Monday, March 2, 2020

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,

I have just read the Draft NISTIR (National Institute of Standards and Technology Interagency Report) 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*.

As we can read in the report, in today's highly connected world, all organizations rely on other organizations for critical products and services. However, today's world of globalization, while providing many benefits, has resulted in a world where organizations no longer fully control—and often do not have full visibility into—the supply ecosystems of the products that they make or the services that they deliver.

With more and more businesses becoming digital, producing digital products and services, and moving their workloads to the cloud, the impact of a cybersecurity event today is greater than ever before and could include personal data loss, significant financial losses, compromise of safety, and even loss of life.

Organizations can no longer protect themselves by simply securing their own infrastructures, since their electronic perimeter is no longer meaningful; threat actors intentionally target the suppliers of more cyber-mature organizations to take advantage of the weakest link.

There are 21 recommendations in this report. Some of them are:

- Know if your data and infrastructure are accessible to suppliers' sub-suppliers.

- Propagate security requirements to suppliers' sub-suppliers.

- Train key stakeholders in your organization and within the supplier's organization.

- Establish protocols for vulnerability disclosure and incident notification.

- Establish protocols for communications with external stakeholders during incidents.

- Train key stakeholders in your organization and within the supplier's organization.

The report defines *Cyber Supply Chain Risk Management (C-SCRM)* as a multidisciplinary approach to identify, assess, and mitigate cyber supply chain risks.

Read more at number 10 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

Number 1 (Page 5)

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST Special Publication 800-171, Revision 2

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

Number 2 (Page 7)

BIS Papers, no 110 - Measuring the effectiveness of macroprudential policies using supervisory bank-level data Monetary and Economic Department, February 2020.

BIS

Number 3 (Page 11)

Irving Fisher Committee on Central Bank Statistics

IFC Report, Central banks and fintech data issues

2020 Survey conducted by the Irving Fisher Committee on Central Bank Statistics (IFC), February 2020

BIS

Number 4 (Page 13)

Basel Committee meets to review vulnerabilities and emerging risks, advance supervisory initiatives and promote Basel III implementation

BIS

Number 5 (Page 16)

Financial markets and monetary policy - is there a hall of mirrors problem?

Richard H Clarida, Vice Chair of the Board of Governors of the Federal Reserve System.

Number 6 (Page 18)

Robotrolling

Number 7 (Page 20)

EU-U.S. Insurance Project

13 Mar 2020, Washington D.C.

Number 8 (Page 22)

Alert (AA20-049A)
Ransomware Impacting Pipeline Operations

Cybersecurity and Infrastructure Security Agency (CISA)

Number 9 (Page 24)

Bruno Tissot speaks about "big data" and its implications for central banks

Number 10 (Page 25)

NIST Offers Strategies to Help Businesses Secure Their Cyber Supply Chains

Number 1

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

NIST Special Publication 800-171, Revision 2

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions.

This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.

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

The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

TABLE 1: SECURITY REQUIREMENT FAMILIES

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

The purpose of this publication is to provide federal agencies with recommended security requirements for protecting the confidentiality of CUI:

(1) when the CUI is resident in a nonfederal system and organization;

(2) when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and

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

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

The requirements are intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations. In CUI guidance and the CUI Federal Acquisition Regulation (FAR), the CUI Executive Agent will address determining compliance with security requirements.

To read more:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

Number 2

BIS Papers, no 110 - Measuring the effectiveness of macroprudential policies using supervisory bank-level data Monetary and Economic Department, February 2020.

One of the main challenges in implementing a new framework for financial stability is evaluating the effectiveness of macroprudential policies.

Most of the evidence produced so far has been obtained from country- or bank-level data using publicly available sources at the annual frequency.

The low granularity of the data makes it very difficult to clearly disentangle supply and demand effects and assess the effectiveness of the policies over time.

Consequently, in 2018 the BIS initiated a research protocol project on "Measuring the effectiveness of macroprudential policies using supervisory bank-level data" with a quarterly frequency.

The project focused on the effectiveness of macroprudential policies on containing excessive household credit growth and bank risk using bank-level data.

When analysing these effects, we control for bank-specific characteristics and macroeconomic variables.

In a second step, the project evaluates whether the responses to a macroprudential shock differ for banks with different characteristics.

