International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750 Web: www.risk-compliance-association.com

Monday, February 8, 2021

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

Dear members and friends,

Voltaire believed that we must judge a man by his questions rather than his answers. *Johann Wolfgang von Goethe* has said that ignorant men raise questions that wise men answered a thousand years ago. But today we very much appreciate some answers to very important questions regarding suspicious activity reports (SARs) and anti-money laundering (AML) considerations.

The Financial Crimes Enforcement Network (FinCEN), jointly with the Federal Reserve, the FDIC, the NCUA and the OCC, are issuing answers to frequently asked questions.

Is a financial institution required to file a SAR based solely on negative news?
No. The existence of negative news related to a customer or other activity at a financial institution does not by itself indicate that the criteria requiring

the filing of a SAR have been met and does not automatically require the filing of a SAR by a financial institution.

A financial institution may review media reports, news articles and/or other references to assist in its performance of customer due diligence, as well as its evaluation of any transactions or activity it considers unusual or potentially suspicious.

For example, negative news may cause a financial institution to review customer activity as well as other related information, such as that of third parties with transactions involving the customer's account.

As with other identified unusual or potentially suspicious activity, financial institutions should comply with applicable regulatory requirements and follow their established policies, procedures, and processes to determine the extent to which it investigates and evaluates negative news, in conjunction with its review of transactions occurring by, at, or through the institution, to determine if a SAR filing is required.

It is good to know. According to *Francis Bacon,* who questions much, shall learn much, and retain much. But sometimes we ask many questions, but we receive no official answers. Not this time.

You can read more at number 4 below. Welcome to the top 10 list.

Best regards,

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

Number 1 (Page 6)

BIS Working Papers No 922

Does regulation only bite the less profitable? Evidence from the too-big-to-fail reforms

Tirupam Goel, Ulf Lewrick and Aakriti Mathur, Monetary and Economic Department, January 2021

Number 2 (Page 9)

The Federal Reserve's New Framework: Context and Consequences

Remarks by Richard H. Clarida, Vice Chair, Board of Governors of the Federal Reserve System, at "The Road Ahead for Central Banks," a seminar sponsored by the Hoover Economic Policy Working Group, Hoover Institution, Stanford University, Stanford, California

Number 3 (Page 11)

Press conference

Christine Lagarde, President of the ECB, Luis de Guindos, Vice-President of the ECB, Frankfurt am Main, 21 January 2021

Number 4 (Page 15)

Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency

BOARD OF GOVERNORS
OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, D.C. 20551

Number 5 (Page 17)

2020 CONSUMER TRENDS REPORT

eiopa
European Insurance and Occupational Pensions Authority

Number 6 (Page 21)

Cybersecurity to the Rescue: Pseudonymisation for Personal Data Protection

ENISA's new report explores pseudonymisation techniques and use cases for healthcare and information sharing in cybersecurity

enisa
European Network and Information Security Agency

Number 7 (Page 25)

Statistical release: BIS international banking statistics

BIS

Number 8 (Page 27)

WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION

EUROPOL

Number 9 (Page 31)

Recommended Options for Improving the Built Environment for Post-Earthquake Reoccupancy and Functional Recovery Time

FEMA nehrp NIST National Institute of Standards and Technology

Number 10 (Page 34)

DARPA Project Drives Simulation Technology for Off-Road Unmanned Vehicles

RACER-Sim to focus on new computer models to advance autonomy capabilities

Number 1

BIS Working Papers No 922

Does regulation only bite the less profitable? Evidence from the too-big-to-fail reforms

Tirupam Goel, Ulf Lewrick and Aakriti Mathur, Monetary and Economic Department, January 2021

BIS

Regulatory reforms following the financial crisis of 2007–08 created incentives for large global banks to lower their systemic importance.

We establish that differences in profitability shape banks' response to these reforms. Indeed, profitability is key because it underpins banks' ability to generate capital and drives the opportunity cost of shrinking.

Our analysis shows that only the less profitable banks lowered their systemic footprint relative to their equally unprofitable peers that were unaffected by the regulatory treatment.

The more profitable banks, by contrast, continued to raise their systemic importance in sync with their untreated peers.

Introduction

Banking regulation builds on the premise that capital requirements can make banks internalise the negative externalities they impose on the financial system.

The case for regulation is particularly strong for large global banks. As the financial crisis of 2007–08 highlighted, the size, complexity and interconnectedness of these banks implies that their failure risks undermining financial stability.

The crisis experience has sparked a stream of research on too-big-to-fail concerns in banking, giving rise to new measures of systemic risks and deepening our understanding of their origin (e.g., Acharya et al. (2012), Adrian and Brunnermeier (2016), Brownlees and Engle (2016), Acharya et al. (2017)).

However, much less is known about the effectiveness of policy reforms to mitigate such risks. A case in point is the framework for global systemically important banks (G-SIBs), which is one element of the broader post-crisis

agenda to address too-big-to-fail concerns. By applying higher capital surcharges to banks that are more systemically important, the G-SIB framework intends to bolster their resilience.

At the same time, it creates incentives for these banks to lower their systemic footprint in order to benefit from capital relief.

In this paper, we assess whether the introduction of the framework – the regulatory treatment – has led G-SIBs to reduce their systemic importance. Our focus is on exploring the framework's differential impact on banks given that the strength of regulatory incentives can vary.

Incentives to lower their systemic importance are likely to be particularly strong for banks that face high costs of raising capital. Yet banks that stand to sacrifice a lot of revenue by downsizing may have few incentives to reduce their systemic footprint.

Our main finding is that profitability plays a determining – but typically overlooked – role in shaping banks' response to the framework. The framework caused the less profitable G-SIBs, measured in terms of their pre-treatment return on assets (ROA), to cut back their systemic importance relative to the less profitable Non G-SIBs (the untreated peers).

The contraction was even stronger for those G-SIBs that were close to the regulatory thresholds that determine their capital surcharges. By contrast, the more profitable G-SIBs have continued to raise their systemic footprint in sync with the more profitable Non G-SIBs.

The wedge in the footprint of the more and less profitable G-SIBs has thus widened substantially post treatment. Nevertheless, the concentration of systemic importance within our global sample of banks has declined somewhat during the period of observation.

The contraction by the less profitable G-SIBs has thus more than compensated for the increase in systemic importance of the more profitable banks.

Moreover, we assess jointly the changes in banks' systemic importance and their market-implied default risks to approximate the evolution of the banks' systemic risk contribution.

This assessment points to a significant decline in the less profitable G-SIBs' systemic risk contribution, and a small but insignificant increase in case of the more profitable G-SIBs.

Our findings are based on a difference-in-differences (DD) specification, which allows us to benchmark G-SIBs' responses to the framework against those of Non G-SIBs.

The DD approach lays the ground for our main analysis based on a triple interaction of G-SIB designation, profitability, and the regulatory treatment.

