Monday, March 16, 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,

Thomas A. Edison believed that the *doctor of the future* will give *no medicine* but will instruct his patient in the care of the human frame, in diet, and the cause and prevention of disease. I see that we live in this future (at least until we have a decent vaccine for Covid-19).

Coronaviruses are a large family of viruses that are known to cause illness ranging from the common cold to more severe diseases such as Middle East Respiratory Syndrome (MERS) and Severe Acute Respiratory Syndrome (SARS).

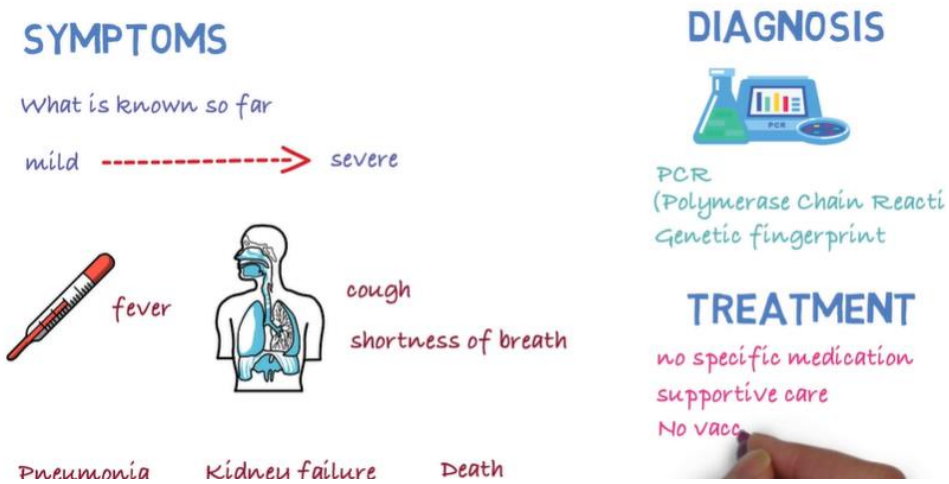
The novel coronavirus (COVID-19) that was identified in 2019 in Wuhan, China, has not been previously identified in humans. We must understand better which is the risk, and what we can do. The World Health Organization (WHO) had an excellent idea, to develop online training as a weapon to fight the new coronavirus.

This course provides a general introduction to COVID-19 and emerging respiratory viruses and is intended for public health professionals, incident managers and personnel working for the United Nations, international organizations and NGOs.

The Cybersecurity and Infrastructure Security Agency (CISA) is working closely with partners to prepare for possible impacts of a COVID-19 outbreak in the United States.
COVID-19 containment and mitigation strategies will rely heavily on healthcare professionals and first responders detecting and notifying government officials of occurrences. In the paper Risk Management for Novel Coronavirus (COVID-19), CISA facilitates communication,

coordination, prioritization and information-sharing between the private sector and the government.

As the situation changes, the virus may affect essential operations for businesses and federal, state, local, tribal, and territorial (SLTT) government entities.



Read more at number 4, 5 and 6 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)

Critical Infrastructure Protection, Additional Actions Needed to Identify Framework Adoption and Resulting Improvements

United States Government Accountability Office

GAO

Report to Congressional Committees

Number 2 (Page 9)

2020 Review of Solvency II: Opportunities and challenges

Keynote speech by Gabriel Bernardino at the conference '2020 Solvency II Review: Challenges and opportunities', Brussels.

Number 3 (Page 13)

Methodological principles of insurance stress testing

eiopa

European Insurance and Occupational Pensions Authority

Number 4 (Page 14)

CISA INSIGHTS
Risk Management for Novel Coronavirus (COVID-19)

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA

CYBER+INFRASTRUCTURE

Number 5 (Page 15)

Online training as a weapon to fight the new coronavirus

World Health Organization

Number 6 (Page 17)

Interim Guidance for Businesses and Employers

Centers for Disease Control and Prevention
CDC 24/7: Saving Lives, Protecting People™

Number 7 (Page 21)

BIS Working Papers No 846
Financial Crises and Innovation

by Bryan Hardy and Can Sever, Monetary and Economic Department, March 2020

BIS

Number 8 (Page 23)

Asking Strategic Questions
A Primer for National Security Professionals

By Andrew Hill and Stephen J. Gerras, Joint Force Quarterly 96.

Number 9 (Page 25)

Consumers urged to secure internet connected cameras

National Cyber Security Centre

Number 10 (Page 27)

Building Hardware to Enable Continuous Data Protections

Program aims to develop novel hardware accelerator to ease computational challenges preventing widespread use of fully homomorphic encryption

DARPA
DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

Critical Infrastructure Protection, Additional Actions Needed to Identify Framework Adoption and Resulting Improvements

United States Government Accountability Office

Report to Congressional Committees

Abbreviations

ASPR - Assistant Secretary for Preparedness and Response
DHS - Department of Homeland Security
DOD - Department of Defense
DOT - Department of Transportation
EPA - Environmental Protection Agency
GSA - General Services Administration
HHS - Department of Health and Human Services
ISAC - Information Sharing and Analysis Center
ISO - International Organization for Standardization
IT - information technology
NIST - National Institute of Standards and Technology
SCC - Sector Coordinating Council
SSA - Sector Specific Agency

Conclusions

Most of the SSAs have not determined the level and type of framework adoption, as we previously recommended. Most of the sectors, however, had efforts underway to encourage and facilitate use of the framework. Even with this progress, implementation of our recommendations is essential to the success of protection efforts.

