

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, May 15, 2023

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,

Following the Digital Services Act (DSA), the European Commission designated 17 Very Large Online Platforms (VLOPs) and 2 Very Large Online Search Engines (VLOSEs) that reach at least 45 million monthly active users. Quiz: How many entities are not European?



Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando, Bing, Google Search, the clock is ticking. Following the designation, you have to comply, *within four months*, with the full set of new obligations under the Digital Services Act (DSA).

Platforms and search engines need to take measures to address risks linked to the dissemination of *illegal content* online and to negative effects on freedom of expression and information.

Users will get clear information on why they are recommended certain information, and will have the right to opt-out from recommendation systems based on profiling;

Platforms will have to identify, analyse and mitigate a wide array of systemic risks ranging from how illegal content and disinformation can be amplified on their services, to the impact on the freedom of expression and media freedom.

Similarly, specific risks around gender-based violence online and the protection of minors online and their mental health must be assessed and mitigated.

The risk mitigation plans of designated platforms and search engines will be subject to an independent audit and oversight by the Commission.

Read more at number 1 below. Welcome to the Top 10 list.

Best regards,

George Lekatis

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

Number 1 (Page 5)

The European Commission adopted the first designation decisions under the Digital Services Act (DSA).

*Number 2 (Page 8)*

Chair Williams Keynotes Baruch Conference on Financial Reporting

*Number 3 (Page 9)*

SEC Issues Largest-Ever Whistleblower Award

*Number 4 (Page 11)*

The European Banking Authority (EBA) today published its annual Report on convergence of supervisory practices for 2022.

*Number 5 (Page 14)*

In crisis and emergency, compulsory license on patents
Proposal for a regulation on compulsory licensing for crisis management (the Compulsory Licensing Regulation).



Number 6 (Page 18)

G20 TechSprint 2023 - Transforming cross border payments

The fourth and 2023 TechSprint is a joint initiative between the BIS Innovation Hub and Reserve Bank of India.



Number 7 (Page 20)

Sweep Targets Darknet Markets

Operation SpecTor spanned three continents, seized millions of dollars, and removed tens of thousands of potentially lethal drugs from circulation



Number 8 (Page 22)

Using math to map social connections



Number 9 (Page 25)

Meta's Q1 2023 Security Reports: Protecting People and Businesses

Guy Rosen, Chief Information Security Officer



Number 10 (Page 29)

Quarterly Adversarial Threat Report



Number 1

The European Commission adopted the first designation decisions under the Digital Services Act (DSA).



The European Commission designated 17 Very Large Online Platforms (VLOPs) and 2 Very Large Online Search Engines (VLOSEs) that reach at least 45 million monthly active users.

Very Large Online Platforms:

- Alibaba AliExpress
- Amazon Store
- Apple AppStore
- Booking.com
- Facebook
- Google Play
- Google Maps
- Google Shopping
- Instagram
- LinkedIn
- Pinterest
- Snapchat
- TikTok
- Twitter
- Wikipedia
- YouTube
- Zalando

Very Large Online Search Engines:

- Bing
- Google Search

Following their designation, the companies will now have to comply, within four months, with the full set of new obligations under the DSA.

These aim at empowering and protecting users online, including minors, by requiring the designated services to assess and mitigate their systemic risks and to provide robust content moderation tools.

This includes:

More user empowerment:

- Users will get clear information on why they are recommended certain information and will have the right to opt-out from recommendation systems based on profiling;
- Users will be able to report illegal content easily and platforms have to process such reports diligently;
- Advertisements cannot be displayed based on the sensitive data of the user (such as ethnic origin, political opinions or sexual orientation);
- Platforms need to label all ads and inform users on who is promoting them;
- Platforms need to provide an easily understandable, plain-language summary of their terms and conditions, in the languages of the Member States where they operate.

Strong protection of minors:

- Platforms will have to redesign their systems to ensure a high level of privacy, security, and safety of minors;
- Targeted advertising based on profiling towards children is no longer permitted;
- Special risk assessments including for negative effects on mental health will have to be provided to the Commission 4 months after designation and made public at the latest a year later;
- Platforms will have to redesign their services, including their interfaces, recommender systems, terms and conditions, to mitigate these risks.

More diligent content moderation, less disinformation:

- Platforms and search engines need to take measures to address risks linked to the dissemination of illegal content online and to negative effects on freedom of expression and information;
- Platforms need to have clear terms and conditions and enforce them diligently and non-arbitrarily;
- Platforms need to have a mechanism for users to flag illegal content and act upon notifications expeditiously;

- Platforms need to analyse their specific risks, and put in place mitigation measures – for instance, to address the spread of disinformation and inauthentic use of their service.

More transparency and accountability:

- Platforms need to ensure that their risk assessments and their compliance with all the DSA obligations are externally and independently audited;

- They will have to give access to publicly available data to researchers; later on, a special mechanism for vetted researchers will be established;

- They will need to publish repositories of all the ads served on their interface;

- Platforms need to publish transparency reports on content moderation decisions and risk management.