Throughout our analysis, we control for fixed and time-varying bank characteristics, as well as for differences in the economic or regulatory developments across jurisdictions over time.

To read more: https://www.bis.org/publ/work922.pdf

Number 2

The Federal Reserve's New Framework: Context and Consequences

Remarks by Richard H. Clarida, Vice Chair, Board of Governors of the Federal Reserve System, at "The Road Ahead for Central Banks," a seminar sponsored by the Hoover Economic Policy Working Group, Hoover Institution, Stanford University, Stanford, California

On August 27, 2020, the Federal Open Market Committee (FOMC) unanimously approved a revised Statement on Longer-Run Goals and Monetary Policy Strategy, which represents a robust evolution of its monetary policy framework.

At its September and December FOMC meetings, the Committee made material changes to its forward guidance to bring it into line with the new policy framework.

Before I discuss the new framework in detail and the policy implications that flow from it, please allow me to provide some background on the reasons the Committee felt that our framework needed to evolve.

Motivation for the Review

As my FOMC colleagues and I indicated from the outset, the fact that the Federal Reserve System chose to conduct this review does not indicate that we believed we were poorly served by the framework in place since 2012.

Indeed, I would argue that over the past eight years, the framework served us well and supported the Federal Reserve's efforts after the Global Financial Crisis (GFC) first to achieve and then, for several years, to sustain—until cut short this spring by the COVID-19 pandemic—the operation of the economy at or close to both our statutorily assigned goals of maximum employment and price stability in what became the longest economic expansion in U.S. history.

Nonetheless, both the U.S. economy—and, equally importantly, our understanding of the economy—have clearly evolved along several crucial

dimensions since 2012, and we believed that in 2019 it made sense to step back and assess whether, and in what possible ways, we might refine and rethink our strategy, tools, and communication practices to achieve and sustain our goals as consistently and robustly as possible in the global economy in which we operate today and for the foreseeable future.

To read more: https://www.bis.org/review/r210114a.pdf

Number 3

Press conference

Christine Lagarde, President of the ECB, Luis de Guindos, Vice-President of the ECB, Frankfurt am Main, 21 January 2021

EUROPEAN CENTRAL BANK
EUROSYSTEM

Ladies and gentlemen, the Vice-President and I are very pleased to welcome you to our press conference. We will now report on the outcome of today's meeting of the Governing Council, which was also attended by the Commission Executive Vice-President, Mr Dombrovskis.

The start of vaccination campaigns across the euro area is an important milestone in the resolution of the ongoing health crisis. Nonetheless, the pandemic continues to pose serious risks to public health and to the euro area and global economies.

The renewed surge in coronavirus (COVID-19) infections and the restrictive and prolonged containment measures imposed in many euro area countries are disrupting economic activity.

Activity in the manufacturing sector continues to hold up well, but services sector activity is being severely curbed, albeit to a lesser degree than during the first wave of the pandemic in early 2020.

Output is likely to have contracted in the fourth quarter of 2020 and the intensification of the pandemic poses some downside risks to the short-term economic outlook.

Inflation remains very low in the context of weak demand and significant slack in labour and product markets. Overall, the incoming data confirm our previous baseline assessment of a pronounced near-term impact of the pandemic on the economy and a protracted weakness in inflation.

In this environment ample monetary stimulus remains essential to preserve favourable financing conditions over the pandemic period for all sectors of the economy.

By helping to reduce uncertainty and bolster confidence, this will encourage consumer spending and business investment, underpinning economic activity and safeguarding medium-term price stability. Meanwhile, uncertainty remains high, including relating to the dynamics of the pandemic and the speed of vaccination campaigns.

We will also continue to monitor developments in the exchange rate with regard to their possible implications for the medium-term inflation outlook. We continue to stand ready to adjust all of our instruments, as appropriate, to ensure that inflation moves towards our aim in a sustained manner, in line with our commitment to symmetry.

Against this background, we decided to reconfirm our very accommodative monetary policy stance.

First, the Governing Council decided to keep the key ECB interest rates unchanged. We expect them to remain at their present or lower levels until we have seen the inflation outlook robustly converge to a level sufficiently close to, but below, 2 per cent within our projection horizon, and such convergence has been consistently reflected in underlying inflation dynamics.

Second, we will continue our purchases under the pandemic emergency purchase programme (PEPP) with a total envelope of €1,850 billion. We will conduct net asset purchases under the PEPP until at least the end of March 2022 and, in any case, until the Governing Council judges that the coronavirus crisis phase is over.

The purchases under the PEPP will be conducted to preserve favourable financing conditions over the pandemic period. We will purchase flexibly according to market conditions and with a view to preventing atightening of financing conditions that is inconsistent with countering the downward impact of the pandemic on the projected path of inflation.

In addition, the flexibility of purchases over time, across asset classesand among jurisdictions will continue to support the smooth transmission of monetary policy.

If favourable financing conditions can be maintained with asset purchase flows that do not exhaust the envelope over the net purchase horizon of the PEPP, the envelope need not be used in full.

Equally, the envelope can be recalibrated if required to maintain favourable financing conditions to help counter the negative pandemic shock to the path of inflation.

We will continue to reinvest the principal payments from maturing securities purchased under the PEPP until at least the end of 2023.

In any case, the future roll-off of the PEPP portfolio will be managed to avoid interference with the appropriate monetary policy stance.

Third, net purchases under our asset purchase programme (APP) will continue at a monthly pace of €20billion. We continue to expect monthly net asset purchases under the APP to run for as long as necessary to reinforce the accommodative impact of our policy rates, and to end shortly before we start raising thekey ECB interest rates.

We also intend to continue reinvesting, in full, the principal payments from maturing securities purchased under the APP for an extended period of time past the date when we start raising the key ECB interest rates, and in any case for as long as necessary to maintain favourable liquidity conditions and an ample degree of monetary accommodation.

Finally, we will continue to provide ample liquidity through our refinancing operations. In particular, our third series of targeted longer-term refinancing operations (TLTRO III) remains an attractive source of funding for banks, supporting bank lending to firms and households.

Let me now explain our assessment in greater detail, starting with the economic analysis. Following a sharp contraction in the first half of 2020, euro area real GDP rebounded strongly and rose by 12.4 percent, quarter on quarter, in the third quarter, although remaining well below pre-pandemic levels.

Incoming economic data, surveys and high-frequency indicators suggest that the resurgence of the pandemic and the associated intensification of containment measures have likely led to a decline in activity in the fourth quarter of 2020 and are also expected to weigh on activity in the first quarter of this year.

In sum, this is broadly in line with the latest baseline of the December 2020 macroeconomic projections.

Economic developments continue to be uneven across sectors, with the services sector being more adversely affected by the new restrictions on social interaction and mobility than the industrial sector.

