Monday, January 25, 2021

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

Dear members and friends,

According to Lord (2006), *transparency* is a condition in which information about priorities, intentions, capabilities, and behavior of powerful organizations is widely available to the global public.

Lord continues: “Transparency is not synonymous with truth. It may reveal actual or perceived facts, actual or perceived falsehoods, behavior, intentions, ideas, values, and opinions. It may reveal neutral, empirically verifiable information or propaganda specifically designed to advance a particular cause or view”.

Although we all know that transparency has become increasingly important to consumers and investors over the last several years, we also know that very few investors examine thoroughly all information available. This is the reason I am always pleased to learn that some experts are really great in visualizing and interpreting the data.

The Securities and Exchange Commission has just announced awards to whistleblowers, who provided high-quality information that led to successful enforcement actions. For example, the SEC awarded more than $100,000 to a whistleblower whose independent analysis led to a successful enforcement action.

Among other things, the whistleblower conducted an analysis using information from publicly available documents to calculate an estimate of an important metric for a company, and then showed that the company's disclosures regarding that metric were implausible.

Read more at number 8 below.

I want also to remind you that *curiosity killed the cat*. If you receive an email that offers a great video attached about Donald Trump and his sex scandals, *do not open it*.

The attachment TRUMP_SEX_SCANDAL_VIDEO.jar installs Qua or Quaverse RAT (QRAT) onto your system.

QRAT is a Remote Access Trojan (RAT) based on Java programming language, that allows adversaries remotely control infected computers. Attackers can:

- steal passwords that are saved on browsers and email clients,
- log keystrokes,
- execute commands,
- access files,
- download and execute files,
- view victim's screen, and much more.

It is very easy to get your device infected. Email attachments, plug-ins "necessary" to access content, downloads from dubious pages, even clicking on advertisements on questionable web pages can result in an infection.

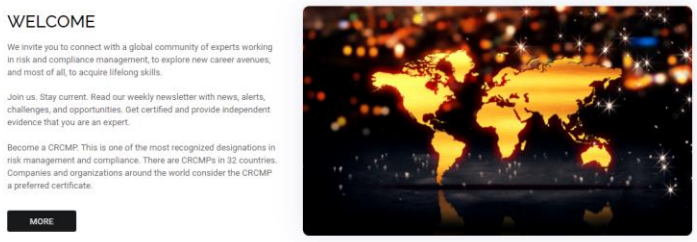
Foreign state-sponsored agents always find opportunities to exploit. If 1% of our employees are curious to see Donald Trump naked, we have a major problem.

Welcome to the top 10 list.

Best regards,

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

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



National Cyber Security Centre

Number 7 (Page 19)

Reviving and Restructuring the Corporate Sector Post-Covid

G30 GROUP OF THIRTY

Number 8 (Page 21)

SEC Issues Over $1.1 Million to Multiple Whistleblowers

Number 9 (Page 23)

Call for expression of interest in the appointment of members of the Board of Appeal of the three European Supervisory Authorities for the financial services sector

Official Journal
of the European Union

Number 10 (Page 25)

Night-Vision Revolution: Less Weight, Improved Performance

Leveraging new tech, DARPA aims for night-vision goggles the size and weight of regular eyeglasses

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

Covid-19 and cyber risk in the financial sector

Bank for International Settlements, Iñaki Aldasoro, Jon Frost, Leonardo Gambacorta, David Whyte

Key takeaways

• The financial sector has been hit by hackers relatively more often than other sectors during the Covid19 pandemic.

• While this has not yet led to significant disruptions or a systemic impact, there are substantial risks from cyber attacks for financial institutions, their staff and their customers going forward.

• Financial authorities are working to mitigate cyber risks, including through international cooperation.

During the Covid-19 pandemic, financial institutions have been at the leading edge of the response to cyber risk.

Their already large exposure to cyber risk has been further accentuated by the move towards more working from home (WFH) and other operational challenges.

This Bulletin serves as a primer on cyber risk and presents initial findings on how the financial sector has met the challenges of the pandemic.

We draw on new data to assess changes in the threat landscape for financial institutions in the pandemic.

Cyber risk: a taxonomy

As the economy and financial system become more digitised, cyber risk is growing in importance.

"Cyber risk" is an umbrella term encompassing a wide range of risks resulting from the failure or breach of IT systems.

According to the FSB Cyber Lexicon (2019), cyber risk refers to "the combination of the probability of cyber incidents occurring and their impact".

A “cyber incident”, in turn, is “any observable occurrence in an information system that:

(i) jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or

(ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not”.

Cyber risk is one form of operational risk (Aldasoro et al (2020b), CPMI-IOSCO (2016)).