By 4 months after notification of the designated decisions, the designated platforms and search engines need to adapt their systems, resources, and processes for compliance, set up an independent system of compliance and carry out, and report to the Commission, their first annual risk assessment.

Risk assessment

Platforms will have to identify, analyse and mitigate a wide array of systemic risks ranging from how illegal content and disinformation can be amplified on their services, to the impact on the freedom of expression and media freedom.

Similarly, specific risks around gender-based violence online and the protection of minors online and their mental health must be assessed and mitigated.

The risk mitigation plans of designated platforms and search engines will be subject to an independent audit and oversight by the Commission.

To read more:

https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413



*Number 2***Chair Williams Keynotes Baruch Conference on Financial Reporting**

Public Company Accounting Oversight Board (PCAOB) Chair Erica Y. Williams discussed a range of topics from the PCAOB's work to inspect and investigate completely in China, to their 2023 inspection priorities, to the state of audit quality and more during a virtual keynote session, which aired today at Baruch College's 21st Annual Financial Reporting Conference.

The Q&A session was moderated by Sr. Assoc. Dean Paquita Davis-Friday, and can be viewed below.



You may visit: <https://www.youtube.com/watch?v=F5DK37eaHoM>



*Number 3***SEC Issues Largest-Ever Whistleblower Award**

The Securities and Exchange Commission announced the largest-ever award, **nearly \$279 million**, to a whistleblower whose information and assistance led to the successful enforcement of SEC and related actions.

This is the highest award in the SEC's whistleblower program's history, more than doubling the \$114 million whistleblower award the SEC issued in October 2020.

"The size of today's award – the highest in our program's history – not only incentivizes whistleblowers to come forward with accurate information about potential securities law violations, but also reflects the tremendous success of our whistleblower program," said Gurbir S. Grewal, Director of the SEC's Division of Enforcement.

"This success directly benefits investors, as whistleblower tips have contributed to enforcement actions resulting in orders requiring bad actors to disgorge more than \$4 billion in ill-gotten gains and interest. As this award shows, there is a significant incentive for whistleblowers to come forward with accurate information about potential securities law violations."

"The whistleblower's sustained assistance including multiple interviews and written submissions was critical to the success of these actions," said Creola Kelly, Chief of the SEC's Office of the Whistleblower. "While the whistleblower's information did not prompt the opening of the Commission's investigation, their information expanded the scope of misconduct charged."

Payments to whistleblowers are made out of an investor protection fund, established by Congress, which is financed entirely through monetary sanctions paid to the SEC by securities law violators.

No money has been taken or withheld from harmed investors to pay whistleblower awards. Whistleblowers may be eligible for an award when they voluntarily provide the SEC with original, timely, and credible information that leads to a successful enforcement action, and adhere to

filing requirements in the whistleblower rules. Whistleblower awards can range from 10 to 30 percent of the money collected when the monetary sanctions exceed \$1 million.

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

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

You may visit: <https://www.sec.gov/news/press-release/2023-89>



Number 4

The European Banking Authority (EBA) today published its annual Report on convergence of supervisory practices for 2022.



The common supervisory impetus across the EU met its goal for most of the supervisory priorities set in the EBA European Supervisory Examination Programme for 2022 (ESEP), although competent authorities are still in the process of building up their capacity to review the risks associated with the digital transformation and environmental, social and corporate governance (ESG).

For the EBA European Supervisory Examination Programme for 2022 (ESEP) you may visit:

<https://www.eba.europa.eu/eba-sets-examination-programme-prudential-supervisors-2022>

Contents

Abbreviations	3
Executive Summary	4
Introduction	4
Selection of the key topics	5
Key topics identified for the 2022 ESEP	7
1. Impact of the COVID-19 pandemic on asset quality and adequate provisioning	7
2. ICT security risk and ICT outsourcing risk, risk data aggregation	9
3. Digital transformation and FinTech players	10
4. ESG risk	12
5. AML/CFT	13
Further considerations	14

Competent authorities also showed ability to react to macro events that affected the financial situation of institutions under their supervision, though timely information exchange and cooperation should be enhanced. Lastly, supervisors consciously applied proportionality in their supervisory practices.

The EBA's 2022 ESEP introduced 5 key topics for supervisory attention throughout the EU, namely the impact of the COVID-19 pandemic on asset

quality, ICT, digital transformation, as well as ESG and Money Laundering/Terrorist Financing (ML/TF) risks.

In 2022, a step forward was made in the supervision of sound lending standards and practices. Supervisory attention in relation to asset quality and non-performing exposures shifted from the monitoring of the implications of the COVID-19 pandemic to the monitoring of the consequences of the Russian invasion of Ukraine and the changed macroeconomic environment.

ICT security and outsourcing risks are followed closely by competent authorities and supervisory colleges, and weaknesses identified need close supervisory attention as they are still considered as high. Competent authorities, overall, were not yet engaged in a comprehensive review of the digital transformation strategies and their implementation by institutions.

Environmental and climate risks are increasingly part of the supervisory activities, but the depth of supervisory assessments depends on how institutions have integrated ESG risk in their business strategies, risk appetite and loan origination practices and their risk, governance and reporting framework.