Finally, the project also analyses how the effectiveness of macroprudential policies can be affected by monetary policy stance, the business cycle and the financial cycle.

The quarterly frequency helps us to analyse the different steps in the transmission mechanisms.

Carlos Cantú, Leonardo Gambacorta and Ilhyock Shim of the BIS were the project's research advisers. Supervisory data are highly confidential.

This means that it is not possible to merge the data into a single data set. The only possibility is to coordinate a common exercise and summarise the different results.

The BIS sent a research protocol to the Asian Consultative Council (ACC) central banks in June 2018.

Five ACC central banks agreed to join the exercise: the Reserve Bank of Australia (RBA), Bank Indonesia (BI), the Reserve Bank of New Zealand (RBNZ), Bangko Sentral ng Pilipinas (BSP) and the Bank of Thailand (BOT).

Each central bank developed its own analysis, following the methodology from the protocol to enhance the comparability of the results.

Preliminary results were presented in two Asian Research Network workshops held in New Zealand and Australia, respectively.

Taking into account the comments from the two workshops, the authors of the five country papers finalised them in September 2019.

Results were summarised using meta-analysis techniques. This volume is a collection consisting of the six papers. Here we provide a synopsis for time-constrained readers.

The first paper, by Carlos Cantú, Leonardo Gambacorta and Ilhyock Shim, summarises the results of the five country papers using a meta-analysis methodology.

It finds that macroprudential policy actions taken by the five countries are largely effective in reducing excessive household credit growth, and that tightening actions have a stronger effect than easing actions.

It also finds that macroprudential policy is effective in reducing bank risk as measured by the non-performing loan (NPL) ratio.

In the paper titled “Assessing the effects of housing policy measures on new lending in Australia”, Corrine Dobson (RBA) shows first that two housing policy measures, announced in Australia in 2014 and 2017, reduced the flow of total new housing lending.

In addition, she considers new loans to owner-occupiers and those to investors separately, and finds that these measures had a stronger effect on the growth of lending to investors, which was the policy’s primary target.

The paper by Rani Wijayanti, Nur M Adhi P and Cicilia A Harun (BI) titled “Effectiveness of macroprudential policies and their interaction with monetary policy in Indonesia” shows that decreases (or increases) in the maximum loan-to-value (LTV) ratio and the macroprudential

intermediation ratio between 2010 and 2018 significantly reduced (or increased) household loan growth, and that such policy measures were more effective when real GDP growth was low or the credit-to-GDP gap was large.

They also find that the use of such policy instruments effectively reduced the NPL ratio.

In their paper titled "The effectiveness of loan-to-value ratio policy and its interaction with monetary policy in New Zealand: an empirical analysis using supervisory bank-level data", Fang Yao and Bruce Lu (RBNZ) show that the LVR policy implemented in New Zealand between 2013 and 2016 reduced housing loan growth on average by 2 percentage points over the six months following each policy announcement.

They also find evidence that the LVR policy has a statistically significant negative impact on the NPL ratio, although the economic magnitude is rather small.

The paper by Veronica B Bayangos and Jeremy De Jesus (BSP) titled "Have domestic prudential policies been effective? Insights from bank-level property loan data" examines the effects of domestic macroprudential policy in the Philippines over the sample period from March 2014 to December 2017.

In particular, the authors consider the following six types of instrument: currency, capital-based, liquiditybased, asset side, reserve requirement and structural.

The paper finds that tightening macroprudential policies has a negative impact on real bank loan commitments to borrowers which lasts up to four quarters. It also shows a negative impact of tightening domestic macroprudential policy on the NPL ratio.

The final paper, titled "The impact of LTV policy on bank lending: evidence from Thailand", by Chantawit Tantasith, Nasha Ananchotikul, Chatlada Chotanakarn, Vorada Limjaroenrat and Runchana Pongsaparn (BOT) analyses the impact of three LTV measures in Thailand based on bank- and contract-level data provided by domestic commercial banks over the period 2004–18.

They find that the policy effect does not manifest itself in the pace of credit growth at the bank level, but rather in the LTV distribution of newly issued loans.

In particular, a loosening measure taken in 2009 prompted banks to increase the LTV ratio for the targeted loan sector, while tightening measures taken in 2011 and 2013 led to a more cautious LTV setting, reflecting the tightened credit standards the policy aimed to achieve.

