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, April 12, 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,

Marcus Tullius Cicero has said, *when you have no basis for an argument, abuse the plaintiff*. Well, the online world has made it so much easier.
What can countries do to address or mitigate the problem of online abuse of public servants? Governments must manoeuvre a regulatory gray area in which it is difficult to distinguish between freedom of speech and protection from harmful verbal abuse.

In an interesting new paper, *Abuse of power: Coordinated online harassment of Finish government ministers* from the NATO Strategic Communications Centre of Excellence, we can understand the problem and the possible solutions. We read:
"Lipstick brigade. Lipstick girls. Feminist quintet. Tampax team. These are all phrases used on Twitter to refer to the current coalition in Finland, in which all five party leaders are women, led by Prime Minister Sanna Marin

of the Social Democratic Party.

When the remarkably young and female leadership came into power in December 2019, they made international headlines as pioneers of gender equality in governance. Their election also provoked online resistance in the form of abusive messages.

Many assumptions about their political inexperience were accompanied by sexist and misogynistic language.

This study reveals the troubling extent to which female ministers receive gendered, sexist, and misogynistic abuse online.

On Finnish Twitter, not only did female politicians receive more abuse than their male counterparts, but the abuse displayed a gendered pattern.

Gendered abuse was used to criticise and delegitimise women in ministerial positions no matter the political topic of the moment, be it the Finnish government's COVID-19 response, its immigration policy, or its involvement in EU affairs."

As social media platforms continue to grow in political importance, so does their use as a means for engaging with and criticising individual government officials with little or no consequences.

Over half of abusive messages were sent by anonymous accounts. Anonymity erases accountability online. This can have the effect of emboldening users to voice their dissatisfaction with ministers through unfiltered, abusive messages.

According to the paper, content moderation is ultimately the responsibility of social media and big tech companies. Social media platforms, Twitter included, are far more adept at moderating content in mainstream languages, most notably English.

The authors expect to witness the development of powerful tools drawing on advances in artificial intelligence to understand content across less-widely spoken languages and allow for the analysis of content with a higher degree of language variation.

As a result, such technology would ensure more equitable security measures across the linguistically diverse digital space, ultimately benefiting the smaller language branches of the Nordic and Baltic regions. Finnish-language Twitter appears to have been comparatively shielded from coordinated inauthentic manipulation, in part due to the complexity

of the local language. It remains to be seen how long this relative protection will last; advances in artificial intelligence may remove this barrier to manipulation.

You can read more at number 9 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

VOLUME 6 • NUMBER 1 WINTER 2021

THE CYBER DEFENSE REVIEW

Number 7 (Page 25)

Information Influence Operations: The Future of Information Dominance

VOLUME 6 • NUMBER 1 WINTER 2021

THE CYBER DEFENSE REVIEW

Number 8 (Page 27)

Microsoft Exchange Vulnerabilities, situation update and mitigation.

Number 9 (Page 29)

Abuse of power: Coordinated online harassment of Finish government ministers.

Number 10 (Page 32)

Statement from Fastway Couriers regarding Data Breach.

Number 1

An Honest Conversation about ESG Regulation

ESG (Environmental, Social, Governance) regulation - Commissioner Elad L. Roisman, U.S. Securities and Exchange Commission

Good morning. I will start by noting that my remarks are my own and do not necessarily represent the views of my fellow Commissioners or the Securities and Exchange Commission ("SEC").

AMAC's Careful and Collaborative Approach

Thank you, Ed [Bernard] and members of this Committee, not only for your work, but for the thoughtful process you have undertaken to develop recommendations for the Commission.

AMAC's approach has been methodical, iterative, and transparent: discussing complex issues, developing subcommittee recommendations in draft form, presenting those ideas to the full Committee, and inviting a lot of engagement.

While such an approach may not yield quick results—and it likely demands increased time and attention from each of you—it provides opportunities to consider new perspectives and new information.

Ultimately, I believe it should make any final recommendations you adopt more comprehensive and useful for the Commission itself.

New Potential Recommendations from the Diversity and Inclusion and Private Investments Subcommittees

Today, I look forward to hearing new potential recommendations, including ideas from the subcommittee on Diversity and Inclusion on how the Commission can help advance diversity and inclusion in the asset management industry.

I am especially interested in whether our securities laws or rules inadvertently create barriers and what we can do overcome those.

From the Private Investments subcommittee, I look forward to hearing your ideas on increasing retail investors' access to investing opportunities in the private market.

Over this past year, we have seen retail investors embrace trends, such as SPAC investments and day trading.

While some will always want to "go-it-alone" in their search for growth opportunities, I am interested in how professional managers can provide more guided access.

Exploring the ESG Subcommittee's Preliminary Recommendation

For the remainder of my remarks, I will focus on ESG, in anticipation of the panel discussing the subcommittee's preliminary recommendation from December 1, 2020.

Many thanks to Ed and the ESG subcommittee for engaging with my team over the past several months.

Like many others at the Commission, I am passionate about our capital markets and want to ensure that investors are getting the material information they need to make investment decisions—regardless of whether the information is characterized as "ESG" or not.

Before I go through several questions I would like to pose for our panelists, let me express my hope that today's atmosphere will foster an open-minded dialogue about the substance of the subcommittee's preliminary recommendation.

ESG is a topic that can feel polarizing. I have heard from some, who feel inclined to question the propriety of SEC regulation in this area, that they fear the reputational risk of being painted as "anti-climate," "anti-social justice," or other shades of immoral if they express their critiques publicly.