ML/TF risks are consistently high and thus covered by most competent authorities and supervisory colleges, however full incorporation in the Supervisory Review and Evaluation Process (SREP) is expected during 2023 with the implementation of the revised SREP Guidelines.

In addition, the EBA concluded that supervisors consciously applied proportionality in their supervisory practices, either in the identification of the set of institutions to review or in the level of the assessment performed.

The interactions and the organisation of the supervisory colleges were overall of a high quality, although improvements in few procedural aspects of joint decisions will still be sought. Also, the EBA found that cooperation and timely information exchange in supervisory colleges should improve when crisis events materialise, also to detect potential emerging risks.

Note

According to Article 1(5)(g) and 29 of its founding Regulation, the EBA shall contribute to enhancing supervisory convergence across the European Union and it shall play an active role in building a common supervisory culture and ensuring the consistent application of the Single Rulebook.

Particularly in the context of the SREP, the EBA shall annually report to the European Parliament and the Council on the degree of convergence of the application of the SREP and supervisory measures as mandated by Article 107 of the Capital Requirements Directive (CRD).

The EBA proactively drives the convergence in supervisory practices through the selection of topics deserving European traction based on its expertise in EU-wide risk analysis, policy development and practical experience of competent authorities, and its role in supervisory colleges by establishing yearly the ESEP. The EBA then assesses whether and how the selected topics are covered in competent authorities' supervisory priorities and activities, including the SREP and in the context of supervisory colleges.

In its 2023 ESEP for prudential supervisors, the EBA set out its supervisory priorities for 2023, including those needing continued attention, and will report on their implementation in its 2023 convergence report. In addition, it is the EBA's common practice to integrate the results of the monitoring activities in its policy work and training activities.

To read more:

<https://www.eba.europa.eu/eba-notes-eu-wide-consistent-implementation-2022-priorities-supervisory-work-programmes-and-further>



Number 5

In crisis and emergency, compulsory license on patents
Proposal for a regulation on compulsory licensing for crisis management (the Compulsory Licensing Regulation).

*Reasons for and objectives of the proposal*

Intangible assets such as inventions, trade secrets and know-how are the cornerstone of the EU economy and competitiveness.

Patent rights, in particular, play a key role in supporting EU innovation and creating the right environment for investment.

For European innovation to flourish, a solid, predictable, and flexible legal framework for intellectual property rights, including patents, needs to be created.

The Unitary Patent system helps further improve and harmonise the EU legal framework on patents.

Beyond this, the Commission action plan on intellectual property rights has identified several areas of patent law that need to be further improved and harmonised.

One of these areas is compulsory licensing. The COVID-19 crisis highlighted that an appropriate balance between patent rights and other rights and interests is a staple of the patent system.

During the COVID-19 crisis, the conflicting interests were access to health products and preserving innovation incentives that are key to developing new health products, such as vaccines and therapeutics.

The pandemic added another element to the discussion: the role intellectual property rights could and should play in a crisis.

In other words, the question became: how we can preserve the balance and incentives for innovation while ensuring swift access to critical products and technologies in crises, even in the absence of voluntary agreements. Patent law already provides a solution: compulsory licensing.

A compulsory license is the possibility for a government to allow a third party to use a patent without the authorisation of the rights-holder, subject to certain conditions.

Compulsory licensing can therefore complement current EU efforts to improve its resilience to crises.

In the aftermath of the COVID-19 crisis, the EU has tabled several EU crisis instruments, such as the Proposal for a Regulation establishing a Single Market Emergency Instrument (SMEI) or Council Regulation (EU) 2022/2372 of 24 October 2022 on a framework of measures for ensuring the supply of crisis-relevant medical countermeasures in the event of a public health emergency at Union level.

These instruments provide the EU with a means of ensuring access to products needed to tackle a crisis in the Internal Market. The instruments focus on voluntary approaches.

As evidenced by the COVID-19 crisis, voluntary agreements remain the most efficient tool to enable rapid manufacturing of patent-protected products, including in crises. However, there may be cases where such voluntary agreements are not available or appropriate.

In such circumstances, compulsory licensing can provide a solution to allow the rapid manufacturing of products needed to tackle a crisis. However, to guarantee that such products can freely circulate within the Internal Market and reach all those in need, the compulsory licensing shall be granted at EU level.

Compulsory licensing has a dual role, as it can incentivise the conclusion of voluntary agreements and also enable the manufacturing of products needed to tackle a crisis in the absence of (appropriate) voluntary agreements. However, for compulsory licensing to fulfil this role, an efficient compulsory licensing scheme needs to be built in the EU, able to rely on the Single Market, complementing EU crisis instruments and in line with the EU's international obligations.

The Agreement on Trade-Related Aspects of Intellectual Property Rights ('TRIPS Agreement') sets the international legal framework on compulsory licensing.

Article 31 of the TRIPS Agreement provides the framework for compulsory licensing in relation to the domestic market, while Article 31bis of the TRIPS Agreement provides the rules for compulsory licensing for the manufacturing and export of pharmaceutical products to countries with public health problems.

