Monday, February 12, 2024

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.

I do not always agree with the judgments of the Court of Justice of the European Union, but I always comply and explain the consequences, something that all the risk and compliance professionals must do.

In Bulgaria, an entry was made in the police records concerning a person, for failing to tell the truth as a witness. That person was ultimately found guilty of that offence and given a one year suspended sentence.

After serving that sentence, that person was legally rehabilitated. He subsequently applied to be removed from the police records. Under Bulgarian law, the data relating to him are retained in those records and may be processed by the authorities, who have access to them without any time limit other than his death.

His application was rejected on the ground that a final criminal conviction, even after legal rehabilitation, is not one of the grounds for removal of the entry from the police records.

On appeal, the Bulgarian Supreme Administrative Court referred questions to the Court of Justice. In its judgment, the Court of Justice holds that the general and indiscriminate storage of biometric and genetic data of persons convicted of an intentional offence, until their death, is contrary to EU law.

Under EU law, national legislation must lay down an obligation for the data controller to review periodically whether that storage is still necessary and to grant the data subject the right to have those data erased if that is no longer the case.

In Article 4(1)(c) and 4(1)(e) of Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, we have:

Article 4(1)(c): Member States shall provide for personal data to be adequate, relevant, and not excessive in relation to the purposes for which they are processed.

Article 4(1)(e): Member States shall provide for personal data to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed.

Under EU law, national legislation must lay down an obligation for the data controller to review periodically whether that storage is still necessary and to grant the data subject the right to have those data erased if that is no longer the case.

This is an interesting judgment, from the Court of Justice of the European Union. I find interesting the fact that the police is not obliged to remove entries from the police records, but is obliged to "review periodically whether that storage is still necessary and to grant the data subject the right to have those data erased if that is no longer the case". The approach "we keep everything until you die" is not legal in the EU, but with some more paperwork we may have the same result, if necessary, of course.

Francis of Assisi has said: "Start by doing what's necessary; then do what's possible; and suddenly you are doing the impossible". This is not legal advice.

Read more at number 2 below. Welcome to the Top 10 list.

Best regards,

George Lekatis
President of the IARCP

INTERPOL

Number 7 (Page 19)

AI breakthrough creates images from nothing

Innovative framework that generates images from nothing can enable new scientific applications

Los Alamos NATIONAL LABORATORY

Number 8 (Page 21)

Former CIA Officer Joshua Adam Schulte Sentenced To 40 Years In Prison For Espionage And Child Pornography Crimes

United States Attorney's Office
Southern District of New York

Number 9 (Page 25)

AI in Support of StratCom Capabilities

Number 10 (Page 28)

U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure

Office of Public Affairs
U.S. Department of Justice

Number 1

SEC Adopts Rules to Enhance Investor Protections Relating to SPACs, Shell Companies, and Projections

The Securities and Exchange Commission adopted new rules and amendments to enhance disclosures and provide additional investor protection in initial public offerings (IPOs) by special purpose acquisition companies (SPACs) and in subsequent business combination transactions between SPACs and target companies (de-SPAC transactions).

SPAC IPOs and de-SPAC transactions can be used as a means for private companies to enter the public markets. Given the complexity of these transactions, the Commission seeks to enhance investor protection in SPAC IPOs and de-SPAC transactions with respect to the adequacy of disclosure and the responsible use of projections. The rules also address investor protection concerns more broadly with respect to shell companies and blank check companies, including SPACs.

“Just because a company uses an alternative method to go public does not mean that its investors are any less deserving of time-tested investor protections,” said SEC Chair Gary Gensler.

“Today’s adoption will help ensure that the rules for SPACs are substantially aligned with those of traditional IPOs, enhancing investor protection through three areas: disclosure, use of projections, and issuer obligations. Taken together, these steps will help protect investors by addressing information asymmetries, misleading information, and conflicts of interest in SPAC and de-SPAC transactions.”

The new rules and amendments require, among other things, enhanced disclosures about conflicts of interest, SPAC sponsor compensation, dilution, and other information that is important to investors in SPAC IPOs and de-SPAC transactions.

The rules also require registrants to provide additional information about the target company to investors that will help investors make more informed voting and investment decisions in connection with a de-SPAC transaction.

The rules more closely align the required disclosures and legal liabilities that may be incurred in de-SPAC transactions with those in traditional IPOs. For example, in certain situations, the rules require the target company to sign a registration statement filed by a SPAC (or another shell company) in connection with a

de-SPAC transaction. This would make the target company a "co-registrant" and assume responsibility for disclosures in that registration statement. In addition, the rules make the Private Securities Litigation Reform Act of 1995 safe harbor from liability for forward-looking statements unavailable to certain blank check companies, including SPACs.

In connection with de-SPAC transactions, the rules include disclosure requirements related to projections, including disclosure of all material bases of the projections and all material assumptions underlying the projections. The rules also update and expand guidance on the use of projections in all SEC filings.

The adopting release is published on SEC.gov and will be published in the Federal Register. You may visit:
https://www.sec.gov/files/rules/final/2024/33-11265.pdf

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 210, 229, 230, 232, 239, 240, and 249

[Release Nos. 33-11265; 34-99418; IC-35096; File No. S7-13-22]

RIN 3235-AM90

Special Purpose Acquisition Companies, Shell Companies, and Projections

AGENCY: Securities and Exchange Commission.

ACTION: Final rules; guidance.

SUMMARY: The Securities and Exchange Commission ("Commission") is adopting rules intended to enhance investor protections in initial public offerings by special purpose acquisition companies (commonly known as SPACs) and in subsequent business combination transactions between SPACs and private operating companies (commonly known as de-SPAC transactions).

The rules will become effective 125 days after publication in the Federal Register.

Compliance with the structured data requirements, which require tagging of information disclosed pursuant to new subpart 1600 of Regulation S-K in Inline XBRL, will be required 490 days after publication of the rules in the Federal Register.

To read more: https://www.sec.gov/news/press-release/2024-8

Number 2

Judgment of the Court in Case C-118/22

Right to erasure: the general and indiscriminate storage of biometric and genetic data of persons convicted of criminal offences, until their death, is contrary to EU law

COURT OF JUSTICE
OF THE EUROPEAN UNION

In Bulgaria, an entry was made in the police records concerning a person in the course of a criminal investigation for failing to tell the truth as a witness.