On the flip side, proponents of this agency's intervention sometimes offer rationales for action that are entirely outside the realm of securities law.

A letter recently arrived at my office advocating for mandatory ESG disclosures and ended by saying: "There is no Planet B."

It is entirely reasonable for a person to feel that climate change deserves immediate attention from lawmakers and still question whether the SEC mandating new disclosures from U.S. public companies is an appropriate step for the agency.

In this forum, I feel confident that we all recognize the fundamental questions here are about the SEC's authority as a regulator and whether this agency's intervention is appropriate to address the problems people have identified in our markets.

This is an entirely healthy and necessary conversation, and it will be critical for us to have the full spectrum of market participants engaged.

If the only people who feel safe to comment are those who want the agency to join the fight against climate change and those whose business models would benefit from new regulation, we will miss hearing from those voices who can alert us to the hidden costs and unintended consequences of our actions.

With that said, I am happy to hear from our expert Committee members today and welcome new panelists to join the dialogue.

Questions for the asset managers

I will start with my questions for those panelists who represent asset managers:

- How have you gauged what investors are looking for when it comes to ESG products? People have invested now around $2 Trillion into funds labeled "ESG," "green," and the like.

  But, it is not clear to me that we understand these investors' objectives, which (as the subcommittee's preliminary recommendation states) may fall outside risk/return alone.

  How do you design and market products tailored to investors' interests?

- To the extent you are focusing on minimizing risk and achieving high returns, what E, S, and G information specifically do you believe you need from issuers, and why?

  How is this information related to valuing potential targets for investment and valuing portfolio companies on an ongoing basis?

- I would like to understand how asset managers are currently seeking out this information.

  I know some request companies provide SASB or TCFD disclosures, or they seek the information in a different manner. How do you choose which approach to take?

- How have European disclosure mandates, such as the Sustainable Finance Disclosure Regulation, factored into this decision-making?

- To the extent that you are looking to increase comparability of issuers' disclosure, why is this important in the case of ESG? In other contexts, we do not demand perfect comparability across all categories of material information.

These questions are all relevant to the concept of materiality—figuring out exactly which ESG information is material is a threshold issue for me as I think about the SEC considering new disclosure requirements.

For Everyone

The next questions are for all panelists and our moderator.

The subcommittee's preliminary recommendation contemplates that the SEC rely on a third-party standard setter to identify what information is material.

How should the SEC oversee such a third party?

Should we extend our oversight further, for example, to ESG-index providers and ESG-rating agencies, since so many "ESG" funds and investment products are derivative of their work?

For Companies

The remainder of my questions are for those panelists who represent public companies. The bulk of the obligations in the subcommittee's preliminary recommendation would fall on your shoulders.

How could the burden could be mitigated for companies who are working with investors to provide them with ESG information?

I understand that liability is one concern, and there may be others.

Were the SEC to require new ESG disclosures, should we consider allowing them to be furnished rather than filed? Should we consider a safe harbor, dependent on particular conditions such as the presence of cautionary language?

Conclusion

While I am nowhere near the end of my questions, I will stop here for now. I look forward to the discussion today, but also encourage everyone to consider sharing your views in the public comment file, which Acting Chair Lee recently opened on these topics.

Finally, my door is open to anyone who wants to discuss these matters directly with me.

Number 2

COVID-19: a watershed for the FSB's work agenda

Launch of the International Regulatory Strategy Group report 'Global Solutions to Global Problems: Promoting Regulatory Coherence in Financial Services for Pandemic Recovery' - Remarks by Dietrich Domanski, Secretary General, Financial Stability Board

Thank you for the invitation to be with you today. This is a timely event, coming almost a year to the day that global equity markets experienced the worst drop since Black Monday in 1987, triggered by the epic shock of the COVID-19 pandemic.

Since then, the pandemic has fundamentally altered our lives, at a very personal level as well as professionally. COVID-19 has also marked a watershed in the work of the Financial Stability Board.

As the first serious test of the resilience of the global financial system since the 2008 financial crisis, COVID19 has provided us with a real-life assessment of the global regulatory framework put in place after 2008 and of international cooperation on financial stability through the FSB.

I would like to elaborate on what this watershed means for the FSB's work in 2021 and beyond.

I'll focus on three themes:

- first, the need to address the lessons learned from COVID-19 for financial stability;

- second, the need to harness the benefits of innovation to support a strong and sustainable recovery from the pandemic; and

- third, the importance of global cooperation, not least to preserve an integrated global financial system.

Addressing the lessons learned from COVID-19 for financial stability

To an important extent, this greater resilience is due to the regulatory reforms enacted post 2008.

The Basel III framework, the shift to mandatory central clearing, and steps taken to end too-big-to-fail have all helped to make the core of the global financial system more resilient.

At the same time, the market turmoil last March has underscored the need to strengthen resilience in non-bank financial intermediation, or NBFI.

With the overall growth of NBFI – due to market driven adjustments and the G20 regulatory reforms – market liquidity has become more central to financial resilience.

Last March, the 'dash for cash' resulted in liquidity mismatches that overwhelmed key funding markets.

Public authorities needed to take a wide range of measures to support liquidity and the supply of credit to the real economy.

These developments define the key areas of a very active FSB policy work agenda for 2021: The first is to draw lessons from COVID-19 for financial stability, including whether the reforms the G20 put in place following the 2008 financial crisis are working as intended, and where they may not be.