There is currently no EU-wide harmonisation of compulsory licensing for the domestic market, including as regards European patents with a unitary

effect. Instead, there is a patchwork of different national rules and procedures on compulsory licensing.

National rules have insufficient territorial reach, since products manufactured under a compulsory license in one Member State either cannot be supplied to another Member State, or can only be supplied in limited quantities.

National procedures are also different from each other, and decision-making is not coordinated at EU level. This limits the ability to rely on the Internal Market to guarantee supplies across all the Union territory.

Against this background, this initiative aims to provide the Internal Market with an efficient compulsory licensing scheme for crisis management.

The initiative has therefore two main objectives.

First, it aims to enable the EU to rely on compulsory licensing in the context of the EU crisis instruments.

Second, it introduces an efficient compulsory licensing scheme, with appropriate features, to allow a swift and appropriate response to crises, with a functioning Internal Market, guaranteeing the supply and the free movement of crisis-critical products subject to compulsory licensing in the internal market.

Article 1

Subject matter

This Regulation has the objective to ensure that in crises the Union has access to crisis-relevant products. To this end, this Regulation lays down rules on the procedure and conditions for the granting of a Union compulsory licence of intellectual property rights that are necessary for the supply of crisis-relevant products to the Member States in the context of a Union crisis or emergency mechanism.

Article 2

Scope

1. This Regulation establishes Union compulsory licensing of the following intellectual property rights in force in one or more Member States:
 - (a) patents, including published patent applications;
 - (b) utility models; or
 - (c) supplementary protection certificates;

To read more:

https://single-market-economy.ec.europa.eu/system/files/2023-04/COM_2023_224_1_EN_ACT_part1_v11.pdf



*Number 6***G20 TechSprint 2023 - Transforming cross border payments**

The fourth and 2023 TechSprint is a joint initiative between the BIS Innovation Hub and Reserve Bank of India.



Following the success of the three previous competitions in the areas of regulatory compliance (regtech) and supervision (suptech), green and sustainable finance and central bank digital currencies (CBDCs), the 2023 TechSprint will focus on three problem statements on cross-border payments formulated by the RBI and the BIS Innovation Hub.

1. Technology solutions to reduce illicit finance risk around anti-money laundering, countering the financing of terrorism and sanctions.
2. Foreign exchange and liquidity technology solutions to enable settlement in emerging market and developing economy currencies.
3. Technology solutions for multilateral cross-border central bank digital currency platforms.

The detailed problem statements are available at:

<https://hackolosseum.apixplatform.com/h1/g20techsprint2023>

To read more: https://www.bis.org/hub/2023_g20_techsprint.htm

Reserve Bank of India and Bank for International Settlements invite cross-border payments solutions for G20 Techsprint

- The Reserve Bank of India (RBI) and the Bank for International Settlements (BIS) are launching the fourth G20 TechSprint hackathon for global innovators.
- The 2023 global competition is seeking solutions to improve cross-border payments.
- Open to developers worldwide, competition will conclude in Q3 2023.

The RBI and the BIS jointly launched the fourth edition of the G20 TechSprint Initiative, a global technology competition to promote

innovative solutions aimed at improving cross-border payments, under India's G20 presidency.

Following the success of the three previous competitions in the areas of regulatory compliance (regtech) and supervision (suptech), green and sustainable finance, and central bank digital currencies (CBDCs), the 2023 TechSprint will focus on three problem statements on cross-border payments, as formulated by the RBI and the BIS Innovation Hub.

- Technology solutions to reduce illicit finance risk around anti-money laundering, countering the financing of terrorism and sanctions.
- Foreign exchange and liquidity technology solutions to enable settlement in emerging market and developing economy currencies.
- Technology solutions for multilateral cross-border central bank digital currency platforms.

“ There is a need to explore solutions to improve efficiency in the cross-border payments space. The time is opportune for innovative tech-based solutions facilitated through standardised protocols and arrangements among nations to solve this problem. There have been increased efforts from RBI, but such efforts need to be expanded and scaled up. When payments across borders become efficient, economic linkages, economic cooperation and economic activities across borders become easier, effective and efficient. ”

T Rabi Sankar, Deputy Governor, RBI

“ While preserving financial integrity, payments should be able to flow seamlessly across borders and between payment systems to promote competition. The BIS Innovation Hub has been working closely with our global membership to experiment with different innovative solutions to improve many of its known issues. By leveraging the important work of the G20 cross-border payments programme, this TechSprint will make an important contribution to this effort, which ultimately aims to improve people's lives all over the world. ”

Cecilia Skingsley, Head of the BIS Innovation Hub



*Number 7***Sweep Targets Darknet Markets**

Operation SpecTor spanned three continents, seized millions of dollars, and removed tens of thousands of potentially lethal drugs from circulation



A massive coordinated operation spanning nine countries and dozens of law enforcement agencies across the United States, Europe, and South America targeting darknet drug markets culminated recently with seizures of more than \$50 million in cash and virtual currency, 1,875 pounds of potentially lethal pills and other drugs, and 288 arrests.