That person was ultimately found guilty of that offence and given a one year suspended sentence.

After serving that sentence, that person was legally rehabilitated. He subsequently applied to be removed from the police records.

Under Bulgarian law, the data relating to him are retained in those records and may be processed by the authorities, who have access to them without any time limit other than his death.

His application was rejected on the ground that a final criminal conviction, even after legal rehabilitation, is not one of the grounds for removal of the entry from the police records.

On appeal, the Bulgarian Supreme Administrative Court referred questions to the Court of Justice.

In its judgment, the Court of Justice holds that the general and indiscriminate storage of biometric and genetic data of persons convicted of an intentional offence, until their death, is contrary to EU law.

The Court notes that the personal data stored in the police records in Bulgaria include, amongst other things, fingerprints, a photograph and a DNA sample taken for profiling purposes.

The records also contain data relating to the criminal offences committed by the data subject and to his or her convictions in that regard.

Those data may be essential for the purposes of verifying whether the data subject is involved in criminal offences other than that in respect of which he or she was convicted by final judgment.

However, such persons do not all present the same degree of risk of being involved in other criminal offences, justifying a uniform period of storage of the data relating to them. Thus, factors such as the nature and seriousness of the offence committed or the absence of recidivism may mean that the risk

represented by the convicted person does not necessarily justify the storage of the data relating to that person in the police records until his or her death.

Consequently, that time limit is appropriate only in specific circumstances which duly justify it. That is not the case where it is applicable generally and indiscriminately to any person convicted by final judgment of an intentional offence.

Under EU law, national legislation must lay down an obligation for the data controller to review periodically whether that storage is still necessary and to grant the data subject the right to have those data erased if that is no longer the case.

To read more:
https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-01/cp240020en.pdf

https://curia.europa.eu/juris/documents.jsf?num=C-118/22

Number 3

Artificial intelligence in central banking

Douglas Araujo, Sebastian Doerr, Leonardo Gambacorta, Bruno Tissot

BIS

Key takeaways

1. Central banks have been early adopters of machine learning techniques for statistics, macro analysis, payment systems oversight and supervision, with considerable success.

2. Artificial intelligence brings many opportunities in support of central bank mandates, but also challenges – some general and others specific to central banks.

3. Central bank collaboration, for instance through knowledge-sharing and pooling of expertise, holds great promise in keeping central banks at the vanguard of developments in artificial intelligence.

Long before artificial intelligence (AI) became a focal point of popular commentary and widespread fascination, central banks were early adopters of machine learning methods to obtain valuable insights for statistics, research and policy (Doerr et al (2021), Araujo et al (2022, 2023)).

The greater capabilities and performance of the new generation of machine learning techniques open up further opportunities. Yet harnessing these requires central banks to build up the necessary infrastructure and expertise.

Central banks also need to address concerns about data quality and privacy as well as risks emanating from dependence on a few providers.

This Bulletin first provides a brief summary of concepts in the machine learning and AI space. It then discusses central bank use cases in four areas:

(i) information collection and the compilation of official statistics;

(ii) macroeconomic and financial analysis to support monetary policy;

(iii) oversight of payment systems; and (iv) supervision and financial stability.

The Bulletin also summarises the lessons learned and the opportunities and challenges arising from the use of machine learning and AI.

It concludes by discussing how central bank cooperation can play a key role going forward.

Overview of machine learning methods and AI

Broadly speaking, machine learning comprises the set of techniques designed to extract information from data, especially with a view to making predictions.

Machine learning can be seen as an outgrowth of traditional statistical and econometric techniques, although it does not rely on a pre-specified model or on statistical assumptions such as linearity or normality.

The process of fitting a machine learning model to data is called training.

The criterion for successful training is the ability to predict outcomes on previously unseen ("out-of-sample") data, irrespective of how the models predict them.

This section describes some of the most common techniques used in central banks, based on the regular stocktaking exercises organised in the central banking community under the umbrella of the BIS Irving Fisher Committee on Central Bank Statistics (IFC).

To read more: https://www.bis.org/publ/bisbull84.pdf

Number 4

The European Supervisory Authorities (ESAs) recommend steps to enhance the monitoring of BigTechs' financial services activities

The European Supervisory Authorities (EBA, EIOPA and ESMA) published a Report setting out the results of a stocktake of BigTech direct financial services provision in the EU.

Table 1: Stocktake results: MAGs as electronic money institutions (EMI), payment institutions (PI), credit institutions (CI), insurance intermediaries/undertakings.

	Group	Subsidiary	Home MS	Host MS
E-Money Institutions	**Alphabet (Google)**	Google Payment Lithuania UAB	LT	12
	Meta Platforms (Facebook)	Facebook Payments International Limited	IE	14
	Amazon	Amazon Payment Europe SCA	LU	16
	Alibaba (Ant Group)	Alipay (Europe) Limited S.A.	LU	4
	Uber	Uber Payments B.V.	NL	10
	NTT Docomo	DOCOMO Digital Payment Services AG	LI*	3
Payment I	**Alphabet (Google)**	Google Payment Ireland Limited	IE	13
	Tencent	Wechat	NL	2
Credit I	**Orange**	Orange Bank	FR	3
	Rakuten	Rakuten Europe Bank S.A.	LU	13
Insurance	**Tesla**	Tesla Insurance ltd (undertaking)	MT	1
	Vodafone	Vodafone Insurance Limited (undertaking)	MT	9
	Amazon	Amazon EU Sarl (intermediary)	LU	2
	Apple	Apple Distribution International (intermediary)	IE	2
	Orange	Orange Slovensko (Intermediary)	SK	/

*LI: until 1 June 2022

The Report identifies the types of financial services currently carried out by BigTechs in the EU pursuant to EU licences and highlights inherent opportunities, risks, regulatory and supervisory challenges.

The ESAs will continue to strengthen the monitoring of the relevance of BigTech in the EU financial services sector, including via the establishment of a new monitoring matrix.

In 2023 the ESAs, via the European Forum for Innovation Facilitators (EFIF), conducted a cross-sectoral stocktake of BigTech subsidiaries providing financial services in the European Union (EU) as a follow-up to the ESAs' 2022 response to the European Commission's Call for Advice on Digital Finance.

