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

Monday, February 27, 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,

To the extent that international trade is negatively affected by geopolitical factors, a trend towards *regionalisation* will emerge, as a mechanism to continue to enjoy the benefits of globalisation but on a smaller scale. As an illustration, in 2022, 44% of global companies were developing regionalised supply networks (up from only 25% in 2021).

This is part from an excellent presentation from Pablo Hernández de Cos, Governor of the Bank of Spain, at the Dialogue with the Governor on the Future of Globalisation, Cañada Blanch Centre for Contemporary Spanish Studies and London School of Economics and Political Science, in London.

Pablo Hernández de Cos explained that in response to these challenges, the EU has recently been launching a series of policies within the so-called *Open Strategic Autonomy agenda* - an emerging set of regulatory, structural and fiscal policies that seek to address the EU's economic

vulnerabilities arising from geopolitical considerations. Under the framework of Open Strategic Autonomy, *three* types of policies have been proposed to reduce the EU's vulnerabilities.

A *first* set of measures aims to assess supply chain dependencies and vulnerabilities and *increase the resilience of the European industrial system*.

Specific examples are the action plan on critical raw materials - aimed at reducing the EU's external dependence in the sourcing of such goods -, the "RePowerEU" initiative - aimed at reducing the EU's energy dependence -, and plans to drive the digitalisation of European economies.

A *second* set of measures aims to protect EU countries from possible abusive practices adopted by third economies - practices that may be related to strategic or political objectives.

These measures include those aimed at monitoring foreign direct investment flows from third countries and other measures designed to limit coercive actions against European companies.

A *third* class of measures aims to preserve the international level playing field by compensating for competitive disadvantages that EU companies might face due to less stringent environmental and state aid policies implemented by third countries.

Examples are the regulation on foreign subsidies that distort the internal market and the Carbon Border Adjustment Mechanism (CBAM).

Pablo Hernández de Cos also explained that it is essential to make progress in extending risk-sharing mechanisms – public and private - in the EU. This should be done in *three* ways.

First, the Economic and Monetary Union (EMU) needs to equip itself with a permanent macroeconomic stabilisation capacity.

Second, it is essential that the Banking Union be completed with the construction of an EU deposit guarantee system.

And *third,* progress in building the Capital Markets Union is essential to increase the resilience of the EMU to macro-financial shocks, better spread the costs of asymmetric or idiosyncratic shocks, reduce the risks of financial fragmentation, and provide a more favourable environment for private investment.

According to Pablo Hernández de Cos, for the time being there is no consistent trend towards "deglobalisation", but rather a change in the nature of globalisation, leading to a rise in the regionalisation of trade and supply chains, a diversification of sourcing and a certain slowdown in global value chain fragmentation.

While the marked slowdown in firms' decisions to relocate part of their production processes abroad ("offshoring") or to repatriate previously offshored activities ("reshoring") is compatible with a deglobalisation phase, other factors qualify this view.

The flattening of trade in goods does indeed hint at a trend slowdown, but the continued growth of international trade in services seems to signal a continuation of globalisation trends in these sectors, driven by technological progress, including data trading and the expansion of *artificial intelligence*.

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

Best regards,

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

Number 1 (Page 6)

(De)globalisation and economic policies in the European context

Pablo Hernández de Cos, Governor of the Bank of Spain, at the Dialogue with the Governor on the Future of Globalisation, Cañada Blanch Centre for Contemporary Spanish Studies and London School of Economics and Political Science, London.

Number 2 (Page 10)

Implementation of G20 Non-Bank Financial Intermediation Reforms, Progress report

FSB FINANCIAL STABILITY BOARD

Number 3 (Page 13)

Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-Service Program and Pay $30 Million to Settle SEC Charges

Number 4 (Page 15)

Statement

Kraken Down: Statement on SEC v. Payward Ventures, Inc., et al.

SEC Commissioner Hester M. Peirce

Number 5 (Page 17)

BIS Working Papers, No 1070

Theory of supply chains: a working capital approach
by Se-Jik Kim and Hyun Song Shin, Monetary and Economic Department

BIS

Number 6 (Page 19)

How Cybersecurity Standards Support the Evolving EU Legislative Landscape

enisa
European Network and Information Security Agency

Number 7 (Page 21)

Predicting pandemics through museum animal collections
Coalition studies UNM museum samples to explore pathogens

Los Alamos NATIONAL LABORATORY

Number 8 (Page 23)

U.S. Department of Justice Disrupts Hive Ransomware Variant
FBI Covertly Infiltrated Hive Network, Thwarting Over $130 Million in Ransom Demands

Number 9 (Page 26)

Screentime: Sometimes It Feels Like Somebody's Watching Me

proofpoint.