We will look at the use of capital and liquidity buffers by financial institutions, and how well crisis management and operational resilience arrangements have functioned.

This work will also examine whether and how procyclicality has affected the financial system.

We will work on these issues in coordination with standard-setting bodies (SSBs), and provide the G20 with an interim report on initial lessons learned in July and a final report in October.

Any lessons learned at this stage will be preliminary, but it is important for us to critically assess our actions.

The second area is CCP financial resources. Recent periods of market turmoil have further demonstrated the positive effect that central clearing can offer for global financial stability.

However, the shift to central clearing has also further increased the systemic importance of central counterparties, as we knew it would.

To this end, the FSB will collaborate with the Committee on Payments and Market Infrastructures and International Organization of Securities Commissions on work that will consider the need for – and develop as appropriate – international policy on the use, composition and amount of financial resources necessary to strengthen the resilience and resolvability of CCPs further, in default and non-default loss scenarios.

Last, but certainly not least, one area where we have already started to draw lessons is NBFI. We have embarked on a comprehensive and ambitious work programme to strengthen the resilience of the NBFI sector while preserving its benefits.

The work programme includes:

(i) work to address specific risk factors that contributed to amplification of the shock;

(ii) work to enhance our understanding of systemic risks in NBFI; and

(iii) investigating policies to address systemic risks in NBFI.

A key focus this year is to develop policy proposals to enhance the resilience of money market funds (MMFs).

The structural vulnerabilities in some types of MMFs relate to the greater role of liquidity risk I mentioned before: liquidity mismatches in MMFs and investors' perception of these funds as being equivalent to cash.

Identifying policy options to enhance MMF resilience will include consideration of the appropriate structure of the MMF sector itself and the role of potential vulnerabilities in the underlying short-term funding markets.

We are working in close collaboration with SSBs and plan to publish a consultative report, with policy proposals to enhance MMF resilience, in July.

To read more: https://www.fsb.org/wp-content/uploads/S180321.pdf

Number 3

EBA consults on changes to its Guidelines on Risk-based AML/CFT supervision

The European Banking Authority (EBA) launched today a public consultation on changes to its Guidelines on Risk-Based Supervision of credit and financial institutions' compliance with anti-money laundering and countering the financing of terrorism (AML/CFT) obligations.

The proposed changes address the key obstacles to effective AML/CFT supervision that the EBA has identified during its review of the existing Guidelines, including the effective use of different supervisory tools to meet the supervisory objectives.

The Guidelines are central to the EBA's mandate to lead, coordinate and monitor the EU financial sector's fight against money laundering and terrorist financing.

The consultation runs until 17 June 2021.

The Guidelines on risk-based AML/CFT supervision were originally published by the European Supervisory Authorities (ESAs) in 2016 and set out steps that competent authorities should take to ensure compliance by credit and financial institutions with their AML/CFT obligations.

Since their publication, the EBA has observed that supervisors across the EU were finding the implementation of the risk-based approach to AML/CFT supervision difficult, which meant that AML/CFT supervision was not always as effective as the legal framework set out in Directive (EU) 2015/849 (AMLD) and the ESAs' Guidelines had envisaged.

The changes the EBA is proposing include practical step-by-step approaches to addressing those aspects of AML/CFT supervision that competent authorities have found particularly challenging.

The revised Guidelines focus on helping the supervisors identify and manage ML/TF risks more effectively, including the risks that may arise from de-risking practices in some sectors or Member States by providing greater detail on ML/TF risk assessments and by requiring to develop a robust supervisory strategy and plan that are based on those risk assessments.

The Guidelines also set out how supervisors can choose the most effective supervisory tools to support different supervisory needs and objectives, and stress the importance of cooperation between different supervisory authorities, and between supervisors and other stakeholders, such as Financial Intelligence Units and financial institutions.

In addition, the Guidelines emphasise the importance for supervisors to develop a good understanding of ML/TF risks associated with tax crimes, which may involve a cooperation with tax authorities in their Member State.

Once implemented, the proposed changes will foster greater convergence of supervisory practices in areas where supervisory effectiveness has been hampered, so far, by divergent approaches in the implementation of the same European legal requirements. This means that they will significantly strengthen Europe's AML/CFT defences.

Consultation process

Comments to the draft Guidelines can be sent by clicking on the "send your comments" button on the EBA's consultation page. The deadline for the submission of comments is 17 June 2021.

All contributions received will be published following the close of the consultation, unless requested otherwise.

The EBA will hold a virtual public hearing on the draft Guidelines on 22 April 2021 from 14:00 to 16:00 Paris time. The dial-in details will be communicated to those who have registered for the meeting.

The scope of the EBA's consultation is limited to the amendments and additions to the original risk-based supervision Guidelines, which will be repealed and replaced with the revised Guidelines.

Legal basis and background

Directive (EU) 2015/849 (AMLD) puts the risk-based approach at the centre of the EU's AML/CFT regime.

It recognises that the risk of money laundering and terrorist financing may vary between countries, sectors and financial institutions and that Member States, competent authorities and credit and financial institutions should identify and assess these risks in order to decide how to best manage them.

Article 48(10) of AMLD mandates the EBA to issue Guidelines addressed to competent authorities on the characteristics of a risk-based approach to supervision and the steps to be taken when conducting supervision on a risk-based basis.