The stocktake showed that BigTech subsidiary companies currently licenced to provide financial services pursuant to EU law mainly provide services in the payments, e-money and insurance sectors and, in limited cases, the banking

sector. However, the ESAs have yet to observe their presence in the market for securities services.

JC 2024 02

01/02/2024

Report on 2023 stocktaking of BigTech direct financial services provision in the EU

Joint-ESA Report

To further strengthen the cross-sectoral mapping of BigTechs' presence and relevance to the EU's financial sector, the ESAs propose to set-up a data mapping tool within the EFIF.

This tool is intended to provide a framework that supervisors from the National Competent Authorities would be able to use to monitor on an ongoing and dynamic basis the BigTech companies' direct and indirect relevance to the EU financial sector.

Figure 1: Potential opportunities arising from intragroup dependencies

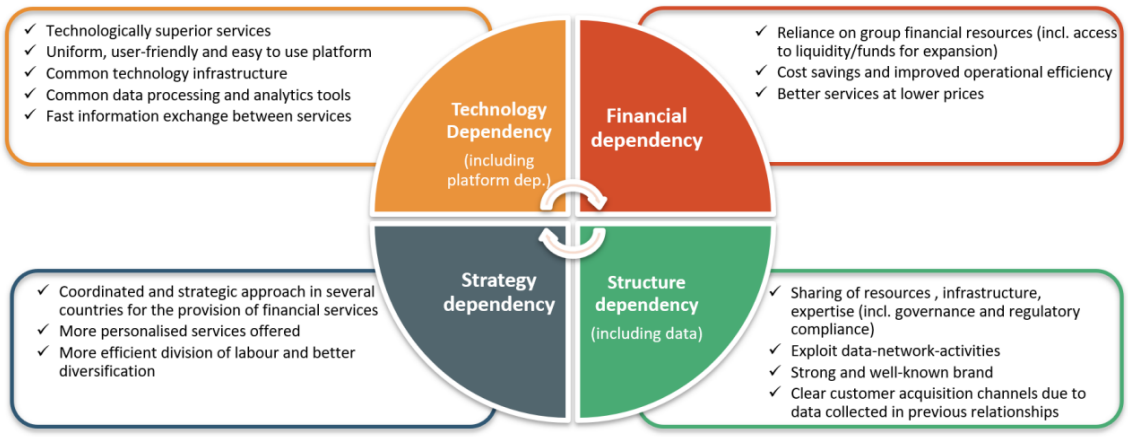
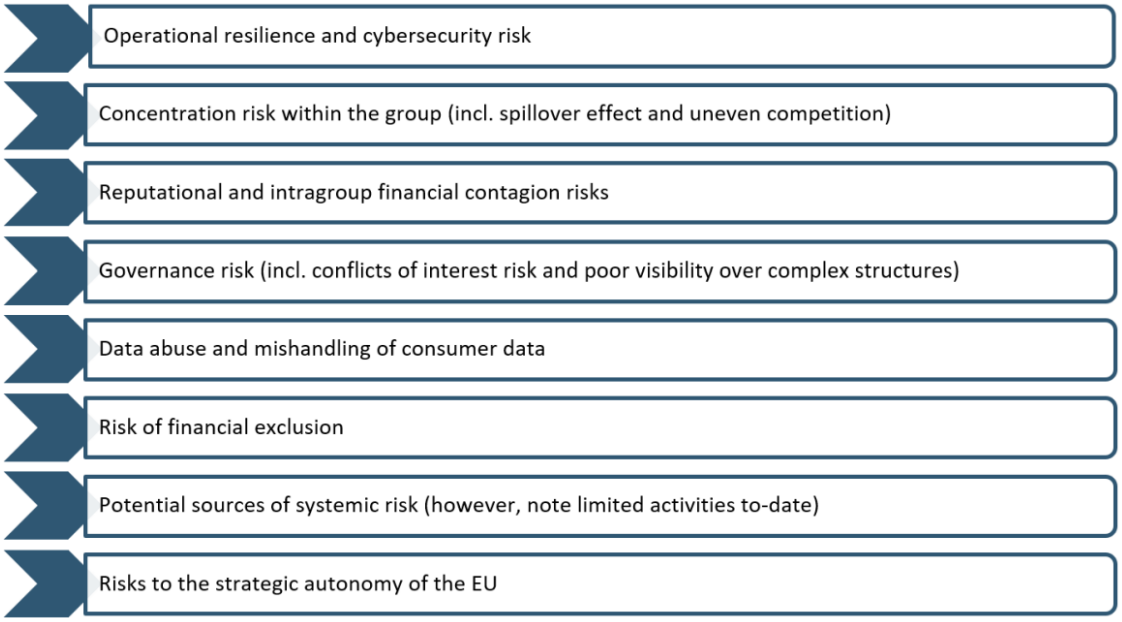


Figure 2: Potential risks arising from intragroup dependencies



The ESA will also continue the cross-disciplinary exchanges in the setting of the EFIF to further foster the exchange of information between EFIF members and other relevant financial and non-financial sector authorities involved in the monitoring of BigTechs' activities (e.g., data protection and consumer protection authorities).

To read more:
https://www.eiopa.europa.eu/system/files/2024-02/Joint%20ESAs%20Report%20-%20Stocktaking%20of%20BigTech%20direct%20financial%20services%20provision%20in%202023.pdf

Number 5

SPOTLIGHT - Insights Into the PCAOB's Interim Inspection Program Related to Audits of Broker-Dealers

There are approximately 3,400 brokers and dealers ("broker-dealers") registered with the U.S. Securities and Exchange Commission (SEC).

When these broker-dealers file their annual reports with the SEC, they are typically required to include their financial statements and supporting schedules, along with audit reports prepared by PCAOB-registered public accounting firms.

During the most recently completed inspection period, 305 PCAOBregistered firms provided audit services to broker-dealers.

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 granted the PCAOB oversight of auditors of those broker-dealers registered with the SEC that are required to file financial statements under Section 17(e)(1)(A) of the Securities and Exchange Act of 1934 ("Exchange Act") and whose financial statements are required to be certified by a registered public accounting firm.

In June 2011, the PCAOB established an interim inspection program to inspect those broker-dealer auditors and to identify and address any significant issues observed.