While selected organizations reported varying levels of improvements, the SSAs have not collected and reported sector-wide improvements as a result of framework use.

The SSAs and organizations identified impediments to collecting and reporting sector-wide improvements, including the lack of precise measurements of improvement, voluntary nature of the framework, and lack of a centralized information sharing mechanism.

However, NIST and DHS have initiatives to help address these impediments.

These included an information security measurement program, cybersecurity framework starter profile, information sharing programs, self-assessment tools, and surveys to support SSAs in measuring and quantifying improvements in the protection of critical infrastructure as a result of using the framework.

However, NIST has yet to establish time frames for completing the information security measurement program and starter profile.

Moreover, the SSAs have yet to report on sector-wide improvements using the initiatives.

Until they do so, the critical infrastructure sectors may not fully understand the value of the framework to better protect their critical infrastructures from cyber threats.

Recommendations

We are making the following 10 recommendations to NIST and the nine sector-specific agencies.

The Director of NIST should establish time frames for completing NIST's initiatives, to include the information security measurement program and the cybersecurity framework starter profile, to enable the identification of sector-wide improvements from using the framework in the protection of critical infrastructure from cyber threats. (Recommendation 1).

The Secretary of Agriculture, in coordination with the Secretary of Health and Human Services, should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 2).

The Secretary of Defense should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 3).

The Secretary of Energy should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 4).

The Administrator of the Environmental Protection Agency should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 5).

The Administrator of the General Services Administration, in coordination with the Secretary of Homeland Security, should take steps to consult with respective sector partner(s), such as the Coordinating Council and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 6).

The Secretary of Health and Human Services, in coordination with the Secretary of Agriculture, should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 7).

The Secretary of Homeland Security should take steps to consult with respective sector partner(s), such as the SCC and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sectors using existing initiatives. (Recommendation 8).

The Secretary of Transportation, in coordination with the Secretary of Homeland Security, should take steps to consult with respective sector partner(s) such as the SCC and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 9).

The Secretary of the Treasury should take steps to consult with respective sector partner(s), such as the SCC, DHS, and NIST, as appropriate, to collect and report sector-wide improvements from use of the framework across its critical infrastructure sector using existing initiatives. (Recommendation 10).

The report:
https://www.gao.gov/assets/710/704808.pdf

Figure 1: Critical Infrastructure Sectors and Related Sector-Specific Agencies

Source: GAO analysis of Presidential Policy Directive-21 and Critical Infrastructure Protection GAO-18-211; Art Explosion (clip art). | GAO-20-299

Number 2

2020 Review of Solvency II: Opportunities and challenges

Keynote speech by Gabriel Bernardino at the conference '2020 Solvency II Review: Challenges and opportunities', Brussels.

Introduction

It gives me great pleasure to join you today for today's discussions on the 2020 review of Solvency II and it is an honour to open the proceedings.

I would like to thank the Commission for organising this event on the opportunities and challenges of this review.

The implementation of Solvency II has been a step change in how insurers approach their relationship to risk. Since its implementation 4 years ago the insurance industry has better aligned capital to risk, uses a risk-based approach to assess and mitigate risks, which means that it can better price them.

Insurers have also significantly strengthened their governance models and their risk management capacity.

These are all positive outcomes that are both good for insurers and for consumers. After all it is consumers that the regime is designed to protect.

This review is a fundamental step in enabling us to continue to protect policyholders and in maintaining the credibility of the regime.

This review is an opportunity to:

1. Ensure that the regime continues to be fit for purpose by being capable to reflect the evolution of the market conditions.

2. To fine tune the regime to ensure that it is more proportionate to the scale and complexity of risks insured by different types of insurers and creates better conditions for insurers to develop new sound business models.

3. To complete the EU regulatory toolbox by introducing a macro prudential dimension and a minimum harmonisation regarding recovery and resolution and insurance guarantee schemes.

Let me touch on these three areas:

Reflecting the evolution of market conditions

Solvency II was designed in very different market conditions. The on-going ultra-low/ negative interest rate environment has a substantial impact on the business model of insurers, especially on the life insurance side.
So the current approach to interest rate risk in the Solvency II standard formula clearly underestimates the real interest risk rate in a low/negative yield environment.

This is something we have to fix urgently, and EIOPA will come with concrete proposals to do so in a sound technical way.

And conscious of the impact of this adjustment, we will also propose a step-by-step approach to build the needed resilience.