The mandate requires the EBA to take specific account of the nature and size of the business, and, where appropriate and proportionate, specific measures shall be laid down.

The revised Guidelines also propose to take into consideration changes in the EU legal framework that came into force since the original guidelines were first issued, as well as new international guidance by the Financial Action Taskforce (FATF) and the Basel Committee on Banking Supervision on this topic.

Number 4

International Financial Hub Initiatives

金融庁
Financial Services Agency

The Japanese Government is committed to expanding Japan's role as an international finance hub.

New policies will help foreign asset managers and other financial institutions enter the Japanese market so that they may contribute to improve Japan's financial and capital markets in tandem with local players and eventually we may better serve as an international financial center in Asia and the world.

Japan as an International Financial Hub

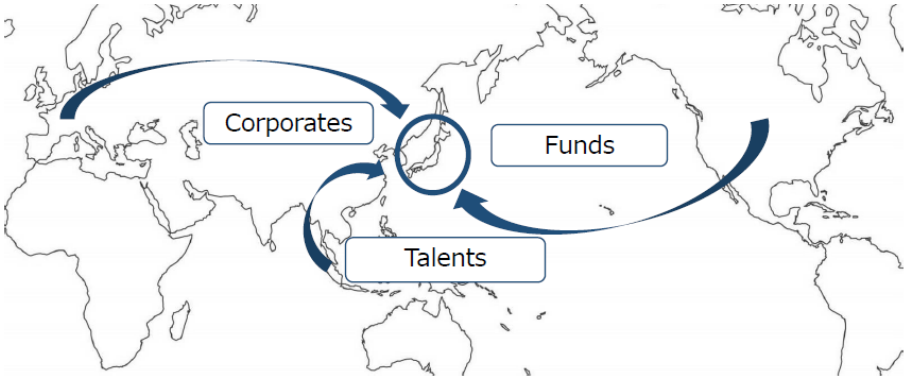
Japan's strengths / potential

- Political stability, good public security, favorable living environment
- Sizable domestic economy, over 18 trillion USD household assets

Japanese Government's Initiatives

- Provide convenience/accessibility through easing regulatory measures
- Enhance the tax system and provide life support by collaborating with other ministries

Japan aims to become an international financial hub that attracts talents, corporates, and funds...



...to make Japan an attractive place for foreign professionals to do business in addition to a tourism destination

Summary of Japanese government's initiatives

Policy package through cross-ministerial collaboration

Tax policy	✓Revision/clarification of corporate, inheritance, and income tax
Regulatory policy	✓One-stop English service for application and registration for newly entering overseas asset managers ✓Introduction of simplified market entry procedures for overseas asset managers
Residence status	✓Special immigration measure for newly entering asset managers as a temporary visitor to commence business without returning to their home country ✓Relax employment requirements for domestic helpers and increase convenience for working spouses for Highly-Skilled Professionals
Company setup and livelihood support	✓One stop company setup support for free ✓Livelihood support such as international school hunting, medical matters, and housing
Information sharing	✓Collectively share related policy measures information through a dedicated website and contact points of diplomatic missions

(1) Tax policy

Revision/clarification

	Current Status	Solution
Corporate tax For Asset management firms	**30%** Performance-based compensation of directors Listed companies : deductible **Private companies : not deductible**	A private, non-family company including a 100% subsidiary of a listed company which mainly operates asset management business should be able to deduct its performance-based compensation with a number of conditions, including where the calculation methods are described in its business reports filed under the Financial Instruments and Exchange Act and disclosed publicly through the JFSA website. (Sequentially applied after relevant law enters into force in 2021 December, expected)
Inheritance tax For heirs of foreign residents in Japan	**0～55%** Living in Japan over 10 years: worldwide assets Living less than 10 years ···tax on only assets in Japan	Assets outside of Japan that a foreign national who entered Japan with a valid working visa holds should be exempt from Japanese inheritance tax regardless of their years of residence in Japan when the heir receives the assets as a non-resident. (2021 April 1st)
Income tax For fund managers	**0～55%** Carried interests - distribution allocated returns in excess of their capital contribution ratio → **Unclear if it is a capital gain or not**	When a profit distribution of a carried interest has an economic rationality, that profit should be taxed as a capital gains tax (20%). (2021 Spring)

（2）Regulatory policy

One-stop and all-in-English regulatory services

Current Status

- Foreign asset management companies must have discussions with different contact points in JFSA and Local Finance Bureaus
- High regulatory compliance cost due to the requirement to file application/registration in Japanese

Solution

"Financial Market Entry Office" was launched in JFSA in January 2021

→ **One-stop English services** for pre-application consultation, registration procedures, and supervision

※ Financial administrative services in English through AI powered translation technology from March 2021

（2）Regulatory policy

Simplified market entry procedure

Current status

In principle, even an asset management firm that serves overseas professional investors (institutional investors) is required to be registered with JFSA in order to conduct asset management business in Japan.