Although fiscal policy measures are continuing to support households and firms, consumers remain cautious in the light of the pandemic and its impact on employment and earnings. Moreover, weaker corporate balance sheets and uncertainty about the economic outlook are still weighing on business investment.

Looking ahead, the roll-out of vaccines, which started in late December, allows for greater confidence in the resolution of the health crisis. However, it will take time until widespread immunity is achieved, and further adverse

developments related to the pandemic cannot be ruled out. Over the medium term, the recovery of the euro area economy should be supported by favourable financing conditions, an expansionary fiscal stance and a recovery in demand as containment measures are lifted and uncertainty recedes.

Overall, the risks surrounding the euro area growth outlook remain tilted to the downside but less pronounced. The news about the prospects for the global economy, the agreement on future EU-UK relations and the start of vaccination campaigns is encouraging, but the ongoing pandemic and its implications for economic and financial conditions continue to be sources of downside risk.

To read more:
https://www.ecb.europa.eu/press/pressconf/2021/html/ecb.is210121~e601112a72.en.html

Number 4

Answers to Frequently Asked Questions Regarding Suspicious Activity Reporting and Other Anti-Money Laundering Considerations

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency

BOARD OF GOVERNORS
OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, D.C. 20551

The Financial Crimes Enforcement Network (FinCEN), jointly with the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC) (collectively, the Federal banking agencies), and in consultation with the staff of certain other federal functional regulators, is issuing answers to frequently asked questions (FAQs) regarding suspicious activity reports (SARs) and other anti-money laundering (AML) considerations for financial institutions covered by SAR rules.

The answers to these FAQs clarify the regulatory requirements related to SARs to assist such financial institutions with their compliance obligations, while enabling financial institutions to focus resources on activities that produce the greatest value to law enforcement agencies and other government users of Bank Secrecy Act (BSA) reporting.

The answers to these FAQs neither alter existing BSA/AML legal or regulatory requirements, nor establish new supervisory expectations; they were developed in response to recent Bank Secrecy Act Advisory Group (BSAAG) recommendations, as described in more detail in FinCEN's Advance Notice of Proposed Rulemaking (ANPRM) on Anti-Money Laundering Program Effectiveness, published in September 2020.

Question 1: Requests by Law Enforcement for Financial Institutions to Maintain Accounts

Can a financial institution maintain an account or customer relationship for which it has received a written "keep open" request from law enforcement, even though the financial institution has identified suspicious or potentially illicit activity?

Yes. Law enforcement may have an interest in ensuring that certain accounts and customer relationships remain open notwithstanding

suspicious or potential criminal activity in connection with the account. A financial institution may decide to maintain an account based on a written "keep open" request from a law enforcement agency, however, it is not obligated to do so.

The written request should be specific and indicate both that the law enforcement agency has requested that the financial institution maintain the account, as well as the purpose and duration of the request.

Keeping such an account open as requested may be highly useful to law enforcement and may further efforts to identify and combat money laundering, terrorist financing, and other illicit financial activities.

A financial institution should not be criticized solely for its decision to maintain an account relationship at the request of law enforcement or for its decision to close the account. Ultimately, the decision to maintain or close an account should be made by a financial institution in accordance with its own policies, procedures, and processes.

It may be useful for financial institutions to maintain documentation of "keep open" requests, including after a request has expired.

If financial institutions keep such an account open as requested by law enforcement, they are still required to comply with all applicable BSA requirements, including requirements to conduct ongoing risk-based monitoring, and as appropriate, file SARs, including continuing activity SARs consistent with FinCEN guidance.

To read more:
https://www.federalreserve.gov/supervisionreg/srletters/SR2102a1.pdf

Number 5

2020 CONSUMER TRENDS REPORT

Given the impact of COVID-19 on the economy and on the insurance and occupational pension sectors, this year's report focuses on the pandemic, to provide an initial and preliminary overview on the impact on the sectors, responses and the challenges which emerged. This includes taking stock as to how EIOPA's measures have been implemented and their impact.

The report only focuses on observations from Q1 and Q2 2020; hence, overall conclusions on the COVID-19 crisis cannot be drawn.

Because of the extrinsic nature of the current crisis, this year's evolutions in consumer behaviours are mostly dictated by external factors which include:

› Forced changes in consumers' habits impacting consumers' insurance needs;

› A deterioration of consumers' disposable income and changes in employers' cashflows; and

› Market shocks and the continued and prolonged low-interest rate environment.

Despite initial concerns, insurers, insurance intermediaries and pension funds have worked hard to guarantee business continuity.

When operational disruptions emerged, they have been isolated and not material.

Evidence from consumer interviews also confirms that business continuity has been ensured rendering the process of buying products, submitting claims and complaints or asking information as 'normal' as possible.

The sudden shift towards digital channels has crystallised some benefits of financial innovation / digitalisation both for insurers and intermediaries as well as for consumers.

However, in particular for more vulnerable and less digitally savvy consumers, intermediaries have also played a key role, being a first point of contact for consumers to seek guidance on their insurance coverage.

Given the increased digitalisation, risks relating to increased fraud both against insurance undertakings, pension funds and against consumers, members and beneficiaries have also emerged.

Looking at growth trends, at the end of Q2 2020 a majority of Member States in the EEA reported a decrease in life insurance GWP:

› The decrease has been led by a -24.2% drop in insurance with profit participation;

› Unit-linked insurance slightly grew, remaining the largest single line of business;

› Considering the heterogeneous nature of the other-life insurance line of business, trends have been dictated by different factors with mortgage life insurance decreasing in several Member States, while term life insurance reported an increase.

Amidst the crisis concerns with regard to unit-linked contracts continued to persist:

› The sharp fall in asset prices observed in March, which was accompanied by redemptions from some investment funds and a deterioration in financial market liquidity, raised some initial concerns.

› Moreover, as consumers may start to surrender their policies early, existing structural problems such as a mismatch between actual and expected returns because of the features (e.g., high risk, complex fee structure) of some unit-linked products may surface. Expected lower returns and market volatility can also further exacerbate existing problems, heightening the impact that high costs can have.

Looking at non-life insurance, the sector grew by 3.3% in the first half of 2020. Growth trends were more heterogeneous and diverse across Europe.

Amidst the crisis accident and health insurance products appear to have continued to offer valuable cover to consumers, reporting the second highest claims ratios and with no major decreases / increases in total claims incurred.

In several Member States, COVID-19 related treatments were covered and/or several initiatives, including good-will payments, have been put in place to ensure that accident and health insurance products continue to offer value to consumers.

Accident and health insurance is the product for which most good-will actions have also been reported.

The fire and other damage to property line of business increased in 26 Member States — in 4 of them by more than 15%.

Given changes in working habits and travel restrictions, at the on-set of the crisis, concerns arose with consumers possibly breaching contractual obligations and loosing coverage. However, insurers showing forbearance towards consumers have been observed, albeit not in a consistent manner.

