Monday, July 20, 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,

Every year we receive several lists that describe the world's *most admired* companies and organizations.

When I was young, I had my own list. One of the organizations that was very high in this old list, is still present in the current lists. But today I read some bad news, and I have a sad feeling.

I read about this organization, from the Office of Inspector General, Office of Audits:

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program that provides information security protections commensurate with the risks and magnitude of harm that could result from unauthorized access, disclosure, modification, or destruction of agency information.

The organization's information security program is managed through the Risk Information Compliance System (RISCS), a data repository that identifies and maintains an inventory of the Agency's hardware and software, including a system security plan (SSP) and a contingency plan for each information system.

To determine the effectiveness of an agency's information security program, FISMA requires each agency's Inspector General or an independent external auditor to conduct an annual independent evaluation using the FY 2019 IG FISMA Reporting Metrics and report the results to the Office of Management and Budget (OMB).

In October 2019, we reported to OMB that for FY 2019 the organization's information security program was rated at Level 2, "Defined," out of five levels, with Level 5, "Optimized," being the most effective.

This evaluation further examines the organization's information security program based on the FISMA guidance by examining SSPs, contingency plans, and IT security handbooks and other governing documents.

To complete this effort, we performed fieldwork at four Centers; reviewed six information systems; interviewed Agency officials, information systems owners, and information security officers; and reviewed relevant public laws, regulations, and policies.

The organization has not implemented an effective Agency-wide information security program. SSP documentation for all six information systems we reviewed contained numerous instances of incomplete, inaccurate, or missing information.

We also performed a limited review of the Agency Common Control (ACC) system, which aggregates and manages common controls across all Agency information systems, and found that many controls were classified as "other than satisfied," indicating they had been assessed as less than effective.

Moreover, the organization's Office of the Chief Information Officer (OCIO) has not addressed these deficiencies in the ACC SSP. At the organization, Chief Information Security Officers (CISO) located at each Center are responsible for providing oversight to ensure that accurate records on the Agency's information systems, including SSPs, are documented in RISCS. However, these weaknesses in SSPs occurred because Center CISO's often are responsible for managing large portfolios of information systems and do not always have resources available to ensure data in RISCS for each system are accurate and complete.

The issues we identified during this review occurred primarily because the OCIO does not consistently require the use of RISCS as the Agency's information security management tool.

Further, the organization's information security personnel are not sufficiently aware of Agency information security policies and procedures, and the current oversight process does not ensure that delinquent information security assessments are identified and mitigated.
As a result, information systems throughout the Agency face an unnecessarily high level of risk that threatens the confidentiality, integrity, and availability of the organization's information.

Of the six information systems reviewed, we found that four were operating without current contingency plans.

While three of the four systems eventually updated their contingency plans in RISCS during the course of our evaluation, these systems had been operating under outdated plans for as long as 4 years.

The fourth system is currently operating under a 2016 contingency plan.

The organization's policy requires information system owners to review contingency plans for accuracy and completeness at least annually or more frequently if significant changes occur to any element of the plan.

The Agency authorizing officials responsible for reviewing and approving information systems, including contingency plans, are not performing regularly scheduled testing to determine whether the information in RISCS is accurate, up-to-date, and usable by senior IT leadership.

Moreover, the number of systems without a current or available contingency plan in RISCS puts the organization at an unnecessarily high risk by hindering the Agency's ability to recover information systems if needed in an effective and efficient manner, thus threatening the confidentiality, integrity, and availability of the organization's information maintained in those systems.

Which is this organization? You can learn at Number 2 below. Welcome to our 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

Number 1 (Page 6)

Building a financial regulatory system suitable for the UK in the new era

Speech delivered by Nausicaa Delfas, Executive Director of International, at the City & Financial Professional Virtual Roundtables.

Number 2 (Page 13)

EVALUATION OF NASA'S INFORMATION SECURITY PROGRAM

NASA National Aeronautics and Space Administration
Office of Inspector General
Office of Audits

Number 3 (Page 17)

Innovation for the benefit of consumers

Opening remarks by Gabriel Bernardino at the European Forum for Innovation Facilitators (EFIF)

Number 4 (Page 23)

Risk Dashboard

ESRB
European Systemic Risk Board
European System of Financial Supervision

Number 5 (Page 26)

25th Meeting of the Cybersecurity Working Group of the European Banking Federation

Number 1

Building a financial regulatory system suitable for the UK in the new era

Speech delivered by Nausicaa Delfas, Executive Director of International, at the City & Financial Professional Virtual Roundtables.

Highlights

- The 'new era' will be defined by developments brought about by Brexit, Covid-19 and technological and societal changes

- On Brexit, we all need to continue to prepare for a range of scenarios, to be ready for the end of the year

- On Covid-19, the regulatory agenda is moving from crisis response to supporting economic recovery

- Non-banks will be critical in enabling recapitalisation to promote growth and recovery from the pandemic

Thank you to City and Financial Global for hosting this series of webinars. I am delighted to be speaking here today.

The past few months have felt like we are already in a 'new era'.

The impact of the coronavirus pandemic has not only changed how we all work, but has also had a profound impact on our economy. Efforts to manage the long term economic impact of Covid-19 are likely to define the regulatory agenda for years to come.

And of course, other developments will also define the 'new era': the changes resulting from EU withdrawal, as well as technological and societal changes.

So today I will focus on the impact of these developments on the financial regulatory system, and the opportunities they present.

But we should first address immediate challenges. So, I will start by discussing where we are on Brexit, and what we still need to do.

Approaching the end of the transition period

The UK left the EU on 31 January 2020, and we are nearly halfway through the transition period, which will end in just under 6 months' time, at 11pm on 31 December 2020. From that point, EU law will no longer apply and firms will need to be ready.

At the FCA, we have been working hard to undertake all the preparations we can to limit the potential for disruption – for example:

1. Together with the Government and the Bank of England, we are ensuring that there will be a robust legal regime on day 1 by onshoring EU law to the UK statute book and our rule book, and by clarifying through use of the Temporary Transitional Power which onshoring changes firms will have to comply with from 1 January next year and which ones they will have until March 2022 to implement.

2. We have introduced arrangements for temporary permission that will allow EEA firms to continue providing services and EEA funds to continue to be marketed in the UK once passporting ends, provided that the relevant notifications are made.

Over 1,000 firms and over 600 fund managers have already notified us, and we will reopen the notification window on 30 September. From 2021, these EEA firms will be called to apply for permanent authorisation to replace their temporary permission.

We plan to consult later this year on the approach we will take when we assess applications from overseas firms. And for those EEA firms who do not notify for a temporary permission or who do not obtain a permanent authorisation in due course, the Government has legislated to allow them to continue to service pre-existing contracts in the UK.

3. We have already entered into a number of MoUs with EU and non-EU authorities to enhance supervisory cooperation.

4. We have provided technical advice to the Treasury on the assessments of equivalence between the UK and the EU. We are also providing technical support to the UK Government in its trade negotiations with the EU and non-EU countries.

Equivalence decisions have not yet been made, and negotiations are ongoing. The outcome will impact on some of the post transition period risks – for example, deeming each other's regulatory frameworks as equivalent is the best way to mitigate risks of disruption from overlapping

Share Trading Obligations and Derivatives Trading Obligations. Similarly, the data adequacy assessments conducted this year will impact transfers of personal data between the EEA and the UK.

Other risks are outside of our control to mitigate. For instance, where EU Member States had individually passed laws to smooth a possible 'hard' exit, some of these laws have now lapsed and there is no guarantee that new laws will be issued.

So, if you intend to continue servicing customers in the EEA from 1 January 2021, you will need to have adapted your business according to the local laws and local regulators' expectations by that date, speaking to local regulators as appropriate, and obtaining permissions and repapering contracts where necessary, whilst treating customers fairly throughout.

In short, my message to you is that we all need to continue to prepare for a range of scenarios, to be ready for the end of the year. We will continue to update the FCA website and engage with you as the year progresses – and we encourage you to continue to raise issues with us.

After the transition period

What will the financial regulatory system look like after Brexit, Covid-19 and other changes heralding this 'new era'?