Moreover, registration procedures could take some time even for an asset management firm with a proven track record overseas

Solution

Facilitate overseas asset managers' entry by introducing the following schemes:

- **Pre-registration entry scheme** (5 years) for those with authorization by regulatory bodies and a proven track record in specified foreign countries
- **Simplified entry scheme for GP managers** with overseas qualified clients

※ The bill will be submitted to the 2021 Diet session

(3) Residence status

Relax residence status requirements

Working visa

○ Introduce an exceptional measure enabling foreigners entering Japan as a "temporary visitor (short-stay)" for the purpose of preparing for company setup to obtain residential status **without returning to their home country** before commencing business under certain conditions

Highly-Skilled Professionals

○ **Add bonus point category for those engaged in asset management business** to be subject to preferential treatment for Highly-Skilled Professionals

● Finance professionals can obtain a Highly-Skilled Professionals visa within the **prioritized administrative review period (around 10 days)**

Domestic helpers/nannies

○ With regard to Highly-Skilled Professionals, under certain conditions,
- ● allow them to hire domestic helpers **even if they do not meet the conditions such as having a child under the age of 13**
- ● increase the maximum number of domestic helpers they can hire from one to **two**

Spouse

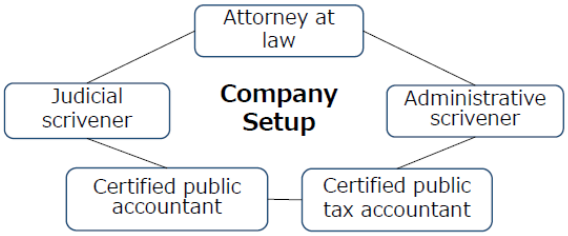
● Spouses of highly-skilled professionals can **work full-time without working visa** under certain conditions

Note: Bullets starting with ○ are preferential treatments for asset managers
"Certain conditions" are under discussion

(4) Company setup and livelihood support

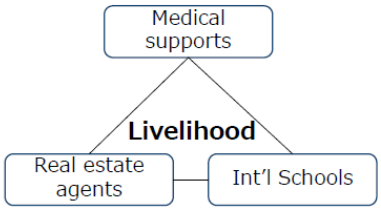
Company setup support

- Company setup in Japan
- Acquisition of Residence status
- Obtaining license and/or registration etc.



Livelihood support

- Medical supports
- Housing
- International Schools



Support by private companies

Implement a trial business project offering a **free one-stop** seamless support service for foreigners and overseas asset management businesses that are considering setting up companies in Japan

Support by the Government

Enhance "Financial Market Entry Office" (slide 5) to cover total relocation support including settling in and establishing a livelihood (in corporation with local governments and Foreign Residents Support Center)

（5）Information sharing

Enhancement of information sharing

Launch a dedicated page under JFSA's website to collectively share information on the following policy measures and total relocation support

(1) Tax policy initiatives
(2) Regulatory policy initiatives
(3) Residence status
(4) Company setup and livelihood support

Contact information

Financial Market Entry Office
marketentry@fsa.go.jp
https://www.fsa.go.jp/en/policy/marketentry/index.html

Disclaimer

This document is prepared by Japanese Financial Services Agency (hereinafter referred to as "JFSA") as the summary of tentative discussions. To identify applicable regulatory requirements in particular, please refer to the respective laws and regulations.

The information contained in this document is based on the Comprehensive Economic Measures and the Tax Reform Proposals which were respectively published on December 8 and 21. The information contained in this document is subject to change due to revisions in laws and regulations and/or the preparation and execution of budgets.

JFSA does not assume any obligation to update, revise or reaffirm any of the information contained in this document, whether as a result of new information, future events, or otherwise.

Although JFSA exerts its best efforts to ensure the accuracy and such of the information contained in this document, the information therein does not necessarily represent the official views of JFSA. JFSA makes no warranty, expressed or implied, as to the accuracy, completeness, usefulness of the information contained in this document, and assumes no responsibility or liability for any disadvantages or whatsoever incurred in connection with the use of those information.

All information contained in this document is prepared solely for informational purposes, and does not constitute a solicitation for investment activities or a recommendation to invest in any particular stocks.

Number 5

ESAs publish Joint Q&As on Bilateral Margining

The European Supervisory Authorities (EBA, EIOPA and ESMA - ESAs) published three Joint Questions and Answers (Q&A) on RTS 2016/2251 on bilateral margin requirements under the European Markets Infrastructure Regulation (EMIR).

The purpose of the Joint Q&As on bilateral margin requirements is to promote common supervisory approaches and practices in the application of EMIR. It provides responses to questions posed by the public, market participants and competent authorities in relation to the practical application of the Regulation.

The Joint Q&As on Bilateral Margining clarify different aspects regarding the bilateral margin regime under EMIR:

- the relief covered by a partial intragroup exemption from bilateral margin requirements;

- the procedure to grant intragroup exemptions from bilateral margin requirements between a financial counterparty and a non-financial counterparty that are based in different Member States; and

- the exemption regime from bilateral margin requirements for derivatives entered into in relation to covered bonds.

To read more:
https://www.eiopa.europa.eu/sites/default/files/joint-committee/joint-esa-qas-bm-emir.pdf

Number 6

Microtargeting as Information Warfare

VOLUME 6 ▪ NUMBER 1 WINTER 2021

THE CYBER DEFENSE REVIEW

Abstract

Foreign influence operations are an acknowledged threat to national security. Less understood is the data that enables that influence. This article argues that governments must recognize microtargeting—data informed individualized targeted advertising—and the current advertising economy as enabling and profiting from foreign and domestic information warfare being waged on its citizens.

The Department of Defense must place greater emphasis on defending service members' digital privacy as a national security risk. Without the ability to defend this vulnerable attack space, our adversaries will continue to target it for exploitation.

Introduction

In September 2020, General Paul Nakasone, NSA Director and Commander of U.S. Cyber Command, called foreign influence operations "the next great disruptor."