Operation SpecTor uncovered vast networks of manufacturers, online supply chains, buyers, re-sellers, and users, revealing that the darknet—a part of the internet accessible through an encrypted browser—provides only a veneer of anonymity.

The drug seizures included about 152 pounds of fentanyl, a synthetic opioid so dangerous that two milligrams—like a few grains of salt—is a potentially lethal dose.

"The availability of dangerous substances like fentanyl on darknet marketplaces is helping to fuel the crisis that has claimed far too many

American lives, “ FBI Director Christopher Wray said in a statement. “That's why we will continue to join forces with our law enforcement partners around the globe to attack this problem together.”

The operation began in late 2021. The Joint Criminal and Opioid Darknet Enforcement (JCODE) team, which the Department of Justice created in 2018, led the effort. The team coordinates complex, multi-agency investigations into virtual marketplaces selling dangerous and illegal drugs around the globe. The FBI was among 12 U.S. agencies working with local partners in the operation.

Overseas, the Bureau worked closely with authorities in Brazil and Europol (which provides investigative support to European law enforcement agencies) to conduct 135 arrests and seize more than \$38 million.

“These darknet marketplaces and vendors are not limited by geographical boundaries, requiring us to work closely with our international partners,” said Kristen Varel, a supervisory special agent in the FBI’s High Tech Organized Crime Unit, which coordinates the JCODE operations. “We focus on those vendors operating on U.S. soil, but we also investigate the marketplace infrastructure, which is frequently located overseas, often in European countries.”

To read more:

<https://www.fbi.gov/news/stories/operation-spector-targets-darknet-markets>



Number 8

Using math to map social connections



Imagine being able to predict how a group of people will behave before they even know it themselves. From the dynamics of a sports team to the complexities of a nation, the ability to anticipate human interactions has long been a goal of scientists and analysts. Now, a team of researchers at Sandia National Laboratories is pioneering a new approach to social analysis.

Sandia cybersecurity expert Mike Brzustowicz believes a well-known mathematical function may provide the key to predicting that level of social interaction.

“The Fourier transform is a mathematical principle that very simply tells you the frequency — the count — of things that you’re observing. A famous use of the principle is transforming sound waves and time into frequency,” Brzustowicz explained.

“We are working with the non-Abelian Fourier transform. This is a totally different thing. It tells you about combinations of entities. So instead of understanding what individual things are happening, it tells you what connections exist between groups of things.”



Nonabelian Fourier Transforms: A Path to Solving Epistasis

The work builds upon what was started with one of Brzustowicz’s collaborators, David Uminsky. Uminsky began the work at the University of San Francisco when trying to analyze genetic sequences and identify mutations. You may visit:

https://research.latinxinai.org/papers/neurips/2018/slides/Slide_David_Uminsky.pdf



Eventually Uminsky and his team reached a point where they lacked the computing power to analyze large number sets and needed the computational capability that Sandia can offer.

“When you talk about a combination of things, there are almost infinitely many combinations of very small groups,” Brzustowicz explained. “The basketball team idea is something my collaborator David Uminsky published a long time ago: There are 15 players on the bench and there are five on the floor at a time. And then with those five on the floor, you look at thousands of combinations of the different players.”

But that is a small system to look at when compared to a community, a state or a nation, or groups of people that are not even geographically related. “Ten years ago, it took forever to process that on a computer, and now it takes me like a second. But when you think of a social network, you may be thinking of hundreds or thousands of people,” Brzustowicz said.

“If you have 20 people together or 30 people, there are so many possible group combinations. You couldn’t maybe write them all down because you wouldn’t have enough memory on your computer, or you wouldn’t be able to annotate them. If we wanted to look at social networks and understand how subgroups interact with social networks, we’re barely getting there. So that’s our challenge.”

Now Brzustowicz and his team are trying to figure out how big a transform they can compute, and what kinds of groups they can predict.

“We’re already doing stuff that’s really cool,” Brzustowicz said. “It’s enviable that we can get to this level, but if we can go further, you know, like no one’s doing this, the non-Abelian Fourier transform.”

He added that Sandia is ideally positioned to figure out where the math goes next.

“I think that’s what the national labs are good at,” Brzustowicz concluded. “We’re not academics, we’re not industry. We’re not bound by those two extremes, bounded by ‘what can you do that will get published’ and bound by, ‘does this make the submit button at Google work better, or make the timeline at Facebook more appealing?’ We’re in the middle where we solve practical problems, but we have these huge resources available to us.”

To read more: https://newsreleases.sandia.gov/social_connections/



Number 9

Meta's Q1 2023 Security Reports: Protecting People and Businesses

Guy Rosen, Chief Information Security Officer



Takeaways

1. As part of our quarterly integrity reporting, we're sharing Q1 updates on our work to combat a range of threats.
2. We detected and took action against malware campaigns targeting people and businesses online, shared our findings with other technology companies and rolled out new security features to help protect people.
3. We took actions against nine separate adversarial networks around the world for engaging in covert influence operations and cyber espionage, and shared our threat insights with industry peers, researchers and governments.