A key milestone in the interim inspection program was the SEC's implementation of changes to the broker-dealer financial reporting rules, which required broker-dealer audits and related attestation engagements to be performed in accordance with PCAOB standards, beginning with fiscal years ended on or after June 1, 2014.

PCAOB attestation standards, AT No. 1 and AT No. 2, set forth a framework of specific procedures that are required in order for auditors to provide their opinion or conclusion on the statements of broker-dealers as presented in compliance reports or exemption reports, in accordance with the requirements of Exchange Act Rule 17a-5.

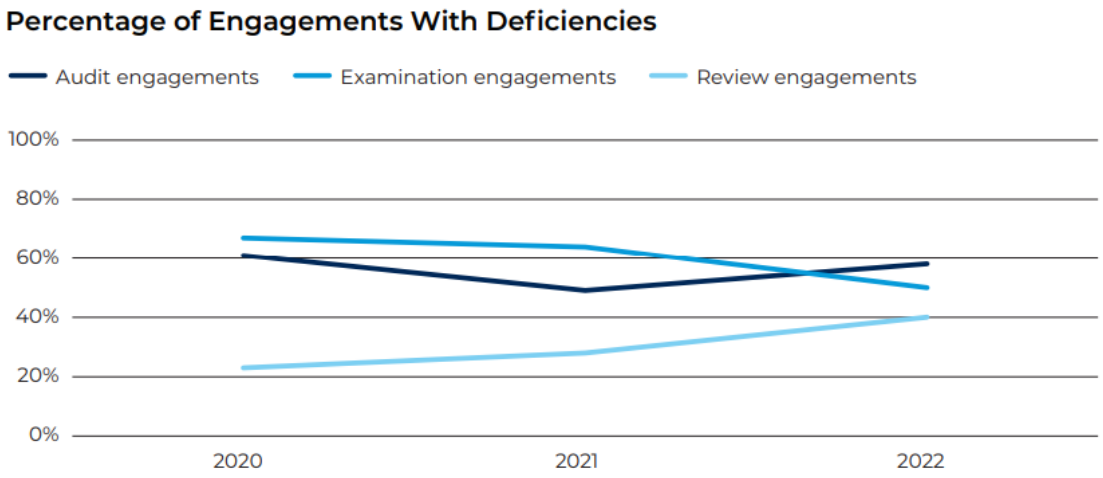
Overseeing broker-dealer audits is a key component of the PCAOB's mission to protect investors and further the public interest in the preparation of informative, accurate, and independent audit reports.

As evidenced by results from the PCAOB interim inspection program, PCAOB staff believes there is a need for significant improvement in the quality of broker-dealer audit and attestation engagements.

This Spotlight is intended to be read alongside the annual reports described in footnote 2 and provides additional insights into Inspection staff's inspection

results, including potential contributing factors to the high deficiency rates, and related reminders for auditors.

CONTENTS



To read more:
https://assets.pcaobus.org/pcaob-dev/docs/default-source/documents/2024-broker-dealer-spotlight.pdf?sfvrsn=b6f72dff_2

PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

SPOTLIGHT

Insights Into the PCAOB's Interim Inspection Program Related to Audits of Broker-Dealers

Number 6

INTERPOL-led operation targets growing cyber threats

Phishing, malware and ransomware incidents at heart of Operation Synergia

SINGAPORE – Some 1,300 suspicious IP addresses or URLs have been identified as part of a global INTERPOL operation targeting phishing, malware and ransomware attacks.

Operation Synergia, which ran from September to November 2023, was launched in response to the clear growth, escalation and professionalisation of transnational cybercrime and the need for coordinated action against new cyber threats.

The operation involved 60 law enforcement agencies from more than 50 INTERPOL member countries, with officers conducting house searches and seizing servers as well as electronic devices.

To date, 70% of the command-and-control (C2) servers identified have been taken down, with the remainder currently under investigation.

Operational details

Authorities detained 31 individuals and identified an additional 70 suspects.

- Most of the C2 servers taken down were in Europe, where 26 people were arrested.
- Hong Kong and Singapore Police took down 153 and 86 servers, respectively.
- South Sudan and Zimbabwe reported the most takedowns on the African continent, arresting four suspects.
- Bolivia mobilized a range of public authorities to identify malware and resulting vulnerabilities.
- Kuwait's worked closely with Internet Service Providers to identify victims, conduct field investigations and offer technical guidance to mitigate impacts.

Operation Synergia demonstrated how cybersecurity is most effective when international law enforcement, national authorities, and private sector partners cooperate to share best practices and pro-actively combat cybercrime.

INTERPOL and its Gateway Partners Group-IB, Kaspersky, TrendMicro, Shadowserver and Ad hoc partner Team Cymru provided analysis and intelligence support throughout the operation.

Bernardo Pillot, Assistant Director to INTERPOL Cybercrime Directorate, said: "The results of this operation, achieved through the collective efforts of multiple countries and partners, show our unwavering commitment to safeguarding the digital space. By dismantling the infrastructure behind phishing, banking malware, and ransomware attacks, we are one step closer to protecting our digital ecosystems and a safer, more secure online experience for all."

Participating countries: Albania, Algeria, Australia , Bangladesh, Belarus, Belgium, Benin, Bolivia, Bosnia and Herzegovina, Brazil, Cameroon, Canada, China, Cyprus, Czech Republic, Dominican Republic, Ecuador, Estonia, Eswatini, France, Georgia, Greece, Guyana, India, Ireland, Israel, Kuwait, Latvia, Lebanon, Lichtenstein, Maldives, Mauritius, Moldova, Nepal, Nicaragua, Nigeria, Palestine, Poland, Qatar, Russia, San Marino, Singapore, South Korea, South Sudan, Spain, Sri Lanka, Switzerland, Tanzania, Thailand, Tonga, Tunisia, Türkiye, Uganda, United Arab Emirates, Uruguay, Zimbabwe.

To read more:
https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-led-operation-targets-growing-cyber-threats

Number 7

AI breakthrough creates images from nothing

Innovative framework that generates images from nothing can enable new scientific applications

A new, potentially revolutionary artificial intelligence framework called "Blackout Diffusion" generates images from a completely empty picture, meaning that the machine-learning algorithm, unlike other generative diffusion models, does not require initiating a "random seed" to get started.

Blackout Diffusion, presented at the recent International Conference on Machine Learning, generates samples that are comparable to the current diffusion models such as DALL-E or Midjourney, but require fewer computational resources than these models.