Trends in income protection insurance have varied significantly across Member States.

The unknown nature of COVID-19, in particular in relation to its long-term implications, may also lead to some changes in product design (e.g., insurers introducing exclusions or putting in place screening procedures to avoid 'silent risks').

The miscellaneous financial loss is the line of business which experienced the highest increase in claims ratios, more than doubling in several Member States.

This could be due to the fact that travel cancellation claims are covered under this line of business.

It could also relate to the fact that some business interruption claims may also fall under this line of business and insurers may have provisioned for expected future claims.

Concerns with regard to travel insurance products also exist. EIOPA in the past highlighted the utility of these products whilst raising concerns on the value some products bring to consumers and on some problematic business models.

The COVID-19 crisis surfaced concerns both in relation to inconsistent consumer outcomes with regard to travel insurance products and in relation to problematic business models.

Exclusions and lack of clarity in terms and conditions have raised particular challenges.

On one hand, exclusions relate to the fact that pandemics raise specific difficulties from an insurance perspective; on the other hand, increasing

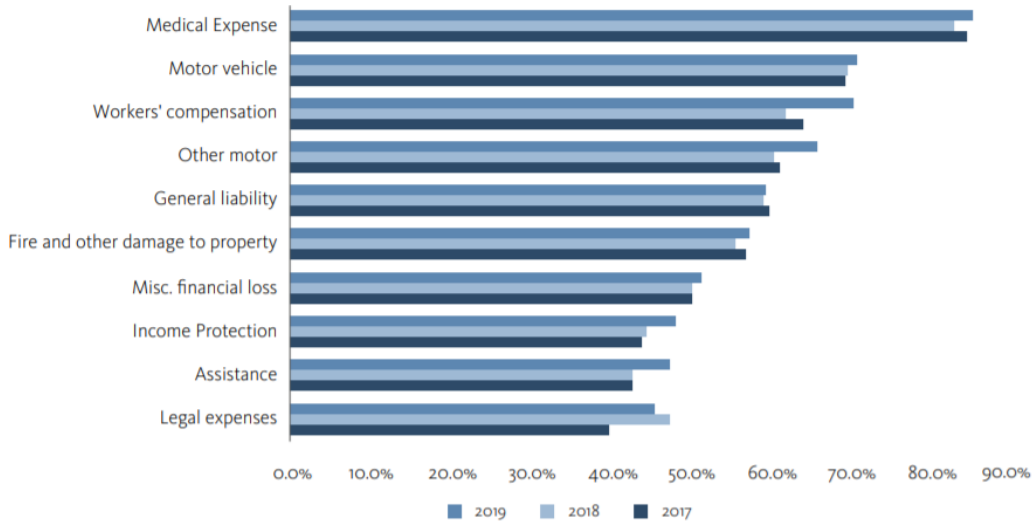
pressure has been put on the sector to pay out claims even though the risk may have not been originally foreseen.

To this extent at the on-set of the crisis EIOPA clearly outlined the risks of imposing retroactive coverage.

EIOPA also highlighted measures to be taken to limit possible consumer detriment, though it is not clear that these have been consistently adopted, raising concerns as to whether consumer detriment has thereby materialized.

To read more:
https://www.eiopa.europa.eu/content/consumer-trends-report-2020_en

Figure 52 — Claims ratio for selected non-life insurance lines of business — 2017-2019



Source: EIOPA Solvency II database.

Number 6

Cybersecurity to the Rescue: Pseudonymisation for Personal Data Protection

ENISA's new report explores pseudonymisation techniques and use cases for healthcare and information sharing in cybersecurity

Pseudonymisation is an established and accepted data protection measure that has gained additional attention following the adoption of the General Data Protection Regulation (GDPR) where it is both specifically defined and many times referenced as a safeguard.

ENISA, in its prior work on this field, has explored the notion and scope of data pseudonymisation, while presenting some basic technical methods and examples to achieve pseudonymisation in practice.

In this new report, ENISA complements its past work by discussing advanced pseudonymisation techniques, as well as specific use cases from the specific sectors of healthcare and cybersecurity.

In particular, the report, building on the basic pseudonymisation techniques, examines advanced solutions for more complex scenarios that can be based on asymmetric encryption, ring signatures and group pseudonyms, chaining mode, pseudonyms based on multiple identifiers, pseudonyms with proof of knowledge and secure multi-party computation.

It then applies some of these techniques in the area of healthcare to discuss possible pseudonymisation options in different example cases, while also exploring the possible application of the data custodianship model.

Lastly, it examines the application of basic pseudonymisation techniques in common cybersecurity use cases, such as the use of telemetry and reputation systems.

Based on the analysis provided in the report, the following basic conclusions and recommendations for all relevant stakeholders are provided.

Defining the best possible technique

As it has been stressed also in past ENISA's reports, there is no fit-for-all pseudonymisation technique and a detailed analysis of the case in question

is necessary in order to define the best possible option. To do so, it is essential to take a critical to look into the semantics (the "full picture") before conducting data pseudonymisation.

In addition, pseudonymisation is only one possible technique and must be combined with a thorough security risk assessment for the protection of personal data.

Data controllers and processors should engage in data pseudonymisation, based on a security and data protection risk assessment and taking due account of the overall context and characteristics of personal data processing.

This may also comprise methods for data subjects to pseudonymise personal data on their side (e.g. before delivering data to the controller/processor) to increase control of their own personal data.

Regulators (e.g. Data Protection Authorities and the European Data Protection Board) should promote risk-based data pseudonymisation through the provision of relevant guidance and examples.

Advanced techniques for advanced scenarios

While the technical solution is a critical element for achieving proper pseudonymisation, one must not forget that the organisational model and its underlying structural architecture are also very important parameters of success.

Advanced techniques go together with advanced scenarios, such as the case of the data custodianship model.

Data controllers and processors should consider possible scenarios that can support advanced pseudonymisation techniques, based – among other – on the principle of data minimisation.

The research community should support data controllers and processors in identifying the necessary trust elements and guarantees for the advanced scenarios (e.g. data custodianship) to be functional in practice.

Regulators (e.g. Data Protection Authorities and the European Data Protection Board) should ensure that regulatory approaches, e.g. as regards new technologies and application sectors, take into account all possible entities and roles from the standpoint of data protection, while remaining technologically neutral.

Establishing the state-of-the-art

Although a lot of work is already in place, there is certainly more to be done in defining the state-of-the-art in data pseudonymisation.

To this end, research and application scenarios must go hand-in-hand, involving all relevant parties (researchers, industry, and regulators) to discuss joined approaches.

The European Commission, the relevant EU institutions, as well as Regulators (e.g. Data Protection Authorities and the European Data Protection Board) should support the establishment and maintenance of the state-of-the-art in pseudonymisation, bringing together all relevant stakeholders in the field (regulators, research community, and industry).

