Monday, March 23, 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,

Cyber insurance is still evolving, as cyber risks change, and organizations still hide the full impact of breaches in order to avoid negative publicity.

This simply means that underwriters have *limited data* to determine the financial impact of attacks. When the risk of cyberattacks is not completely understood, how can they calculate the premium? Actuaries are the unsung heroes of the insurance industry.
After all, only an actuary can tell "*since the first time I saw you, my interest in you has compounded continuously*".

I have just read an interesting presentation with title *"Cyber underwriting: Managing the risks of digital finance"*, by Fausto Parente, Executive Director of European Insurance and Occupational Pensions Authority (EIOPA) at the AFORE 4th Annual FinTech and Regulation Conference in Brussels. He said:

"In the old days, they used to say *knowledge is power*. Today, it's more likely to be *data is power*. In the world of insurance for example, products, policies and pricing are all *powered by data*."

He continued: "The increasing frequency of cyber attacks, coupled with stricter regulation regarding cyber security as well as continued technological developments are all expected to increase demand for cyber insurance in the near future.

First and foremost, we have seen that a *lack of data* is one of the biggest obstacles to a detailed understanding of the fundamental aspects of cyber risk and the provision of proper coverage.

It's understandable of course that companies are *reluctant* to share information on their security measures and their history of cyber incidents. The information is extremely sensitive, but it is also incredibly valuable to underwriters.

And this lack of quantitative information on incidents makes it difficult for insurers to *properly price* risk and estimate the liability of exposures. It also hampers cyber risk measurement and management for insurers."

Well, Fausto Parente hit the nail on the head.

Actuaries need data. When you tell them *"look at those white horses over there",* they will answer *"they're white on this side, anyway."* It will not be easy to give them accurate, complete and appropriate cyber risk data.

Read more at number 2 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

BIS

Number 6 (Page 18)

New action to disrupt world's largest online criminal network

Tom Burt - Corporate Vice President, Customer Security & Trust

Microsoft

Number 7 (Page 21)

Coronavirus used as bait by phishers

National Cyber Security Centre

Number 8 (Page 22)

From the White House Coronavirus Task Force

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

Number 9 (Page 24)

Keynote speech by President von der Leyen, president of the European Commission, at the BusinessEurope Day 2020

Number 10 (Page 34)

How Low Can You Go? Lower Than Ever Before

NIST scientists make most sensitive measurements to date of silicon's conductivity for future solar cell, semiconductor applications.

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

Number 1

Guidance for Resolution Plan Submissions of Certain Foreign-based Covered Companies

The Board of Governors of the Federal Reserve System (Board) and the Federal Deposit Insurance Corporation (FDIC) (together, the "agencies") are inviting comments on proposed guidance for the 2021 and subsequent resolution plan submissions by certain *foreign banking organizations ("FBOs")*.

The proposed guidance is meant to assist these firms in developing their resolution plans, which are required to be submitted pursuant to Section 165(d) of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act").

The scope of application of the proposed guidance would be FBOs that are triennial full filers and whose intermediate holding companies ("U.S. IHCs") have a score of 250 or more under the second methodology ("method 2") of the global systemically important bank ("GSIB") surcharge framework.

The proposed guidance, which is largely based on prior guidance, describes the agencies' expectations regarding a number of key vulnerabilities in plans for a rapid and orderly resolution under the U.S. Bankruptcy Code (i.e., capital; liquidity; governance mechanisms; operational; legal entity rationalization and separability; and derivatives and trading activities).

The proposed guidance also updates certain aspects of prior guidance based, in part, on the agencies' review of certain FBOs' most recent resolution plan submissions and changes to the resolution planning rule. The agencies invite public comment on all aspects of the proposed guidance.

Comments should be received on or before May 5, 2020.

Section 165(d) of the Dodd-Frank Act and the jointly issued implementing regulation require certain financial companies, including certain foreign-based firms, to report periodically to the Board and the FDIC their plans for rapid and orderly resolution under the U.S. Bankruptcy Code (the "Bankruptcy Code") in the event of material financial distress or failure.

With respect to a covered company that is organized or incorporated in a jurisdiction other than the United States or that is an FBO, the Rule requires that the firm's U.S. resolution plan include specified information with respect to the subsidiaries, branches, and agencies, and identified critical operations and core business lines, as applicable, that are domiciled in the United States or conducted in whole or material part in the United States.

The Rule also requires, among other things, each financial company's full resolution plan to include a strategic analysis of the plan's components, a description of the range of specific actions the company proposes to take in resolution, and a description of the company's organizational structure, material entities, and interconnections and interdependencies.

In addition, the Rule requires that all resolution plans include a confidential section that contains any confidential supervisory and proprietary information submitted to the Board and the FDIC and a section that the agencies make available to the public.

Public sections of resolution plans can be found on the agencies' websites.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20200306b1.pdf

Number 2

Cyber underwriting: Managing the risks of digital finance

Speech by Fausto Parente at the AFORE 4th Annual FinTech and Regulation Conference, Brussels.

Introduction

Thank you for inviting me to today's conference. It's always so interesting to hear about the different aspects of FinTech and the pace of innovation. I'm also pleased to be here with the Chairs from my fellow supervisory authorities. Digital finance and FinTech are areas that we all follow closely.

We've heard a lot today about the vast potential of FinTech and how it is changing the lives of business and people.

The digitalisation of finance is dependent on many things, but the core drivers are technology and data. Data is valuable, especially the type of data held by financial institutions. And technology is vulnerable.

And that leaves companies and people open to the risks of cyber crime.

Earlier this morning we heard about the need for operational resilience and the importance of cyber security. The threat of cyber attacks are a serious risk to business. Ask any CEO what keeps him up at night, and cyber attacks and data theft are likely to be high on the list of answers.

So today, I would like to talk to you about two things: the importance of respecting data, and the importance of protecting the people through cyber insurance.

Data is power

Let me start with a few words on the importance of how we treat data.

In the old days, they used to say 'knowledge is power'. Today, it's more likely to be 'data is power'.

In the world of insurance for example, products, policies and pricing are all powered by data.

This is what makes it so valuable: with data an insurance company is able to offer the consumer just what they need and hopefully at just the right price. It should be a win-win for provider and policyholder.

And more choice and lower costs are what makes consumers so ready to share their data.

But what happens when data is not used ethically? When people find themselves excluded from insurance? Or when the holders of the data do not act responsibly?

At EIOPA, we believe that data needs to be respected. It must be used fairly and organisations holding data must act responsibly.

Because of this, last year we set up a consultative expert group on digital ethics in insurance to help us develop principles of digital responsibility in insurance.

We want these principles to have European values at their core while at the same time recognising the important role that insurance plays in our economy and also in our society.

So we are not reinventing the wheel. Nor are we ignoring the work on artificial intelligence being done by the European Commission and other bodies. Instead we want to operationalise best practice for the insurance sector.

