

Paul Creffield, from the NCA's National Cyber Crime Unit, said: "Through the identification of UK customers of WeLeakInfo, we were able to locate and arrest those who we believe have used stolen personal credentials to commit further cyber and fraud offences.

"The NCA and UK law enforcement take such offences extremely seriously and they can result in huge financial loss to victims.

"We were also able to pin point those on the verge of breaking the law and warn them that should they continue, they could face a criminal conviction. Cyber skills are in huge demand and there are great prospects in the tech industry for those who choose to use their skills legally.

"Cyber criminals rely on the fact that people duplicate passwords on multiple sites and data breaches create the opportunity for fraudsters to exploit that.

"Password hygiene is therefore extremely important. Advice on this and guidance on how to mitigate against cyber attacks can be found on the National Cyber Security Centre's website – www.ncsc.gov.uk"

The NCA and UK policing's Cyber Choices programme aims to prevent young people inadvertently slipping into cyber crime and divert them to more positive pathways in tech.

Number 10

NIST Software Tool Improves Your Doctor's Vaccination Advice

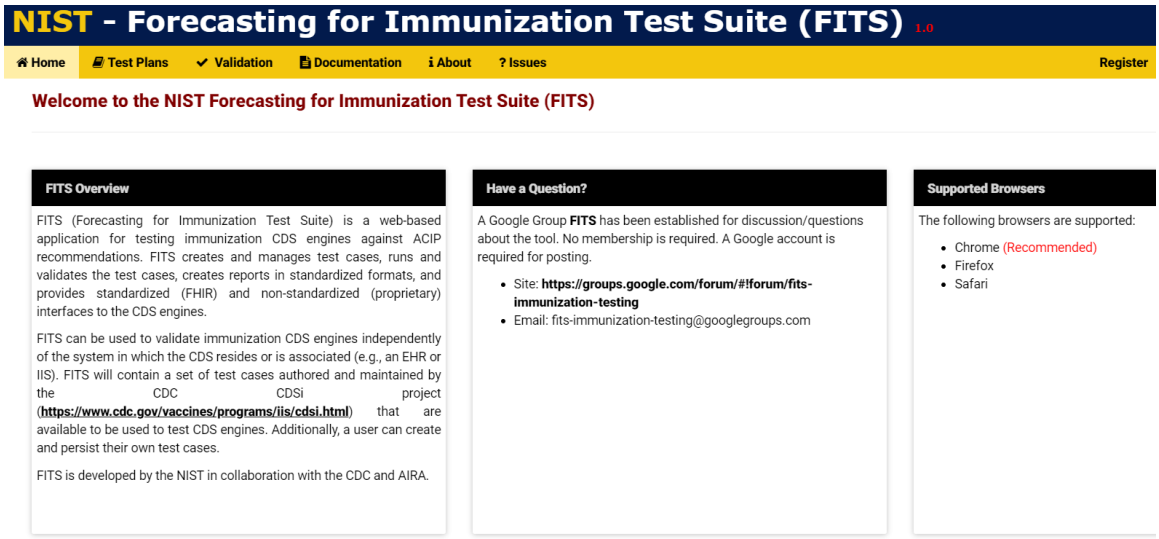
Agency's testing tools have increased the correctness and consistency of computerized vaccination recommendations.

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

Behind the scenes at your doctor's office, there's a complicated set of information that your providers have to absorb before telling you which vaccinations to get and when.

A software tool created at the National Institute of Standards and Technology (NIST) is helping them make better decisions.

The software tool — called the Forecasting for Immunization Test Suite, or FITS — is helping ensure that your doctors are getting correct and up-to-date recommendations about when patients should get their vaccines. You may visit: https://fits.nist.gov/fits/#/home



While your doctor remains responsible for the final decision, computers are vital resources in the process, as immunization schedules change in response to new medical research and providers must work to stay abreast of it.

The FITS tool allows state health care systems to test these computers to find out whether they are providing valid answers for a patient's circumstances.

"Children get more vaccinations these days and get them more often," said NIST computer scientist Mike Indovina. "As medical knowledge is constantly being updated, the schedules become a moving target. It's difficult for doctors to keep up and know which vaccines a patient should get next — especially if life happens and, for example, their patient misses a visit."

To help doctors keep up, state health care systems use computerized Immunization Information Systems (IIS), which not only keep track of patients' immunization records but also have software that recommends future vaccinations.

It's no longer as easy as following a schedule, because the software gets modified several times a year as researchers gather new data about vaccines.

"They might find out that a particular disease is on the rise and that changes to the vaccination schedules are needed, such as with the hep-A vaccine this year due to a recent spike in hepatitis A cases. Or a brand-new vaccine formula for an illness might come out," Indovina said. "They're constantly tweaking the software for these kinds of reasons. It could change the timing for an existing vaccine, or it could change which formulation you receive."

The FITS tool, which NIST developed with the assistance of the Centers for Disease Control and Prevention (CDC), puts IIS software through its paces by executing more than 800 test cases the CDC created. Each test case — which concerns a single person's situation and vaccination schedule — should generate a specific immunization recommendation, or "forecast," by the IIS. FITS measures how closely these forecasts align with the recommendations and standards created by the medical community. FITS also automates the testing process and allows the test cases to be developed, maintained and shared nationwide.

To read more:
https://www.nist.gov/news-events/news/2020/12/nist-software-tool-improves-your-doctors-vaccination-advice

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.