Our approach going forward will be guided by our continued commitment to the highest international standards, and by what is right for the UK's markets, building on the strengths of the existing UK regulatory and legal system.

Last week the Chancellor stated that the next phase of the Financial Services Future Regulatory Framework Review will look at how financial services regulation will be made in the UK after the transition period, including the role of Parliament, the Treasury, the financial services regulators, and how stakeholders are involved in the process.

One area that gives an indication of what this might look like is the UK's approach to the investment firms' prudential regime.

We published a Discussion Paper last week and the Government set out its plans to delegate responsibility to regulators to make detailed requirements - this delegation would be underpinned by a new framework for accountability, that is also intended to ensure that we consider equivalence and competitiveness when we make new rules.

This is consistent with our regulatory principles in FSMA and the Chancellor's remit letter: that we should have regard to economic growth, competitiveness and trade, when we advance our statutory objectives of promoting consumer protection, market integrity and competition.

In our view, maintaining a strong and robust regulatory and supervisory system, and our commitment to achieving the highest international standards, go hand in hand with the UK's competitiveness as a global financial centre.

We support open markets, with mechanisms to defer regulatory and supervisory oversight to other jurisdictions, so long as we are comfortable that their rules provide equivalent outcomes to the UK's and we have strong cooperation arrangements in place.

Deference reduces costs and frictions for firms and minimises unnecessary market fragmentation, and is a longstanding commitment recognised at the G20.

We remain committed to working with partners across the globe to shape international standards.

Just last week, IOSCO published a report on 'Good Practices on Processes for Deference', which sets out what authorities could consider when undertaking deference assessments of individual jurisdictions or individual firms. We contributed to that report and are supportive of that work.

Outside of international committees, we are providing technical advice and support to the Government as it looks at future trade opportunities. Yesterday, the Treasury issued a joint statement with Switzerland on a shared ambition to work towards mutual recognition of each other's regulatory and supervisory regimes, taking an outcomes-based approach.

The Chancellor also announced that the Treasury has assessed Swiss stock markets as equivalent, which holds out the prospect of reciprocal access to the Swiss and UK stock exchanges being facilitated after the transition period.

We are also continuing our programme of international engagement, for example, through the upcoming UK-Singapore Financial Dialogue, discussing future cooperation and recent trends and impacts on our economies, including our respective responses to Covid-19.

The impact of Covid-19 and other changes

As the impact of Covid-19 became manifest in global financial markets, we have worked intensely to maintain open and orderly markets, recognising the essential role they play in supporting businesses, governments and the broader economy.

In doing so, we have coordinated with partners here in the UK, EU and globally. We have shared insights on market developments and coordinated responses, for example with the Financial Stability Board, IOSCO and ESMA. I have certainly valued our work together towards common goals.

Following the initial phase of the crisis, we are now looking at conduct and resilience of the markets in the medium and longer term, as well as broader trends that existed before the crisis, but which have become ever more important in the recovery.

I will focus on a few key themes.

In terms of market resilience, we know that the global financial system as a whole is more resilient than it was 10 years ago. But we will naturally be reviewing what happened over the early phase of the pandemic, when the impacts of lockdown measures implemented across multiple jurisdictions were very clearly felt in markets.

In doing this, we need to focus on developing a complete picture of how all elements of the system – banks, non-banks, and market infrastructures – are interconnected, and how they function under extreme stress. Only then can we identify any potential vulnerabilities.

We need to be balanced and scrupulous in our analysis, and acknowledge the fundamental purpose of the system – that financial markets exist to allocate capital and to manage risk.

Some already say that there may be vulnerabilities that need addressing in the non-bank sector, and if this proves to be the case then care should be taken that in attempting to take risk out of that sector, we do not simply transfer it to another part of the system.

Crucially, it is important that any possible change to existing frameworks do not undermine markets' ability to perform their essential functions.

We must recognise that the non-bank sector will be critical in enabling recapitalisation to promote growth and recovery from the pandemic. So, the benefits of a vibrant market should be considered alongside the potential risks.

The Government announced(link is external) last week its plan to give the FCA enhanced powers to help manage and direct an orderly wind-down of critical benchmarks such as LIBOR, in particular with regard to 'tough legacy' contracts.

We will be publishing statements of policy, setting out our intended approach to potential use of these powers, ahead of taking any action, and will seek the views of stakeholders here in the UK and internationally as we prepare those statements.

Firms' operational resilience has been tested in the crisis, and overall performed well – despite increased reliance on dispersed working. In the UK, we are consulting with the PRA through to October 2020 on new requirements to strengthen operational resilience in financial services – with the aim of staying ahead of evolving risks, to ensure ongoing financial stability and market integrity.

The disruption caused by Covid-19 has demonstrated the value of technology in overcoming some of these challenges. Digital innovation may help address issues from the longer-term decline in the use of cash, increase the availability of mass market financial advice, and reduce the need for manual processes in businesses.

We are committed to supporting innovation that works for all, including vulnerable consumers and smaller firms. We know that our regulatory framework needs to keep pace – focussing on outcomes, and being forward looking. To that end, our digital sandbox will be open for applications this summer.

Sustainable finance remains an area of key interest to investors. As the UK prepares to host COP26 and moves to a 'green recovery', the role of private finance is front and centre.

The pandemic has also elevated social considerations such as supply chain sustainability, employee welfare and corporate culture.

The FCA's focus is on well-functioning markets, including clear disclosure, and internationally we are co-leading the work on climate-related financial disclosures at an IOSCO Task Force.

And as highlighted in our Business Plan, to ensure we are well positioned to tackle these and other challenges, we are working to continuously transform our own approach – for example through the use of data and analytics.

Conclusion

We are going through a period of tremendous change, and there remain many challenges to overcome. But we also have tremendous opportunities: the opportunity to maintain high standards in our regulated markets, delivering the right outcomes for consumers; to tackle the challenges of Brexit and Covid-19 in an agile way, and for the long term.

We stand ready to work with you all, as well as fellow regulators and authorities – in the UK and abroad – to deliver a connected and robust financial system that will thrive in the new era.

Number 2

EVALUATION OF NASA'S INFORMATION SECURITY PROGRAM

NASA
National Aeronautics and Space Administration
Office of Inspector General
Office of Audits

In fiscal year (FY) 2019, NASA spent approximately $2.3 billion on computer systems, networks, and information technology (IT) services used to control spacecraft, collect and process scientific data, and provide security for critical Agency infrastructure among other things.

Given NASA's mission and the valuable technical and intellectual capital it produces, the information maintained within the Agency's IT infrastructure presents a high-value target for hackers and criminals.

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program that provides information security protections commensurate with the risks and magnitude of harm that could result from unauthorized access, disclosure, modification, or destruction of agency information.

NASA's information security program is managed through the Risk Information Compliance System (RISCS), a data repository that identifies and maintains an inventory of the Agency's hardware and software, including a system security plan (SSP) and a contingency plan for each information system.

To determine the effectiveness of an agency's information security program, FISMA requires each agency's Inspector General or an independent external auditor to conduct an annual independent evaluation using the FY 2019 IG FISMA Reporting Metrics and report the results to the Office of Management and Budget (OMB).

In October 2019, we reported to OMB that for FY 2019 NASA's information security program was rated at Level 2, "Defined," out of five levels, with Level 5, "Optimized," being the most effective.

This evaluation further examines NASA's information security program based on the FISMA guidance by examining SSPs, contingency plans, and IT security handbooks and other governing documents.

To complete this effort, we performed fieldwork at four Centers; reviewed six information systems; interviewed Agency officials, information systems owners, and information security officers; and reviewed relevant public laws, regulations, and policies.