To read more: https://www.bis.org/publ/bppdf/bispap110.pdf

Number 3

Irving Fisher Committee on Central Bank Statistics

IFC Report, Central banks and fintech data issues

2020 Survey conducted by the Irving Fisher Committee on Central Bank Statistics (IFC), February 2020

Fintech, or technological innovation used to support or provide financial services, has developed markedly in recent years, transforming the financial landscape and creating a number of challenges for public authorities (IMF-WB (2018), Carstens (2019)).

These challenges are particularly material for central banks, as the "future of central banking is inextricably linked to innovation".

The transformation of financial markets is affecting the way they conduct their policies to ensure, among their policies to ensure, among other objectives, monetary and financial stability as well the smooth functioning of payment systems (CPMI (2018), Barontini and Holden (2019), Boar et al (2020)).

As regards central bank statisticians and their need for high-quality data to support policymaking, fintech gives rise to a number of issues.

For example, what are the data sources available to measure fintech and how are they actually used? Which additional information is needed to support the conduct of central bank policies, and what are the data gaps? How should these gaps be addressed, considering costs/benefits trade-offs and the various stakeholders involved? And how should adequate statistical frameworks be developed for collecting comprehensive information given the global nature of the financial system?

To shed light on those various issues, the Irving Fisher Committee on Central Bank Statistics (IFC) conducted a survey among its members in 2019. The main results are the following:

1. Fintech is developing in the majority of the jurisdictions, through different channels.

First, a growing number of recently incorporated entities leveraging on technology ("fintechs") have emerged to provide financial services; they are particularly engaged in the provision of payments, clearing, and settlement services, as well as in credit intermediation.

Second, traditional financial institutions are also embracing technologically enabled financial innovation and adjusting their business models accordingly; this is particularly the case for well established credit institutions and payment service providers.

2. The survey reveals a *significant need for fintech data among central bank users,* with the strongest requests expressed by those units in charge of payment systems.

Information demands are particularly high in jurisdictions where fintech is the most developed. Users are typically interested in lists of fintech entities and on statistics on fintech credit.

3. Fintech creates important data gaps, reflecting three main developments.

First, fintechs can be classified outside the financial sector if for instance they were initially set up as IT companies; such classification issues can be reinforced by the fact that these firms are often small, diverse, and not easy to identify.

A second problem relates to the lack of granularity of the current statistical framework, since major data collection exercises group together non-bank financial institutions.

For example, the financial accounts include a number of rapidly growing types of intermediaries providing financial services (eg crowdfunding, peer-to-peer lending) into the “other financial institutions” sector.

Third, traditional financial institutions have been embracing innovation by sponsoring technological start-ups treated as directly controlled affiliates, implying that their fintech activities are blurred in consolidated groups’ reports.

To read more: https://www.bis.org/ifc/publ/ifc_report_fintech_2002.pdf

Number 4

Basel Committee meets to review vulnerabilities and emerging risks, advance supervisory initiatives and promote Basel III implementation

The Basel Committee on Banking Supervision met in Basel on 26-27 February 2020 to review risks impacting the banking system, advance a range of supervisory initiatives and promote the implementation of Basel III.

The Committee dedicated a portion of its meeting to discussing progress on a strategic review initiated last year. The Committee has consulted with members and stakeholders on its future priorities, its structure and its processes.

Members discussed the feedback received and exchanged initial views on the way forward. The Committee aims to finalise its review in the course of the year.

The Committee discussed the financial stability implications of the coronavirus outbreak (Covid-19) for the banking system and exchanged information on the business continuity measures that banks and authorities have put in place.

The Committee encourages banks and supervisors to remain vigilant in light of the evolving situation and notes the importance of effective cross-border information sharing and cooperation when dealing with such shocks.

The Committee reviewed vulnerabilities associated with leveraged loans and collateralised loan obligations (CLOs). Among financial participants, banks have the largest direct exposures to these markets; banks are also exposed through a number of indirect channels.

The Committee agreed to continue work in three areas related to leveraged loans and CLOs: members' supervisory approaches to measuring and mitigating risks; the current regulatory treatment of these exposures; and the need to further quantify banks' direct and indirect exposures.

Committee members discussed progress made by banks in preparing for the transition from the London interbank offered rate (Libor) to alternative

reference rates. In December 2019, the Committee and the Financial Stability Board launched a survey on exposures to Libor and associated supervisory measures.