Nearly every intelligence agency in the United States government has been sounding the alarm over targeted influence operations enabled by social media companies since at least 2016, even though some of these operations started earlier.

What often goes unstated and even less understood is the digital surveillance economy underlying these platforms and how this economic structure of trading free access for data collection about individuals' lives poses a national security threat.

Harvard sociologist Shoshana Zuboff calls this phenomenon "surveillance capitalism [which] unilaterally claims human experience as free raw material for translation into behavioral data."

This behavioral data is transformed into increasingly accurate micro-targeted advertising.

The new surveillance capitalism has enabled massive information warfare campaigns that can be aimed directly at target populations. The predictive power of surveillance capitalism is not only being leveraged for advertising

success but increasingly harnessed for mass population control enabled by massive amounts of individually identifiable, commercially available data with virtually no oversight or regulation.

This is not to say there is no oversight—data use and collection by the intelligence community is subject to significant oversight and regulation.

This article, critically, is not about data use laws and areas that are already regulated. Technology companies such as Facebook or Google exist in ungoverned spaces and are not subject to regulations like specific industries such as banking, education, or health care providers.

For example, medical companies are clearly bound by Health Insurance Portability and Accountability Act (HIPAA) and the banking industry is bound by Sarbanes Oxley, which includes data regulation components. Conversely, the tech companies actually have a shield from liability based on the Communications Decency Act, Section 230.

This law places tech companies outside of regulatory restrictions rather than providing any meaningful limit on their actions and as a result creates a national security risk for the Department of Defense (DoD).

You can read more at page 63:
https://cyberdefensereview.army.mil/Portals/6/Documents/2021_winter_cdr/CDR_Winter_2021.pdf

Number 7

Information Influence Operations: The Future of Information Dominance

VOLUME 6 ▪ NUMBER 1 WINTER 2021

THE CYBER DEFENSE REVIEW

Abstract

This paper proposes the development and inclusion of Information Influence Operations (IIOs) in Cyberspace Operations.

IIOs encompass the offensive and defensive use of cyberspace to influence a targeted population. This capability will enable the evolution of strategic messaging in cyberspace and allow response to near peer efforts in information warfare.

Introduction

This paper proposes that Information Influence Operations (IIOs) be developed and utilized within U.S. Cyber Command's (USCYBERCOM) capability set.

When correctly employed, IIOs will become a critical capability that is key to the future of cyberspace operations.

IIOs must become the new "light touch", the guiding hand gently pushing public opinion, and ultimately shaping global perception and narratives in support of US strategic interests.

LTG Stephen Fogarty stated: "the command [Army Cyber Command] must mimic enemy capabilities and better integrate and synchronize information operations, military deception, psychological operations, electronic warfare, all intelligence disciplines."

Today, most leaders consider cyber effects either an intelligence collection source or a means of causing real-world impact, such as turning off a power grid or causing significant disruption to an enemy's C2 network.

Those views require revision to take full advantage of the value of cyberspace. The unrealized value of cyberspace, and what makes it so dangerous, is it allows direct access to the individual and to the public at large.

This access, when used correctly, provides actors in cyberspace the ability to influence public opinion and shape the narrative of ongoing operations.

Influencers

As communications technology and the Internet have proliferated, capabilities previously limited to major companies and government are now accessible to anyone with an Internet connection. The traditional consumers of news can now play a major part in producing it.

Bob Franklin and Lily Canter assert that "Advances in technology have profoundly impacted war reporting, affording audiences new ways in which to visualize conflict.

Satellites, smartphones, laptops, and mobile broadband have enabled war reporters to communicate immediately and
bring conflict live to air.

Nevertheless, as new technologies open up innovative ways for journalists to convey the horrors of warfare, they similarly create opportunities for propaganda, censorship, and control."

The communications capabilities referenced have contributed to
the creation of a power vacuum in the information realm of cyberspace.

This vacuum is being filled not by traditional media and governments but by small groups of content creators and "influencers" whom have rapidly capitalized on the massive reach provided by new technologies.

These "influencers" are capable of wielding influence over millions and have used this influence for a multitude of purposes from philanthropy and advertising to political ends. The future of cyber operations is the use of IIOs in cyberspace to wield influence.

You can read more at page 133:
https://cyberdefensereview.army.mil/Portals/6/Documents/2021_winter_cdr/CDR_Winter_2021.pdf

Number 8

Microsoft Exchange Vulnerabilities, situation update and mitigation.

On 2nd March 2021, Microsoft released security updates for Microsoft Exchange server suite.

Active exploitation has been observed ever since on premises running MS Exchange installations.

Although the initial focus of malicious attacks was observed mainly in the US, incidents rapidly expanded around the globe, including in the EU by an increasing number of hacking groups.

In the EU, an increasing number of MS Exchange installations have also been found to be the target of malicious attacks.

Although the initial focus of attacks was on exfiltration of information, attackers seem to be exploiting the MS exchange vulnerabilities to plant ransomware in order to gain profits.

Cases of such systems infected with the DearCry ransomware have been reported.

On 7th March 2021, the European Banking Authority (EBA) published a statement on their website announcing that their Microsoft Exchange servers had been the victim of a cyber-attack, as a result of the recently-disclosed zero-day vulnerabilities in the servers.

The incident has been mitigated according to a later statement by EBA, without affecting confidentiality of EBA systems and data.