In particular we are paying attention to:

- Fairness and non-discrimination – including data biases and the fairness around the use of price optimisation practices;

- Transparency and explainability – being clear on how data is used and any trade-offs with accuracy;

- Governance – touching on accountability, security and resilience. Security of data is perhaps the most important thing here.

Because cyber attacks and data thefts cost.

They leave companies liable for fines of millions of euro. On top of that, there is the cost to a company's reputation, which is harder to quantify and very difficult – sometimes impossible – to earn back.

So cyber resilience is essential for any organisation and an effective cyber insurance market is a core component of a sound cyber resilience framework.

The cyber insurance market today

A sound cyber insurance market is an enabler of the digital economy.

From raising awareness of the risks and losses that can result from cyber attacks to facilitating responses and recovery, a well-developed cyber insurance market can play a valuable role in risk management.

And the European cyber insurance market is growing rapidly.

This is in part due to the overall increase in written contracts offered by insurers, and also because of the growing number of insurers providing cyber insurance.

And we expect the market to continue to grow.

The increasing frequency of cyber attacks, coupled with stricter regulation regarding cyber security as well as continued technological developments are all expected to increase demand for cyber insurance in the near future.

It's also likely that as businesses make their own investigations and investment into cyber security, they will become more aware of the growing need for insurance cover against cyber attacks.

Cyber underwriting to build European resilience

We need to work together to strengthen cyber resilience and create a strong cyber insurance market.

At EIOPA we have been studying the evolution of cyber insurance in Europe for some years now, including regular dialogue with insurance companies, and we have just published our cyber underwriting strategy.

Our strategy outlines the areas that we see need strengthening and sets out our approach and proposed actions.
First and foremost, we have seen that a lack of data is one of the biggest obstacles to a detailed understanding of the fundamental aspects of cyber risk and the provision of proper coverage.

It's understandable of course that companies are reluctant to share information on their security measures and their history of cyber incidents. The information is extremely sensitive but it is also incredibly valuable to underwriters.

And this lack of quantitative information on incidents makes it difficult for insurers to properly price risk and estimate the liability of exposures. It also hampers cyber risk measurement and management for insurers.

Therefore, we believe that we need to develop at European level a standardised cyber incident reporting framework that enables the sharing of aggregated data, anonymised to protect sensitive information, so that insurers and reinsurers can develop adequate pricing and risk management models.

To do this, we will engage with different bodies, including national authorities, the EBA and ESMA, as well as ENISA to explore and promote the development of a harmonised cyber incident reporting taxonomy so that we can put the data to work to underpin cyber underwriting modelling.

We also believe that there needs to be a common understanding of contractual definitions. Policyholders and insurers must share the same understanding of contract terms. Clear and transparent cyber coverage is essential from a consumer protection perspective. This is just as important for big companies as it is for individuals.

At European level, EIOPA will work other EU institutions can help to accelerate and promote engagement between industry and consumer associations which, in the long run, will help to maintain consumer confidence and avoid the potential for disputes.

As a supervisor, we are also working closely with national supervisors to ensure that appropriate underwriting standards are in place and that national supervisors have the capacity to supervise these. Technology changes, the nature of cyber attacks change, supervisors must be able to keep pace with these changes.

Continuing European cooperation

Cyber attacks are complex. They are dangerous. And they are ever more sophisticated.

Because of this, cyber risk is seen as a potentially systemic risk for the financial system and the real economy.

So we need a common approach to mitigate this risk.

And this involves continuing to work together to find shared solutions. Because a shared approach will mean a more effective approach.

And so in addition to working with national supervisors to foster a common approach to supervision, we will also continue our very valuable dialogue with industry, consumer associations and other stakeholders to raise awareness of cyber security and insurance issues.

And at European level, we will continue our close cooperation, not only with the EBA and ESMA, but also with other EU bodies, so that we can strengthen Europe's over all resilience to cyber attacks.

In conclusion

Let me say in conclusion that it is no surprise that cyber security and cyber risks are a top concern not only for the financial sector, but for all industry and, indeed, for all people.

The digital era, and digital finance in particular, has brought us many benefits. But if too many people suffer because they are not better protected, we will quickly lose faith not only in the company that caused the suffering but also in technology itself.

This should not happen.

Let's work together to make sure that the risks resulting from digitalisation are considered and managed appropriately, including through an appropriate cyber insurance framework, so that digital finance continues to work for the people.

Ladies and gentlemen, thank you very much.

Number 3

EBA launches consultation to update methodology to identify G-SIIs

The European Banking Authority (EBA) launched a consultation to update the identification methodology of global systemically important institutions (G-SIIs) and related capital buffer rates.

The need for this revision was prompted, on one hand, by the revised framework for global systemically important banks (G-SIBs) published by the Basel Committee on Banking Supervision (BCBS) in July 2018 and, on the other hand, by the recent mandate given to the EBA to draft an additional methodology for the allocation of G-SII buffer rates to identified G-SIIs.

The consultation runs until 5 June 2020.

Considering that the list of EU G-SIBs identified by the BCBS and the list of G-SIIs identified by relevant authorities in EU Member States are identical, the EBA will need to update its Regulatory Technical Standard (RTS) for identifying G-SIIs, its Implementing Technical Standard (ITS) on ex-post disclosure rules applicable to identified G-SIBs.

In addition, the EBA guidelines frame ex-ante disclosure rules for very large institutions that may be later identified as G-SIIs.

Consultation process

Comments to this consultation can be sent to the EBA by clicking on the "send your comments" button on the consultation page. Please note that the deadline for the submission of comments is 5 June 2020. A public hearing will be held on 27 March 2020 from 14:00 to 16:00 CET at the EBA premises in Paris.

Legal basis

The final RTS, ITS and Guidelines have been developed in accordance with Directive (EU) 2019/878 (CRD V), and on the basis of internationally agreed standards, such as the framework established by the FSB, as well as the standards developed by the BCBS.

The identification as G-SII, which leads to higher additional capital requirements, takes place in December every year.

The higher additional capital requirement applies one year after the publication by competent authorities in each Member State of banks' scoring results so as to allow institutions enough time to adjust to the new buffer requirement.

The EBA methodology to identify global systemically important institutions (G-SIIs) closely follows the approach of the Basel Committee on Banking Supervision (BCBS) for identifying global systemically important banks (G-SIBs, in BCBS terminology).

The list of EU G-SIBs identified by the BCBS and the G- SIIs identified by Member States' authorities are identical.

This is in line with Directive (EU) 2019/878, which requires the methodology to take into account international agreed standards.

In July 2018, the BCBS published a revised assessment methodology to identify G-SIBs and assign higher loss absorbency requirements.

Consequently, the RTS on the identification methodology to identify G-SIIs has to be updated.