We know that safety and security are top of mind for people using our apps, including businesses and advertisers. Today, as part of our quarterly integrity reporting, we're sharing updates on our work to combat a range of threats, including covert influence operations, cyber espionage and malware campaigns.

In my first year as Meta's chief information security officer, my focus has been bringing together teams working on integrity, security, support, and operations so that we can work together in the most effective way possible.

Each of these efforts has been ongoing for many years, and a key focus for us has been sharing progress, bringing in outside experts and working with other companies to tackle industry-wide threats.

It's been more than 10 years since our bug bounty program began working with the security research community, 10 years since we first published transparency reports on government data requests, over five years since we started sharing takedowns of covert influence operations and five years since we published our first community standards enforcement report.

We've learned a lot through this work, including the importance of sharing both qualitative and quantitative insights into our integrity work. And it's

been encouraging to see our peers join us in expanding their trust and safety reporting. We're committed to continuing these efforts, and today's updates are good examples of this work.

Countering Malware Campaigns Across the Internet

My teams track and take action against hundreds of threat actors around the world, including malware campaigns. Here are a few things that stood out from our latest malware work.

First, our threat research has shown time and again that malware operators, just like spammers, are very attuned to what's trendy at any given moment. They latch onto hot-button issues and popular topics to get people's attention. The latest wave of malware campaigns have taken notice of generative AI technology that's captured people's imagination and excitement.

Since March alone, our security analysts have found around 10 malware families posing as ChatGPT and similar tools to compromise accounts across the internet. For example, we've seen threat actors create malicious browser extensions available in official web stores that claim to offer ChatGPT-related tools.

In fact, some of these malicious extensions did include working ChatGPT functionality alongside the malware. This was likely to avoid suspicion from the stores and from users.

We've detected and blocked over 1,000 of these unique malicious URLs from being shared on our apps, and reported them to our industry peers at file-sharing services where malware was hosted so they, too, can take appropriate action.

This is not unique to the generative AI space. As an industry, we've seen this across other topics popular in their time, such as crypto scams fueled by the interest in digital currency. The generative AI space is rapidly evolving and bad actors know it, so we should all be vigilant.

Second, we've seen that our and industry's efforts are forcing threat actors to rapidly evolve their tactics in attempts to evade detection and enable persistence.

One way they do this is by spreading across as many platforms as they can to protect against enforcement by any one service. For example, we've seen malware families leveraging services like ours and LinkedIn, browsers like Chrome, Edge, Brave and Firefox, link shorteners, file-hosting services like

Dropbox and Mega, and more. When they get caught, they mix in more services including smaller ones that help them disguise the ultimate destination of links.

Another example is when some malware families masquerading as ChatGPT apps switched their lures to other popular themes like Google's Bard or TikTok marketing support, in response to detection.

These changes are likely an attempt by threat actors to ensure that any one service has only limited visibility into the entire operation. When bad actors count on us to work in silos while they target people far and wide across the internet, we need to work together as an industry to protect people.

That's why we designed our threat research to help us scale our security work in a number of ways — it disrupts malicious operations on our platform and helps inform our industry's defenses against threats that rarely target one platform. The insights we gain from this research help drive our continuous product development to protect people and businesses.

In the months and years ahead, we'll continue to highlight how these malicious campaigns operate, share threat indicators with our industry peers and roll out new protections to address new tactics. For instance, we're launching a new support flow for businesses impacted by malware. Read more about our work to help businesses stay safe on our apps.

Disrupting Cyber Espionage and Covert Influence Operations

In today's Q1 Adversarial Threat report, we shared findings about nine adversarial networks we took action against for various security violations.

Six of these networks engaged in coordinated inauthentic behavior (CIB) that originated in the US, Venezuela, Iran, China, Georgia, Burkina Faso and Togo, and primarily targeted people outside of their countries. We removed the majority of these networks before they were able to build authentic audiences.

Nearly all of them ran fictitious entities — news media organizations, hacktivist groups and NGOs — across the internet, including on Facebook, Twitter, Telegram, YouTube, Medium, TikTok, Blogspot, Reddit, WordPress, Freelancer[.]com, hacking forums and their own websites.

Half of these operations were linked to private entities including an IT company in China, a US marketing firm and a political marketing consultancy in the Central African Republic.

We also disrupted three cyber espionage operations in South Asia, including an advanced persistent threat (APT) group we attributed to state-linked actors in Pakistan, a threat actor in India known in the security industry as Patchwork APT, and the threat group known as Bahamut APT in South Asia.

Each of these APTs relied heavily on social engineering to trick people into clicking on malicious links, downloading malware or sharing personal information across the internet.

This investment in social engineering meant that these threat actors did not have to invest as much on the malware side. In fact, for at least two of these operations, we saw a reduction in the malicious capabilities in their apps, likely to ensure they can be published in official app stores.

In response to the security community continuing to disrupt these malicious efforts, we've seen these APTs to be forced to set up new infrastructure, change tactics and invest more in hiding and diversifying their operations, which likely degraded their operations. Read more about this threat research in our Q1 Adversarial Threat Report (at Number 10, below).