Cyber risks can be classified based on their cause/method, actor, intent and consequence (Aldasoro et al (2020a), Curti et al (2019)).

The causes or methods vary, and include both unintended incidents and intentional attacks.

Examples of the former are accidental data disclosure, and implementation, configuration and processing errors.

Such incidents are frequent. Yet around 40% of cyber incidents are intentional and malicious, rather than accidental, ie they are cyber attacks (Aldasoro et al (2020c)).

Some cyber attacks involve threat actors inserting themselves into a trusted data exchange.

Malware (ie “malicious software”) is software designed to cause damage to IT devices and/or steal data (for example, so-called Trojans, spyware and ransomware).

Man-in-the-middle attacks occur when attackers insert themselves into a two-party transaction (Graph 1, first panel), accessing or manipulating data or transactions.

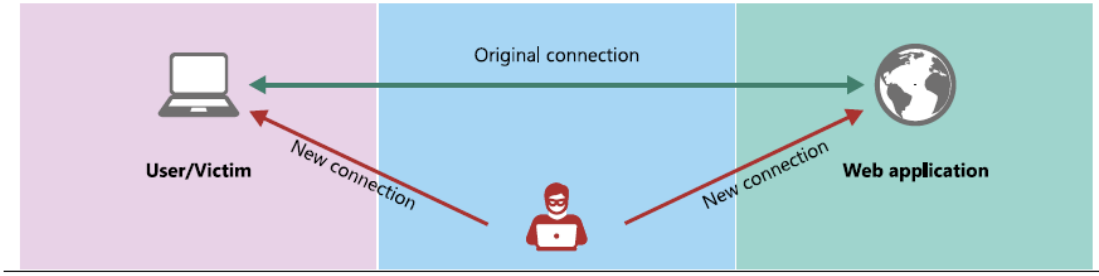
Cross-site scripting is a web security vulnerability that allows attackers to compromise the interactions a victim has with a vulnerable application. Phishing is stealing sensitive data or installing malware with fraudulent emails that appear to be from a trustworthy source (Graph 1, second panel).

To gain a victim’s trust, phishing attacks may imitate trusted senders.

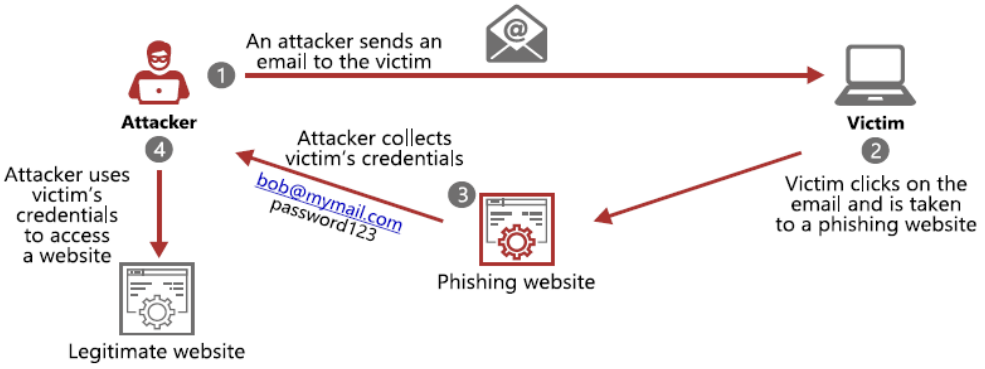
After gaining entrance, these may help attackers to gain credentials and entry into a system.