The survey results and a report on remaining challenges to benchmark transition will be provided to G20 Finance Ministers and Central Bank Governors in July.

In the interim, the Committee stressed the need for banks to dedicate the necessary resources to understanding the impact of benchmark rate reforms on their business and making the necessary preparations for a smooth transition.

The Committee has published a newsletter today outlining regulatory and supervisory implications related to benchmark rate reforms. You may visit: https://www.bis.org/publ/bcbs_nl24.htm

The Committee recently established a high-level Task Force on Climate-related Financial Risks.

The Committee discussed the Task Force's workplan and future deliverables, which include:

- A set of analytical reports on climate-related financial risks, including a literature review, and reports on the transmission channels of such risks to the banking system and on measurement methodologies.

- The development of effective supervisory practices to mitigate climate-related financial risks.

The Committee also reviewed a stocktake of members' current initiatives in this area. A summary of this stocktake will be published in March.

As part of its ongoing Regulatory Consistency Assessment Programme, the Committee approved the reports assessing the implementation of the Net Stable Funding Ratio and Large Exposures standards in Hong Kong SAR, Indonesia and Singapore. These reports will be published next month.

Members also reviewed the implementation status of Basel III across its member jurisdictions. The Committee received updates from its members on the progress made in implementing Basel III. Members reiterated their commitment to implement Basel III in a full, timely and consistent manner and agreed to continue monitoring the situation and keep one another informed.

The Committee also agreed to publish the following documents:

- A consultation paper aimed at strengthening the operational resilience of banks - to be published in March.

- A report on members' experience in using the countercyclical capital buffer - to be published in due course.

Number 5

Financial markets and monetary policy - is there a hall of mirrors problem?

Richard H Clarida, Vice Chair of the Board of Governors of the Federal Reserve System, at the 2020 US Monetary Policy Forum, sponsored by the Initiative on Global Markets at the University of Chicago Booth School of Business, New York City.

Thank you to the conference organizers for inviting me here to discuss what former Chair Bernanke has famously referred to as a "hall of mirrors" problem: a situation in which a central bank's reaction function and financial market prices interact in economically suboptimal and potentially destabilizing ways.

In my remarks today, I will lay out the way I think about the interplay between financial markets and monetary policy, with a focus on how I myself seek to integrate noisy but often correlated signals about the economy that I glean from models, surveys, and financial markets.

Three Observations

I begin with three unobjectionable observations.

First, because of Friedman's long and variable lags, monetary policy should be—and, at the Fed, is—forward looking.

Policy decisions made today will have no effect on today's inflation or unemployment rates, so good policy needs to assess where the economic fundamentals are going tomorrow to calibrate appropriate policy today.

Of course, financial markets are also forward looking.

An asset's value today depends upon its expected future cash flows discounted by a rate that reflects the expected path of the policy rate plus an appropriate risk premium.

Thus, central banks and financial markets are looking at the same data on macro fundamentals to make inferences about the future path of the economy, and, of course, any decisions on the policy path made by the central bank will influence asset prices through the discount factor.

So optimal monetary policy will (almost) always be correlated with asset prices. Correlation is not evidence of causation, and the hall of mirrors problem at its essence is about inferring causation from correlation.

To read more:
https://www.bis.org/review/r200223b.pdf

Number 6

Robotrolling

Inauthentic English- and Russian-language conversations on Twitter about the NATO presence in Poland and the Baltic States peaked on 4 and 5 December, respectively, coinciding with the 2019 NATO Leaders' Meeting in London.

Robotic accounts focused heavily on the meeting this quarter, particularly on English-language Twitter, which saw roughly 3 times the usual level of bot activity.

On VK, an anomalous increase in activity from anonymous human - controlled accounts coincided with the meeting.

Due to the contentious atmosphere surrounding the meeting in London, a considerable increase in the proportion of posts generated by bots was observed on English-language Twitter this quarter.

At the same time, Russian-language bot activity on Twitter decreased to the lowest level observed thus far.

In this issue of Robotrolling, we dig deeply into a sample of political pages amassed by a COE report on commercial social media manipulation in order to identify patterns in inauthentic activity on Facebook.