The evolution of market conditions also requires an adjustment in the extrapolation of interest rates.

The current approach does not reflect the market consistent nature of Solvency II and is conducive to the underestimation of technical provisions.

Proportionality and long-term nature of business models

Proportionality has always been an important element in Solvency II. Looking at the experience in the practical implementation of the regime, EIOPA believes that further steps can be taken to increase it, both on the requirements and in the supervisory process.

That is why we have consulted on possible changes in reporting and disclosure: increasing the application of risk-based thresholds that will reduce substantially the reporting requirements for less complex and less riskier undertakings; streamlining and standardising the public disclosure with a clear separation of the information for market participants and simple and short information for consumers; simplifying requirements for captives.

We are now working on ways to increase the effectiveness of the proportionality embedded in the supervisory review process.

But the review also gives us an opportunity to work on sound adjustments to allow insurers to better develop long-term products and long-term investments.

On the top of the consulted material we have been working on a number of elements that hopefully will be tested in the holistic impact assessment in March.

On the volatility adjustment, we are looking at the recalibration of application ratios with the aim that insurers are rewarded for holding illiquid liabilities rather than been penalised for holding liquid liabilities.

On the risk margin, we are exploring ways to reduce its size and volatility, especially for the long-term liabilities, based on the fact that the future capital requirements are not fully independent.

On equity risk, we are reviewing the criteria for the ability to hold equity long-term, by making a link with long-term illiquid liabilities and taking into account that equity investments are managed on a portfolio basis rather than on an individual asset basis.

We are also exploring ways to include a better recognition of non-proportional reinsurance as a legitimate risk-mitigation technique.

All of these adjustments will improve risk-sensitivity, facilitate the design of truly long-term illiquid liabilities and incentivise long-term investments.

Completing the regime

By introducing a macro-prudential dimension we will equip supervisors with better tools to monitor the building up of possible systemic risk in line with the recently approved international framework.

Another important area is the freedom of establishment and to provide services in the Single Market.

While this freedom provides clear benefits to policyholders, we have also witnessed an unfortunately growing number of failures and near misses of insurers, many of them doing business on cross-border basis.

We need to act to stop misuse of these freedoms that has the potential to undermine trust in the Single Market.

Furthermore, we believe that the existing fragmented landscape of national recovery and resolution frameworks could cause significant barriers to the

orderly resolution of insurers, particularly in the case of cross-border groups.

Similarly, there is the need for a minimum harmonised framework for insurance guarantee schemes in terms of scope, coverage and funding to protect policyholders in case of failure.

This is a question of trust and confidence of European consumers in the insurance sector.

What are EIOPA's next steps?

We are analysing very carefully the feedback received and engaging extensively with the different stakeholders.

In March, we will follow up with a holistic impact assessment.

This is an important step for us as it will enable us to collect information on the combined impact of our proposals. It is likely that the holistic impact assessment will still contain some options but I assure you it will be much more streamlined.

By then, we will be reaching the final leg of this part of the journey. Our Opinion to the European Commission is due by 30 June 2020 and we will keep that date.

In conclusion

Europe's insurance sector is significant part of the financial sector. It finances the economy, it provides a large number of jobs and, most importantly, it provides peace of mind and protection for policyholders.

And ultimately, this is why we have Solvency II. So that we can better protect the policyholders.

So, to maintain a robust and credible Solvency II that is part of a Europe that protects and a Europe that puts finance at the service of the economy and citizens. That is our challenge. Ladies and gentlemen, thank you for your time. Enjoy the debate.

Number 3

Methodological principles of insurance stress testing

eiopa
European Insurance and Occupational Pensions Authority

Supervisory bottom-up stress test

A supervisory bottom-up stress test is an exercise run by a supervisor or regulatory authority, in which participating institutions are requested to perform the calculations.

The supervisor provides the stress testing framework, methodologies, adverse stress scenarios, prescribed shocks and guidance on the application of the shocks.

Participants calculate the impact of the prescribed shocks on their balance sheets and capital requirements according to the guidance provided and using their own models.

Supervisory top-down stress test

A supervisory top-down stress test is an exercise performed and run by a supervisor or regulatory authority.

The supervisor determines the impact of a scenario directly based on the regulatory data provided by the insurers using its own framework, models and specifications (i.e. no calculations required from individual institutions).

Bottom-up and top-down tests can be run in isolation but can also be seen as complementary exercises in which top-down approaches can be used in a bottom-up stress test for validation purposes.

The paper:
https://www.eiopa.europa.eu/sites/default/files/publications/methodological-principles-insurance-stress-testing.pdf

Number 4

CISA INSIGHTS
Risk Management for Novel Coronavirus (COVID-19)

The Threat and How to Think About It

This product is for executives to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread of Novel Coronavirus, or COVID-19.

According to the U.S. Centers for Disease Control and Prevention (CDC), COVID-19 has been detected in locations around the world, including multiple areas throughout the U.S. This is a rapidly evolving situation and for more information, visit the CDC's COVID-19 Situation Summary.