Selected causes of cyber attacks Graph 1

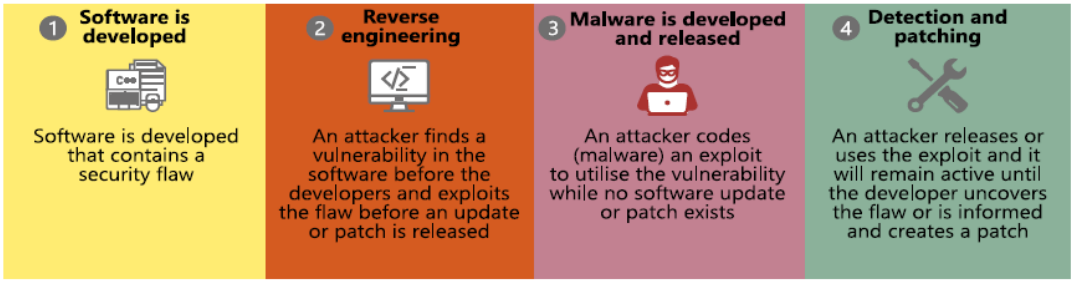
Man-in-the-middle



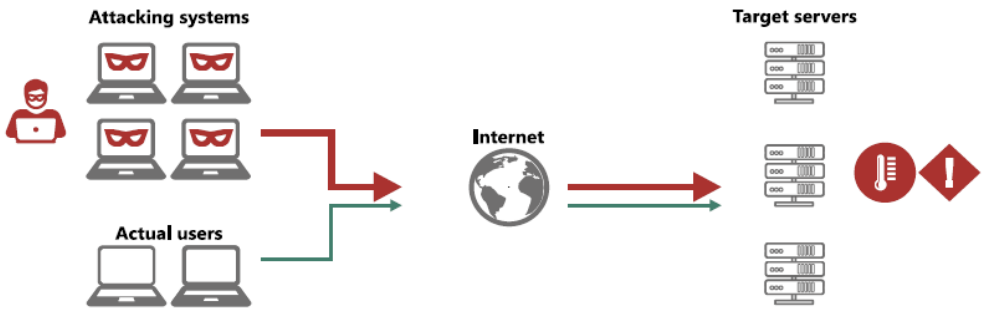
Phishing



Timeline of zero-day vulnerabilities



Distributed denial-of-service (DDoS) attack

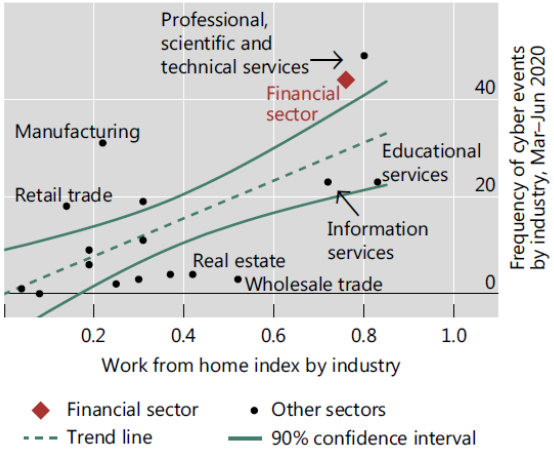


Source: Authors' elaboration.

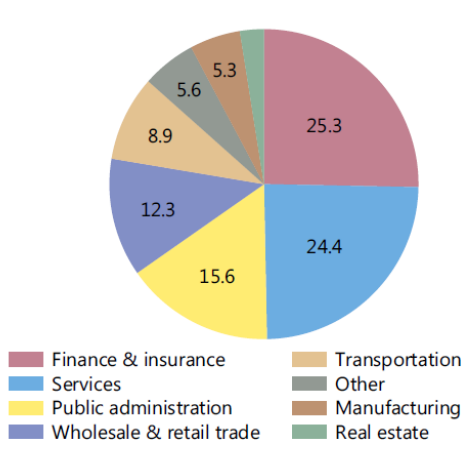
Password cracking is the process of recovering secret passwords stored in a computer system or transmitted over a network.

The financial sector has been hit by cyber attacks during the pandemic Graph 2

WFH index versus cyber events during Covid-19[1]



Covid-19-related cyber events by sector[2]



[1] Excludes the health sector. [2] Based on cases classified by Advisen as Covid-19-related. Includes data up to 9 September 2020. The sample in the graph excludes the health sector (57 Covid-related cases) and affecting health-related items of the manufacturing sector (163 cases).

Sources: Dingel and Neiman (2020); Advisen; authors' calculations.

To read more: https://www.bis.org/publ/bisbull37.pdf

Number 2

Cyberattack on EMA

EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Update 1

The full investigation launched by the European Medicines Agency (EMA), in close cooperation with law enforcement and other relevant entities, demonstrated that data has been breached. An initial review revealed that a limited number of documents belonging to third parties were unlawfully accessed. The concerned companies are being informed.

The Agency remains fully functional and its timelines related to the evaluation and approval of COVID-19 vaccines and treatments are not affected.

EMA will continue to provide information in due course, to the extent possible, given its duty towards the ongoing investigations.

Update 2

EMA has engaged a specialised third-party service provider to support the full investigation that is currently being carried out in close cooperation with law enforcement and other relevant entities. This company will contribute to the additional security measures that are being put in place in response to the data breach.

So far, the investigation has revealed that a limited number of documents belonging to third parties were unlawfully accessed. The concerned third parties identified at this stage have been contacted and duly informed.

The Agency remains fully functional and its timelines related to the evaluation and approval of COVID-19 vaccines and treatments are not affected.

EMA will continue to provide information in due course, to the extent possible, given its duty towards the ongoing investigations.

Update 3

The ongoing investigation of the cyberattack on EMA, carried out by the Agency in close collaboration with law enforcement and other relevant entities, has revealed that the data breach was limited to one IT application. The perpetrators primarily targeted data related to COVID-19 medicines

and vaccines and unlawfully accessed documents belonging to third parties. The companies concerned at this stage have been contacted and duly informed.