"Generative modeling is bringing in the next industrial revolution with its capability to assist many tasks, such as generation of software code, legal documents and even art," said Javier Santos, an AI researcher at Los Alamos National Laboratory and co-author of Blackout Diffusion.

"Generative modeling could be leveraged for making scientific discoveries, and our team's work laid down the foundation and practical algorithms for applying generative diffusion modeling to scientific problems that are not continuous in nature."

Diffusion models create samples similar to the data they are trained on. They work by taking an image and repeatedly adding noise until the image is unrecognizable. Throughout the process the model tries to learn how to revert it back to its original state.

Current models require input noise, meaning they need some form of data to start producing images.

"We showed that the quality of samples generated by Blackout Diffusion is comparable to current models using a smaller computational space," said Yen Ting Lin, the Los Alamos physicist who led the Blackout Diffusion collaboration.

Another unique aspect of Blackout Diffusion is the space it works in. Existing generative diffusion models work in continuous spaces, meaning the space they work in is dense and infinite. However, working in continuous spaces limits their potential for scientific applications.

"In order to run existing generative diffusion models, mathematically speaking, diffusion has to be living on a continuous domain; it cannot be discrete," Lin said.

The theoretical framework the team developed, on the other hand, works in discrete spaces (meaning each point in the space is isolated from the others by some distance), which opens up opportunities for a variety of applications such as text and scientific applications.

The team tested Blackout Diffusion on a number of standardized datasets, including the Modified National Institute of Standards and Technology database; the CIFAR-10 dataset, which has images of objects in 10 different classes; and the CelebFaces Attributes Dataset, which consists of more than 200,000 images of human faces.

In addition, the team used the discrete nature of Blackout Diffusion to clarify several widely conceived misconceptions about how diffusion models internally, providing a critical understanding of generative diffusion models.

They also provide design principles for future scientific applications. “This demonstrates the first foundational study on discrete-state diffusion modeling and points the way toward future scientific applications with discrete data,” Lin said. The team explains that generative diffusion modeling can potentially drastically speed up the time spent running many scientific simulations on supercomputers, which would both support scientific progress and reduce the carbon footprint of computational science.

Some of the diverse examples they mention are subsurface reservoir dynamics, chemical models for drug discovery and single-molecule and single-cell gene expression for understanding biochemical mechanisms in living organisms.

To read more: https://discover.lanl.gov/news/0111-ai-breakthrough/

Number 8

Former CIA Officer Joshua Adam Schulte Sentenced To 40 Years In Prison For Espionage And Child Pornography Crimes

United States Attorney's Office
Southern District of New York

February 1, 2024 - Damian Williams, the United States Attorney for the Southern District of New York; Matthew G. Olsen, the Assistant Attorney General for National Security; and James Smith, the Assistant Director in Charge of the New York Field Office of the Federal Bureau of Investigation ("FBI"), announced that JOSHUA ADAM SCHULTE was sentenced to 40 years in prison by U.S. District Judge Jesse M. Furman for crimes of espionage, computer hacking, contempt of Court, making false statements to the FBI, and child pornography.

SCHULTE's theft is the largest data breach in the history of the CIA, and his transmission of that stolen information to WikiLeaks is one of the largest unauthorized disclosures of classified information in the history of the U.S.

This sentencing followed SCHULTE's convictions at trials that concluded on March 9, 2020, July 13, 2022, and September 13, 2023.

U.S. Attorney Damian Williams said: "Joshua Schulte betrayed his country by committing some of the most brazen, heinous crimes of espionage in American history. He caused untold damage to our national security in his quest for revenge against the CIA for its response to Schulte's security breaches while employed there.

When the FBI caught him, Schulte doubled down and tried to cause even more harm to this nation by waging what he described as an 'information war' of publishing top secret information from behind bars.

And all the while, Schulte collected thousands upon thousands of videos and images of children being subjected to sickening abuse for his own personal gratification. The outstanding investigative work of the FBI and the career prosecutors in this Office unmasked Schulte for the traitor and predator that he is and made sure that he will spend 40 years behind bars – right where he belongs."

According to court documents and evidence at trial:

From 2012 to 2016, SCHULTE was employed as a software developer in the Center for Cyber Intelligence ("CCI"), which conducts offensive cyber operations: cyber espionage relating to terrorist organizations and foreign governments.

SCHULTE and other CCI developers worked on tools that were used in, among other things, human-enabled operations: cyber operations that involved a person with access to the computer network being targeted by the cyber tool. In addition to being a developer, SCHULTE was also temporarily one of the administrators of one of the servers and suite of development programs used to build cyber tools.

In March 2016, SCHULTE was moved within branches of CCI as a result of personnel disputes between SCHULTE and another developer. Following that transfer, in April 2016, SCHULTE abused his administrator powers to grant himself administrator privileges over a development project from which he had been removed as a result of the branch change.

SCHULTE's abuse of administrator privileges was detected, and CCI leadership directed that administrator privileges would immediately be transferred from developers, including SCHULTE, to another division. SCHULTE was also given a warning about self-granting administrator privileges that had previously been revoked.

SCHULTE had, however, secretly opened an administrator session on one of the servers before his privileges were removed. On April 20, 2016, after other developers had left the CCI office, SCHULTE used his secret server administrator session to execute a series of cyber-maneuvers on the CIA network to restore his revoked privileges, break in to the backups, steal copies of the entire CCI tool development archives (the "Stolen CIA Files"), revert the network back to its prior state, and delete hundreds of log files in an attempt to cover his tracks. SCHULTE's theft of the Stolen CIA Files is the largest data breach in CIA history.

From his home computer, SCHULTE then transmitted the Stolen CIA Files to WikiLeaks, using anonymizing tools recommended by WikiLeaks to potential leakers, such as the Tails operating system and the Tor browser. On May 5, 2016, having transmitted the Stolen CIA Files to WikiLeaks, SCHULTE wiped and reformatted his home computer's internal hard drives.

On March 7, 2017, WikiLeaks began publishing classified data from the Stolen CIA Files. Between March and November 2017, there were a total of 26 disclosures of classified data from the Stolen CIA Files that WikiLeaks denominated as Vault 7 and Vault 8 (the "WikiLeaks Disclosures").