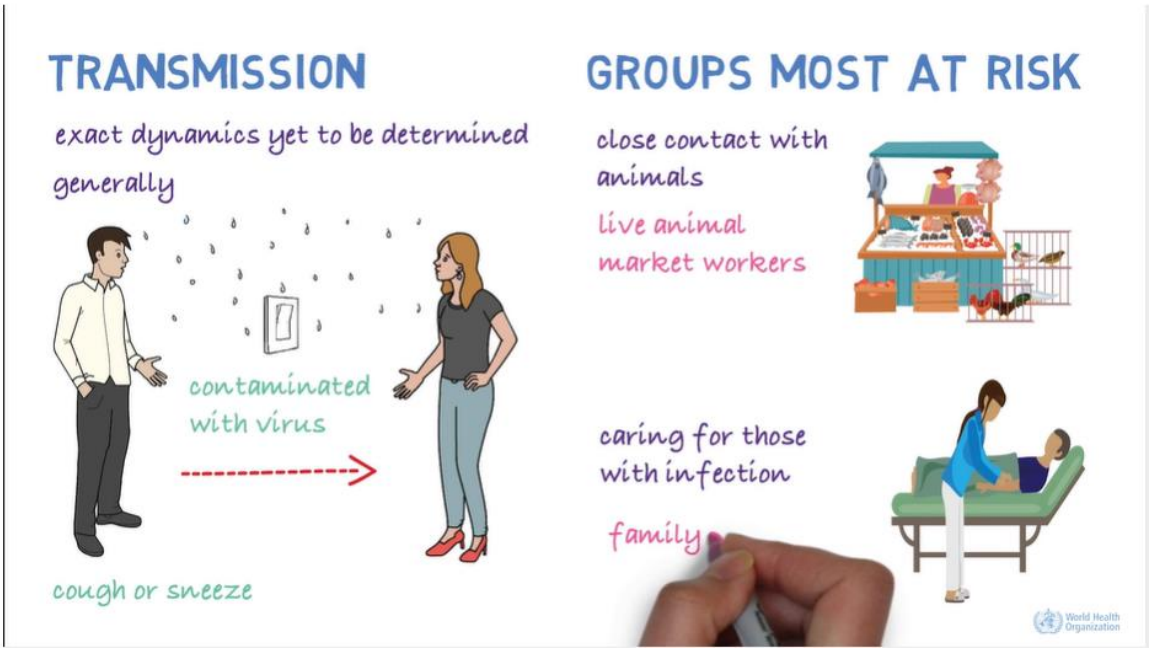
To read more:
https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf

https://www.cdc.gov/coronavirus/2019-ncov/summary.html

Number 5

Online training as a weapon to fight the new coronavirus

The learning team of the WHO Health Emergencies Programme worked with technical experts to quickly develop and publish the online course – you may visit: https://openwho.org/courses/introduction-to-ncov



Approximately 3000 new users have registered for the training every day since its launch, demonstrating the high level of interest in the virus among health professionals and the general public.

In addition, more than 200 000 people have viewed the introductory video to the course on YouTube.

The high engagement levels emerged as the international community launched a US$675 million preparedness and response plan to fight further spread of the new coronavirus and protect states with weaker health systems.

The free learning resource is available to anyone interested in novel coronavirus on WHO's open learning platform for emergencies, OpenWHO.org.

The platform was established 3 years ago with emergencies such as nCoV in mind, in which WHO would need to reach millions of people across the globe with real-time, accessible learning materials.

The online training – entitled "Emerging respiratory viruses, including nCoV: methods for detection, prevention, response and control" – is currently being produced in all official UN languages and Portuguese.

"Our job is to work with technical health experts to package knowledge using adult learning principles, quickly so that it is most useful to health workers and our staff," said Heini Utunen, who manages OpenWHO for the WHO Health Emergencies Programme (WHE).

"Our online platform – OpenWHO – is already accessed by users from every country on earth, providing more than 60 courses in 21 languages. Delivering trainings in the local language of responders is really important, especially in an emergency".

WHE has been investing in learning and training to strengthen preparedness and real-time response to health emergencies.

The programme developed its first-ever learning strategy in 2018 and has a small dedicated Learning and Capacity Development Unit that allows WHE to develop trainings quickly and get know-how to those who most need it at the front line.

For the latest information on the new coronavirus, visit the 2019-nCoV page.

Number 6

Interim Guidance for Businesses and Employers

Centers for Disease Control and Prevention
CDC 24/7: Saving Lives, Protecting People™

This interim guidance is based on what is currently known about the coronavirus disease 2019 (COVID-19). The Centers for Disease Control and Prevention (CDC) will update this interim guidance as needed and as additional information becomes available.

The following interim guidance may help prevent workplace exposures to acute respiratory illnesses, including COVID-19, in non-healthcare settings. The guidance also provides planning considerations if there are more widespread, community outbreaks of COVID-19.