As the investigation proceeds, and all potentially suspicious activity is analysed, the Agency will ensure that any additional third party whose documents may have been subject to unauthorised access is notified.

The Agency and the European medicines regulatory network remain fully functional and timelines related to the evaluation and approval of COVID-19 medicines and vaccines are not affected.

EMA will continue to provide information in due course, to the extent possible, given its duty towards the ongoing investigation.

Update 4

The ongoing investigation of the cyberattack on EMA revealed that some of the unlawfully accessed documents related to COVID-19 medicines and vaccines belonging to third parties have been leaked on the internet. Necessary action is being taken by the law enforcement authorities.

The Agency continues to fully support the criminal investigation into the data breach and to notify any additional entities and individuals whose documents and personal data may have been subject to unauthorised access.

The Agency and the European medicines regulatory network remain fully functional and timelines related to the evaluation and approval of COVID-19 medicines and vaccines are not affected.

EMA will continue to provide information in due course, to the extent possible, given its duty towards the ongoing investigation.

You may visit:
https://www.ema.europa.eu/en/news/cyberattack-ema-update-4

Number 3

Good practices in innovation on cybersecurity under the NCSS

The online Digital Single Market (DSM) is in increasing jeopardy from various forms of cyberattacks.

The need for a strong and effective EU Network and Information Security (NIS) Industry becomes two-fold; on the one hand the DSM needs NIS protection for commercial services, critical infrastructure and the everyday life of its citizens, who depend on online services.

On the other hand, the DSM offers opportunities and tools that can facilitate the growth of the EU NIS Industry.

Growth of the NIS industry can occur with direct benefits in terms of revenue for NIS suppliers, growth of the EU GDP and boost of employment in the cybersecurity sector; the latter is of particular importance considering that cybersecurity is one of the faster growing segments of the ICT industry.

To achieve this, innovation in cybersecurity is a key enabler.

ENISA supports the efforts aimed to enhance the overall level of cybersecurity in the Member States (MS) both at a national and EU level.

This report supports that effort by analysing how Member States are approaching innovation as a strategic priority under National Cyber Security Strategies (NCSS).

The analysis is structured around several aspects of innovation such as: Innovation Priorities, Industrialisation and Collaboration and Market and Policy.

Each of these aspects is at the same time divided into two dimensions. Innovation priorities can be divided into Innovation in technologies and services, and into economic incentives and investments.

Industrialisation and collaboration can be divided into industrialisation processes and activities, and stakeholders' collaboration.

Market and Policy can be divided into Market and Technology Alignment and Market regulation.

Each dimension can be supported by several activities and mechanisms.

Moreover, this study identifies a set of challenges and good practices, as experts perceive them, across the different innovation dimensions.

The identification of these challenges may help in identifying relevant actions for addressing them and also in drafting future innovation strategic objectives.

Finally, this report identifies seven recommendations that can be taken into account both at National and EU level to support the development of cybersecurity innovation strategies and enhance their impact:

1. Support and develop sector specific innovation priorities.

2. Support sufficient and adequate level of funding.

3. Involve stakeholders while developing and implementing innovation strategies.

4. Take into account the positive impact of regulatory frameworks on innovation.

5. Support industries in positioning new cybersecurity offerings in the market.

6. Promote EU level certification of services/products.

7. Promote NIS training and educational measures.

These recommendations form a roadmap for enhancing innovation on cybersecurity under NCSS.

Stakeholders who are involved in defining national cybersecurity strategies may take into account the results of this study, in particular, may take into account the identified challenges, good practices and suggested recommendations.

To read more:
https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss

Number 4

Joint statement - FBI, CISA, ODNI, NSA

On behalf of President Trump, the National Security Council staff has stood up a task force construct known as the Cyber Unified Coordination Group (UCG), composed of the FBI, CISA, and ODNI with support from NSA, to coordinate the investigation and remediation of this significant cyber incident involving federal government networks.

The UCG is still working to understand the scope of the incident but has the following updates on its investigative and mitigation efforts.

This work indicates that an Advanced Persistent Threat (APT) actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks.

At this time, we believe this was, and continues to be, an intelligence gathering effort. We are taking all necessary steps to understand the full scope of this campaign and respond accordingly.

The UCG believes that, of the approximately 18,000 affected public and private sector customers of Solar Winds' Orion product, a much smaller number have been compromised by follow-on activity on their systems.

We have so far identified fewer than ten U.S. government agencies that fall into this category, and are working to identify and notify the nongovernment entities who also may be impacted.

This is a serious compromise that will require a sustained and dedicated effort to remediate.