The research community should continue its efforts on advancing the existing work on data pseudonymisation, addressing special challenges appearing from emerging technologies, such as Artificial Intelligence.

The European Commission and the relevant EU institutions should support and disseminate these efforts.

Towards the broader adoption of data pseudonymisation

Recent developments, e.g. in international personal data transfers, show clearly the need to further advance appropriate safeguards for personal data protection.

This will only be intensified in the future by the use of emerging technologies and the need for open data access.

It is, thus, important to start today the discussion on the broader adoption of pseudonymisation in different application scenarios.

Regulators (e.g. Data Protection Authorities and the European Data Protection Board), the European Commission and the relevant EU institutions should disseminate the benefits of data pseudonymisation and provide for best practices in the field.

To read more:
https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases

enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Number 7

Statistical release: BIS international banking statistics

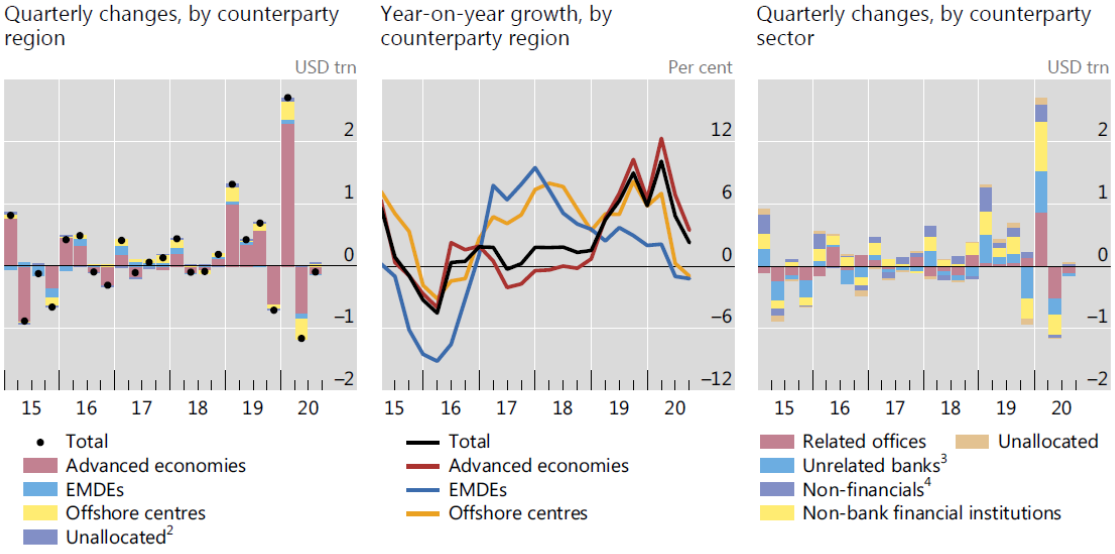
• Global cross-border claims changed little in aggregate in Q3 2020 after large fluctuations in Q1 and Q2.

• Cross-border claims on emerging market and developing economies continued to fall, driven again by claims on Latin America and the Caribbean.

• Since the start of the pandemic, the size of banks' balance sheets has increased sharply with the accumulation of claims on governments and monetary authorities.

• A new interactive chart for visualising bilateral cross-border positions based on the locational banking statistics is now available online.

Global cross-border claims declined modestly in Q3 2020 after large fluctuations[1] Graph 1



[1] Quarterly changes are adjusted for breaks in series and exchange rate fluctuations. The year-on-year growth rates are calculated based on the adjusted changes for the past four quarters. [2] Includes international organisations and unallocated cross-border claims. [3] Includes central banks and banks unallocated by subsector between intragroup and unrelated banks. [4] Includes non-banks unallocated by subsector.

Source: BIS locational banking statistics.

Global cross-border claims barely budged

Banks' cross-border claims registered a modest contraction of $93 billion in the course of Q3 2020 on an FX- and break-adjusted basis (Graph 1, left-hand panel). This quarterly contraction was quite muted (0.3% of

previous quarter stock) compared with the large fluctuations in Q1 and Q2 2020, of +$2.7 trillion and –$1.2 trillion, respectively.

Year-on-year growth rates continued to fall from their recent Q1 2020 peak, when cross-border positions had surged (centre panel).

Claims on both advanced economies (AEs, –$131bn) and emerging market and developing economies (EMDEs, –$13bn) declined. As earlier in the year, these movements were in part driven by intragroup positions (Graph 1, right-hand panel).

The decline in claims on AEs centred on related offices (–$114bn), especially on those in the United States (–$81bn). The unwinding of central bank dollar swap lines, which had swelled intragroup positions in Q1, contributed to this decline.

By contrast, claims on offshore centres expanded by $41bn (left-hand panel), especially vis-à-vis Hong Kong SAR (+$39bn) and the Cayman Islands (+$24bn). More than half of the increase on Hong Kong was in the form of intragroup claims.

Some of the larger movements vis-à-vis AEs involved non-bank financial institutions (NBFIs).

Claims on the United Kingdom (–$50bn), the Netherlands (–$50bn), Luxembourg (–$46bn), France (–$40bn) and Italy (–$39bn) all fell, mostly vis-à-vis NBFIs. These declines were partly offset by increases in claims on Japan (+97bn) and Germany (+65bn), notably on their resident banks and NBFIs.

The modest aggregate decline also conceals large differences on the creditor side. Banks located in China, France and the United Kingdom saw the greatest increases in cross-border claims while those in Spain , Germany and the United States reported outsize declines.

To read more: https://www.bis.org/statistics/rppb2101.pdf

Number 8

WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION

Law enforcement and judicial authorities worldwide have this week disrupted one of most significant botnets of the past decade: EMOTET. Investigators have now taken control of its infrastructure in an international coordinated action.

This operation is the result of a collaborative effort between authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine, with international activity coordinated by Europol and Eurojust. This operation was carried out in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT).

EMOTET has been one of the most professional and long lasting cybercrime services out there. First discovered as a banking Trojan in 2014, the malware evolved into the go-to solution for cybercriminals over the years.

The EMOTET infrastructure essentially acted as a primary door opener for computer systems on a global scale. Once this 27nauthorized access was established, these were sold to other top-level criminal groups to deploy further illicit activities such data theft and extortion through ransomware.

Spread via Word documents

The EMOTET group managed to take email as an attack vector to a next level. Through a fully automated process, EMOTET malware was delivered to the victims' computers via infected e-mail attachments.

A variety of different lures were used to trick unsuspecting users into opening these malicious attachments. In the past, EMOTET email campaigns have also been presented as invoices, shipping notices and information about COVID-19.

All these emails contained malicious Word documents, either attached to the email itself or downloadable by clicking on a link within the email itself. Once a user opened one of these documents, they could be prompted to "enable macros" so that the malicious code hidden in the Word file could run and install EMOTET malware on a victim's computer.