To read more:

<https://about.fb.com/news/2023/05/metasp-q1-2023-security-reports/>



Number 10

Quarterly Adversarial Threat Report



Our public threat reporting began about six years ago when we first shared our findings about [coordinated inauthentic behavior \(CIB\)](#) by a Russian influence operation.

Since then, we have expanded our ability to respond to a wider range of adversarial behaviors as global threats have continued to evolve.

To provide a more comprehensive view into the risks we tackle, we've also expanded our regular threat reports to include cyber espionage and other emerging threats — all in one place, as part of the quarterly reporting series.

In addition to sharing our analysis and threat research, we're also publishing threat indicators to contribute to the efforts by the security community to detect and counter malicious activity elsewhere on the internet (See Appendix).

We expect the make-up of these reports to continue to evolve in response to the changes we see in the threat environment and as we expand to cover new areas of our Trust & Safety work.

This report is not meant to reflect the entirety of our security enforcements, but to share notable trends and investigations to help inform our community's understanding of the evolving security threats we see.

We welcome ideas from our peers across the defender community to help make these reports more informative, and we'll adjust as we learn from feedback.

For a quantitative view into our Community Standards' enforcement, including content-based actions we've taken at scale and our broader integrity work, please visit Meta's Transparency Center here:

<https://transparency.fb.com/data/>

Summary of our findings

1. Our quarterly threat report provides a view into the risks we see across multiple adversarial behaviors including CIB and cyber espionage.

2. We took action against three cyber espionage operations in South Asia. One was linked to a group of hackers known in the security industry as Bahamut APT (advanced persistent threat), the other to the group known as Patchwork APT and one to the state-linked actors in Pakistan. Here is what stood out from our threat research (See Section 1 for details):

2a. Diversifying social engineering efforts: These APTs relied heavily on social engineering and invested in making some of their fake accounts into more varied and elaborate fictitious personas with backstops across the internet so they can withstand scrutiny by their targets, platforms and researchers.

While we saw them continue using traditional lures like women looking for a romantic connection, they also developed personas posing as recruiters, journalists or military personnel.

2b. Continued reliance on low-sophistication malware: This investment in social engineering to trick people into clicking on malicious links or sharing sensitive information means that threat actors did not have to invest as much on the malware side.

In fact, our investigations showed that cheaper, low-sophistication malware can be effective in targeting people when used together with social engineering. For at least two of these operations, we observed a reduction in the malicious capabilities in their apps, likely to ensure they can be published in official app stores.

2c. Impact of public disruptions and threat reporting: As the security community continued to disrupt these APTs, they have been forced to set up new infrastructure, change tactics, and invest more in hiding and diversifying their operations in order to persist, which likely degraded their operations.

3. In our Q1 Adversarial Threat report, we're sharing findings about six separate covert influence operations we took down for violating our policy against CIB. They originated in the United States and Venezuela, Iran, China, Georgia, Burkina Faso and Togo.

More than half of them targeted audiences outside of their countries. We removed the majority of these networks before they were able to build authentic audiences. Here is what stood out from our CIB threat research (See Section 2 for details):

4. Creating fictitious entities across the internet: In an attempt to build credibility, nearly all of these operations invested in creating fictitious entities across the internet, including news media organizations, hacktivist groups, and NGOs.

They operated on many platforms, including on Facebook, Twitter, Telegram, YouTube, Medium, TikTok, Blogspot, Reddit, Wordpress, freelancer[.]com, hacking forums and their own websites.

5. Fake hacktivists from Iran: The operation from Iran posted claims of having hacked organizations in Israel, Bahrain and France, including news media, logistics and transport companies, educational institutions, an airport, a dating service and a government institution.

Some of these individual claims have been reported by the press in these countries, but we cannot confirm if any of them are credible. This is not the first time an Iran-origin operation claimed to have hacked government systems; a similar claim was promoted by another CIB network we removed ahead of the US 2020 election.


6. For-hire operations: As we called out in our past reporting, we continue to see for-hire organizations behind covert influence operations globally, with half of the operations in this report attributed to private entities. This included an IT company in China, a marketing firm in the United States and a political marketing consultancy in the Central African Republic.

7. The evolution of China-origin operations: Finally, this report brings the total of the China-origin CIB networks we removed since 2017 to six, with half of them reported in the last seven months.

These latest takedowns signal a shift in the nature of the China-based CIB activity we've found with new threat actors, novel geographic targeting, and new adversarial tactics. Yet, we continue to find and remove them before they are able to build their audience.


These latest networks experimented with a range of tactics we haven't seen in China-based operations before (though we've observed them elsewhere over the years, including in operations linked to troll farms, and marketing and PR firms).

The latest behaviors included creating a front media company in the West, hiring freelance writers around the world, offering to recruit protesters, and co-opting an NGO in Africa.

M  **MOVIE DATE**


[HOME](#) [ABOUT](#) [WORKING](#) [REVIEWS](#) [CONTACT US](#)

Host a **MOVIE DATE** with friends while social distancing




Movie Date is an entertainment app that provides you the comfort of cinema at home absolutely free of charge!