Since its initial discovery, the UCG, including hardworking professionals across the United States Government, as well as our private sector partners have been working non-stop.

These efforts did not let up through the holidays.

The UCG will continue taking every necessary action to investigate, remediate, and share information with our partners and the American people.

As the lead agency for threat response, the FBI's investigation is presently focused on four critical lines of effort: identifying victims, collecting evidence, analyzing the evidence to determine further attribution, and sharing results with our government and private sector partners to inform operations, the intelligence picture, and network defense.

As the lead for asset response, CISA is focused on sharing information quickly with our government and private sector partners as we work to understand the extent of this campaign and the level of exploitation.

CISA has also created a free tool for detecting unusual and potentially malicious activity related to this incident.

In an Emergency Directive posted December 14, CISA directed the rapid disconnect or power-down of affected SolarWinds Orion products from federal networks.

CISA also issued a technical alert providing technical details and mitigation strategies to help network defenders take immediate action.

CISA will continue to share any known details as they become available.

As the lead for intelligence support and related activities, ODNI is coordinating the Intelligence Community to ensure the UCG has the most up-to-date intelligence to drive United States Government mitigation and response activities.

Further, as part of its information-sharing mission, ODNI is providing situational awareness for key stakeholders and coordinating intelligence collection activities to address knowledge gaps.

Lastly, the NSA is supporting the UCG by providing intelligence, cybersecurity expertise, and actionable guidance to the UCG partners, as well as National Security Systems, Department of Defense, and Defense Industrial Base system owners.

NSA's engagement with both the UCG and industry partners is focused on assessing the scale and scope of the incident, as well as providing technical mitigation measures.

The UCG remains focused on ensuring that victims are identified and able to remediate their systems, and that evidence is preserved and collected. Additional information, including indicators of compromise, will be made public as they become available.

CISA suspicious activity detection tool:
https://github.com/cisagov/Sparrow

Number 5

MoUs with UK authorities in the area of insurance and pensions

On 5 March 2019, the European Insurance and Occupational Pensions Authority (EIOPA) and all national competent authorities (NCAs) of the European Economic Area (EEA) with competencies in insurance agreed memoranda of understanding (MoUs) with the Bank of England in its capacity as the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) of the United Kingdom (UK).

The MoUs took effect on 1 January 2021, at the end of the transition period following the departure of the UK from the European Union.

The following MoUs were agreed:

- A multilateral MoU on supervisory cooperation, enforcement and information exchange between the EEA NCAs and the UK Authorities.

- A bilateral MoU between EIOPA and the UK Authorities on information exchange and mutual assistance in the field of insurance regulation and supervision.

These MoUs ensure cooperation in the fields of insurance prudential and conduct supervision, for mutual assistance and regular exchange of information.

In addition, EIOPA has agreed a multilateral memorandum of understanding with the Pensions Regulator, which also came into effect on 1 January 2021.

Visit the dedicated webpage for more information related to the UK's departure from the European Union at:
https://www.eiopa.europa.eu/brexit-communication

Number 6

HMRC warn of COVID-19 scam text messages

National Cyber Security Centre

Cyber criminals are continuing to exploit COVID-19 concerns - this time with scam text messages about a non-existent government grant.

The message offers the prospect of financial support as the UK moves into another lockdown, but no such grant exists and HMRC has warned people to be vigilant to this threat.

The phishing scam takes the victim to a fake website masquerading as GOV.UK which asks for financial information. A number of spelling and grammatical mistakes in the message give a clue that it is a scam.

It's important to know that HMRC will never offer a tax refund by text, email or phone. HMRC have issued some advice for those concerned about this particular scam. You may visit:
https://www.gov.uk/government/organisations/hm-revenue-customs/contact/reporting-fraudulent-emails

275 HMRC-related scams have been uncovered since March with HMRC taking action against 254 scam webpages. They have also responded to more than 300,000 reports of phone scams from the public.

The NCSC has also published advice on how to spot and deal with suspicious text messages, emails and phone calls. You may visit:
https://www.ncsc.gov.uk/guidance/suspicious-email-actions

Don't forget that you can also report phishing emails direct to the NCSC using the Suspicious Email Reporting Service (SERS).

Number 7

Reviving and Restructuring the Corporate Sector Post-Covid

G30 GROUP OF THIRTY

The coronavirus pandemic, by dramatically changing consumption patterns and business operations, is triggering a major corporate solvency crisis in many countries.

Apart from policies directly supporting employment, initial policy responses to support businesses focused heavily on liquidity issues. Some liquidity support is still needed, but the crucial issue now is solvency.

Policymakers need to act urgently, as the solvency crisis is already eroding the underlying strength of the business sector in many countries.