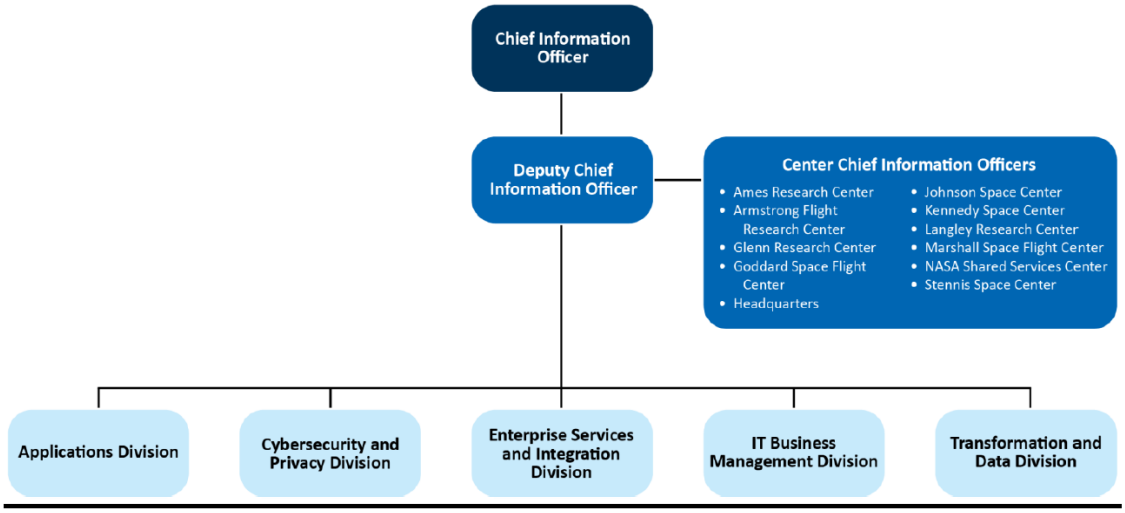
NASA has not implemented an effective Agency-wide information security program. SSP documentation for all six information systems we reviewed contained numerous instances of incomplete, inaccurate, or missing information.

We also performed a limited review of the Agency Common Control (ACC) system, which aggregates and manages common controls across all Agency information systems, and found that many controls were classified as "other than satisfied," indicating they had been assessed as less than effective.

Moreover, the NASA Office of the Chief Information Officer (OCIO) has not addressed these deficiencies in the ACC SSP.

At NASA, Chief Information Security Officers (CISO) located at each Center are responsible for providing oversight to ensure that accurate records on the Agency's information systems, including SSPs, are documented in RISCS.

Figure 1: Office of the Chief Information Officer Organizational Chart as of May 2020



Source: NASA.

However, these weaknesses in SSPs occurred because Center CISO's often are responsible for managing large portfolios of information systems and do not always have resources available to ensure data in RISCS for each system are accurate and complete.

The issues we identified during this review occurred primarily because the OCIO does not consistently require the use of RISCS as the Agency's information security management tool.

Further, NASA information security personnel are not sufficiently aware of Agency information security policies and procedures, and the current oversight process does not ensure that delinquent information security assessments are identified and mitigated.

As a result, information systems throughout the Agency face an unnecessarily high level of risk that threatens the confidentiality, integrity, and availability of NASA's information.

Of the six information systems reviewed, we found that four were operating without current contingency plans.

While three of the four systems eventually updated their contingency plans in RISCS during the course of our evaluation, these systems had been operating under outdated plans for as long as 4 years.

The fourth system is currently operating under a 2016 contingency plan. NASA policy requires information system owners to review contingency plans for accuracy and completeness at least annually or more frequently if significant changes occur to any element of the plan.

The Agency authorizing officials responsible for reviewing and approving information systems, including contingency plans, are not performing regularly scheduled testing to determine whether the information in RISCS is accurate, up-to-date, and usable by senior IT leadership.

Moreover, the number of systems without a current or available contingency plan in RISCS puts NASA at an unnecessarily high risk by hindering the Agency's ability to recover information systems if needed in an effective and efficient manner, thus threatening the confidentiality, integrity, and availability of NASA information maintained in those systems.

During our review of selected OCIO IT security handbooks and other related governance documents, we found that 27 of 45 documents had not been reviewed and approved in more than 1 year and 8 that not been reviewed in over 3 years.

OCIO policy states that IT security handbooks shall be reviewed or updated on an annual basis or more frequently if appropriate.

However, the OCIO policy management process does not provide adequate oversight of this process or a reliable list of policies requiring review.

OCIO officials stated that they intend to change the review process in FY 2020 but expressed concern about the sufficiency of resources to complete this task.

Failure to update NASA policy and procedures in a timely manner increases the risk that Agency personnel will employ out-of-date information security practices. The timely review and update of IT governance documents is a basic internal control necessary for the effective and efficient operation of Agency information systems.

To read more:
https://www.oversight.gov/sites/default/files/oig-reports/IG-20-017.pdf

Number 3

Innovation for the benefit of consumers

Opening remarks by Gabriel Bernardino at the European Forum for Innovation Facilitators (EFIF)

Introduction

It's my pleasure to welcome you today to this meeting of the European Forum for Innovation Facilitators.

I would like to extend a warm welcome to my colleagues from our fellow European Supervisory Authorities – the European Banking Authority and the European Securities and Markets Authority.

It is always a pleasure to work on joint initiatives with them and I would like to thank the EBA for their excellent chairing of this forum over the last year. Rest assured that we will try our best to build on their progress.

Of course, I would have preferred to welcome you in person in Frankfurt but – like everyone else – we have had to adapt. Nonetheless, we can still enjoy a fruitful discussion, just this time in a virtual environment.

Even now, if we look back to the start of the Coronavirus disruption, I think that we already can see just how quickly people and businesses have been able to adapt and innovate and just how easy it has been for people to turn to digital solutions.

People have relied on technology to get them through their day. From chatting to friends and family to ordering shopping, even the most reluctant consumers have embraced the online world available at the touch of a smartphone button.

And of course, financial services are no exception.

Smartphone applications and robo-advice solutions enabling 24/7 access from everywhere, contactless payment cards or smart watches for

payments, mobile banking, crowdfunding, peer-to-peer lending and insurance solutions, and insurers who will accept smartphone films from policyholders as a way of supporting claims. These are just some examples of how people are going digital.

And so while the impact of the Coronavirus may not yet be clear, one thing is certain: There is growing appetite and acceptance for financial innovation.

And our role is to make it happen.

But we have to make it happen in a way where the risks and opportunities are balanced. Where we take a sound approach ensuring a balance between enhanced financial innovation and well-functioning consumer protection and financial stability frameworks.

Financial innovation for the benefit of consumers

As consumers eagerly embrace digital technology, we must not let them down.

We must make sure that innovation is for the benefit of consumers.

Without question, digital technology is bringing opportunities for providers and consumers alike. Thanks to innovation consumers can benefit from a wider range of products and services that are tailored specifically to their habits and needs.

Take car insurance as an example.

Car telematics offer customers all sorts of benefits. Like premium discounts based on driving habits, preventive push-notifications or alerts in case of bad weather conditions, or road assistance in case of accident or car theft of the vehicle.

These are just some of the positive aspects of innovation.

But innovation also has risks.

The Internet of Things harnesses data to better understand customer needs and provide better customer service. The greater the capacity to process data, the more precise the products, policies and pricing that can be offered.

But increasingly we are seeing issues linked to fairness and consumers at risk of bias or exclusion.

And we need to find the right balance between enabling financial innovation and safeguarding consumer protection and financial stability.

And for me, one thing is clear: Consumer outcomes should always come first.

This is one of the reasons why EIOPA has set up its Consultative Expert Group on Digital Ethics in insurance.

The group is looking at three areas – fairness and non-discrimination; transparency and explainability; and governance – and will report back later in the year.

We are not reinventing the wheel, or working in isolation, but rather we are looking at the work done by the European Commission on artificial intelligence and other international standard setting bodies and we are adapting the general principles to the specificities of the insurance sector. We aim to provide guidance to the market in the operationalisation of digital ethics principles for insurance.

Because at the end of the day, if companies cannot demonstrate that that they treat their customers' data responsibility, then customers will not trust those companies with their business.

And innovation will have no value.

The role of the European Forum for Innovation Facilitators in supporting innovation

So how do we foster trust in innovation?

The role of this forum is vital.