We demonstrate that the 2019 elections in Ukraine were the primary focus of actors willing to pay for inflated social media engagement.

Our analysis also reveals several shared traits among political manipulators on Facebook and provides a network visualisation that shows the connections between them.

As a new year of Robotrolling begins, we review trends observed in VK groups over the past 18 months.

A steady reduction in the proportion of content shared in communities dedicated to the so-called Novorossia region and the Donbass coincides

with inauthentic content increasingly being posted in community spaces such as private groups or pages.

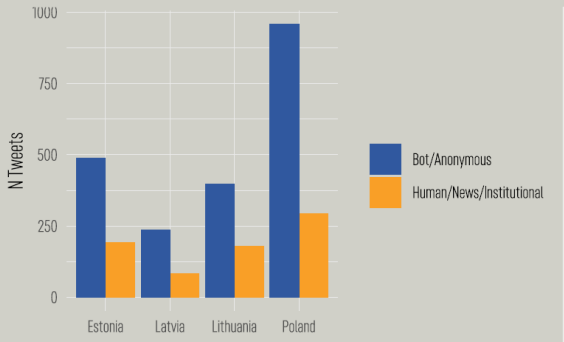


Figure 2: Total number of tweets mentioning NATO and Estonia, Latvia, Lithuania, or Poland, by account type.

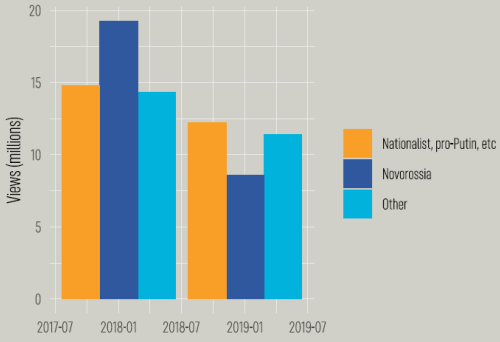


Figure 3: Views of content about NATO in the Baltics and Poland, posted to community spaces on VK and subdivided by community cluster.

Figure 4: Timeline of VK and Twitter mentions.

To read more: https://www.stratcomcoe.org/publications

Number 7

EU-U.S. Insurance Project

13 Mar 2020, Washington D.C.

The EU-U.S. Public Forum will take place at the premises of the U.S. Chamber of Commerce in Washington, DC.

9:00 - 9:15a.m. **Welcoming Remarks and Forum Objectives**

- Steven Seitz, Director, Federal Insurance Office
- Doug Ommen, Commissioner, Iowa Insurance Division
- Gabriel Bernardino, Chairman of the EIOPA Board of Supervisors

9:15 - 10:15 a.m. **Panel 1 – Confronting Cross-Border Insurer Cybersecurity Risks**

Cyber risk continues to grow and evolve, both for the insurance industry itself and for the U.S. and EU markets and businesses served by insurers. This past year, the EU-US Insurance Project has examined cross-border cybersecurity incidents and how to coordinate responses to such incidents. This panel will address how the insurance industry and regulators can enhance insurance sector cybersecurity, including how best to continue and enhance cross-border coordination and information sharing among all stakeholders.

- *Moderator*: Steven Seitz, Federal Insurance Office, U.S. Department of the Treasury
- Jillian Froment, Director, Ohio Department of Insurance
- Petra Hielkema, Director Insurance Supervision, De Nederlandsche Bank (DNB)
- Kelly Ann Harris, Vice President, Corporate Counsel – Cybersecurity & Privacy, Prudential
- Neville Dunne, Chief Operating Officer, Zurich Insurance plc, Ireland

10:30 – 11:30 a.m. **Panel 2 –Development of the Cyber Insurance Market: Challenges and Opportunities of Insuring and Reinsuring Cyber Risk**

This panel will discuss approaches for collecting data and developing techniques supporting more sophisticated assessment of cyber risks and potential accumulation risks. Taking into account the global character of cyber risks panelists will elaborate on whether globally harmonized standards could facilitate further understanding and underwriting of cyber risks. The discussion will further include the role and use of risk pools to provide additional capacity to tackle the potential systemic nature of cyber risk.