Recommended strategies for employers to use now:

1. Actively encourage sick employees to stay home:

- Employees who have symptoms of acute respiratory illness are recommended to stay home and not come to work until they are free of fever (100.4° F [37.8° C] or greater using an oral thermometer), signs of a fever, and any other symptoms for at least 24 hours, without the use of fever-reducing or other symptom-altering medicines (e.g. cough suppressants). Employees should notify their supervisor and stay home if they are sick.

- Ensure that your sick leave policies are flexible and consistent with public health guidance and that employees are aware of these policies.

- Talk with companies that provide your business with contract or temporary employees about the importance of sick employees staying home and encourage them to develop non-punitive leave policies.

- Do not require a healthcare provider's note for employees who are sick with acute respiratory illness to validate their illness or to return to work, as healthcare provider offices and medical facilities may be extremely busy and not able to provide such documentation in a timely way.

- Employers should maintain flexible policies that permit employees to stay home to care for a sick family member. Employers should be aware

that more employees may need to stay at home to care for sick children or other sick family members than is usual.

2. Separate sick employees:

CDC recommends that employees who appear to have acute respiratory illness symptoms (i.e. cough, shortness of breath) upon arrival to work or become sick during the day should be separated from other employees and be sent home immediately. Sick employees should cover their noses and mouths with a tissue when coughing or sneezing (or an elbow or shoulder if no tissue is available).

3. Emphasize staying home when sick, respiratory etiquette and hand hygiene by all employees:

- Place posters that encourage staying home when sick, cough and sneeze etiquette, and hand hygiene at the entrance to your workplace and in other workplace areas where they are likely to be seen.

- Provide tissues and no-touch disposal receptacles for use by employees.

- Instruct employees to clean their hands often with an alcohol-based hand sanitizer that contains at least 60-95% alcohol, or wash their hands with soap and water for at least 20 seconds. Soap and water should be used preferentially if hands are visibly dirty.

- Provide soap and water and alcohol-based hand rubs in the workplace. Ensure that adequate supplies are maintained. Place hand rubs in multiple locations or in conference rooms to encourage hand hygiene.

- Visit the coughing and sneezing etiquette and clean hands webpage for more information.

4. Perform routine environmental cleaning:

- Routinely clean all frequently touched surfaces in the workplace, such as workstations, countertops, and doorknobs. Use the cleaning agents that are usually used in these areas and follow the directions on the label.

- No additional disinfection beyond routine cleaning is recommended at this time.

- Provide disposable wipes so that commonly used surfaces (for example, doorknobs, keyboards, remote controls, desks) can be wiped down by employees before each use.

5. Advise employees before traveling to take certain steps:

- Check the CDC's Traveler's Health Notices for the latest guidance and recommendations for each country to which you will travel. Specific travel information for travelers going to and returning from China, and information for aircrew, can be found at on the CDC website.

- Advise employees to check themselves for symptoms of acute respiratory illness before starting travel and notify their supervisor and stay home if they are sick.

- Ensure employees who become sick while traveling or on temporary assignment understand that they should notify their supervisor and should promptly call a healthcare provider for advice if needed.

- If outside the United States, sick employees should follow your company's policy for obtaining medical care or contact a healthcare provider or overseas medical assistance company to assist them with finding an appropriate healthcare provider in that country. A U.S. consular officer can help locate healthcare services. However, U.S. embassies, consulates, and military facilities do not have the legal authority, capability, and resources to evacuate or give medicines, vaccines, or medical care to private U.S. citizens overseas.

6. Additional Measures in Response to Currently Occurring Sporadic Importations of the COVID-19:

- Employees who are well but who have a sick family member at home with COVID-19 should notify their supervisor and refer to CDC guidance for how to conduct a risk assessment of their potential exposure.

- If an employee is confirmed to have COVID-19, employers should inform fellow employees of their possible exposure to COVID-19 in the workplace but maintain confidentiality as required by the Americans with Disabilities Act (ADA). Employees exposed to a co-worker with confirmed COVID-19 should refer to CDC guidance for how to conduct a risk assessment of their potential exposure.

The severity of illness or how many people will fall ill from COVID-19 is unknown at this time. If there is evidence of a COVID-19 outbreak in the

U.S., employers should plan to be able to respond in a flexible way to varying levels of severity and be prepared to refine their business response plans as needed.

For the general American public, such as workers in non-healthcare settings and where it is unlikely that work tasks create an increased risk of exposures to COVID-19, the immediate health risk from COVID-19 is considered low.

The CDC and its partners will continue to monitor national and international data on the severity of illness caused by COVID-19, will disseminate the results of these ongoing surveillance assessments, and will make additional recommendations as needed.

To read more:
https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html

Number 7

BIS Working Papers No 846
Financial Crises and Innovation

by Bryan Hardy and Can Sever, Monetary and Economic Department, March 2020

Focus

Growth and productivity are persistently low following financial crises. This paper examines how financial crises affect innovation. Patents are an important measure of the kind of innovative activity that can lead to productivity gains.