In addition, Article 131 of Directive (EU) 2019/878 requires the EBA to design an additional identification methodology for G-SIIs based both on the existing international standards and on the cross-border activities of the group excluding those between participating Member States as referred to in Article 4 of Regulation (EU) 806/2014 of the European Parliament and of the Council.

In accordance with the G-SIB assessment methodology published by the BCBS, the cross- jurisdictional claims and liabilities of an institution are indicators of its global systemic importance and of the impact that its failure can have on the global financial system.

Those indicators, which shall refer to 31 December, reflect the specific concerns, for instance, about the greater difficulty in coordinating the resolution of institutions with significant cross-border activities.

The progress made in terms of the common approach to resolution resulting from the reinforcement of the single rulebook and from the establishment of the Single Resolution Mechanism (SRM) has significantly

developed the ability to orderly resolve cross-border groups within the banking union.

Therefore, and without prejudice to the capacity of competent or designated authorities to exercise their supervisory judgment, an alternative score reflecting that progress should be calculated.

When doing so, competent or designated authorities should consider that score when assessing the systemic importance of credit institutions, without affecting the data supplied by EU authorities to the BCBS for the determination of international denominators.

These EBA RTS deliver on that mandate by specifying the additional identification methodology for global systemically important institutions (G-SIIs) to allow the recognition of the specificities of the integrated European resolution framework within the context of the SRM.

This EU additional methodology may be used by supervisorsto frame the discussions held at the Basel Committee for the purpose of defining the annual list of G-SIBs and related higher capital buffer requirements.

The draft RTS will apply from the 2021 G-SIIs assessment exercise based on end-2020 information.

The Pillar 3 disclosure, according to Article 441 of the CRR2, should be aligned with the BCBS template GSIB1 – “Disclosure of G-SIB indicators”, included in the BCBS March 2017 Pillar 3 standards – “Pillar 3 disclosure requirements – consolidated and enhanced framework”.

The BCBS template has to be fully consistent with the data submitted to the relevant supervisory authorities, for subsequent remittance to the Committee in the context of its annual data collection exercise for the assessment and identification of G-SIBs.

Similarly, in the EU framework, the Pillar 3 disclosure template has to be fully consistent with the template reported by institutions with a leverage ratio exposure measure above EUR 200 billion, for the purpose of the identification exercise and that is disclosed ex-ante by these institutions.

To read more:
https://eba.europa.eu/eba-launches-consultation-update-methodology-identify-g-siis

Number 4

Camouflage for the Digital Domain

NATO STRATCOM COE

Discoverability of geolocation

Protecting the geolocation of personnel, equipment, infrastructure, and installations of military units is crucial for mission success.

Today's digitalised society generates an abundance of open information that an adversary can exploit to obtain sensitive geolocation information.

While geolocation information is easily accessed using digital sources, it can also be provided directly by conflict participants and the general public via digital platforms.

Geolocation data allows an adversary to discover and adapt to the position and movements of forces, thus serving as a tactical, operational, or strategic force multiplier.

It also often enables or improves kinetic targeting and battle damage assessments. Geolocation data can also be useful information for enemy influence activities against friendly forces.

The paper:
https://www.stratcomcoe.org/camouflage-digital-domain

Number 5

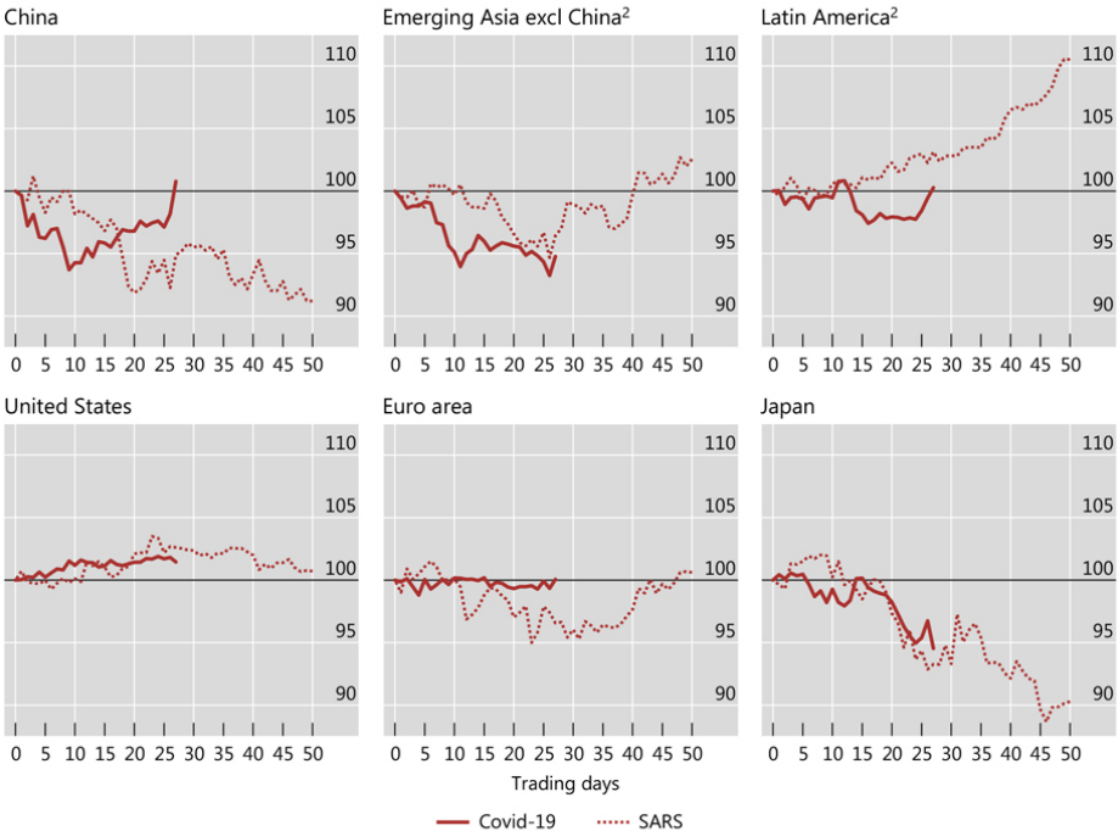
Covid-19 and SARS: what do stock markets tell us?

BIS

The rapid spread of Covid-19 since mid-January invariably brings up a comparison with the early 2003 outbreak of severe acute respiratory syndrome (SARS).

Compared with SARS, Covid-19 front-loads costs for China and emerging Asia[1]

Index of cumulative idiosyncratic returns — Graph B



[1] Reference point "Day 0" for SARS and Covid-19 is, respectively, 7 February 2003 (China notifies the SARS outbreak to the World Health Organization) and 19 January 2020 (the day before Chinese officials acknowledge that Covid-19 might be transmissible between humans). For Covid-19, updated to 25 February 2020. [2] Simple averages of regional economies.