The problem is worse than it appears on the surface, as massive liquidity support, and the confusion caused by the unprecedented nature of this crisis, are masking the full extent of the problem, with a “cliff edge” of insolvencies coming in many sectors and jurisdictions as support programs lose funding and existing net worth is eaten up by losses.

However, the difficulty of predicting the duration and recovery path after the pandemic, and of differentiating between structural versus temporary changes in demand, makes it hard to determine the long-term viability of enterprises during the pandemic.

This complicates the targeting and design of measures to support the corporate sector.

This solvency crisis differs sharply from the global financial crisis, which centered on the financial system and on liquidity problems.

Some of the answers from that previous crisis are valid now, but new approaches are also needed.

The first wave of liquidity-focused policy measures has prevented much more severe consequences for the corporate sector, jobs, and for the economy more broadly.

As the crisis progresses, jurisdictions now need to develop policy responses that accommodate structural changes in the economy triggered by the pandemic, and address the following problems that make the initial response unsustainable:

• Inadequate targeting of support, which fails to sufficiently tailor the policy response to the situations of different firms

• An excessive focus on credit provision, which risks overburdening firms with debt, promoting inefficient use of resources, and engendering future problems

• Excessive direct government decision-making and suboptimal use of private sector expertise that could be used to better direct support

• A level of public spending that would be unsustainable over the potential duration of the ongoing economic crisis.

In this report we recommend for policymakers:

• A set of universal core principles to guide the design of the policy response

• A set of potential tools with which to respond

• A decision framework to determine appropriate policy responses for a specific jurisdiction.

To read more:
https://group30.org/images/uploads/publications/G30_Reviving_and_Restructuring_the_Corporate_Sector_Post-Covid.pdf

Number 8

SEC Issues Over $1.1 Million to Multiple Whistleblowers

The Securities and Exchange Commission announced awards totaling more than $1.1 million to five whistleblowers who provided high-quality information that led to successful enforcement actions.

In the first order, the SEC awarded three whistleblowers almost $500,000 in connection with two related enforcement actions. The first whistleblower provided information that prompted the opening of an investigation. The second and third whistleblowers provided information that significantly contributed to the success of the actions, and contributed additional, helpful assistance to the investigative staff.

In the second order, the SEC awarded nearly $600,000 to a whistleblower whose information caused the opening of an investigation. The whistleblower continued to provide helpful assistance by meeting with investigative staff in-person, providing documents, and identifying witnesses. The whistleblower also repeatedly reported the concerns internally in an effort to remedy the violations.

In the third order, the SEC awarded more than $100,000 to a whistleblower whose independent analysis led to a successful enforcement action. Among other things, the whistleblower conducted an analysis using information from publicly available documents to calculate an estimate of an important metric for a company, and then showed that the company's disclosures regarding that metric were implausible.

"These awards underscore the breadth of ways that company insiders, as well as whistleblowers not affiliated with a company, can positively impact SEC investigations," said Jane Norberg, Chief of the SEC's Office of the Whistleblower. "Whistleblowers who provide high-quality information or analysis may be eligible for an award where their information causes staff to open an investigation or meaningfully advances an existing investigation."

The SEC has awarded approximately $737 million to 133 individuals since issuing its first award in 2012. All payments are made out of an investor protection fund established by Congress that is financed entirely through monetary sanctions paid to the SEC by securities law violators. No money has been taken or withheld from harmed investors to pay whistleblower

awards. Whistleblowers may be eligible for an award when they voluntarily provide the SEC with original, timely, and credible information that leads to a successful enforcement action. Whistleblower awards can range from 10-30% of the money collected when the monetary sanctions exceed $1 million.

As set forth in the Dodd-Frank Act, the SEC protects the confidentiality of whistleblowers and does not disclose information that could reveal a whistleblower's identity.

For more information about the whistleblower program and how to report a tip, visit www.sec.gov/whistleblower.

Number 9

Call for expression of interest in the appointment of members of the Board of Appeal of the three European Supervisory Authorities for the financial services sector

Official Journal
of the European Union

1. Description of the Authorities

The European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA), are created by Regulation (EU) No 1093/2010, Regulation (EU) No 1094/2010, and Regulation (EU) No 1095/2010 respectively.

Together, they constitute European Supervisory Authorities for the financial services sectors, and are members of the European System of Financial Supervision.

They have as their goals for their respective sectors of competence, among others:

— bringing about a sound, effective and consistent level of regulation and supervision,

— ensuring the integrity, transparency, efficiency and orderly functioning of financial markets,

— strengthening international supervisory coordination,

— preventing regulatory arbitrage and promoting equal conditions of competition,

— ensuring that the taking of investment and other risks are appropriately regulated and supervised,

— enhancing customer protection, and

— enhancing supervisory convergence across the internal market.