Attacks for hire

EMOTET was much more than just a malware. What made EMOTET so dangerous is that the malware was offered for hire to other cybercriminals to install other types of malware, such as banking Trojans or ransomwares, onto a victim's computer.

This type of attack is called a 'loader' operation, and EMOTET is said to be one of the biggest players in the cybercrime world as other malware operators like TrickBot and Ryuk have benefited from it.

Its unique way of infecting networks by spreading the threat laterally after gaining access to just a few devices in the network made it one of the most resilient malware in the wild.

Disruption of EMOTET's infrastructure

The infrastructure that was used by EMOTET involved several hundreds of servers located across the world, all of these having different functionalities in order to manage the computers of the infected victims, to spread to new ones, to serve other criminal groups, and to ultimately make the network more resilient against takedown attempts.

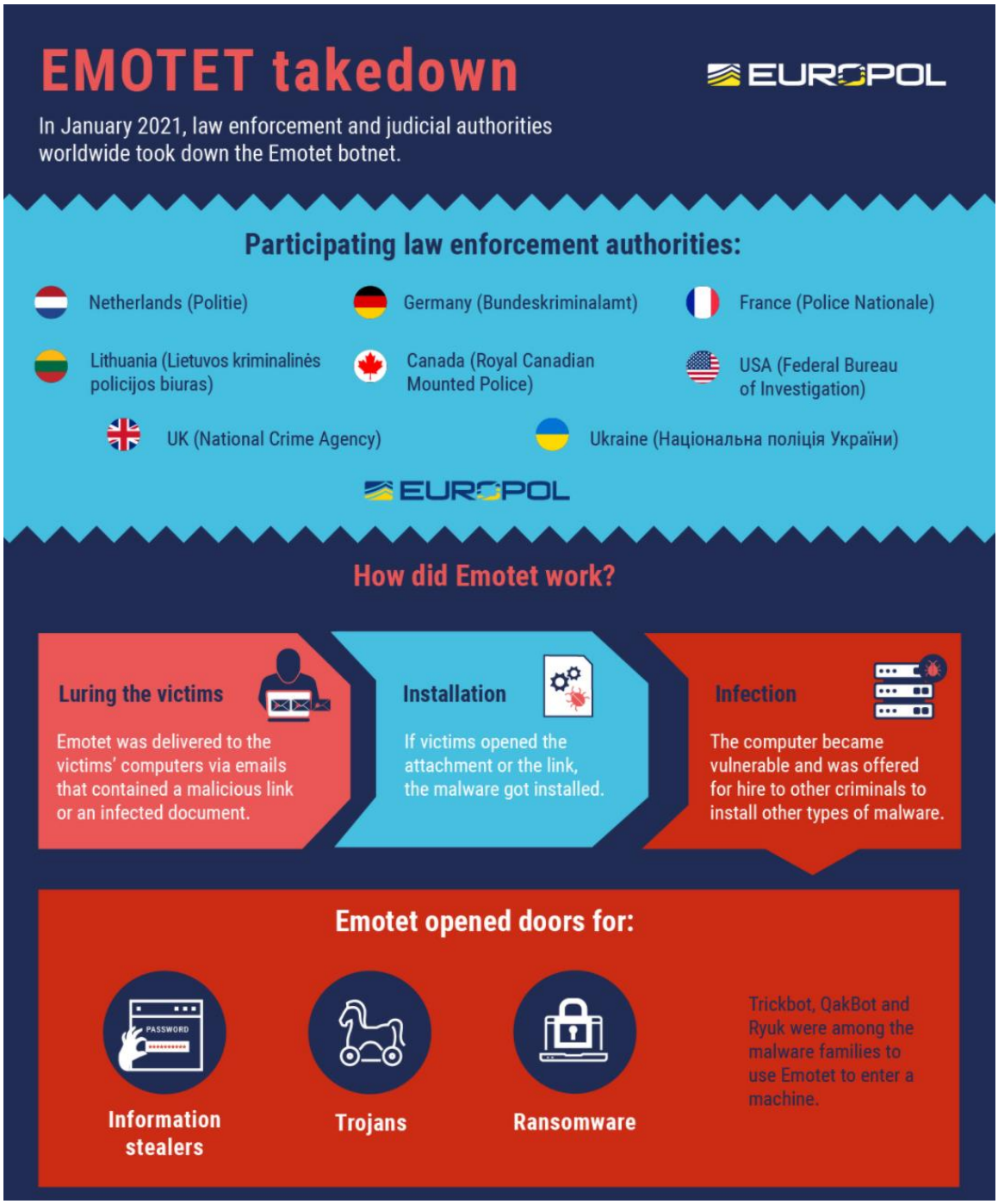
To severely disrupt the EMOTET infrastructure, law enforcement teamed up together to create an effective operational strategy. It resulted in this week's action whereby law enforcement and judicial authorities gained control of the infrastructure and took it down from the inside. The infected machines of victims have been redirected towards this law enforcement-controlled infrastructure. This is a unique and new approach to effectively disrupt the activities of the facilitators of cybercrime.

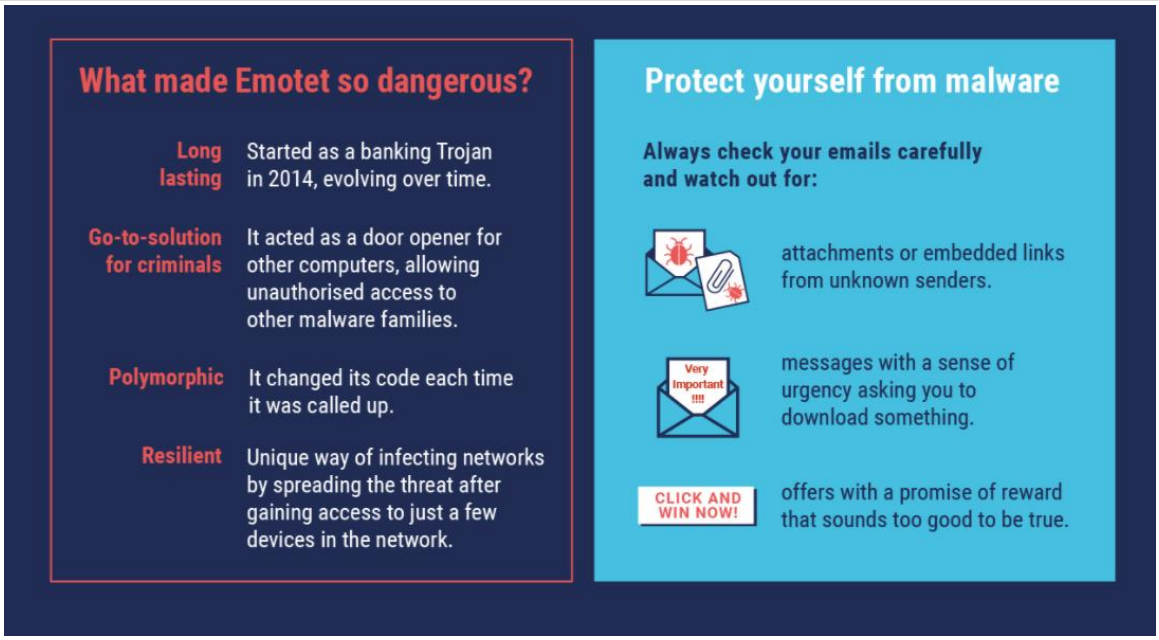
How to protect oneself against loaders

Many botnets like EMOTET are polymorphic in nature. This means that the malware changes its code each time it is called up. Since many antivirus programmes scan the computer for known malware codes, a code change may cause difficulties for its detection, allowing the infection to go initially undetected.