Sources: Datastream; BIS calculations.

In this box, we provide a preliminary assessment of the relative impact of the Covid-19 and SARS epidemics on various economies through the lens of equity investors.

An advantage of looking at the stock markets of different countries is that equity valuations should encompass both the local and global risk factors that the investors view as important.

Fluctuations in the global risk factor - gauged, for instance, through the returns on the MSCI Global index - may be driven by investors' concerns about the global economic fallout of a virus outbreak.

Such fluctuations are likely to have a differential effect on each country's stock market performance; moreover, the magnitude of these effects is likely to have changed in the nearly two decades between the two epidemics.

Nevertheless, we can calculate "idiosyncratic" stock returns, the portion of a country-specific stock return that is not explained by fluctuations in the global risk factor, as the residual from a regression of the country's returns on the returns on the MSCI Global index.

The comparison of the idiosyncratic country-specific returns during periods in which the Covid-19 and SARS epidemics unfolded can thus provide a cleaner assessment of the relative fallouts from the two outbreaks across countries and time, at least as perceived by equity investors.

To read more: https://www.bis.org/publ/qtrpdf/r_qt2003w.htm

Number 6

New action to disrupt world's largest online criminal network

Tom Burt - Corporate Vice President, Customer Security & Trust

Microsoft

Microsoft and partners across 35 countries took coordinated legal and technical steps to disrupt one of the world's most prolific botnets, called Necurs, which has infected more than nine million computers globally.

This disruption is the result of eight years of tracking and planning and will help ensure the criminals behind this network are no longer able to use key elements of its infrastructure to execute cyberattacks.

A botnet is a network of computers that a cybercriminal has infected with malicious software, or malware.

Once infected, criminals can control those computers remotely and use them to commit crimes.

Microsoft's Digital Crimes Unit, BitSight and others in the security community first observed the Necurs botnet in 2012 and have seen it distribute several forms of malware, including the GameOver Zeus banking trojan.

The Necurs botnet is one of the largest networks in the spam email threat ecosystem, with victims in nearly every country in the world. During a 58-day period in our investigation, for example, we observed that one Necurs-infected computer sent a total of 3.8 million spam emails to over 40.6 million potential victims.

Necurs is believed to be operated by criminals based in Russia and has also been used for a wide range of crimes including pump-and-dump stock scams, fake pharmaceutical spam email and "Russian dating" scams.

It has also been used to attack other computers on the internet, steal credentials for online accounts, and steal people's personal information and confidential data.

Interestingly, it seems the criminals behind Necurs sell or rent access to the infected computer devices to other cybercriminals as part of a botnet-for-hire service.

Necurs is also known for distributing financially targeted malware and ransomware, cryptomining, and even has a DDoS (distributed denial of

service) capability that has not yet been activated but could be at any moment.

On Thursday, March 5, the U.S. District Court for the Eastern District of New York issued an order enabling Microsoft to take control of U.S.-based infrastructure Necurs uses to distribute malware and infect victim computers.

With this legal action and through a collaborative effort involving public-private partnerships around the globe, Microsoft is leading activities that will prevent the criminals behind Necurs from registering new domains to execute attacks in the future.

This was accomplished by analyzing a technique used by Necurs to systematically generate new domains through an algorithm. We were then able to accurately predict over six million unique domains that would be created in the next 25 months.

Microsoft reported these domains to their respective registries in countries around the world so the websites can be blocked and thus prevented from becoming part of the Necurs infrastructure.

By taking control of existing websites and inhibiting the ability to register new ones, we have significantly disrupted the botnet.

Microsoft is also taking the additional step of partnering with Internet Service Providers (ISPs) and others around the world to rid their customers' computers of malware associated with the Necurs botnet.

This remediation effort is global in scale and involves collaboration with partners in industry, government and law enforcement via the Microsoft Cyber Threat Intelligence Program (CTIP).

Through CTIP, Microsoft provides law enforcement, government Computer Emergency Response Teams (CERTs), ISPs and government agencies responsible for the enforcement of cyber laws and the protection of critical infrastructure with better insights into criminal cyber infrastructure located within their jurisdiction, as well as a view of compromised computers and victims impacted by such criminal infrastructure.

For this disruption, we are working with ISPs, domain registries, government CERTs and law enforcement in Mexico, Colombia, Taiwan, India, Japan, France, Spain, Poland and Romania, among others.

Each of us has a critical role to play in protecting customers and keeping the internet safe.

To make sure your computer is free of malware, you may visit: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download

Number 7

Coronavirus used as bait by phishers

National Cyber Security Centre

Several cyber security researchers have uncovered a surge in the number of phishing emails using the coronavirus as a lure.

Cyber criminals have been exploiting the pandemic to steal money or sensitive information through phishing campaigns in several countries.

By creating fake websites and emails masquerading as legitimate, attackers have been able to infect victims with malware.

Unfortunately, cyber criminals are opportunistic and can often look to exploit current events and public concerns.

See the NCSC's suspicious email advice to learn more about spotting and dealing with phishing emails at:
https://www.ncsc.gov.uk/guidance/suspicious-email-actions

Number 8

From the White House Coronavirus Task Force

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

Keeping the workplace safe
Encourage your employees to…

Practice good hygiene

- Stop handshaking – use other noncontact methods of greeting
- Clean hands at the door and schedule regular hand washing reminders by email
- Create habits and reminders to avoid touching their faces and cover coughs and sneezes
- Disinfect surfaces like doorknobs, tables, desks, and handrails regularly
- Increase ventilation by opening windows or adjusting air conditioning

Be careful with meetings and travel

- Use videoconferencing for meetings when possible
- When not possible, hold meetings in open, well-ventilated spaces
- Consider adjusting or postponing large meetings or gatherings
- Assess the risks of business travel

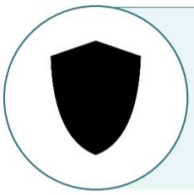
Handle food carefully

- Limit food sharing
- Strengthen health screening for cafeteria staff and their close contacts
- Ensure cafeteria staff and their close contacts practice strict hygiene

All households

- Clean hands at the door and at regular intervals
- Create habits and reminders to avoid touching their face and cover coughs and sneezes
- Disinfect surfaces like doorknobs, tables, and handrails regularly
- Increase ventilation by opening windows or adjusting air conditioning

Households with vulnerable seniors or those with significant underlying conditions



Significant underlying conditions include heart, lung, kidney disease; diabetes; and conditions that suppress the immune system

- Have the healthy people in the household conduct themselves as if they were a significant risk to the person with underlying conditions. For example, wash hands frequently before interacting with the person, such as by feeding or caring for the person
- If possible, provide a protected space for vulnerable household members
- Ensure all utensils and surfaces are cleaned regularly

Households with sick family members

- Give sick members their own room if possible, and keep the door closed
- Have only one family member care for them
- Consider providing additional protections or more intensive care for household members over 65 years old or with underlying conditions