The WikiLeaks Disclosures were one of the largest unauthorized disclosures of classified information in the history of the U.S., and SCHULTE's theft and disclosure immediately and profoundly damaged the CIA's ability to collect foreign intelligence against America's adversaries; placed CIA personnel, programs, and assets directly at risk; and cost the CIA hundreds of millions of dollars. The effect was described at trial by the former CIA Deputy Director of Digital Innovation as a "digital Pearl Harbor," and the disclosure caused exceptionally grave harm to the national security of the U.S.

Following the WikiLeaks Disclosures, SCHULTE was voluntarily interviewed on multiple occasions by the FBI in March 2017. During those interviews, SCHULTE repeatedly lied, including denying being responsible for the theft of the Stolen CIA Files or for the WikiLeaks Disclosures and spinning fake narratives about ways the Stolen CIA Files could have been obtained from CIA computers, in the hope of deflecting suspicion away from SCHULTE and diverting law enforcement resources to false leads.

In March 2017, the FBI searched SCHULTE's apartment in New York pursuant to a search warrant and recovered, among other things, multiple computers, servers, and other electronic storage devices, including SCHULTE's personal desktop computer (the "Desktop Computer"), which SCHULTE built while living in Virginia and then transported to New York in November 2016.

On the Desktop Computer, FBI agents found layers of encryption hiding tens of thousands of videos and images of child sexual abuse materials, including approximately 3,400 images and videos of disturbing and horrific child pornography and the rape and sexual abuse of children as young as two years old, as well as images of bestiality and sadomasochism. SCHULTE collected some of these files during his employment with the CIA and continued to stockpile child pornography from the dark web and Russian websites after moving to New York.

While detained pending trial, in approximately April 2018, SCHULTE sent a copy of the affidavit in support of the warrant to search his apartment, which a protective order entered by the Court prohibiting SCHULTE from disseminating, to reporters from two different newspapers, and SCHULTE acknowledged in recorded phone calls that he knew he was prohibited from sharing protected material like the affidavit.

Despite being warned by the Court not to violate the protective order further, in the summer and fall of 2018, SCHULTE made plans to wage what he proclaimed to be an "information war" against the U.S. government. To pursue these ends, SCHULTE obtained access to contraband cellphones while in jail that he used to create anonymous, encrypted email and social media accounts.

SCHULTE also attempted to use the contraband cellphones to transmit protected discovery materials to WikiLeaks and planned to use the anonymous email and social media accounts to publish a manifesto and various other postings containing classified information about CIA cyber techniques and cyber tools. In a journal, SCHULTE wrote that he planned to "breakup diplomatic relationships, close embassies, [and] end U.S. occupation across the world[.]"

SCHULTE successfully sent emails containing classified information about the CCI development network and the number of employees in particular CIA cyber intelligence groups to a reporter.

As a result of this conduct, on March 9, 2020, SCHULTE was found guilty at trial of contempt of court and making material false statements.

On July 13, 2022, SCHULTE was found guilty at trial of eight counts: illegal gathering and transmission of national defense information in connection with his theft and dissemination of the Stolen CIA Files, illegal transmission and attempted transmission of national defense information, unauthorized access to a computer to obtain classified information and information from a department or agency of the U.S. in connection with his theft of the Stolen CIA Files, and two counts of causing transmission of harmful computer commands in connection with his theft of the Stolen CIA Files.

Finally, on September 13, 2023, SCHULTE was found guilty at trial on charges of receiving, possessing, and transporting child pornography.

In addition to the prison term, SCHULTE, 35, of New York, New York, was sentenced to a lifetime of supervised release.

Mr. Williams praised the outstanding efforts of the Counterintelligence Division and the Child Exploitation and Human Trafficking Task Force of the FBI's New York Field Office, as well as the extraordinary work of FBI computer scientists from the Cyber Action Team. Mr. Williams also thanked the FBI Washington Field Office, the CIA Office of General Counsel, and the National Security Division's Counterintelligence and Export Control Section for their assistance.

This case is being handled by the Office's National Security and International Narcotics Unit. Assistant U.S. Attorneys David W. Denton Jr., Michael D. Lockard, and Nicholas S. Bradley are in charge of the prosecution.

To read more:
https://www.justice.gov/usao-sdny/pr/former-cia-officer-joshua-adam-schulte-sentenced-40-years-prison-espionage-and-child

Number 9

AI in Support of StratCom Capabilities

The report aims to guide information environment assessment (IEA) practitioners. This includes understanding the information environment and audiences, particularly in online campaigns, and covers necessary technical elements and legal factors.

Contents

Key questions addressed include:
- What artificial intelligence (AI) functions are essential for Strategic Communications?
- Which models need improvement?
- What is the projected future of AI in this field?

The report offers current knowledge to enhance practitioners' ability to navigate an AI-driven information environment securely, efficiently and in line with legal requirements.