We study patent data from a broad sample of countries and financial crises and consider impacts up to 10 years after a crisis.

Contribution

This is the first cross-country study on how financial crises affect patenting. Our sample includes crisis episodes of different types across many different countries.

This allows us to establish general patterns connecting financial crises and innovative activity.

We distinguish between types of crises and recessions to understand these outcomes better.

Findings

Some industries are more reliant on external funding, such as from banks, to finance their activities. We find that these industries decrease their patenting more following a financial crisis than other industries.

The effect is persistent, lasting upwards of 10 years, and is specific to banking crises.

This indicates that when firms lose access to bank credit, they may be forced to drop new and ongoing R&D projects. This results in fewer patents over the following years.

These results provide a link between financial crises and the sustained decline in output and productivity observed after a recession.

Abstract

Financial crises are accompanied by permanent drops in economic growth and output.

Technological progress and innovation are important drivers of economic growth. This paper studies how financial crises affect innovative activities.

Using cross-country panel data on patenting at the industry-level, we identify a financial channel whereby disruptions in financial markets impact patenting activity.

Specifically, we find that patenting decreases more following banking crises for industries that are more dependent on external finance.

This financial channel is not at play during currency crises, sovereign debt crises, or recessions more generally, suggesting that disruption in banking activity matters for investment in innovative activities.

The effect on patenting is economically large and long-lasting, resulting in less patenting, in terms of both total quantity and quality, for 10 years or longer after a banking crisis.

The average patent quality, however, does not appear to decline. We show the results are not likely to be driven by reverse causality or omitted variables.

These findings provide a link between banking crises and the observed patterns of lower long-term growth. Liquidity support in the aftermath of banking crises appears to help reduce the effects through the financial channel over the short term.

To read more: https://www.bis.org/publ/work846.pdf

Number 8

Asking Strategic Questions
A Primer for National Security Professionals

By Andrew Hill and Stephen J. Gerras, Joint Force Quarterly 96.

Your teachers lied to you: some questions really are stupid. At best, a bad question wastes time and energy by distracting from what is important.

At worst, it sets one up for failure, either by asking the wrong question or presuming the wrong answer to the right question.

These problems are even more pronounced in the military, where a powerful culture of obedience responds to a leader's curiosity with a frenzy of activity that may or may not be useful.

Because leaders have so much power over which questions organizations ask, it is essential that leaders understand the basic characteristics of good strategic questions.

We use the term *strategic* to differentiate the questions that shape and inform strategy—the focus of this article—from the wide variety of questions that organizations may explore.

For example, what are the essential characteristics of 21st-century military leaders?

Are we selecting for and developing these characteristics?

What are U.S. military options in dealing with [nation X]?

How will [nation X] respond to different military actions?

What are the most significant current capability needs of the U.S. Army?

How should we prioritize those needs?

These are all strategic questions—difficult to answer, but useful to ask and explore. In this article, we propose guidelines for asking questions designed to improve an organization's performance amid competitive uncertainty.

To read more:
https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-96/jfq-96.pdf

Number 9

Consumers urged to secure internet connected cameras

This week, with the support from Which? (https://www.which.co.uk/news/2020/03/consumers-urged-to-secure-internet-connected-cameras-in-the-home/), we published new consumer advice and guidance on how to secure internet connected cameras in the home (https://www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home).

We're all becoming more reliant on 'smart' technology, and things like connected security cameras and baby monitors help make our lives easier. However, insecure default settings can leave devices vulnerable to cyber criminals.

In rare cases, live feeds or images from smart cameras can be accessed by unauthorised users and that's why we outlined three steps people can take to make their devices safer:

- If your camera comes with a default password, change it to a secure one – connecting three random words which you'll remember is a good way to do this. You can usually change your password using the app you use to manage the device.

- Keep your camera secure by regularly updating security software. Not only does this keep your devices secure, but often adds new features and other improvements.

- If you do not use the feature that lets you remotely access the camera from the internet, it is recommended you disable it.

The NCSC is supporting the Department for Digital, Culture, Media & Sport (DCMS) in the development of future UK legislation, which will ensure consumer smart devices sold in the UK adhere to three rigorous security requirements. These are:

1. Device passwords must be unique and not resettable to any universal factory setting

2. Manufacturers must provide a public point of contact so anyone can report a vulnerability

3. Manufacturers & retailers must state the minimum length of time for which the device will receive security updates.

More information at:
https://www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home

Number 10

Building Hardware to Enable Continuous Data Protections

Program aims to develop novel hardware accelerator to ease computational challenges preventing widespread use of fully homomorphic encryption

The safety and security of critical information – whether it is sensitive intellectual property (IP), financial information, personally identifiable information (PII), intelligence insight, or beyond – is of vital importance.

Conventional data encryption methods or cryptographic solutions, such as Advanced Encryption Standards (AES), translate data into a secret "code" that can only be decoded by people with access to a decryption key.