This forum enables a valuable dialogue between supervisors, innovation facilitators and innovators.

Innovators can get better understanding of the regulatory landscape while supervisors can stay ahead of the latest technological developments within financial services.

This forum also plays a unique role in fostering cross-border cooperation between facilitators.

Through this forum, national competent authorities can meet regularly to share experience and expertise with their innovation facilitators.

And through this forum we can contribute to reaching common views on the regulatory treatment of innovative products, services and business models.

Because, if Europe is to fulfil its potential and take a leading role in financial innovation, it is essential that there is a common approach to supervision and regulatory treatment of products and services.

And it's true that the Single Market can be difficult to navigate. The reality is that the current patchwork of national implementations of conduct rules makes it very difficult to scale innovative solutions cross-border.

We should ask ourselves if this is for the benefit of European consumers. I don't think so.

The European Commission has recently consulted widely to shape its Digital Finance Strategy. In fact, we – along with EBA and ESMA – have contributed.

We should take advantage of the ambition of this strategy and appetite for innovation to renew our efforts to help innovators overcome the obstacles that they face in scaling up.

Because we need our firms to be able to compete worldwide in the field of innovation.

We have a good starting point. When we launched this forum in 2019 – on the basis of our report on regulatory sandboxes and innovation hubs – we set ourselves an ambitious agenda.

And we have made progress. I am pleased to say that since the inception of this forum there are now some 40 innovation facilitators in operation across Europe. This is double the number that we started with.

And – with commitment and cooperation – we can make more progress.

Because we really are at a point where financial innovation is taking off. The Coronavirus crisis has accelerated the trend towards digital transformation and we cannot afford to be left behind. Nor can we afford to leave consumers behind.

So not only do we need to foster innovation, but we need to foster innovation that consumers believe in.

And our success will depend upon our ability to offer practical solutions that help create the right environment for financial innovators to succeed and the right environment for consumers to benefit.

In conclusion

Let me conclude by sharing with you my own vision: Firms that can scale up their innovative digital solutions within Europe, selling simple and value for money products on a cross border basis without facing any kind of obstacles, for the benefit of European consumers.
This vision demands two main elements:

The development of a European 28th regime on the digital distribution of simple mass products that should include a set of distribution and disclosure requirements adapted to the lower risk of these simple products.

These requirements should ensure a high level of consumer protection but at the same time significantly lower the current costs of distribution and compliance.

Strong and intrusive European conduct supervision involving a network of National Competent Authorities to ensure that consumers of these products are indeed protected throughout Europe in a consistent manner.

In the meantime, I see the EFIF as a forum that can take important steps into the right direction. Our work matters and it matters all the more so during this current crisis.

Therefore I encourage you to continue the work with the same level of enthusiasm that you have all shown since the inception of the EFIF.

Let me conclude by stating the obvious: Innovation is here and it is here to stay.

We need to work with it, so that innovation works for businesses and for consumers.

Because we need consumers to have trust in innovation.

And consumers will only trust in innovation if they have trust in the innovators. Innovation must empower consumers, but it must also protect them.
And we can make sure that it does. If we work together, we can build on the achievements of this forum to make a positive and valuable change across Europe.

And with that, I will leave you to a morning of fruitful and energetic discussion.

Thank you.

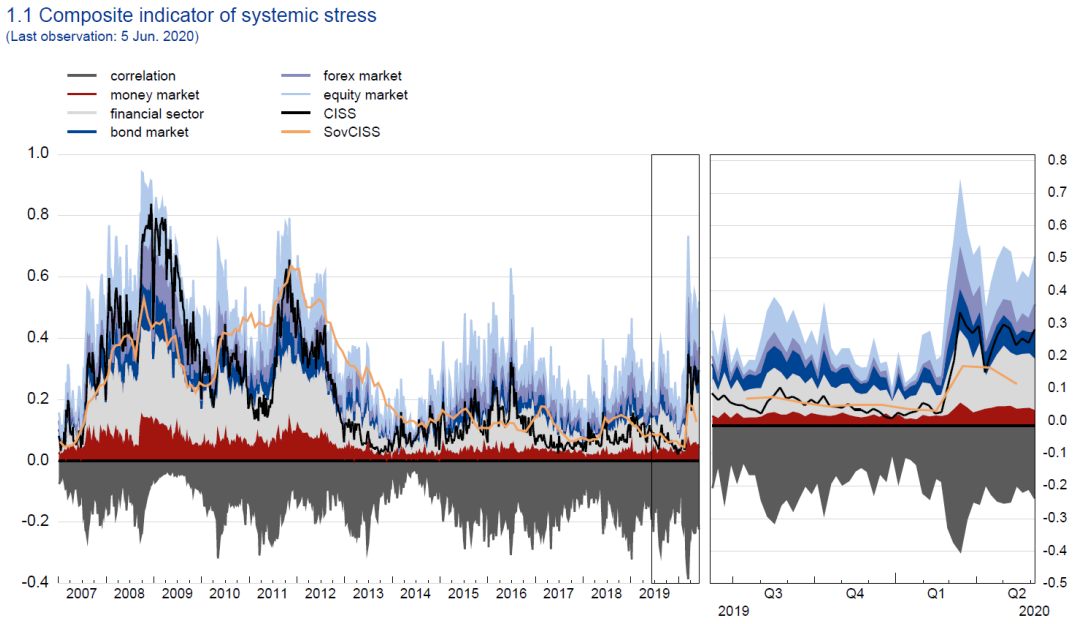
Number 4

Risk Dashboard

ESRB
European Systemic Risk Board
European System of Financial Supervision

The ESRB risk dashboard is a set of quantitative and qualitative indicators of systemic risk in the EU financial system. It is published quarterly, one week after its adoption by the General Board, and is accompanied by an overview note that explains the recent development of the indicators, and two annexes that explain the methodology and describe the indicators.

The risk dashboard should not be considered to be a policy statement on systemic risks. Additional indicators that support systemic risk assessment in the EU financial system are available in the Macro-prudential database maintained by the ECB.



Market-based indicators of systemic stress in the European Union (EU) showed positive signs of recovery from the economic shock caused by the outbreak of the coronavirus (COVID-19).

During the second quarter of 2020 the indicators of systemic stress gradually decreased and stabilised at a lower level.

Similarly, indicators of implied volatility, which measure market uncertainty, decreased notably across various market segments and the probability of the simultaneous default of large and complex banking groups and EU sovereigns also fell.

Instead, there was some variation in the implied volatility of short-term interest rates, as the level of volatility of interest rates denominated in pound sterling continued to rise while the volatility for US dollar interest rate decreased, with large fluctuations.

EU equity indices and price/earnings ratios recovered most of their losses.

However, equity prices of financials, particularly banks and insurance companies, recovered only moderately and did not return to their pre-COVID-19 levels.

Regarding macroeconomic developments, euro area monetary financial institution (MFI) credits and deposits rose significantly in the first quarter of 2020.

The total amount of four-quarter cumulated credit flows increased by around €600 billion owing mainly to a large increase in credit to non-euro area residents and somewhat smaller increases in credit to non-financial corporations (NFCs) and to the general government.

Total deposits soared by approximately the same amount as credits because of the positive contribution of the deposits of the Eurosystem, NFCs, and other financial institutions.

There were no significant changes in the domestic credit-to-GDP gap in the fourth quarter of 2019.