Keeping commercial establishments safe

Encourage your employees and customers to…

Practice good hygiene

- Stop handshaking – use other noncontact methods of greeting
- Clean hands at the door, and schedule regular hand washing reminders by email
- Promote tap and pay to limit handling of cash
- Disinfect surfaces like doorknobs, tables, desks, and handrails regularly
- Increase ventilation by opening windows or adjusting air conditioning

Avoid crowding

- Use booking and scheduling to stagger customer flow
- Use online transactions where possible
- Consider limiting attendance at larger gatherings

To learn more:
https://www.cdc.gov/coronavirus/2019-ncov/index.html

https://www.cdc.gov/coronavirus/2019-ncov/downloads/community-mitigation-strategy.pdf

Number 9

Keynote speech by President von der Leyen, president of the European Commission, at the BusinessEurope Day 2020

Good morning, Mr President Pierre Gattaz, Ladies and Gentlemen,
Thank you very much for this opportunity to share my thoughts today with you and to listen to your views.

It is just a few weeks ago, six weeks ago, that I have been at the World Economic Forum in Davos and I had a meeting with the International Business Council.

And someone asked me the very right question. He said: 'Do we want Europe to be a global player or a playground for others?' And this is the big question indeed. It is as simple as that. And I have no doubt about the answer.

I am absolutely confident that Europe will continue to be a global player in the world of tomorrow. And I am confident, because I know what European businesses are capable of. We are the continent of innovators, we are the continent of pioneers, of entrepreneurs.

We are a continent of family companies that have resisted all crises and that have reinvented century-old productions. We are leaders in a huge number of sectors – from the automotive to clean energy, from chemicals to satellites.

But we also know that industry is changing faster than ever before. And we have to define a new industrial way for Europe in this rapidly changing world. I see basically three main drivers of this change. The first one is, of course you know it all, technology: It is about big data, it is about Artificial Intelligence.

They are completely reshaping the way we do things. And this is not just about self-driving cars. It is way more, it is a revolution that is touching all sectors of our economy – from pharma to fashion, from big factories to every small family enterprise.

It is indeed all about data. Data is the fuel of our economy. Artificial Intelligence will soon help companies, for example, to reduce their energy bills by smartly allocating the energy over day and night. In the companies, it will provide a better consumer and customer service, it will transform our design and production processes.

All this, you know it better than me, is already happening, and many of you see this in your daily business and your daily work. The challenge for Europe is not just to adapt to these changes. The challenge is that we want to shape our own digital future. And I am confident that we are able to do that.

The second main driver is the sorry state of our environment. 2050: That is the year Europe aims to become carbon-neutral, climate-neutral. And it is no longer impossibly distant.

If I think of my children, they will be a little bit younger than I am now in 2050. And I have – and you all have – a glimpse of the possible environment they will likely experience, and it is a sobering glimpse, if we do not change dramatically. And honestly, I feel a profound sadness that they might be dealing with severe problems of our making. And you know these problems.

Just to name a few: It is the reduced biodiversity – we are losing 1 million of species –, it is the rising sea levels – we know today already what islands will disappear, and what cities, it is already a fact. It is the increasing desertification, which causes a huge amount of security problems and conflict potential. Science is clear: Human-caused climate disruption is one of the best-studied phenomena in this world.

And the majority has understood this. But some are still deploying the notion that you can downplay climate change and want to continue with business as usual. I think this is not only unacceptable with regard to our children and their right to live in harmony with nature as we have it, but it would also be a huge missed economic opportunity.

Businesses all across Europe demonstrate that a different growth model is possible – a growth model that creates jobs and economic value while respecting our environment. And be it the small enterprises that are renouncing single use plastics or the big steel industries that have launched a transition towards fossil-free steel.

Some of you have started to develop their own ‘sectoral green deal'. The steel sector is already doing that. Others, like the chemical sector, are on the

point of joining. All this is great news, it is necessary great news for the environment, but also for Europe's competitiveness.

At the end of last year, 44 of Europe's largest investors, representing EUR 6 trillion of assets, asked us – the European Union, the European Commission – to urgently pass a climate law.

Why that? They want reliability! They want clarity! They want us to be dedicated to go towards that goal. And rightly so! And indeed, as you have said, President Gattaz, yesterday, we have made our proposal for the first ever European Climate Law.

It will help you plan your long-term investment, it will provide a clear sense of direction all across our Union. I see the climate transition as a huge opportunity for the European economy and for the European business.

We can develop and deploy clean technologies that the whole world will want to adopt – to cut pollution and to enhance productivity. We can set new standards and we can become the exporters of knowledge-driven clean technologies.

We can be a world leader also taking the most ethical choices. We have the first advantage of the first-movers. So we are ahead of other continents, of other sectors, which is not in every case the reality of the European business. And this is why I think of the European Green Deal as our new growth strategy.

A strategy for growth that is not constrained by fossil fuels and that is not constrained by the constant need for more resources. But rather a strategy for growth that offers maximum added value with renewable resources while gaining the trust of our society. Because people have a gut feeling on what is going on. And they want a different approach to growth.

The third driver of change for our industry is geopolitics, and the growing pressures from international competitors: You know it all, it is trade disputes, it is the return of protectionism. And yes, the global competition is fierce. But European businesses – be they large or be they small – have the quality and the capacity for innovation and to thrive in this difficult environment.

Through the years, many of you have become stronger thanks to the Single Market. And you have made the jump to the global markets, to become world leaders in your sectors. European companies have prospered thanks to our unique set of free trade agreements and thanks to a global trade

system that is based on rules. We have many, many success stories to be proud of – from telecom to railways, from aircraft to agriculture.

But indeed, we also have to ensure that our industries and their workers are competing in a fair environment, not only at home, but also abroad. In these years, we have witnessed unilateral and arbitrary action against our industries.

And there is hostility against the WTO, and against the idea of a level playing field for companies all over the world. So the challenge we face is to safeguard this level playing field for European industries – internally and externally. You must be able to innovate and compete in fairness, because this determines European prosperity now and in the future.

And in this context, allow me indeed to make a few remarks about our relationship with the United States, because you mentioned it, President Gattaz. I just want to emphasise, first of all, with all the disputes we do have and all the issues we do have with the United States and the White House at the moment being, I am a strong believer in the transatlantic friendship and the solid foundation we have for this transatlantic friendship.

There are zillions of contacts with our American friends: business contacts, personal friendships, our researchers, scientists, culturally. So we should always keep that in mind when tackling the obvious problems that are out there, without any question.

I had a good meeting with President Trump in Davos. And I believe that there might be a momentum towards improving our relations on a positive footing.

Of course, and this for you to know, I am absolutely aware that any deal that might be worked out needs to be balanced and compliant with WTO rules and it has to be compliant with the existing European Union mandate as you mentioned it, President Gattaz. So back to the initial question: Will Europe be a global player or will it be a playground for others?