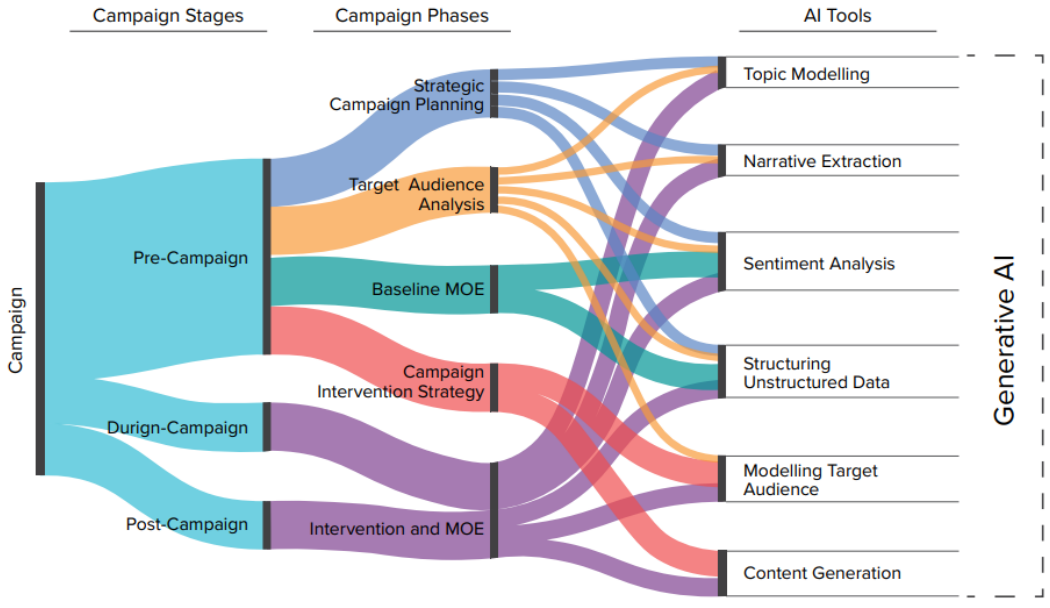
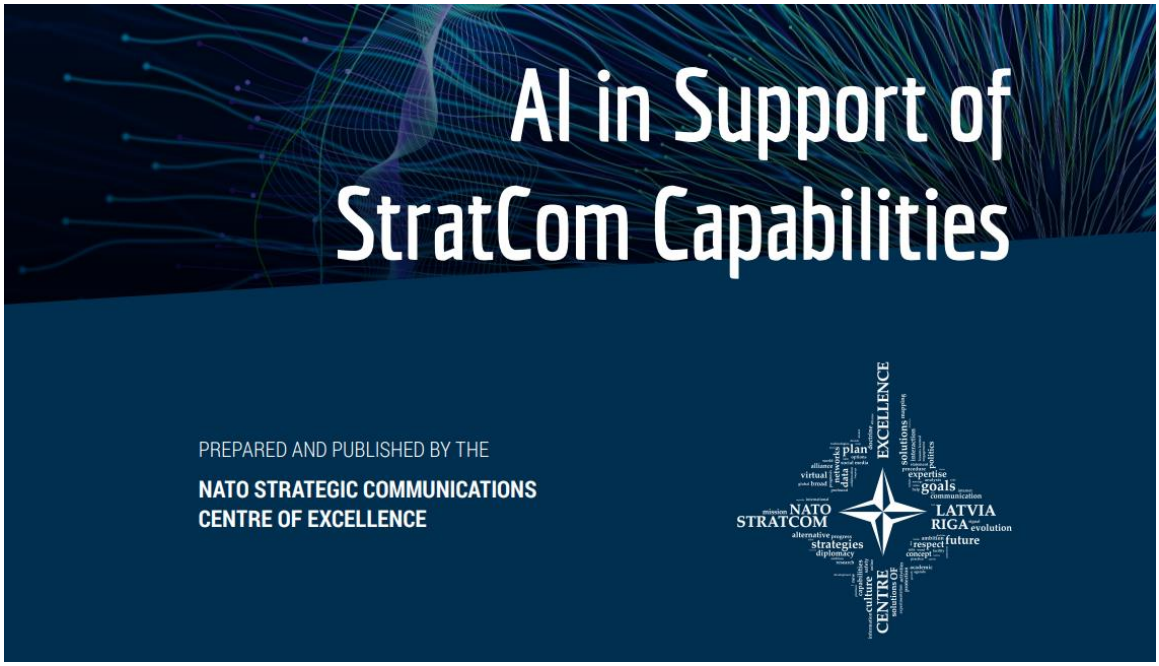


FIGURE 9. Summary of usage of AI tools in various stages of a StratCom campaign

To read more:
https://stratcomcoe.org/publications/ai-in-support-of-stratcom-capabilities/296



Number 10

U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure

Office of Public Affairs
U.S. Department of Justice

Court-Authorized Operation Removed Malware from U.S.-Based Victim Routers and Took Steps to Prevent Reinfection

A December 2023 court-authorized operation has disrupted a botnet of hundreds of U.S.-based small office/home office (SOHO) routers hijacked by People's Republic of China (PRC) state-sponsored hackers.

The hackers, known to the private sector as "Volt Typhoon," used privately-owned SOHO routers infected with the "KV Botnet" malware to conceal the PRC origin of further hacking activities directed against U.S. and other foreign victims.

These further hacking activities included a campaign targeting critical infrastructure organizations in the United States and elsewhere that was the subject of a May 2023 FBI, National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), and foreign partner advisory.

The same activity has been the subject of private sector partner advisories in May and December 2023, as well as an additional secure by design alert released by CISA.

The vast majority of routers that comprised the KV Botnet were Cisco and NetGear routers that were vulnerable because they had reached "end of life" status; that is, they were no longer supported through their manufacturer's security patches or other software updates. The court-authorized operation deleted the KV Botnet malware from the routers and took additional steps to sever

their connection to the botnet, such as blocking communications with other devices used to control the botnet.

“The Justice Department has disrupted a PRC-backed hacking group that attempted to target America’s critical infrastructure utilizing a botnet,” said Attorney General Merrick B. Garland. “The United States will continue to dismantle malicious cyber operations – including those sponsored by foreign governments – that undermine the security of the American people.”

“In wiping out the KV Botnet from hundreds of routers nationwide, the Department of Justice is using all its tools to disrupt national security threats – in real time,” said Deputy Attorney General Lisa O. Monaco. “Today’s announcement also highlights our critical partnership with the private sector – victim reporting is key to fighting cybercrime, from home offices to our most critical infrastructure.”

“China’s hackers are targeting American civilian critical infrastructure, pre-positioning to cause real-world harm to American citizens and communities in the event of conflict,” said FBI Director Christopher Wray. “Volt Typhoon malware enabled China to hide as they targeted our communications, energy, transportation, and water sectors. Their pre-positioning constitutes a potential real-world threat to our physical safety that the FBI is not going to tolerate. We are going to continue to work with our partners to hit the PRC hard and early whenever we see them threaten Americans.”

“Today, the FBI and our partners continue to stand firmly against People's Republic of China cyber actors that threaten our nation's cyber security,” said FBI Deputy Director Paul Abbate. “We remain committed to thwarting malicious activities of this type and will continue to disrupt and dismantle cyber threats, safeguarding the fabric of our cyber infrastructure.”

“This operation disrupted the efforts of PRC state-sponsored hackers to gain access to U.S. critical infrastructure that the PRC would be able to leverage during a future crisis,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division. “The operation, together with the release of valuable network defense guidance by the U.S. government and private sector partners, demonstrates the Department of Justice’s commitment to enhance cybersecurity and disrupt efforts to hold our critical infrastructure at risk.”