These methods protect data as it is transmitted across a network or at rest while in storage. Processing or computing on this data however requires that it is first decrypted, exposing it to numerous vulnerabilities and threats.

Fully homomorphic encryption (FHE) offers a solution to this challenge. FHE enables computation on encrypted data, or ciphertext, rather than plaintext, or unencrypted data – essentially keeping data protected at all times.

The benefits of FHE are significant, from enabling the use of untrusted networks to enhancing data privacy.

Despite its potential, FHE requires enormous computation time to perform even simple operations, making it exceedingly impractical to implement with traditional processing hardware.

FHE relies on a particular type of cryptography called lattice cryptography, which presents complex mathematical challenges to would-be attackers that require technologies beyond the current state of the art to solve.

While effective at keeping data protected, the challenge with modern lattice-based FHE is the unavoidable accumulation of noise with each calculation performed.

With each homomorphic computation, a certain amount of noise – or error – is generated that corrupts the encrypted data representation.

Once this noise accumulation reaches a certain point, it becomes impossible to recover the original underlying plaintext. Essentially, the data in need of protection is now lost.

Computational structures called “bootstrapping” help address this untenable noise accumulation, reducing it to a level that is comparable to the original plaintext, but produces massive compute overhead to perform.

“While a number of solutions have been developed, running FHE in software on standard processing hardware remains a nearly impossible challenge,” said DARPA program manager, Dr. Tom Rondeau.

“Under previous programs like the Programming Computation on Encrypted Data (PROCEED) program, DARPA helped uncover FHE algorithms and proved what could be possible with FHE running on standard CPUs. It also shed light on the compute penalty and critical limitations of the technology.

Today, DARPA is continuing to invest in the exploration of FHE, focusing on a re-architecting of the hardware, software, and algorithms needed to make it a practical, widely usable solution.”

DARPA developed the Data Protection in Virtual Environments (DPRIVE) program to design and implement a hardware accelerator for FHE computations that aims to significantly reduce the current computational burden to drastically speed up FHE calculations.

DPRIVE specifically seeks to reduce the computational run time overhead by many orders of magnitude compared to current software-based FHE computations on conventional CPUs, and accelerate FHE calculations to within one order of magnitude of current performance on unencrypted data.

Key to DPRIVE is the exploration of Large Arithmetic Word Size (LAWS) data representations. LAWS can help address the challenges of noise accumulation with FHE computations and the compute overhead currently encountered using conventional CPU architectures and software, creating enormous improvements in processing speed and computation runtime.

Current standard CPUs are based on 64-bit words, which are the units of data that determine a particular processor’s design.

Word size directly relates to the signal-to-noise ratio of how encrypted data is stored and processed, as well as the error generated each time an FHE calculation is processed.

Recent studies demonstrate that using words that are thousands of bits long – or LAWS – increases the signal-to-noise ratio in FHE computations, which equates to less noise accumulating with each compute step.

This means that more calculations can be performed before the irreparable noise threshold is reached where data can no longer be recovered.
It also means the overhead compute burden from costly operations like bootstrapping is dramatically reduced.

Unfortunately, current processing hardware – the traditional 64-bit CPUs – are not built to handle these extremely long word lengths.

While virtualization of larger bit word sizes is possible, processing them on traditional CPUs requires reducing them down to word sizes of 64-bits or less while continuing to encounter the associated overhead challenges.

DPRIVE seeks to develop a hardware accelerator that can process LAWS without this word size reduction and overhead, instead natively processing on LAWS of 1024 bits or more.

To develop the target accelerator, DPRIVE will explore new integrated approaches to the full FHE hardware and software stacks.

Specifically, the program seeks to develop novel approaches to memory management, flexible data structures and programming models, and formal verification methods that ensure the design of the FHE implementation is effective and accurate.

As the co-design of FHE algorithms, hardware, and software will be critical to the program, it will require teams with varied technical expertise to take on the research objectives.

"DPRIVE is looking to solve a really hard technical challenge that will involve a deep understanding of mathematics, algorithms, software, hardware, and circuit design.

I expect that there are very few organizations that have the needed expertise in all of these areas, which are each critical to the program's success. As a result, I anticipate very interesting teams will form to cover the breadth of the research," said Rondeau.

DARPA is hosting a Proposers Day meeting on March 2, 2020, in Cupertino, California to provide more information about DPRIVE to interested researchers.

Find out more at:
https://beta.sam.gov/opp/45fa60ee9d194ba9992dc054eba962b6/view?keywords=DPRIVE&sort=-relevance&index=opp&is_active=true&page=1

Full program details are available in the Broad Agency Announcement, which is posted here:
https://beta.sam.gov/opp/9ee364e4fff749678383ffd6cc447cfd/view?keywords=darpa%20DPRIVE&sort=-relevance&index=opp&is_active=true&page=1&date_filter_index=0&inactive_filter_values=false

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.