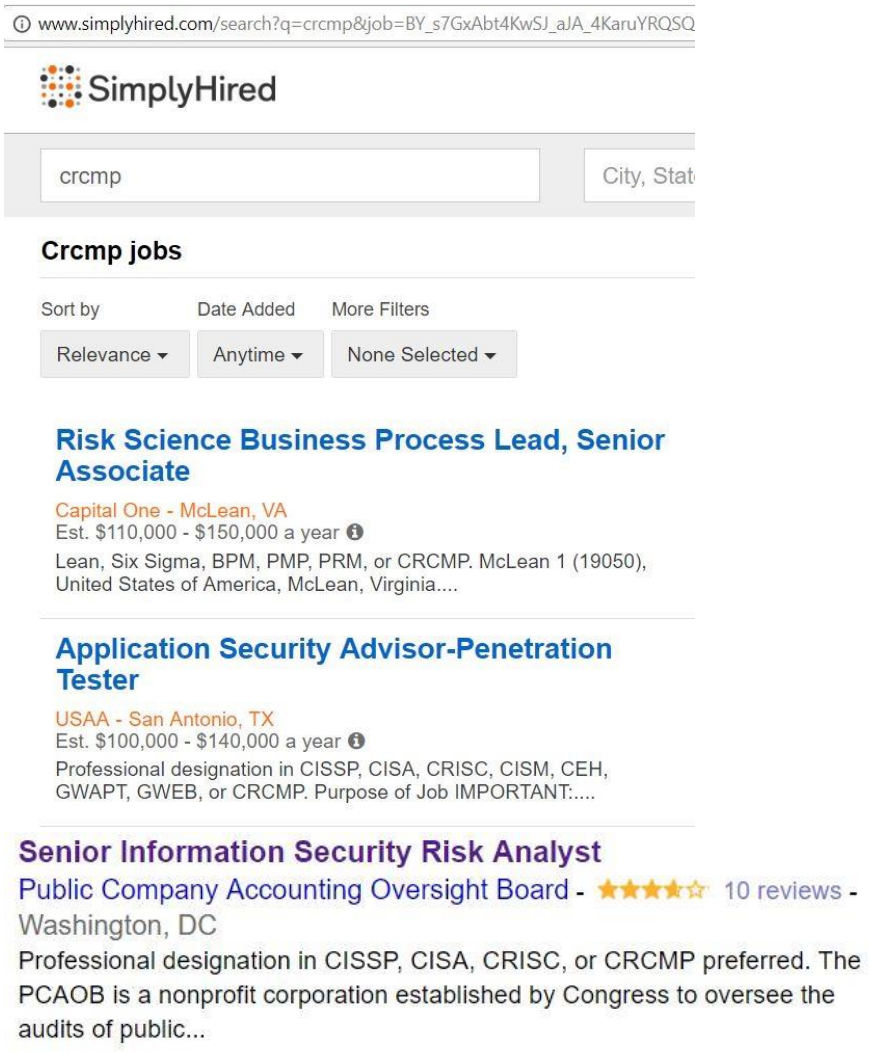
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

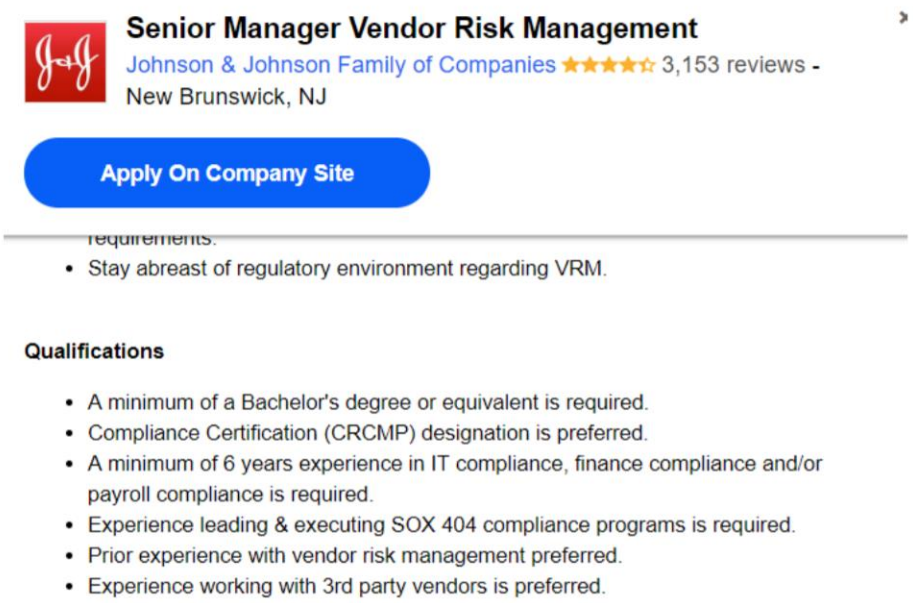
You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.
You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become a Certified Risk and Compliance Management Professional (CRCMP), a Certified Information Systems Risk and Compliance Professional (CISRCP), a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, and / or a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I.





Senior Manager Vendor Risk Management

Johnson & Johnson Family of Companies ★★★★☆ 3,153 reviews -
New Brunswick, NJ

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

- A minimum of a Bachelor's degree or equivalent is required.
- Compliance Certification (CRCMP) designation is preferred.
- A minimum of 6 years experience in IT compliance, finance compliance and/or payroll compliance is required.
- Experience leading & executing SOX 404 compliance programs is required.
- Prior experience with vendor risk management preferred.
- Experience working with 3rd party vendors is preferred.

Companies and organizations like Accenture, American Express, USAA etc. consider the Certified Risk and Compliance Management Professional (CRCMP) program a preferred certificate. There are CRCMPs in 32 countries.

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

For the Certified Risk and Compliance Management Professional (CRCMP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For the Certified Information Systems Risk and Compliance Professional (CISRCP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

For the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CRCMP_Re_I.htm

For *instructor-led* training, you may contact us. We can tailor all programs to meet specific requirements.