The EU Cyber Crises Liaison Organisation Network (CyCLONe) and the EU CSIRTs network are monitoring the situation and collecting information.

Scans conducted by researchers indicate that on March 5th there were around 250,000 vulnerable servers.

That number dropped to around 60,000 over the next 10 days. The initial rush to patch by companies with good security posture has considerably lowered the number of vulnerable systems exposed.

There are indications that threat actors are targeting Exchange Servers from infrastructure hosted in a number of EU countries, Hong Kong, United States, Belize, Japan, and Singapore.

Wide scanning activities for the vulnerabilities have been observed from systems in the EU, the United States, Hong Kong and China. Botnet operators are likely to be leveraging the vulnerabilities to expand their operations.

The LemonDuck botnet has been observed exploiting the vulnerabilities recently. Ransomware operators are also leveraging the vulnerabilities and it is likely that this activity will continue.

The new DearCry ransomware has been deployed following successful exploitation with victims observed in some EU countries, Indonesia, India and the United States.

To read more:
https://www.enisa.europa.eu/publications/situational-report-on-microsoft-exchange-vulnerabilities

Number 9

Abuse of power: Coordinated online harassment of Finish government ministers.

This report is an explorative analysis of abusive messages targeting Finnish ministers on the social media platform Twitter.

The purpose of this study is to understand the scope of politically motivated abusive language on Finnish Twitter, and to determine if, and to what extent, it is perpetrated by inauthentic accounts.

To this end, we developed a mixed methodology, combining AI-driven quantitative visualisations of the networks delivering messages of abuse with a qualitative analysis of the messages in order to understand the themes and triggers of abusive activity.

We collected Twitter data between 12 March and 27 July 2020, a period spanning the state of emergency declared in response to the COVID-19 pandemic.

This report is informed by the findings of three recent Finnish studies, one of which investigated the extent and effects of online hate speech against politicians while the other two studied the use of bots to influence political discourse during the 2019 Finnish parliamentary elections.

The first study, released by the research branch of the Finnish government in November 2019, found that a third of municipal decision-makers and nearly half of all members of Finnish Parliament have been subjected to hate speech online.

The two studies tracking inauthentic activity during the 2019 parliamentary elections identified bot interference but concluded that the impact of these bots on Finland's political environment appeared limited.

Based on these findings, and on our comprehensive literature review, we developed two hypotheses:

1. We expect to observe abusive language targeting Finnish politicians, with female politicians receiving gendered abuse;

2. We expect to observe low levels of coordinated inauthentic activity in the Finnish information space, with increased levels of inauthentic activity during periods of political significance.

Our quantitative and qualitative analyses confirmed both hypotheses and yielded multiple findings.

Our investigation demonstrated that the messaging directed at Finnish government officials is largely free from automated activity.

When it comes to abusive messaging, we find a number of users singularly focused on harassing the government.

While both left- and right-leaning communities engaged in abusive activity, the bulk of abusive messaging originated from clusters of right-wing accounts.

Overall, we observed very low levels of both bot and coordinated activity. The majority of bots we identified were operating in foreign languages and either not generally focused on Finland or used to push certain causes in multiple languages.

We repeatedly came across a cluster of accounts throughout our monitoring period that posted the same messages about animal cruelty and climate change.

These accounts predominantly post in English and appear in some cases to be automated or semi-automated. However, they represent a very small part of the conversation.

Likewise, a small cluster of automated accounts amplified messaging by a number of right-wing voices. Again, there was a degree of coordination here, but these amplifications looked more like attempts at self-promotion rather than systematic manipulation of the information space.

If large-scale inauthentic coordination exists in the Finnish information environment, we are either looking in the wrong place, or it is so sophisticated or so small in scale that it evades our detection methods.

We found that the main topics triggering abusive messages were the COVID-19 pandemic, issues of immigration, Finnish-EU relations, and socially liberal politics.

We observed that female Finnish ministers received a disproportionate number of abusive messages throughout our monitoring period.

A startling portion of this abuse contained both latent and overtly sexist language, as well as sexually explicit language.

Although we found large volumes of offensive and abusive messaging, we did not observe threats of physical violence.

Introduction

Lipstick brigade. Lipstick girls. Feminist quintet. Tampax team. These are all phrases used on Twitter to refer to the current coalition in Finland, in which all five party leaders are women, led by Prime Minister Sanna Marin of the Social Democratic Party.

When the remarkably young and female leadership came into power in December 2019, they made international headlines as pioneers of gender equality in governance.

Their election also provoked online resistance in the form of abusive messages. Many assumptions about their political inexperience were accompanied by sexist and misogynistic language.

The paper:
https://www.stratcomcoe.org/abuse-power-coordinated-online-harassment-finnish-government-ministers

Number 10

Statement from Fastway Couriers regarding Data Breach.

Fastway Couriers confirms that one of its IT systems has been subject of a cyber-attack, the consequence of which has been that client data, including customers' personal information, has been compromised.

The data in question is information used for the purposes of delivery (name, address, email and/or phone).

No financial data or other personal data has been compromised, nor is this stored on any Fastway system.

On learning of the cyber breach, Fastway advised the Data Protection Commission and the Gardai. Fastway has made the requisite data breach submission to the Data Protection Commission.

The cyber-attack was identified by Fastway's third-party IT development contractor on February 25th and was fully mitigated by 9am on February 26th. The third-party contractor advised Fastway of the breach on March 2nd.