In addition, ESMA carries out the direct supervision of credit rating agencies, trade and securitisation repositories within the EU, as well as third-country central counterparties (TC-CCPs), in particular for those of

systemic importance or likely to become of systemic importance for the financial stability of the Union or of one or more of its Member States.

ESMA is also entrusted with powers to directly supervise critical and third-country benchmarks as well as data reporting services providers.

Finally, among others, ESMA also performs tasks relevant to over-the-counter (OTC) derivatives, short-selling of securities and critical market infrastructures.

To this end, in addition to adopting non-binding acts such as guidelines and recommendations, and draft technical standards, each Authority may also adopt binding decisions in certain circumstances addressed to national supervisory authorities or to individual financial institutions, which, together with certain other decisions, will be appealable acts.

EBA and ESMA have their seats in Paris, France, and EIOPA has its seat in Frankfurt am Main, Germany. Each of the Authorities was established on 1 January 2011.

To read more:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2021:006A:FULL&from=EN

Number 10

Night-Vision Revolution: Less Weight, Improved Performance

Leveraging new tech, DARPA aims for night-vision goggles the size and weight of regular eyeglasses

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

For decades U.S. warfighters have benefitted from advanced night-vision technology, allowing pilots to fly low-level missions on pitch-black nights and ground forces to conduct operations against adversaries in the dark.

But current night-vision goggle (NVG) technology requires cumbersome binocular-like optics mounted on a helmet, offering limited field of view (FOV) and putting unhealthy strain on the wearer's neck.

Building on recent scientific advances in photonics and optical materials pioneered in DARPA's Defense Sciences Office (DSO), a new effort seeks to develop next-generation NVGs that are as lightweight and compact as a pair of regular eyeglasses or sunglasses.

DARPA today announced its Enhanced Night Vision in eyeglass form (ENVision) program. ENVision aims to create lightweight NVGs that offer a wide FOV across multiple infrared (IR) spectrum bands without needing separate optics for each IR band.

The goal is to enable night vision through fog, dust, and other obscurants as well as provide thermal vision – all via a single flat lens. A Proposers Day for interested participants is being held via webinar on January 21, 2021.

"Our warfighters experience significant neck strain from current NVGs caused by the weight of the optics extending 4-5 inches in front of their helmets," said Rohith Chandrasekar, program manager in DARPA's Defense Sciences Office.

"If you've never worn NVGs for hours at a time imagine wearing a baseball cap all day with a two-pound weight attached to the front of the bill – that gives you a small sense of the stress experienced. Extended use of such systems leads to a condition where the neck no longer has energy to keep the head upright requiring warfighters to use their hands to lift and point their heads. NVG wearers also have to swivel their heads frequently for peripheral vision since current optics only provide a 40-degree field of view compared to the 120-degree wide view we have with our eyes, which only makes use of NVG systems more painful."

Besides the weight and field-of-view constraint, current NVGs provide only a narrow segment of the IR portion of the spectrum (typically near-IR) that limits what types of threats the viewer can see at night. Efforts to expand FOV and IR bandwidth to date have involved increasing the number of optics, which increases weight.

The ENVision program is designed to break the paradigm that increased performance can only be achieved by an increase in weight.

“DARPA investments over the past decade have led to breakthroughs in the areas of planar optics, detection materials, and novel light-matter interactions,” Chandrasekar said. “ENVision will leverage these advancements, amongst others, to develop enhanced night-vision devices in lightweight eyeglass form factors.”

ENVision will also investigate the possibility of night vision using direct photon up-conversion from infrared to visible photons using thin materials.

“This will further simplify NVG systems by advancing from the multi-step conversion currently used to a single step up-conversion process,” Chandrasekar said. “Some of these processes even conserve the momentum of photons, which, in theory, could enable night vision without the need for any optics.”

The ENVision program focuses on developing prototypes of multi-band, wide-FOV night vision systems and investigating methods to amplify photon up-conversion processes from any IR band to visible light.

For more information about the upcoming Proposers Day, including registration details, please visit: https://go.usa.gov/xARnH

A Broad Agency Announcement solicitation is expected to be available on beta.SAM.Gov in the coming weeks.

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

It is our goal to minimize disruption caused by technical errors.