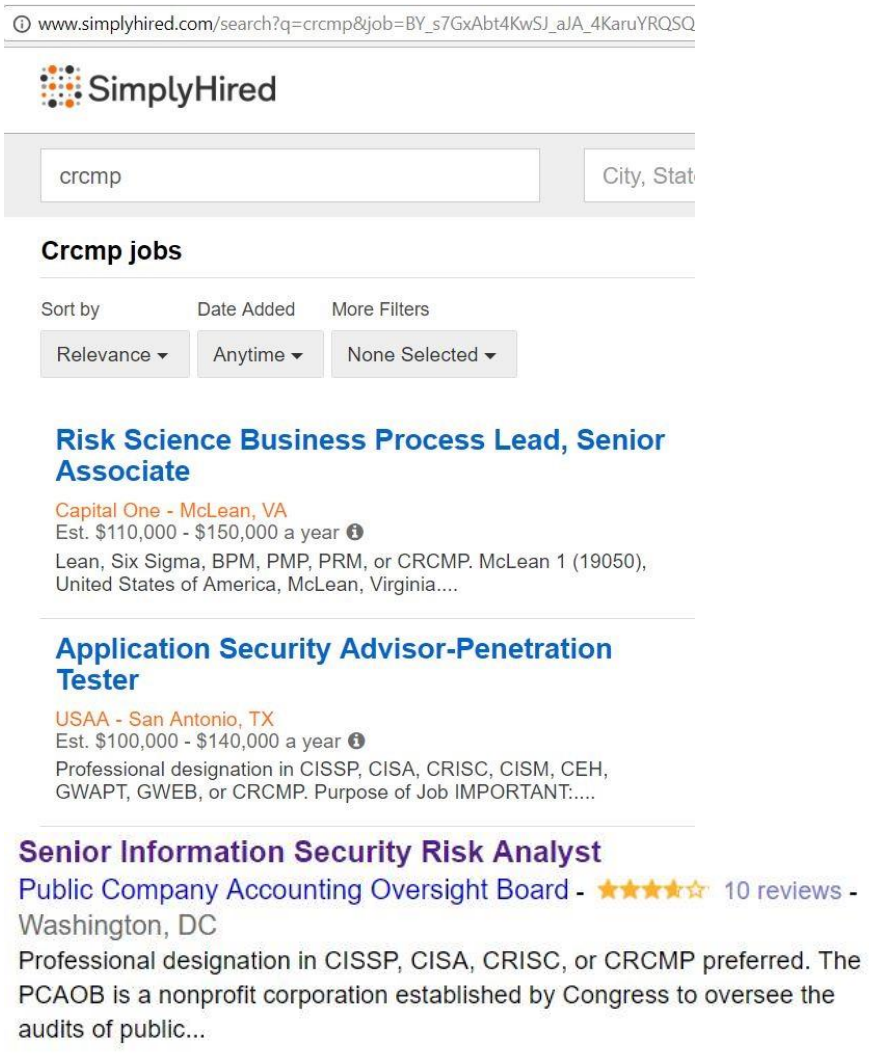
International Association of Risk and Compliance Professionals

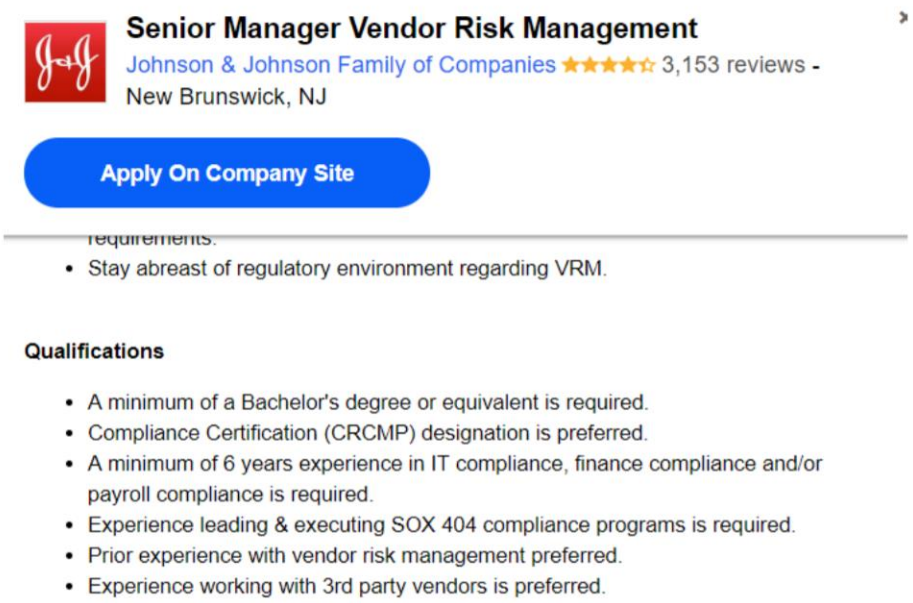
You can explore what we offer to our members:

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