- *Moderator*: Gabriel Bernardino, Chairman of the EIOPA Board of Supervisors
- Jillian Froment, Director, Ohio Department of Insurance
- Dr. Frank Grund, Chief Executive Director of Insurance and Pension Supervision, Federal Financial Supervisory Authority, Germany
- Matthew McCabe, Senior Vice President, Marsh USA, Inc.
- Joshua Motta, CEO, Coalition, Inc.
- Giles Taylor, Chief Risk and Compliance Officer, Lloyd's Brussels

11:45 – 12:45 p.m. **Panel 3 – The Future of Big Data and AI in Insurance: Challenges and Opportunities for Insurers and Regulators**

Panelists will discuss insurers' use of third-party vendors and how the regulatory framework addresses big data accuracy and new vendors operating in the insurance marketplace. Panelists will also discuss privacy protections and disclosures to applicants and policyholders. Panelists will explore the associated opportunities and risks of insurers' use of AI and corresponding regulatory responses in the US and EU, such as the development of AI principles including ethical aspects. Finally, panelists will discuss the regulatory review of predictive models, including but not limited to assessing transparency and explainability issues arising from the use of ML algorithms.

- *Moderator*: Jillian Froment, Director, Ohio Department of Insurance
- Doug Ommen, Commissioner, Iowa Insurance Division
- Domhnall Cullinan, Director of Insurance Supervision, Central Bank of Ireland
- Timothy Jones, Chief Innovation Officer, Transamerica
- Peter Kochenburger, Deputy Director of the Insurance Law Center and Associate Clinical Professor of Law at the University of Connecticut School of Law
- Marcin Detyniecki, Group Chief Data Scientist and Head of R&D, AXA Group

The public event will include discussions of key areas linked to the Project initiatives addressing challenges and opportunities for the insurance sector in the European Union and the United States related to cyber security risks and the cyber insurance market, and the use of big data.

Representatives of the European Commission (EC), European Insurance and Occupational Pensions Authority (EIOPA), the Federal Insurance Office of the U.S. Department of the Treasury (FIO) and the National Association of Insurance Commissioners (NAIC), will lead the Forum. Other EU and US authorities will also participate in this event.

Panel sessions will include discussions amongst regulators, industry and consumer representatives on approaches, practices and solutions addressing the multi-fold challenges, risks and opportunities regarding these covered topics.

The Programme is available at:
https://www.eiopa.europa.eu/content/agenda-eu-us-insurance-project-public-forum-13-march-2020-washington

Number 8

Alert (AA20-049A)
Ransomware Impacting Pipeline Operations

Cybersecurity and Infrastructure Security Agency (CISA)

The Cybersecurity and Infrastructure Security Agency (CISA) encourages asset owner operators across all critical infrastructure sectors to review the below threat actor techniques and ensure the corresponding mitigations are applied.

CISA responded to a cyberattack affecting control and communication assets on the operational technology (OT) network of a natural gas compression facility.

A cyber threat actor used a Spearphishing Link [https://attack.mitre.org/techniques/T1192/] to obtain initial access to the organization's information technology (IT) network before pivoting to its OT network.

The threat actor then deployed commodity ransomware to Encrypt Data for Impact on both networks. Specific assets experiencing a Loss of Availability on the OT network included human machine interfaces (HMIs), data historians, and polling servers.

Impacted assets were no longer able to read and aggregate real-time operational data reported from low-level OT devices, resulting in a partial Loss of View for human operators.

The attack did not impact any programmable logic controllers (PLCs) and at no point did the victim lose control of operations.

Although the victim's emergency response plan did not specifically consider cyberattacks, the decision was made to implement a deliberate and controlled shutdown to operations.

This lasted approximately two days, resulting in a Loss of Productivity and Revenue, after which normal operations resumed. CISA is providing this Alert to help administrators and network defenders protect their organizations against this and similar ransomware attacks.

Network and Assets

- The victim failed to implement robust segmentation between the IT and OT networks, which allowed the adversary to traverse the IT-OT boundary and disable assets on both networks.

- The threat actor used commodity ransomware to compromise Windows-based assets on both the IT and OT networks. Assets impacted on the organization's OT network included HMIs, data historians, and polling servers.

- Because the attack was limited to Windows-based systems, PLCs responsible for directly reading and manipulating physical processes at the facility were not impacted.

- The victim was able to obtain replacement equipment and load last-known-good configurations to facilitate the recovery process.

- All OT assets directly impacted by the attack were limited to a single geographic facility.