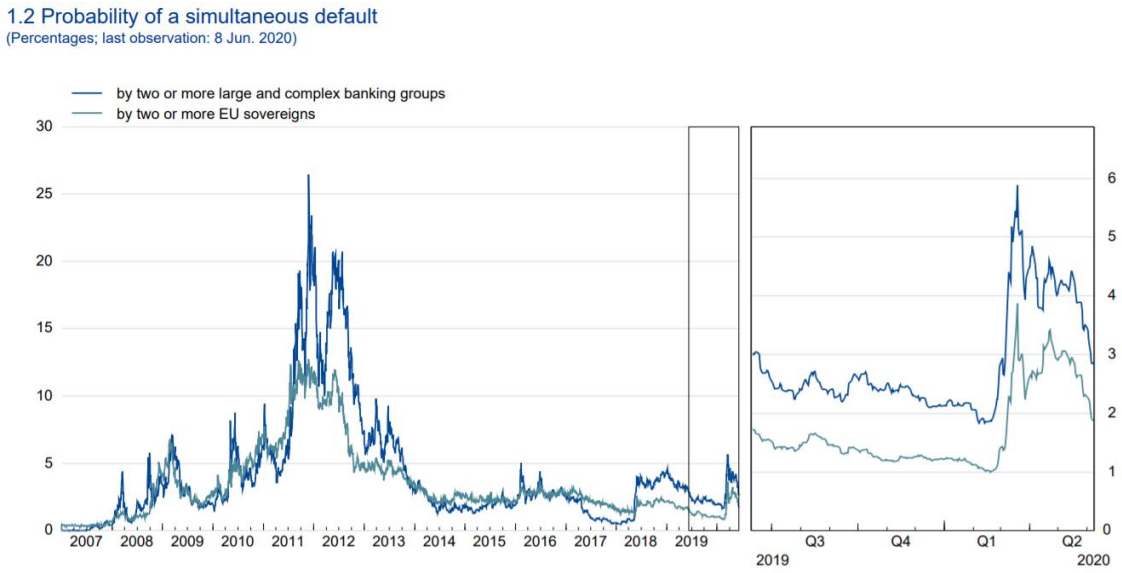
A deep economic contraction prevailed in the EU and the euro area throughout the first quarter of 2020 as a result of the stringent lockdown measures implemented in most the Member States, a collapse of global trade and the confidence shock affecting the economy.

In the first quarter of 2020, EU GDP and euro area GDP plummeted by 2.6% and 3.1% year on year respectively.

More than half of EU Member States suffered an economic slump, with Italy, France and Spain being the most severely hit countries (recording falls in GDP of 5.4%, 5.1%, and 4.1% respectively in the first quarter of 2020).

The outlook for the EU economy is surrounded by considerable uncertainty with regard to the depth and length of the coronavirus pandemic and its ultimate economic implications.

Even larger impacts on production and unemployment are expected in the second quarter of 2020, while the European Commission and the ECB forecasts do not anticipate a sustained recovery before 2021.



To read more: https://www.esrb.europa.eu/pub/rd/html/index.en.html

Number 5

25th Meeting of the Cybersecurity Working Group of the European Banking Federation

The European Union Agency for Cybersecurity (ENISA) co-hosted the 25th meeting of the cybersecurity working group of the European Banking Federation (EBF)

The meeting has been an opportunity for professionals from banking institutions to share good practices and lessons learned about cybersecurity challenges, threats, and incidents faced over the past year. The group also discussed new and emerging policy developments in the sector as well as current and future technological challenges

The European Union Agency for Law Enforcement Cooperation (EUROPOL) provided insights on threat intelligence in the financial sector.

The American Bankers Association (ABA) gave a presentation to reflect on the importance of the Sheltered Harbor initiative.

Besides, the European Banking Federation supports ENISA by playing an active role as member of the European Stakeholders Cybersecurity Certification Group.

This year ENISA has been supporting the financial community with the mapping of stakeholders and EU initiatives in relation to cybersecurity. Previous initiatives of ENISA in the industry include the Payment Service Directive 2 (PSD 2) implementation interactive map, Blockchain

cybersecurity as well as support in the information sharing community through the European Information Sharing and Analysis Centre FI-ISAC. You may visit:
https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/finance/european-fi-isac-a-public-private-partnership

Number 6

HMRC phishing scam targets passport information

National Cyber Security Centre

A phishing scam designed to steal personal and financial details from self-employed workers is now trying to capture passport information from victims.

Details from a threat report in June explain how people are informed via SMS that they may be eligible for a tax refund. They are then redirected to a fake web page that looks like the official HMRC site (at: https://www.ncsc.gov.uk/report/weekly-threat-report-12th-june-2020)

The recent addition to this scam includes requesting passport information as part of a 'verification' process.

HMRC will never send notifications of a tax rebate or ask that personal or payment information, including passport information, be disclosed by email or text message.

Have you spotted a suspicious email?

If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS):

report@phishing.gov.uk

You should forward any suspicious emails and details of suspicious phone calls purporting to be from HMRC to phishing@hmrc.gov.uk and any suspicious text messages to 60599.

Number 7

DHS, DOT, and HHS Issue New Guidance for Airline Industry Partners to Facilitate Safe Air Travel

The U.S. Departments of Homeland Security, Transportation, and Health and Human Services has issued joint guidance specifically for the air travel industry to better protect passengers, crew, and other airport workers from the COVID-19 pandemic during our economic recovery.

This guidance, the "Runway to Recovery: The United States Framework for Airlines and Airports to Mitigate the Public Health Risks of Coronavirus," lays out a framework for implementing public health measures in the aviation sector to minimize the risk of COVID-19 transmission.

The guidance:
https://www.transportation.gov/sites/dot.gov/files/2020-07/Runway_to_Recovery_07022020.pdf

"As we reopen the economy under President Trump's Opening Up America Again guidelines, we are taking aggressive measures to protect the American people from COVID-19 as they reengage their travel plans," said Acting Secretary of Homeland Security Chad F. Wolf.

"Air travel is critical to our economic recovery and DHS has been working closely with our partners in the aviation industry throughout every step of our response to this pandemic to ensure that we are facilitating travel in a safe and secure manner."

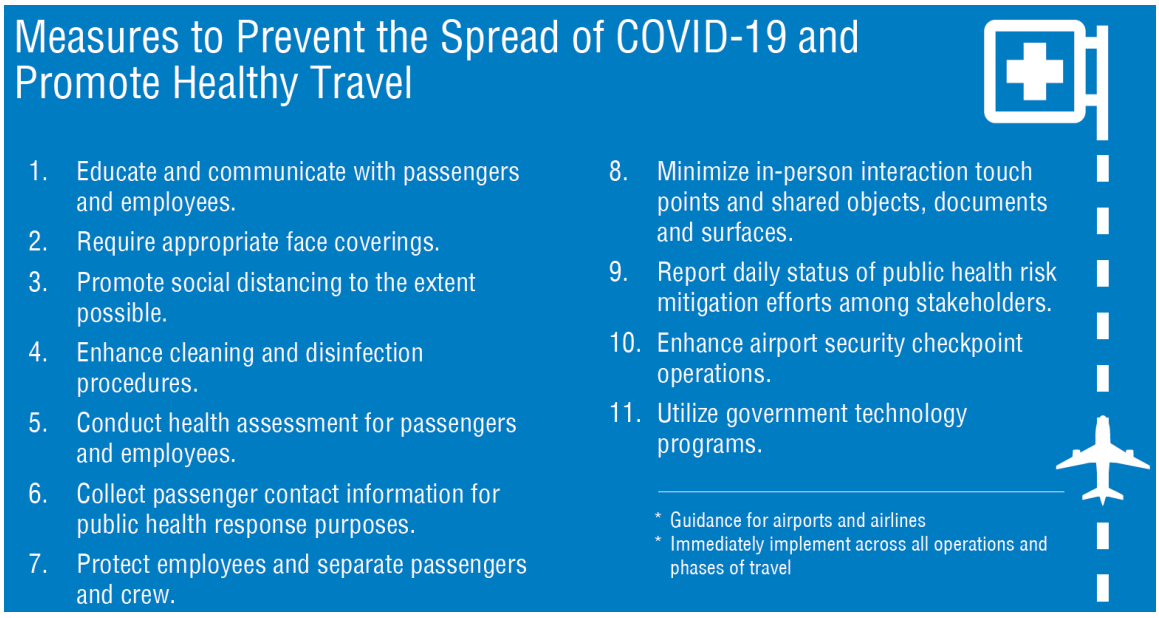
The guidelines call for public health measures to be implemented at each step in the air travel process, including before, during, and after the flight to