[DOWNLOAD](#)

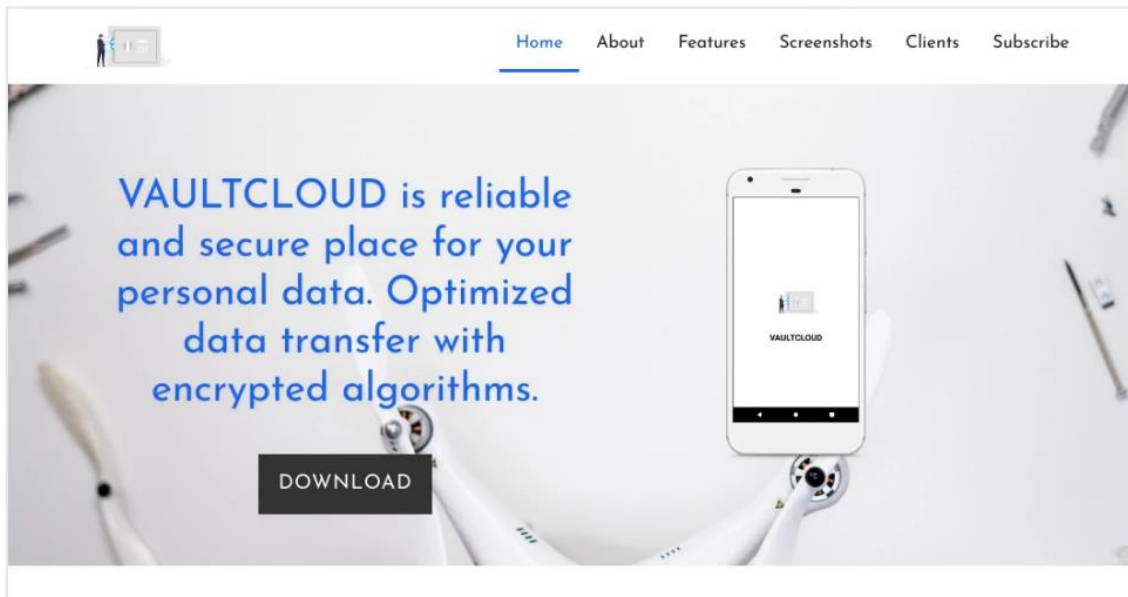
 **CV**
WRITER

[DOWNLOAD](#) [ABOUT US](#) [OUR CLIENTS](#) [OUR WORK](#) [CONTACT US](#)



Upgrade Your CV Upgrade Your Career.





Coordinated inauthentic behavior (CIB)

We view CIB as coordinated efforts to manipulate public debate for a strategic goal, in which fake accounts are central to the operation. In each case, people coordinate with one another and use fake accounts to mislead others about who they are and what they are doing. When we investigate and remove these operations, we focus on behavior rather than content — no matter who's behind them, what they post or whether they're foreign or domestic.

Continuous CIB enforcement: We monitor for efforts to come back by the networks we previously removed. Using both automated and manual detection, we continuously remove accounts and Pages connected to networks we took down in the past.

The report:

<https://about.fb.com/wp-content/uploads/2023/05/Meta-Quarterly-Adversarial-Threat-Report-Q1-2023.pdf>



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 prejudice 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 prejudice the interpretation that the Courts might place on the matters at issue.

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

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

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

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

International Association of Risk and Compliance Professionals (IARCP)

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](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](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,
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,
- a Travel Security Trained Professional (TSecTPro).

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 32 countries.

Companies and organizations around the world consider the CRCMP a preferred certificate:

Senior Information Security Risk Analyst

Public Company Accounting Oversight Board - ★★★★★ 10 reviews - Washington, DC

Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...

www.simplyhired.com/search?q=crcmp&job=BY_s7GxAbt4KwSJ_aJA_4KaruYRQSQ



Crcmp jobs

Sort by

Date Added

More Filters

Relevance ▾

Anytime ▾

None Selected ▾

Risk Science Business Process Lead, Senior Associate

Capital One - McLean, VA

Est. \$110,000 - \$150,000 a year ⓘ

Lean, Six Sigma, BPM, PMP, PRM, or CRCMP. McLean 1 (19050), United States of America, McLean, Virginia....

Application Security Advisor-Penetration Tester

USAA - San Antonio, TX

Est. \$100,000 - \$140,000 a year ⓘ

Professional designation in CISSP, CISA, CRISC, CISM, CEH, GWAPT, GWEB, or CRCMP. Purpose of Job IMPORTANT:....



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.

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 the Travel Security Trained Professional (TSecTPro), distance learning and online certification program, you may visit:

https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm

Certified Cyber (Governance Risk and Compliance) Professionals - CC(GRC)Ps, have a 50% discount for the Travel Security Trained Professional (TSecTPro) program (\$148 instead of \$297).

You have a \$100 discount after you purchase one of our programs. The discount applies to each additional program. For example, you can purchase the CRCMP program for \$297, and then purchase the CISRCP program for \$197 (instead of \$297), the CC(GRC)P program for \$197 (instead of \$297), the CRCMP(Re)I program for \$197 (instead of \$297), and the TSecTPro program for \$197 (instead of \$297).

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