“Using traditional law enforcement tools to disrupt state-of-the-art technologies, the U.S. Attorney’s Office for the Southern District of Texas protected Americans from PRC government-sponsored cyber-criminals who used U.S. based routers to hack into American targets,” said U.S. Attorney Alamdar S. Hamdani for the Southern District of Texas. “This case demonstrates my office’s ongoing commitment to defending our critical infrastructure from PRC initiated cyber-attacks. We thank the FBI and the Justice Department’s National Security Division for its work, and we will continue to work shoulder to shoulder with them to shield our country from state-sponsored hackers.”

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN THE MATTER OF THE SEARCH OF SPECIFIED ROUTERS IN THE UNITED STATES INFECTED WITH KV BOTNET MALWARE	Case No. 4:23-MC-5432 **(UNDER SEAL)**

AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41(b)(6)(B) FOR A SEARCH AND SEIZURE WARRANT

I [redacted] a Special Agent with the Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. The FBI is investigating foreign state-sponsored actors ("hackers") who have intruded into small-office/home-office ("SOHO") routers in this District and elsewhere and infected them with malware. This malware links the SOHO routers into a network of nodes, or a botnet, which the hackers use as proxies to conceal their identities while committing additional computer intrusions against separate U.S. victims.

"The FBI's dismantling of the KV Botnet sends a clear message that the FBI will take decisive action to protect our nation's critical infrastructure from cyber-attacks," said Special Agent in Charge Douglas Williams of the FBI Houston Field Office. "By ensuring home and small-business routers are replaced after their end-of-life expiration, everyday citizens can protect both their personal cyber security and the digital safety of the United States. We need the American public's vigilance and support to continue our fight against malicious PRC-sponsored cyber actors."

As described in court documents, the government extensively tested the operation on the relevant Cisco and NetGear routers. The operation did not impact the legitimate functions of, or collect content information from, hacked routers. Additionally, the court-authorized steps to disconnect the routers from the KV Botnet and prevent reinfection are temporary in nature. A router's owner can reverse these mitigation steps by restarting the router. However, a restart that is not accompanied by mitigation steps similar to those the court order authorized will make the router vulnerable to reinfection.

The FBI is providing notice of the court-authorized operation to all owners or operators of SOHO routers that were infected with the KV Botnet malware and remotely accessed pursuant to the operation. For those victims whose contact information was not publicly available, the FBI has contacted providers (such as a victim's internet service provider) and has asked those providers to provide notice to the victims.

FBI Houston Field Office and Cyber Division, U.S. Attorney's Office for the Southern District of Texas, and National Security Cyber Section of the Justice Department's National Security Division led the disruption effort. The Justice Department's Criminal Division's Computer Crime and Intellectual Property Section and Office of International Affairs provided valuable assistance. These efforts would not have been successful without the partnership of numerous private-sector entities.

If you believe you have a compromised router, please visit the FBI's Internet Crime Complaint Center or report online to CISA. The remediated routers remain vulnerable to future exploitation by Volt Typhoon and other hackers, and the FBI strongly encourages router owners to remove and replace any end-of-life SOHO router currently in their networks.

The FBI continues to investigate Volt Typhoon's computer intrusion activity.

To read more:
https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

[redacted]

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

United States Courts
Southern District of Texas
FILED
January 09, 2024
Nathan Ochsner, Clerk of Court

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
SPECIFIED ROUTERS IN THE UNITED STATES INFECTED WITH KV BOTNET MALWARE

Case No. **4:24-mc-5018**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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.

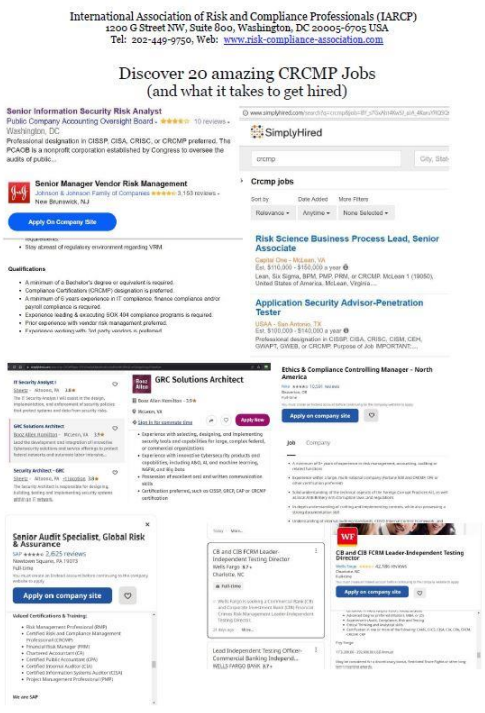
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

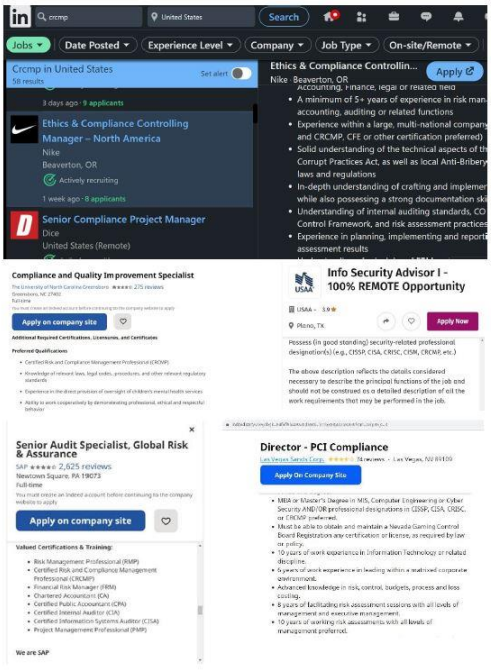
Our training and certification programs:

1. 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

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 57 countries. Companies and organizations around the world consider the CRCMP a preferred certificate.

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





2. 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

3. 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

4. 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

5. 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

The International Association of Risk and Compliance Professionals (IARCP) is a business unit of Compliance LLC, incorporated in Wilmington NC and offices in Washington DC, a provider of risk and compliance training and executive coaching in 57 countries. To learn more: https://www.risk-compliance-association.com/Privacy.htm

You may contact:

Lyn Spooner
Email: lyn@risk-compliance-association.com

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