To read more: https://www.us-cert.gov/ncas/alerts/aa20-049a

Number 9

Bruno Tissot speaks about "big data" and its implications for central banks

Experts from the Bank for International Settlements (BIS) explain their work and discuss current issues for the global economy.

As a hub for central banks and other financial regulatory and supervisory authorities, the BIS seeks to build a greater collective understanding of the world economy, foster international cooperation and support policy making.

You may visit:
http://bispodcast.libsyn.com/bruno-tissot-speaks-about-big-data-and-its-implications-for-central-banks

Number 10

NIST Offers Strategies to Help Businesses Secure Their Cyber Supply Chains

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

Reducing the cybersecurity risk to one of the most vulnerable aspects of commerce — global supply chains — is the goal of a new publication by the National Institute of Standards and Technology (NIST), whose computer security experts have distilled a set of effective risk management techniques into a draft guidebook for businesses. NIST is seeking public comment on the draft for the next 30 days.

Key Practices in Cyber Supply Chain Risk Management (Draft NISTIR 8276 - https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8276-draft.pdf) provides a set of strategies to help businesses address the cybersecurity issues posed by modern information and communications technology products, which are commonly built using components and services supplied by third-party organizations.

The composed nature of these devices and systems makes them difficult to secure effectively against malware and other threats, placing manufacturers, service providers and end users at risk.

“The seed of the problem is that everything is interconnected nowadays,” said NIST’s Jon Boyens, one of the draft report’s authors. “Products are very sophisticated, and with our globalized economy, companies often outsource the tasks of developing components and code to other companies, involving multiple tiers of suppliers.”

Vulnerabilities in the cyber supply chain — really a complex network of connections rather than a single strand — involve not only microchips and their internal code, but also the support software for a device and the other companies that have access to its components.

Put them all together, and it can be a daunting task to anticipate every systemic weakness that an adversary might exploit.

Many recent cyber breaches have been linked to supply chain risks. A recent high-profile attack from the second half of 2018, Operation ShadowHammer, is estimated to have affected up to a million users.

A 2013 attack by the Dragonfly group targeted companies with industrial control systems, such as those distributing energy within the U.S. This attack infected companies in critical industries with malware. Symantec's 2019 Internet Security Threat Report found supply chain attacks increased by 78 percent in 2018.

The NIST report is a high-level document intended to be easily understood and applied in managing these risks. Its core is a 27-page section outlining eight key practices that have proved to be useful, from establishing a formal risk management program to collaborating closely with key suppliers.

Each key practice is accompanied by a set of recommendations, and because each organization will have its own specific needs, the authors also include guidance on how to apply these recommendations.

Acknowledging that companies in different economic sectors might manage supply chain risk differently, the authors also offer a set of 24 case studies in risk management that feature a variety of businesses ranging from aerospace and IT manufacturers to consumer goods companies. These case studies, along with a summary of the findings, are available at NIST's Cyber Supply Chain Risk Management Key Practices page.

"Many companies share the same suppliers, but their overall supply chains are still very different," Boyens said. "To supplement our report you can look for the case studies that are relevant to your industry."

The April 2018 update to the NIST Cybersecurity Framework added a new section about supply chain risk management, and the new report cross-references the framework so that organizations can use both sets of NIST guidance together, Boyens said.

Public comments on Draft NISTIR 8276 can be submitted until March 4, 2020, to scrm-nist@nist.gov, and NIST will consider them before releasing a final version, planned for Spring 2020.

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.