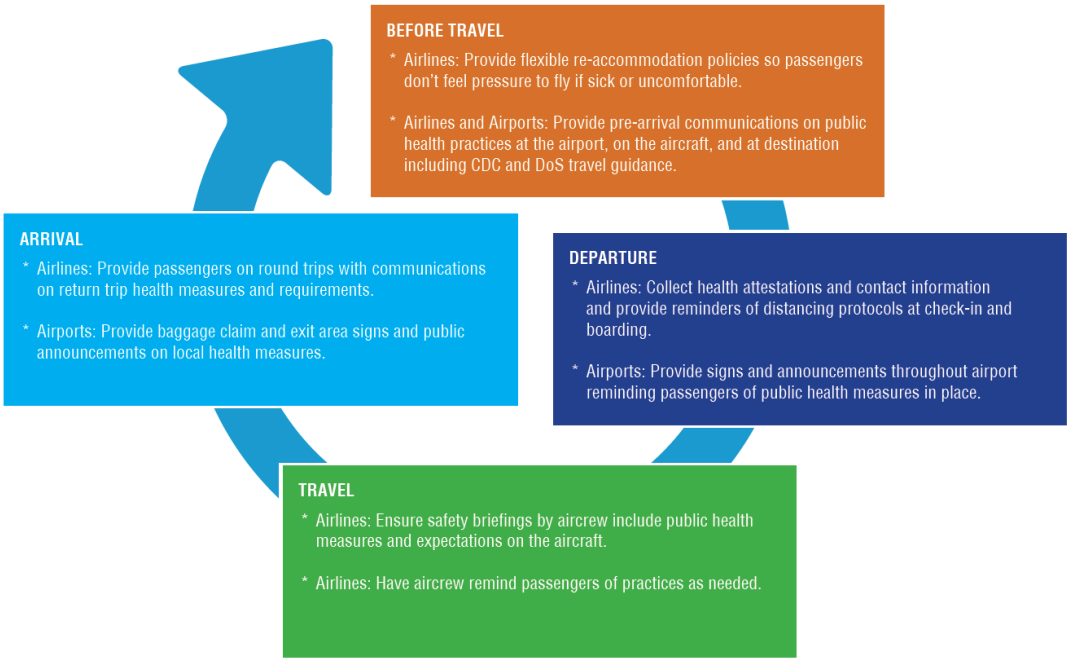
minimize the chance for transmission of the virus. Some of the recommendations for airlines and airports include:

- Create barriers to disease transmission;
- Increase social distancing measures;
- Minimize points of contact with surfaces and people;
- Ensure cleanliness of all areas with potential for human contact;
- Know how passengers arriving on international flights can be reached if exposed to COVID 19; and
- Specialized training for aviation workers, especially airline crew.

The industry guidelines combine the expertise of three federal agencies, DHS, HHS, and DOT, each of which contributed specialized expertise on infectious diseases, public safety, and transportation operations into these guidelines.

It is important to note that the Transportation Security Administration (TSA) has already implemented many of the guidelines being proposed for the airline industry through their "Stay Healthy. Stay Secure." campaign (https://www.tsa.gov/news/press/releases/2020/06/30/tsa-administrator-pekoske-announces-stay-healthy-stay-secure). The U.S. Government will continually assess these measures, in close consultation with airlines and airports, as Americans begin to travel again.




BEFORE TRAVEL
* Airlines: Provide flexible re-accommodation policies so passengers don't feel pressure to fly if sick or uncomfortable.
* Airlines and Airports: Provide pre-arrival communications on public health practices at the airport, on the aircraft, and at destination including CDC and DoS travel guidance.
DEPARTURE
* Airlines: Collect health attestations and contact information and provide reminders of distancing protocols at check-in and boarding.
* Airports: Provide signs and announcements throughout airport reminding passengers of public health measures in place.
TRAVEL
* Airlines: Ensure safety briefings by aircrew include public health measures and expectations on the aircraft.
* Airlines: Have aircrew remind passengers of practices as needed.
ARRIVAL
* Airlines: Provide passengers on round trips with communications on return trip health measures and requirements.
* Airports: Provide baggage claim and exit area signs and public announcements on local health measures.

Number 8

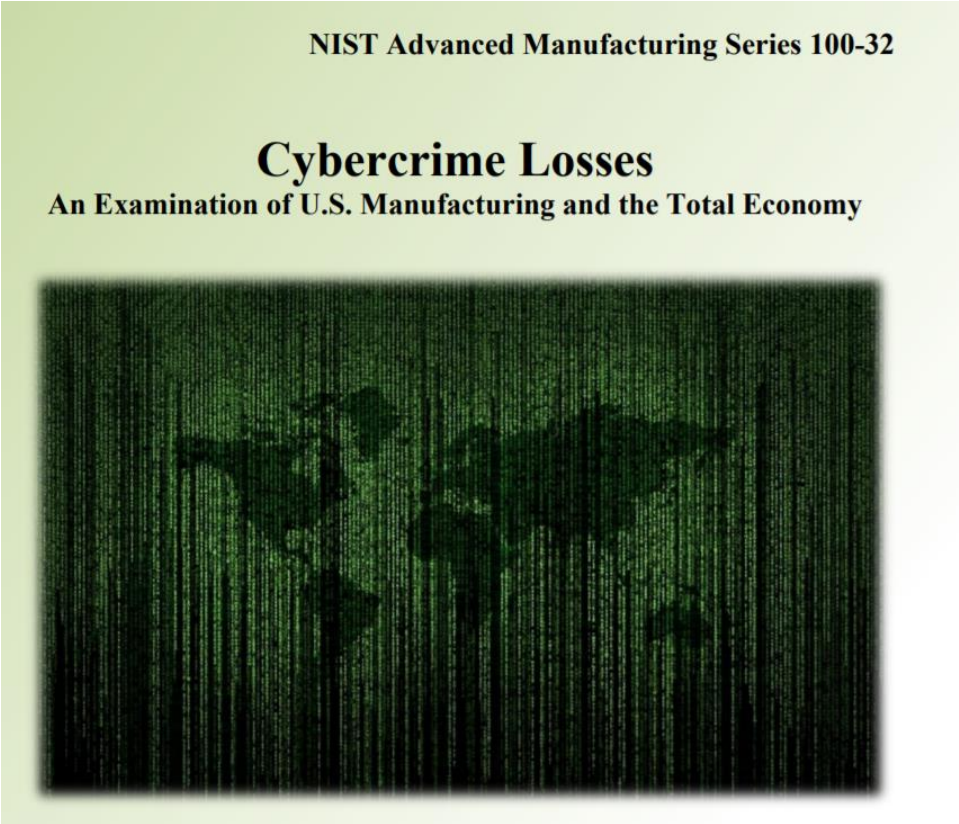
Cybercrime: It's Worse Than We Thought

By: Douglas S. Thomas

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

The cyber world is relatively new, and unlike other types of assets, cyber assets are potentially accessible to criminals in far-off locations. This distance provides the criminal with significant protections from getting caught; thus, the risks are low, and with cyber assets and activities being in the trillions of dollars, the payoff is high.

When we talk about cybercrime, we often focus on the loss of privacy and security. But cybercrime also results in significant economic losses. Yet the data and research on this aspect of cybercrime are unfortunately limited. Data collection often relies on small sample sizes or has other challenges that bring accuracy into question. In a recent NIST report (https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.100-32.pdf , I looked at losses in the U.S. manufacturing industry due to cybercrime by examining an underutilized dataset from the Bureau of Justice Statistics, which is the most statistically reliable data that I can find.



I also extended this work to look at the losses in all U.S. industries.

The data is from a 2005 survey of 36,000 businesses with 8,079 responses, which is also by far the largest sample that I could identify for examining aggregated U.S. cybercrime losses.

Using this data, combined with methods for examining uncertainty in data, I extrapolated upper and lower bounds, putting 2016 U.S. manufacturing losses to be between 0.4% and 1.7% of manufacturing value-added or between $8.3 billion and $36.3 billion.

The losses for all industries are between 0.9% and 4.1% of total U.S. gross domestic product (GDP), or between $167.9 billion and $770.0 billion.

The lower bound is 40% higher than the widely cited, but largely unconfirmed, estimates from McAfee.