The data that was compromised relates to the customers of Fastway clients. Names, addresses and contact details of 446,143 parcel receivers were compromised. The data compromised relates to Fastway deliveries, in-flight or undelivered parcels over a period of approximately 30 days from mid-January onwards.

"It is distressing that our IT system was compromised by a malicious hack as we are exceptionally careful in every aspect of our data protection obligations," said Danny Hughes, CEO of Fastway Couriers. "I deeply regret that people's personal data has been compromised and I apologise to our clients and their customers. I want to stress that nobody's financial data was at risk and the issue is limited to delivery information only. We will continue to work closely with the DPC, the Gardai and our clients to manage this situation in line with best practice."

Fastway has engaged an IT consultancy to conduct an incident response and independent review of the cyber-attack.

Should you need further information please contact us on dp@fastway.ie

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.

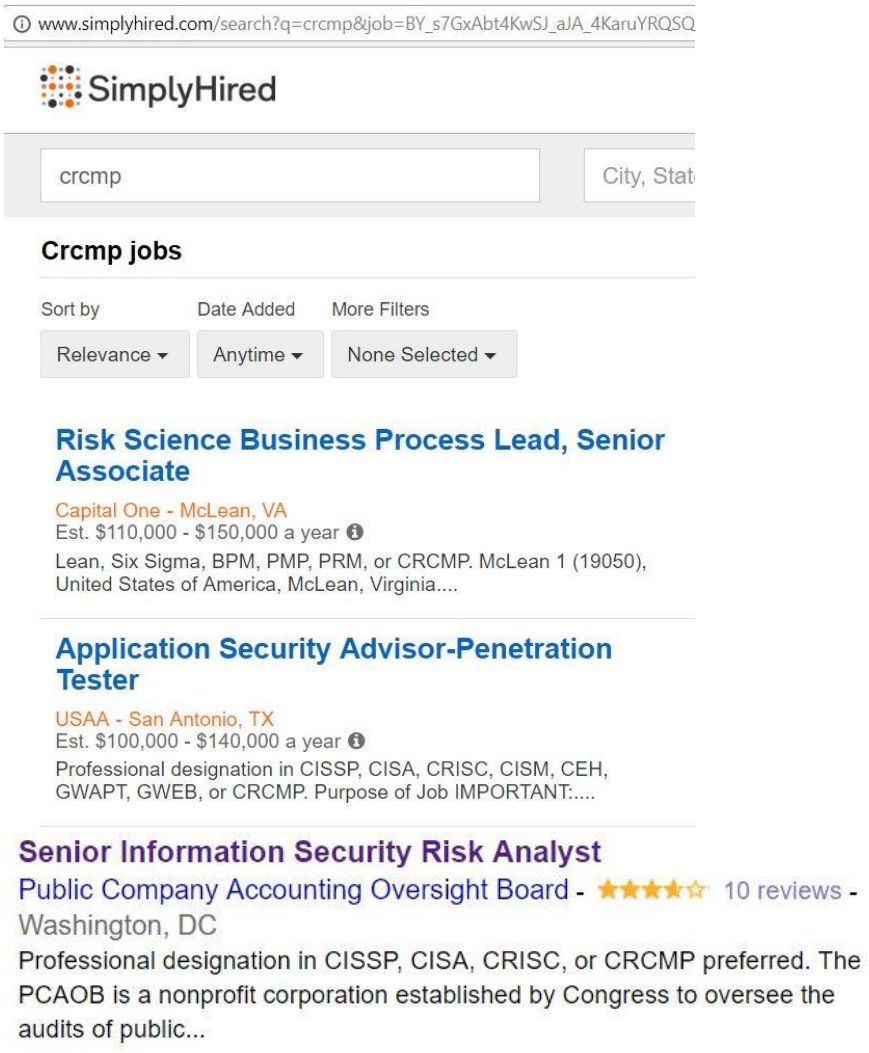
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

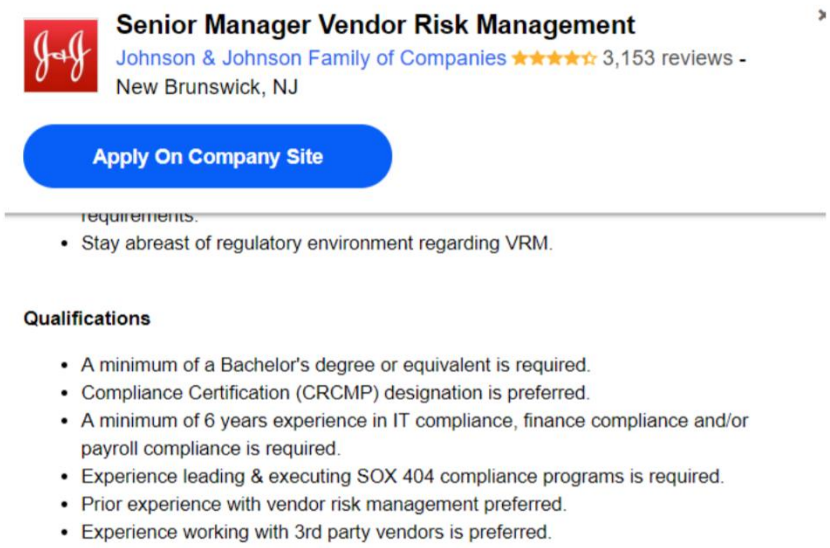
You can explore what we offer to our members:

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 around the world 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.