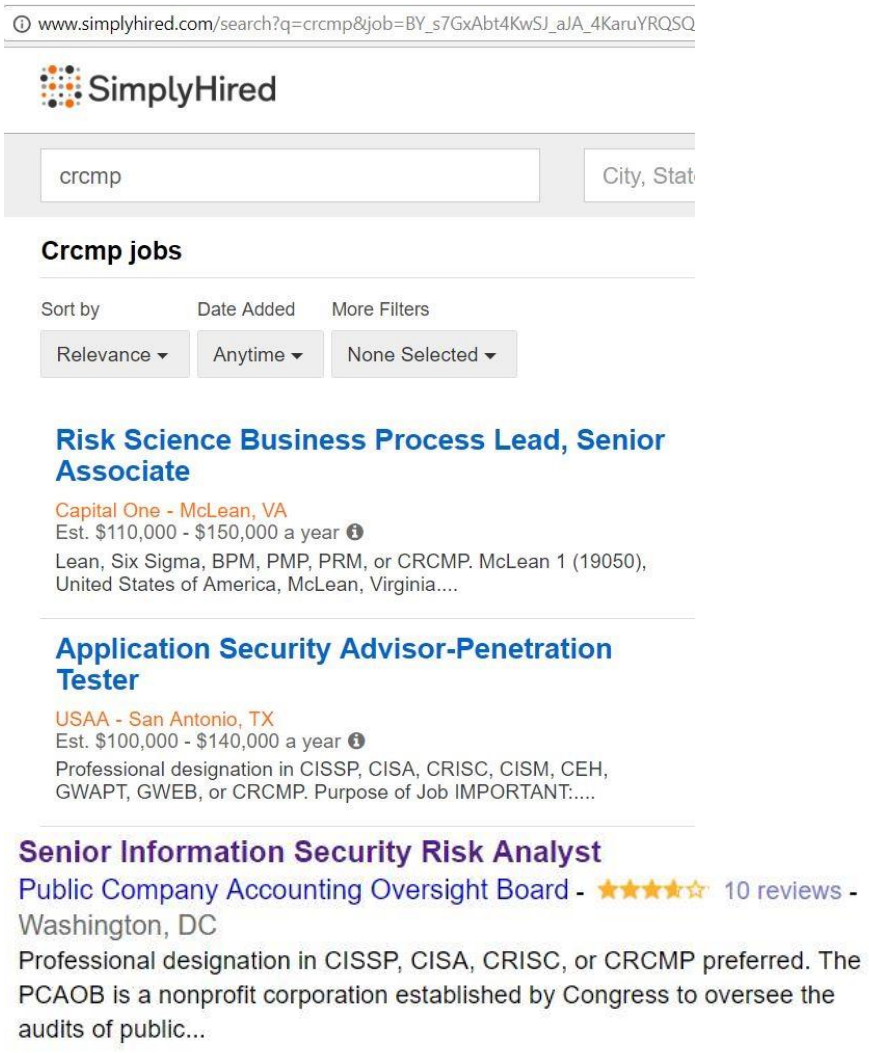
International Association of Risk and Compliance Professionals

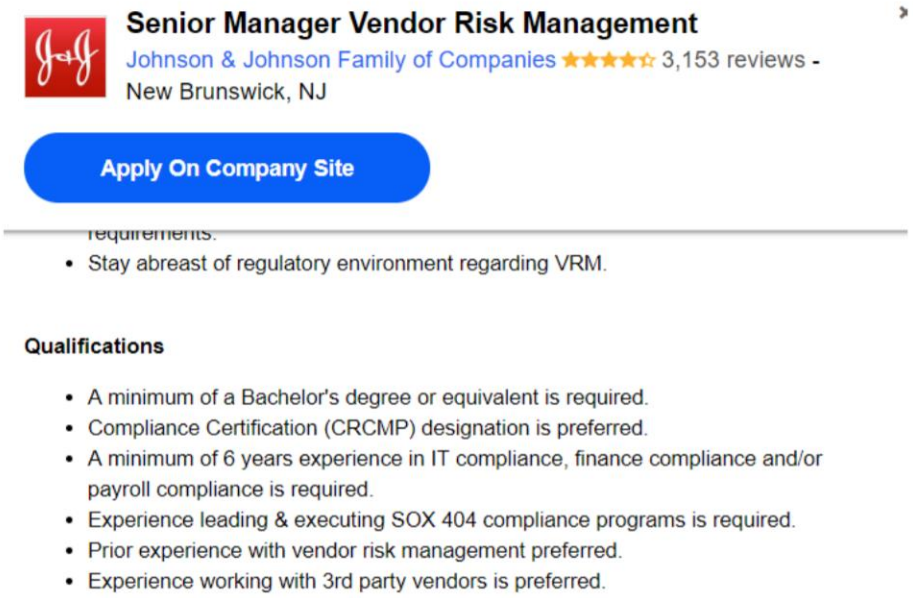
You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.
You may visit:
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.

4. *IARCP Authorized Certified Trainer (IARCP-ACT) Program* - 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:
https://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 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:
https://www.risk-compliance-association.com/Approved_Centers.html