What makes the estimates startling is that, despite being higher than commonly cited values, the assumptions I used to calculate losses pushed the lower bound estimate down significantly, meaning the true loss may be much higher.

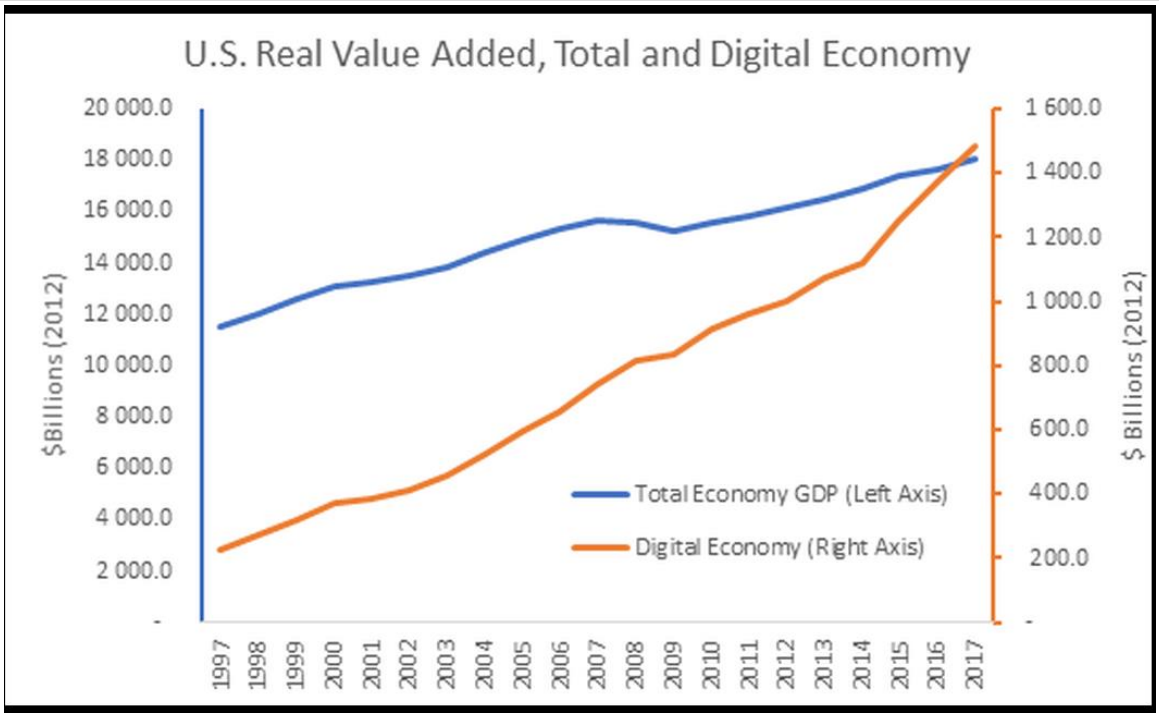
I calculated the low value assuming that those who did not respond to the Bureau of Justice Statistics survey did not experience any losses.

This amounted to 77% of the 36,000 businesses surveyed being presumed as having no loss; thus, the true loss is most likely higher than the low estimate.

Additionally, the 2005 data from the Bureau of Justice Statistics comes from a time when cybercrime was considered to be less of a problem and the digital economy was smaller.

If the Bureau of Justice Statistics data is representative, that is, if the average losses of the respondents' companies equals the actual average U.S. losses per company, then the losses approach the high estimate of $36.3 billion for manufacturing and $770 billion for all industries.

This would make total cybercrime losses greater than the GDP of many U.S. industries, including construction, mining and agriculture. If the losses per company have increased faster than inflation, which is likely, then the losses would be even higher.



To read more:
https://www.nist.gov/blogs/taking-measure/cybercrime-its-worse-we-thought

Number 9

Understanding fake news: A bibliographic perspective.
Andrew Park, Matteo Montecchi, Cai 'Mitsu' Feng, Kirk Plangger, and Leyland Pitt

False information that appears similar to trustworthy media content, or what is commonly referred to as 'fake news', is pervasive in both traditional and digital strategic communication channels.

This paper presents a comprehensive bibliographic analysis of published academic articles related to fake news and the related concepts of 'truthiness', 'post-factuality', and 'deepfakes'.

Using the Web of Science database and VOSViewer software, papers published on these topics were extracted and analysed to identify and visualise key trends, influential authors, and journals focusing on these topics.

Articles in our dataset tend to cite authors, papers, and journals that are also within the dataset, suggesting that the conversation surrounding fake news is still relatively centralised.

Based on our findings, this paper develops a conceptual fake-news framework—derived from variations of the intention to deceive and/or harm—classifying fake news into four subtypes: mis-information, dis-information, mal-information, and non-information.

We conclude that most existing studies of fake news investigate mis-information and dis-information, thus we suggest further study of mal-information and noninformation.

This paper helps scholars, practitioners, and global policy makers who wish to understand the current state of the academic conversation related to fake news, and to determine important areas for further research.

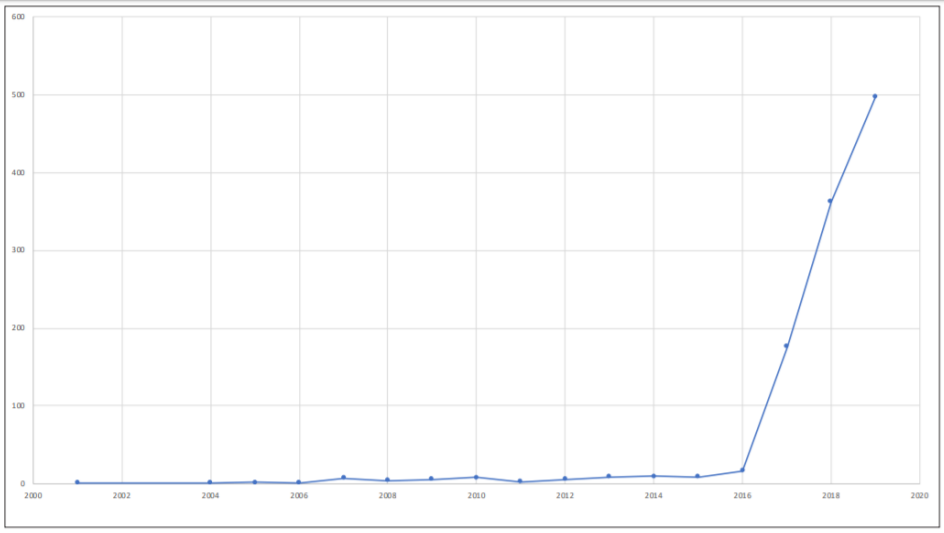


Figure 1. Number of documents feature search terms related only to fake news published – 2001 to October 2019

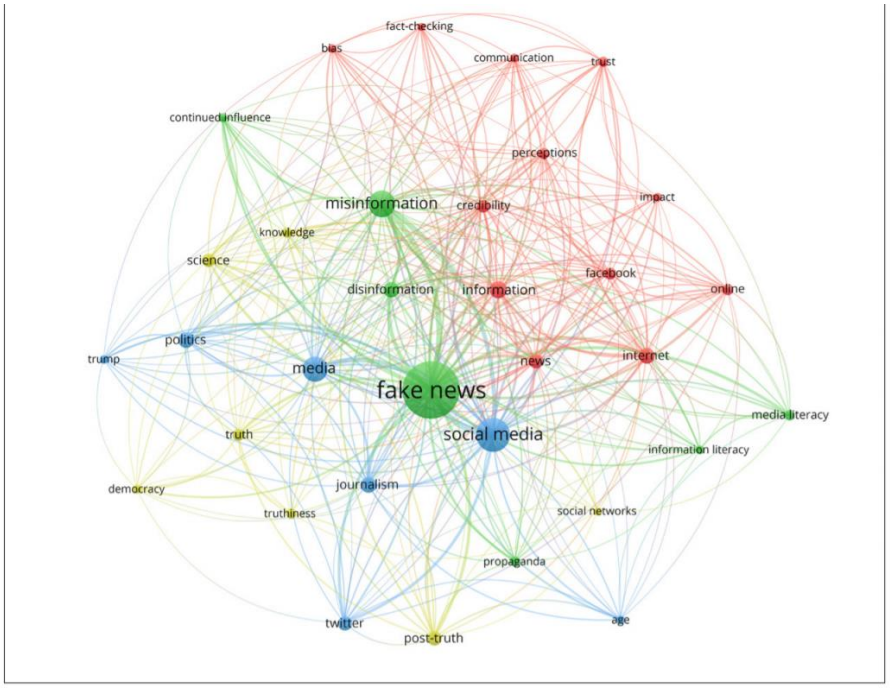


Figure 4. Map of co-occurrence of keywords (Created by VOSviewer)

You can read more at page 142/217, *Academic journal "Defence Strategic Communications" Vol 8:* https://www.stratcomcoe.org/academic-journal-defence-strategic-communications-vol-8-0

Number 10

Disrupting the flow of terrorist funding is critical to curtailing their activities.