After the first 100 days in office, let me tell you that I have seen a resolute Europe. I have seen a Europe from the business sector, and from youth movements and from the civil societies – that is clearly demanding for ambitious goals, for ambitious policies.

And we have set out goals in our clearest possible way: We want climate neutrality. We want digital leadership. We will not just adapt to the change, we will shape it, with our own capacity for innovation. And by doing so, make Europe more competitive in the world.

A continent that has a vision, a continent that has foresight, a continent that has resolution, a continent that takes control of its own future and a continent that masters its own destiny.

And it is with this in mind that we have presented the European Green Deal and our digital strategy. And next week indeed, we will introduce our industrial strategy and our SME strategy. And let me take five thoughts out of those two to discuss briefly with you.

First of all – and you are absolutely right, President Gattaz –, we need to invest in Europe's most unique asset, and that is our Single Market. With its size, it can offer scale-efficiencies and purchasing power to match the U.S. and China. We should not underestimate that. But indeed, our Single Market has to catch up with a changing industry.

All companies today are becoming, and have to become, digital. So the challenge for us is to truly digitalise now the Single Market, truly digitalise it. And our challenge is to make it work better for all these businesses.

So for example, we have to invest in a new network of digital innovation hubs all across Europe. Or we want to set up European data spaces and European supercomputers. I am a big believer that we have a huge opportunity with these European data spaces.

We have started it already for the researchers. That is: You have a data space where you do not only store your own data but that enables you to get access to other researchers' data at the same time. And the same has to go for the business sector, the same actually has to go for governments.

They have an enormous amount of data that are being never ever used – 85% of all our data we collect are never used or underused. So we should share them because there is a huge amount of innovation in it, of entrepreneurship, missed opportunities. And if we have these European data spaces, there is access to it.

Another example: Medical researchers are able right now to use the potential of the supercomputers in Barcelona and Bologna to identify a cure to the Coronavirus. So in other words, thanks to European funds, we are funding the next generation of supercomputers for our businesses, for our researchers.

Second topic: We must get away from the old model where we take resources from the environment, put them in a product, just to turn them then into waste. Our current linear production methods create huge quantities of greenhouse gas emissions.

If you just think of the mining of raw materials, the import, the transformation into a product, the landfill of waste we throw away – all this creates an immense amount of carbon dioxide and waste. If we want climate neutrality – and there are good reasons for it, it is an existential need – we definitely need to move on to the so-called circular models of production.

You know the examples of re-use. For example, the cost of manufacturing mobile phones could be reduced by 50% per device if industry made phones easier to take apart, if we improved in reverse cycles, and if we offered incentives to return them.

The other example, you know it, high-end washing machines. They would be accessible for households, not by selling them, but by leasing machine loads. What is the difference? If you sell the machine, there is a certain incentive to be aware of the fact that at a certain time, it breaks and you exchange it for the next one.

If you sell the machine load – so you just lease the machine to the household – the incentives are completely different. So the incentive for the manufacturer is that you develop a washing machine that is long-lasting, as long as possible, so that you can sell way more machine loads to the household. You sell the service; you do not sell the product anymore. And there is a huge incentive to recycle the product, and not to throw it away.

There is an environmental reason to choose the circular economy – without any question – but I think there is also a huge economic one. Because Europe relies massively on the import of raw materials from abroad.

We import half of all our resources we consume, half of it we import. This is expensive – you know it better than me – it exposes companies to price fluctuations and it makes us dependant on others for a number of critical raw materials.

Look at what is happening now with the Coronavirus, it just takes us two to three weeks, and we all here know what it does to our supply chains. So the circular economy is not only a matter of sustainability – it is also a matter of sustainability without any question – but also a matter of competitiveness and a matter of sovereignty.

Third topic: Europe needs an industry that remains competitive on the global stage while going green and digital. The European Union's competition law has served Europe well – without any question – by contributing to a level playing field. And we all know being competitive abroad requires competition at home.

But in a fast changing world, not least with Europe embarking on its major twin transition, our competition rules will be revised to ensure they remain fit for today's world.

For example, if we want to incentivise fossil-free productions, we cannot accept that at the same time, carbon-heavy products are reimported from abroad. This is neither sustainable, nor is it fair to our industry.

Therefore, we are committed to developing a Carbon Border Adjustment Mechanism. Yesterday I have launched our impact assessment for that. All relevant sectors will be consulted in the most transparent and inclusive manner.

And there is another factor: If we want a level playing field in our Single Market, we must also react to subsidies that distort competition, not only when it comes to Member States but also when we look at our trading partners from other regions of this world.

And this is why we want an Instrument on Foreign Subsidies. We want to remain open to foreign investors – without any question – but there has to be a certain level of reciprocity. We need this reciprocity.

The same rights foreign firms enjoy within our borders, European firms should also enjoy abroad! I think this is a matter of fairness. And for that reason, I call on Member States and the European Parliament to finalise now the International Procurement Instrument that we need for that.

We are an open economy – without any question – we are thriving in a global economy. But this openness should not be taken for granted. If we are faced with unfairness, we are ready to address that.

The fourth point: Europe must master the key technologies of tomorrow. If we build our technological sovereignty, we will also create new business opportunities for our companies.

There is for example the story of our Battery Alliance that makes a very good example. And right in front of me sits the patron of our Battery Alliance, it is Maroš Šefčovič, the Vice-President. Batteries will be strategic in a cleaner and more digital environment. But Europe still relies massively on batteries that are entirely or partly made abroad. This is why we decided to join forces with Member States and the private sector.

And so the European Battery Alliance was born. It is thanks to it that the most innovative, long-lasting and clean batteries for electric cars will soon be ‘made in Europe'.

The same model can be applied in other strategic sectors: just think of hydrogen to produce clean steel, think of secure 5G and 6G networks, think of AI-driven diagnostics in the medical sector or the robots for healthcare, think of the industrial Internet of Things, but also of course of cybersecurity, and there are many, many other examples.

These technologies will be crucial for Europe's prosperity and security in the future. So we must guarantee our autonomy all along these value chains that are necessary to produce these topics. And in a more competitive world, this is not only an investment in our competitiveness, but it is also an investment in our own sovereignty.

Speaking of investment, this is the fifth point: Massive investments will be needed, both public and private. We want you to invest. But we want to invest with you also. And we want to make it easier for you to invest. I am talking about investment in research. I am talking about investment in new technologies. But also about investment in the deployment and the take-up of these technologies by companies of all sizes.

Talking about the European Green Deal. It is not so much about investing into basic R&D, because this takes 20, 30, 40 years until it is market-feasible. The technologies are out there already. We have them. But they are not deployable at the moment being, they are not market-feasible. So this is the point where we have to step in and help and invest and nurture.