A combination of both updated cybersecurity tools (antivirus and operating systems) and cybersecurity awareness is essential to avoid falling victim to sophisticated botnets like EMOTET. Users should carefully check their email and avoid opening messages and especially attachments from unknown senders. If a message seems too good to be true, it likely is and emails that implore a sense of urgency should be avoided at all costs.

As part of the criminal investigation conducted by the Dutch National Police into EMOTET, a database containing e-mail addresses, usernames and passwords stolen by EMOTET was discovered. You can check if your e-mail address has been compromised. As part of the global remediation strategy, in order to initiate the notification of those affected and the cleaning up of the systems, information was distributed worldwide via the network of so-called Computer Emergency Response Teams (CERTs).




What made Emotet so dangerous?
Long lasting
Started as a banking Trojan in 2014, evolving over time.
Go-to-solution for criminals
It acted as a door opener for other computers, allowing unauthorised access to other malware families.
Polymorphic
It changed its code each time it was called up.
Resilient
Unique way of infecting networks by spreading the threat after gaining access to just a few devices in the network.
Protect yourself from malware
Always check your emails carefully and watch out for:
attachments or embedded links from unknown senders.
Very Important !!!!
messages with a sense of urgency asking you to download something.
CLICK AND WIN NOW!
offers with a promise of reward that sounds too good to be true.

Number 9

Recommended Options for Improving the Built Environment for Post-Earthquake Reoccupancy and Functional Recovery Time

The most recent reauthorization of the National Earthquake Hazards Reduction Program (NEHRP), P.L. 115-307, includes a heightened focus on achieving community resilience and a new requirement for the National Institute of Standards and Technology (NIST) and the Federal Emergency Management Agency (FEMA) to jointly convene a Committee of Experts to assess and recommend options for improving the built environment and critical infrastructure to reflect performance goals stated in terms of post-earthquake reoccupancy and functional recovery time.

To comply with this mandate, NIST and FEMA developed a plan of action in which FEMA funded a Project Technical Panel, responsible for report development, and NIST funded a Project Review Panel, responsible for report review.

The Committee of Experts consisted of the Project Technical Panel, with 17 outside experts and representation from all interest groups named in the reauthorization, and the Project Review Panel, with 10 outside experts and similar representation.

To facilitate national-level stakeholder interaction, NIST hosted five stakeholder workshops that were used to gather additional information and feedback.

This report provides a set of options in the form of recommendations, tasks, and alternatives for improving the built environment, which have been developed and assessed by the Committee of Experts.

It describes community resilience, defines the concepts of reoccupancy and functional recovery, and explains the relationship among these three ideas.

It explains why reoccupancy and functional recovery concepts are needed, describes a target performance state, and identifies potential cost and benefits associated with implementing enhanced seismic design.

To fulfill the Congressional mandate, this report addresses the issue of functional recovery for seismic hazard.

Although this report does not discuss the unique challenges associated with improving functional recovery for other hazards, recommendations in this report could be leveraged and adapted for other natural hazards.

The motivation for this report is the risk that the United States faces each year from all forms of natural hazards, including hurricanes, floods, wildfires, and earthquakes.

Natural hazard events can affect communities through damage that results in injury and loss of life, interruption of lifeline services, displacement of residents and businesses, and economic and socio-cultural impacts.

Almost half of the U.S. population – 150 million people – reside in portions of 42 states that are at risk of experiencing a damaging earthquake within the next 50 years.

Earthquakes have caused disastrous impacts in the past and are expected to cause more in the future.

In regions of high seismic risk where an earthquake hasn't occurred for some time, scenario studies predict deaths in the thousands, injuries in the tens of thousands, and hundreds of billions of dollars in direct economic losses, along with long-term, destabilizing impacts to community function.

In all cases, whether historic or scenario-based, the loss of life and property, and the negative impacts to the economy, were a direct result of the inability of the built environment to withstand the effects of earthquakes and other natural hazards.

Because federal, state, and local, governments have critical functions in disaster recovery, they all can play an important role in facilitating the process to reduce the costs of recovery.

To protect U.S. communities and taxpayers against future losses on the scale of those experienced in Hurricane Katrina, or predicted in earthquake scenario studies, a change in building codes, building practices, and societal values is needed.

To support resilience goals at the community level, there is a need to establish a link between the design, construction, and retrofit of individual buildings and lifeline infrastructure systems, and community resilience, as measured by time to recovery of function; but this link is currently missing.

The concepts of reoccupancy and functional recovery have been introduced to serve as this link, defined as follows:

- Reoccupancy is a post-earthquake performance state in which a building is maintained, or restored, to allow safe re-entry for the purposes of providing shelter or protecting building contents.

- Functional recovery is a post-earthquake performance state in which a building or lifeline infrastructure system is maintained, or restored, to safely and adequately support the basic intended functions associated with the pre-earthquake use or occupancy of a building, or the pre-earthquake service level of a lifeline infrastructure system.

To read more:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1254.pdf

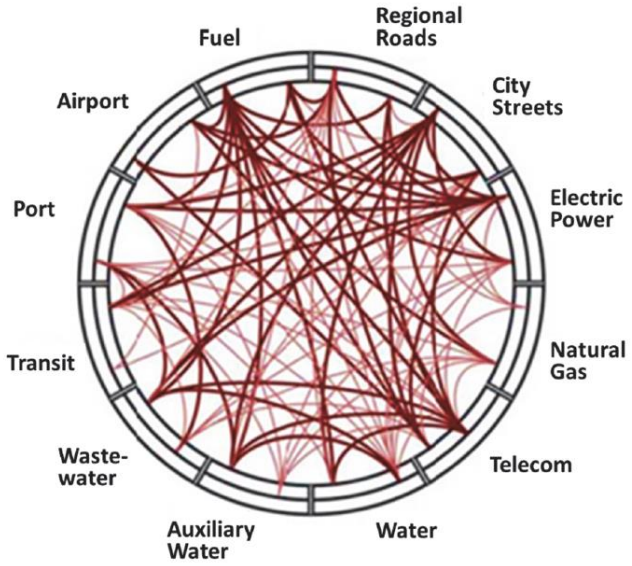


Figure 4-1 Interdependencies of lifeline infrastructure systems in San Francisco (ABAG, 2014); connection points on the outer ring show which systems rely on the designated operator, and connection points on the inner ring show which systems the designated operator relies upon.