Any crime which results in a profit can be used to finance terrorism. This means that a country may face terrorism finance risks even if the risk of a terrorist attack is low.

Sources of terrorist funding include, but are not limited to, low-level fraud, kidnapping for ransom, the misuse of non-profit organizations, the illicit trade in commodities (such as oil, charcoal, diamonds, gold and the narcotic "captagon"), and digital currencies.

By disrupting the flow of terrorist funding and by understanding the funding of previous attacks, we can help prevent attacks in the future.

Strategic cooperation

We maintain relationships with a number of bodies to help drive high-level policies and cooperation to counter terrorist financing:

- the Financial Action Taskforce (FATF), an intergovernmental body that develops international standards to combat money laundering and the financing of terrorism;

- FATF-style regional bodies, who disseminate best practices in their respective region;

- The Egmont Group, a network of 159 financial intelligence units from around the world.

Investigative support

On a hands-on level, we seek to encourage better cooperation between financial intelligence units (FIUs) and police in our member countries, to encourage the sharing of intelligence and analysis.

A key part of this is promoting the extension of I-24/7, our secure global police communications system, to FIUs across the world. In addition, we

are championing the systematic inclusion of financial information in INTERPOL alerts related to terrorist subjects of interest.

We also advise our member countries on specific cases, connecting investigators across borders and continents, ensuring that all INTERPOL's capabilities are used when appropriate.

Case study

The example below shows how our global network of countries, alerts and specialized support can lead to fast and concrete results in investigations.

One of our member countries in Europe requested assistance with a live terrorist financing investigation in which the suspect had financed the travel of family members and others to conflict zones by transferring funds valued circa EUR 18,000.

Our specialized officers offered advice in order to streamline the investigation and liaised with four other member countries from Africa, Americas and the Middle East where funds had been transferred.

At the request of the investigating country, INTERPOL published a Red Notice for the suspect who was subsequently arrested in another, previously unconnected, member country and extradited for prosecution.

To learn more:
https://www.interpol.int/Crimes/Terrorism/Tracing-terrorist-finances

http://www.fatf-gafi.org/

https://egmontgroup.org/

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.

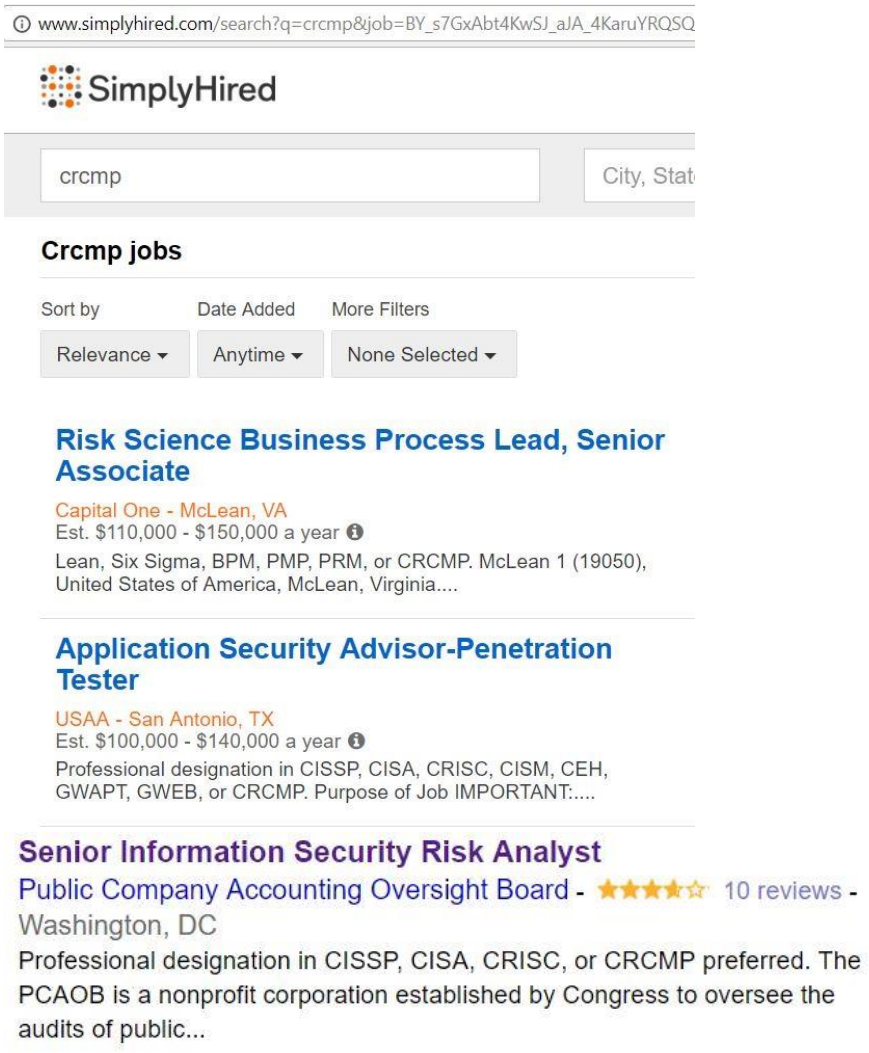
International Association of Risk and Compliance Professionals

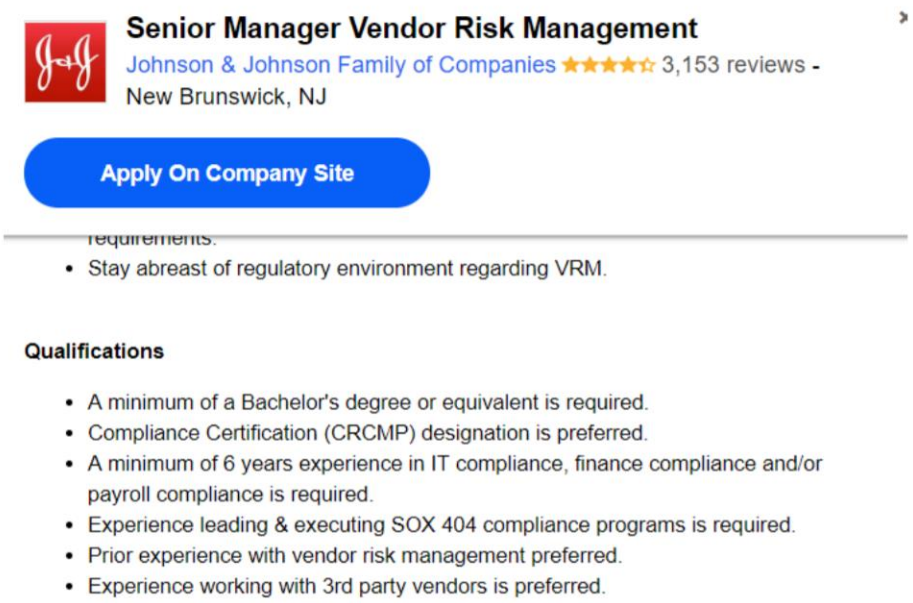
You can explore what we offer to our members:

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