Or for example take hydrogen. Hydrogen will become key for the industrial sectors – we had it several times now cited today. But the market is not there yet to sustain its development and deployment in ready solutions.

There was a need to stimulate investment across different sectors and industries. And for this reason, we created with the industry a Public Private Partnership on hydrogen. And today, Europe is one of the global leaders on hydrogen stations and fuel cell buses.

So we are now ready to expand this very positive model of innovation with a new generation of impact-driven Public Private Partnerships supported by the European budget. I think this is the combination we do need.

We want to stimulate investment and we want innovation all across the value chain. We want to involve industries, be they large or be they small. We want to create lead markets for new technologies.

And for that, if these are our goals, if we aim at that, we want to make life easier for investors.

The European classification for sustainable investments – that is the first step to take. We will also strengthen the rules on disclosure of environmental information by companies, we will define high quality standards for green bonds.

Yes, I know, this is a lot – but it is necessary. And we do all of this so that investors can identify what investment is sustainable and what investment is not. Because your investment decisions of today are vital to make the twin transition – the digital one and the green one – happen.

And I fully agree with you, President Gattaz. You said that a stable and a predictable policy environment, stable and predictable, for you is key to foster investment.

Ladies and Gentlemen,

Europe has always been the home of industry and small and medium businesses. For centuries, it has been an industry pioneer for innovation. And for centuries has helped improve the way people around the world produce, consume and do business. Europe's business has powered our economy, it has provided stable living conditions for many.

This is always the goal why we do all this. And it has created a social hub around which our communities are built that is stable and that is reliable – and this is the European way.

Throughout its long history, industry has proven its ability to lead the change. Yes, it has been difficult sometimes, yes, the road has been bumpy – but in the very end, we have been able to lead change.

And it must do the same now as Europe's markets embark on the twin transition on digitalisation and on the European Green Deal. This is what will truly make a difference between success and failure. It will make the difference in our ability to join forces between public and private sector.

We, as the European Union, have an essential role to play, we are aware of that – with investment, with regulations and with incentives. But it is Europe's business that must lead the transition. The only way to find solutions that work for all is to create them together.

A new business way for Europe has to be partially made in Brussels – without any question – but it cannot totally be made in Brussels. Our future will be co-designed and co-created with you. It is when we manage to join forces that we see Europe at its best.

This is the essence of our social market economy. It has always been the essence of our social market economy – and I am convinced it will always be the essence of our social market economy the European way.

Private investment and common good – this is the European way. Innovation and responsibility – this is the European way. Competitiveness and sustainability – this is the European way. This is the new industrial way for Europe we are thinking of. And I cannot wait to get to work towards it, with leaders like you.

And in this best sense: Long live Europe!

Number 10

How Low Can You Go? Lower Than Ever Before

NIST scientists make most sensitive measurements to date of silicon's conductivity for future solar cell, semiconductor applications.

Silicon, the best-known semiconductor, is ubiquitous in electronic devices including cellphones, laptops and the electronics in cars.

Now, researchers at the National Institute of Standards and Technology (NIST) have made the most sensitive measurements to date of how quickly electric charge moves in silicon, a gauge of its performance as a semiconductor.

Using a novel method, they have discovered how silicon performs under circumstances beyond anything scientists could test before — specifically, at ultralow levels of electric charge.

The new results may suggest ways to further improve semiconductor materials and their applications, including solar cells and next-generation high-speed cellular networks. The NIST scientists report their results in Optics Express.

Unlike previous techniques, the new method does not require physical contact with the silicon sample and allows researchers to easily test relatively thick specimens, which enable the most accurate measurements of semiconductor properties.

The NIST researchers had previously done a proof-of-principle test of this method using other semiconductors. But this latest study is the first time researchers have pitted the new light-based technique against the conventional contact-based method for silicon.

It's too soon to say exactly how this work might be used someday by industry. But the new findings could be a foundation for future work focused on making better semiconducting materials for a variety of applications, including potentially improving efficiency in solar cells, single-photon light detectors, LEDs and more.

For example, the NIST team's ultrafast measurements are well-suited to tests of high-speed nanoscale electronics such as those used in fifth-generation (5G) wireless technology, the newest digital cellular

networks. In addition, the low-intensity pulsed light used in this study simulates the kind of low-intensity light a solar cell would receive from the Sun.

“The light we use in this experiment is similar to the intensity of light that a solar cell might absorb on a sunny spring day,” said NIST’s Tim Magnanelli. “So the work could potentially find applications someday in improving solar-cell efficiency.”

The new technique is also arguably the best way to get a fundamental understanding of how the movement of charge in silicon is affected by doping, a process common in light sensor cells that involves adulterating the material with another substance (called a “dopant”) that increases conductivity.

Digging Deep

When researchers want to determine how well a material will perform as a semiconductor, they assess its conductivity. One way to gauge conductivity is by measuring its “charge carrier mobility,” the term for how quickly electric charges move around within a material. Negative charge carriers are electrons; positive carriers are referred to as “holes” and are places where an electron is missing.

The conventional technique for testing charge carrier mobility is called the Hall method. This involves soldering contacts onto the sample and passing electricity through those contacts in a magnetic field. But this contact-based method has drawbacks: The results can be skewed by surface impurities or defects, or even problems with the contacts themselves.

To get around these challenges, NIST researchers have been experimenting with a method that uses terahertz (THz) radiation.

NIST’s THz measurement method is a rapid, noncontact way to measure conductivity that relies on two kinds of light. First, ultrashort pulses of visible light create freely moving electrons and holes within a sample — a process called “photodoping” the silicon. Then, THz pulses, with wavelengths much longer than the human eye can see, in the far infrared to microwave range, shine on the sample.

Unlike visible light, THz light can penetrate even opaque materials such as silicon semiconductor samples. How much of that light penetrates or is absorbed by the sample depends on how many charge carriers are freely moving. The more freely moving charge carriers, the higher the material’s conductivity.

"No contacts are needed for this measurement," said NIST chemist Ted Heilweil. "Everything we do is just with light."

Finding the Sweet Spot

In the past, researchers performed the photodoping process using single photons of visible or ultraviolet light.

The problem with using only one photon for doping, though, is that it typically penetrates only a small way through the sample. And since the THz light completely penetrates the sample, researchers can effectively use this method to study only very skinny silicon samples — on the order of 10 to 100 billionths of a meter thick (10 to 100 nanometers), about 10,000 times thinner than a human hair.

However, if the sample is that thin, researchers are stuck with some of the same issues as with the conventional Hall technique — namely, surface defects can skew the results. The thinner the sample, the bigger the impact of surface defects.

The researchers were torn between two objectives: Increase the thickness of the silicon samples, or increase the sensitivity they get from using single photons of light.

The solution? Illuminate the sample with two photons at once instead of one at a time.