Number 10

DARPA Project Drives Simulation Technology for Off-Road Unmanned Vehicles

RACER-Sim to focus on new computer models to advance autonomy capabilities

DARPA's Robotic Autonomy in Complex Environments with Resiliency - Simulation (RACER-Sim) project is seeking innovations in technologies that bridge the gap from simulation to the real world and significantly reduce the cost of off-road autonomy development. DARPA invites proposals for promising solutions that support these goals.

While the past decade has seen increased use of simulation in developing field robotics, the military off-road environment is especially challenging and complex.

Computers need to re-create three-dimensional surfaces, compliant soils and vegetation, and hundreds of obstacle classes.

Software also needs to take into account lower fidelity or limited mapping data, unique platform-surface interactions, continuous motion planning, and no defined road networks or driving rules.

In addition, modeling high speed off-road performance of sensors / modalities, sensor-to-terrain representations, autonomous platforms, and autonomous control remains a software and processing challenge.

"Because these challenges haven't been effectively met, the practical use of current virtual models to advance off-road field robotics capabilities is limited and doesn't yet allow a demonstrable simulation-to-real world capability, said Dr. Stuart Young, RACER program manager. "The large reality gap of current software models and complexities of their use discourage developers and prevent them from leveraging the full benefits of simulation."

Over a four-year timeline, RACER-Sim will investigate technologies that are applicable to the off-road environment in the areas of algorithm development, simulation element technologies, and simulator content generation.

The RACER-Sim Broad Agency Announcement (BAA) has been posted to beta.SAM.gov

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

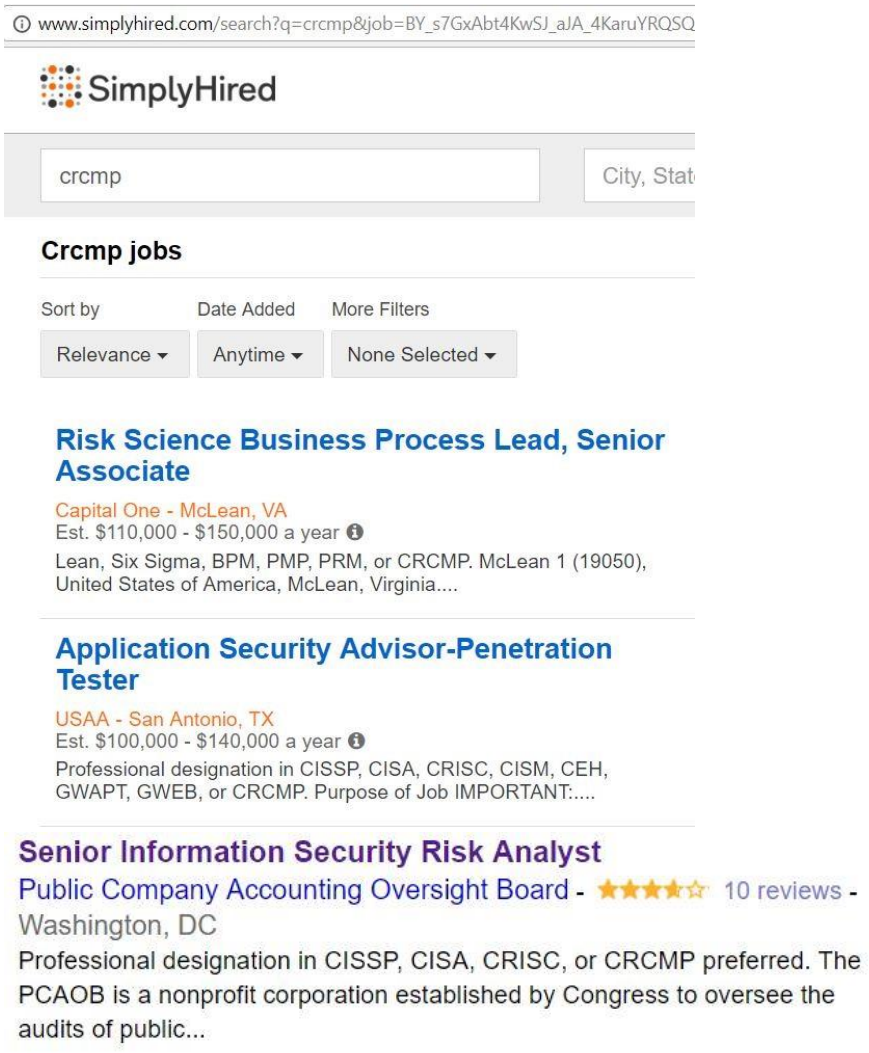
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

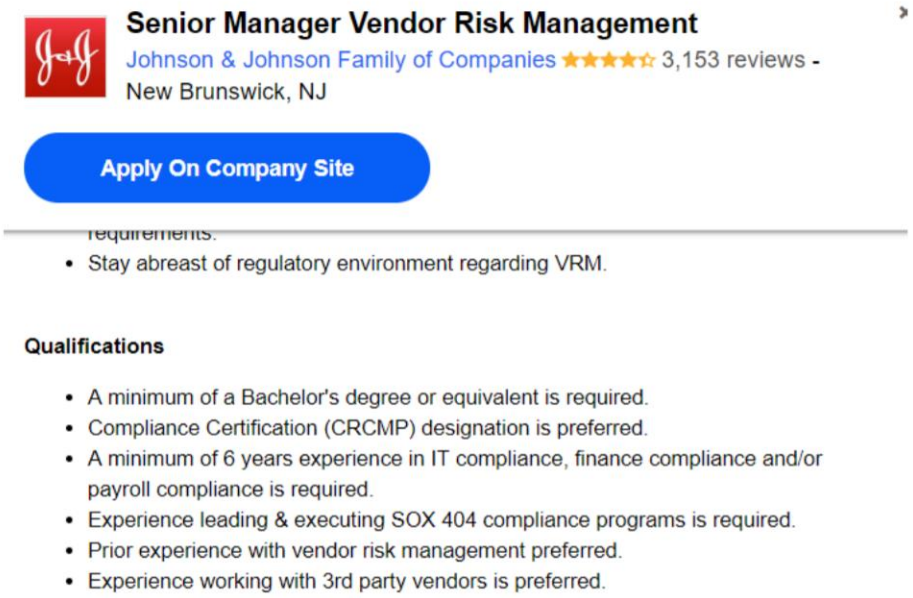
You can explore what we offer to our members:

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

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

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





Senior Manager Vendor Risk Management

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

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

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

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

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

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

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

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

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

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