However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

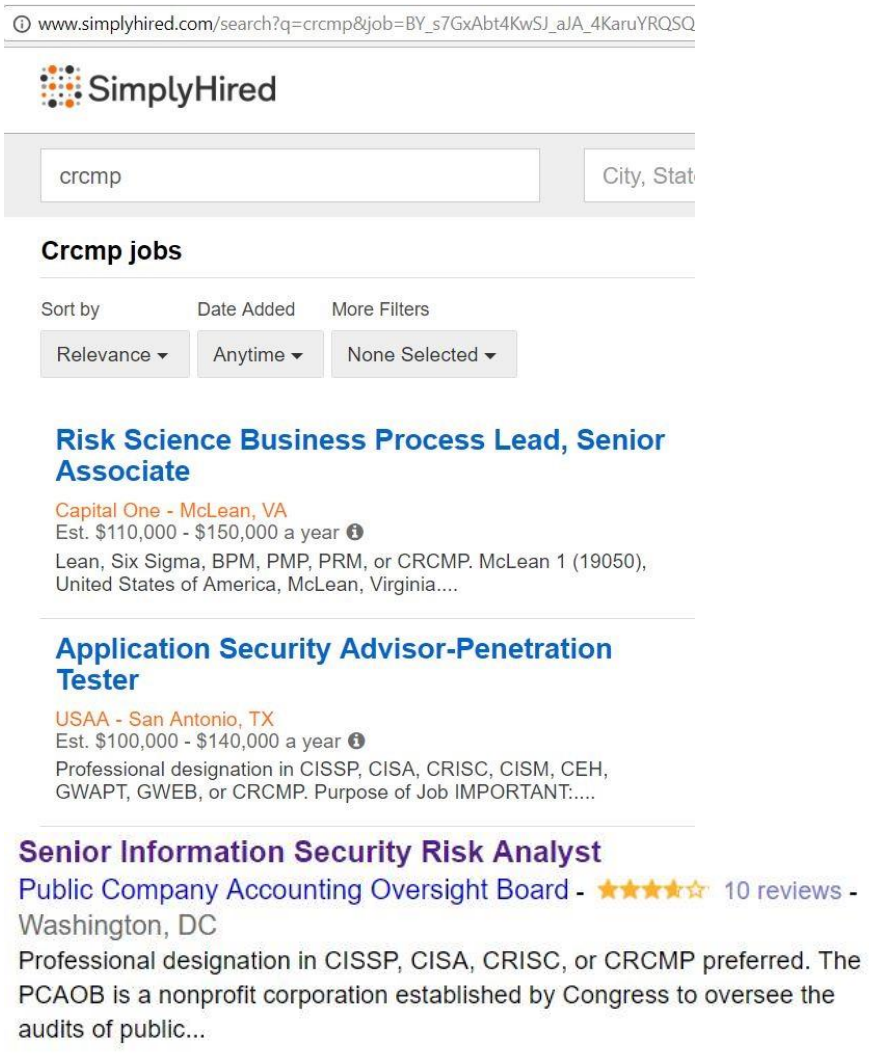
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

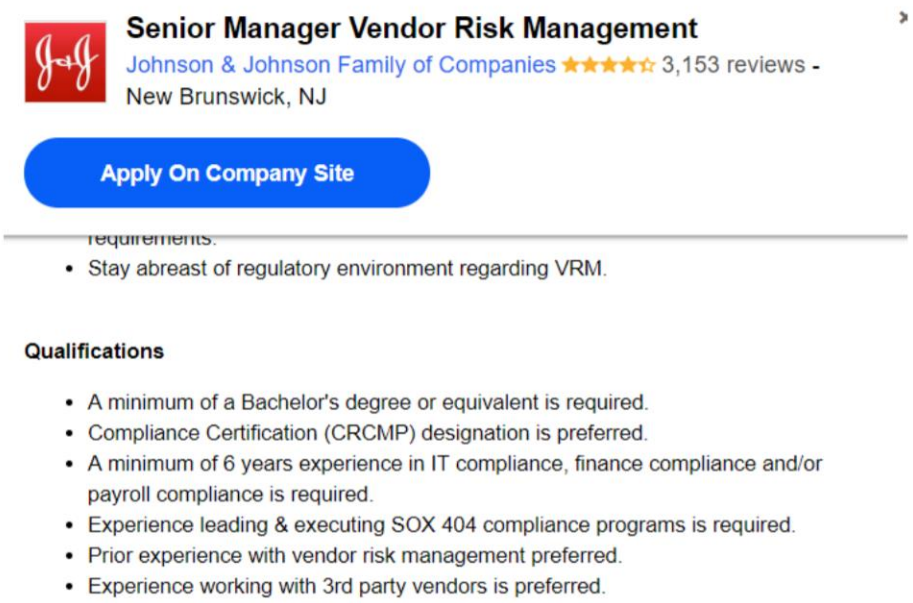
You can explore what we offer to our members:

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

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

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





Senior Manager Vendor Risk Management

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

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

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

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

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

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

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

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

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

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