By shining two near-infrared photons on the silicon, scientists are still only using a small amount of light. But it's enough to get through much thicker samples while still creating the fewest possible electrons and holes per cubic centimeter.

"With two photons being absorbed at once, we can get deeper into the material and we can see a lot fewer electrons and holes generated," Magnanelli said.

Using a two-photon measurement means the researchers can keep the power levels as low as possible, but still fully penetrate the sample. A conventional measurement can resolve no fewer than one hundred trillion carriers per cubic centimeter. Using its new method, the NIST team resolved a mere 10 trillion, at least 10 times more sensitivity — a lower threshold for measurement.

The samples studied so far are thicker than some other samples — about half a millimeter thick. That's thick enough to avoid surface defect issues.

And in lowering the threshold for measuring free holes and electrons, the NIST researchers found a couple of surprising results:

Other methods had shown that as researchers create fewer and fewer electrons and holes, their instruments measure higher and higher carrier mobility in the sample — but only up to a point, after which the carrier density gets so low that the mobility plateaus.

By using their noncontact method, NIST researchers found that the plateau occurs at a lower carrier density than previously thought, and that the mobilities are 50% higher than measured before.

“An unexpected result like this shows us things we didn’t know about silicon before,” Heilweil said. “And though this is fundamental science, learning more about how silicon works could help device makers use it more effectively. For example, some semiconductors may work better at lower doping levels than currently used.”

The researchers also used this technique on gallium arsenide (GaAs), another popular light-sensitive semiconductor, to demonstrate that their results are not unique to silicon.

In GaAs, they found that the carrier mobility continues to increase with lower charge carrier density, about 100 times lower than the conventionally accepted limit.

Future NIST work might focus on applying different photodoping techniques to samples, as well as varying the samples’ temperature. Experimenting with thicker samples may provide even more surprising results in semiconductors.

“When we use the two-photon method on thicker samples we may produce even lower carrier densities that we can then probe with the THz pulses,” Heilweil said.

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.

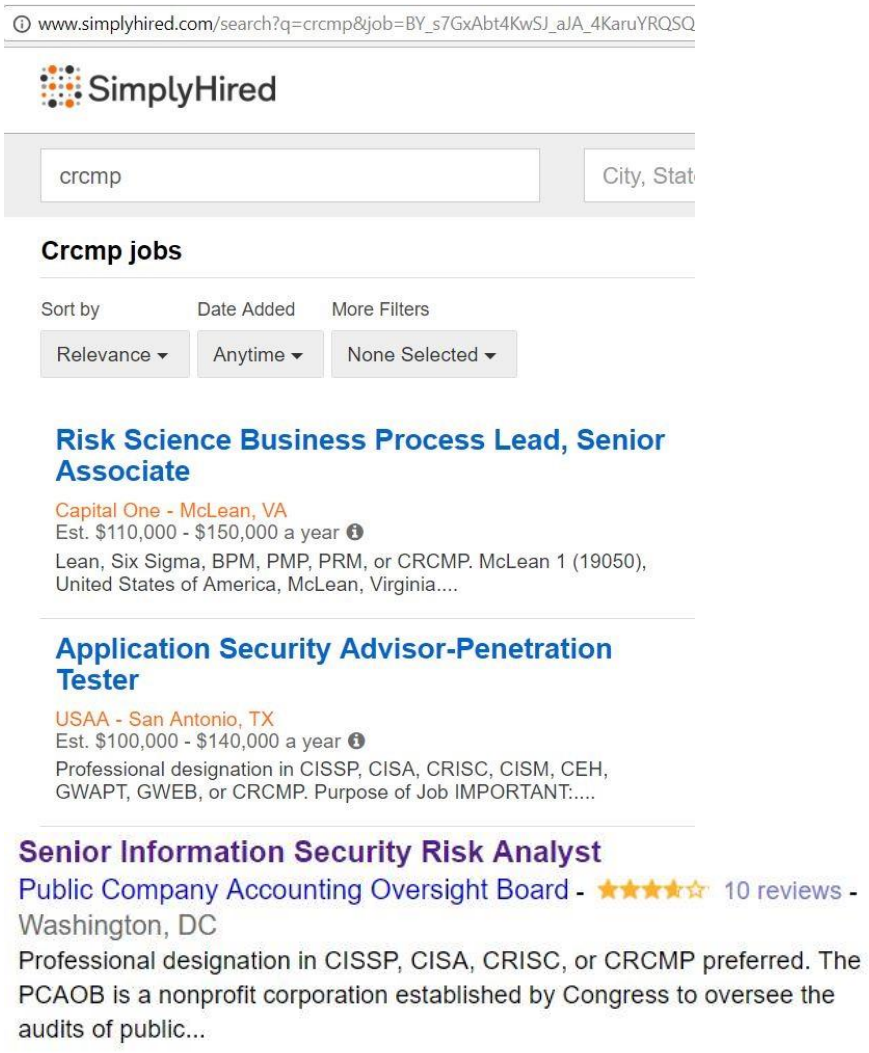
International Association of Risk and Compliance Professionals

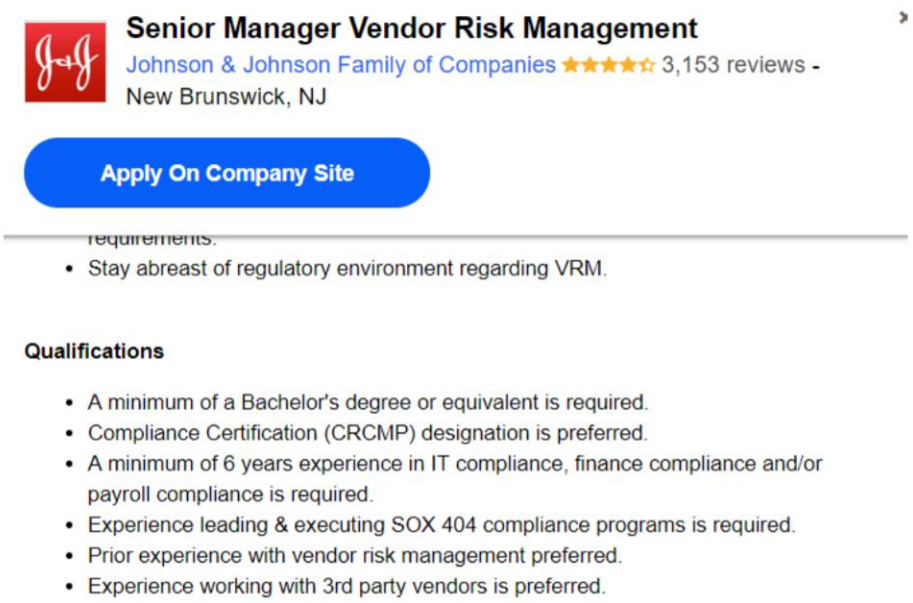
You can explore what we offer to our members:

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