Number 10 (Page 27)

We had a security incident. Here's what we know.

reddit

Number 1

(De)globalisation and economic policies in the European context

Pablo Hernández de Cos, Governor of the Bank of Spain, at the Dialogue with the Governor on the Future of Globalisation, Cañada Blanch Centre for Contemporary Spanish Studies and London School of Economics and Political Science, London.

Let me start by thanking Professor Andrés Rodríguez-Pose, the Cañada Blanch Centre for Contemporary Spanish Studies of the London School of Economics (LSE) and the LSE for their kind invitation, and for giving me the opportunity to hold this dialogue with you on a fascinating topic: the future of globalisation.

The questions currently surrounding this topic are of the utmost importance for highly open and integrated economies, such as the euro area and the UK.

The two extraordinary shocks that have recently hit the global economy, the Covid-19 pandemic and, above all, the Russian invasion of Ukraine, have disrupted global value chains and commodity markets, and generated an environment of heightened uncertainty and geopolitical tensions.

Added to the past and present episodes of trade tensions between the US and China, among others, these shocks have prompted renewed questions regarding the future of globalisation and the increasing importance of geopolitical factors in shaping international economic relations.

Although the globalisation of goods was slowing down even before the pandemic, concerns about the resilience of global value chains and the supply security of strategic products are now becoming more apparent in decisions made by firms and policy measures considered by governments.

For their part, governments have become more concerned that trade and financial openness may create dependencies on third countries that increase vulnerability to geopolitical shocks.

Accordingly, they have started to include geopolitical considerations in their economic decision-making, with policy initiatives that aim to limit such external vulnerabilities, for example, by encouraging the local

production of strategic products such as semiconductors or by screening incoming foreign direct investment on grounds of national security.

These issues are particularly important for the EU, given its high degree of trade and financial openness, which is larger than that of other geopolitical powers such as the United States or China.

For example, in 2019 the share of foreign trade reached 54% of GDP in the euro area (up from 31% in 1999), which is double that of the US (26%), while the share of global value chain participation in trade is 20 percentage points higher in the euro area than in the United States.

Likewise, the euro area is more financially open than the US, as measured by the stock of gross external assets and liabilities with respect to GDP.

This openness has been a major advantage for Europe for many years and one of the main reasons for its prosperity.

This openness has allowed the EU to benefit from lower import prices, larger export opportunities, more foreign competition, technology diffusion and, ultimately, productivity gains.

But it has also become an element of vulnerability in a more volatile global geopolitical environment. This is currently evident in the EU's external energy dependence.

In this context, I would like to focus my speech today on three issues. I will begin by focusing on the implications of the changing patterns of globalisation for the European economy.

In particular, I will provide an analysis of the vulnerabilities and dependencies affecting the EU's trade and financial flows, based on a report soon to be published by the Eurosystem.

In the second section, I will take stock of the European policy response to reduce those vulnerabilities and exposures and the dilemmas it faces. I will also provide some insights into how I think European policies should react.

In the last part of my talk, I will focus on the implications of this trend for the ECB’s monetary policy.

In its recent strategy review, the ECB looked carefully at the consequences of globalisation for the conduct of monetary policy.

The obvious question is whether we should now expect similar effects with opposite sign as a result of a possible increase in fragmentation.

EU vulnerabilities in a globalised environment

The EU is deeply integrated into the global economy and has strong links with other major geopolitical powers, such as the US in terms of finance and trade, China in terms of trade and, before the war, Russia in terms of energy and raw materials supply.

What are the main vulnerabilities observed as a consequence of this high degree of integration?

One source of vulnerability in the face of rising geopolitical tensions is Europe's high external dependency with respect to some products which are key to the EU economy, but which are imported from a handful of non-EU countries.

China accounts for a large share of goods imports into the EU. China is also the main exporter to the EU of several electronic products (such as computers and optical devices), for which domestic production capacity is also relatively low.

This situation is not unique to the EU. As a consequence, China is becoming the "OPEC of industrial inputs".

This dependence on Chinese imports already had significant consequences for the European manufacturing sector during the pandemic.

There is evidence that the Chinese supply chain disruptions that occurred in the early months of the pandemic had a considerable impact on manufacturing output in the euro area, temporarily reducing it by 7%.

The EU is also dependent on third countries for semiconductor production.

European companies involved in the manufacture of these products concentrate almost exclusively on the upstream stage of the production chain, providing manufacturing equipment and high-purity materials used in chip production.

However, European companies account for a negligible share of other critical stages of the production chain, such as chip design or assembly.

They are also heavily dependent on foreign suppliers: almost 80% of the suppliers of European semiconductor companies are based outside the EU.

To read more:
https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/IntervencionesPublicas/Gobernador/Arc/Fic/IIPP-2023-02-09-hdc-en.pdf

Number 2

Implementation of G20 Non-Bank Financial Intermediation Reforms, Progress report

FSB FINANCIAL STABILITY BOARD

This report describes progress in implementing reforms that had been agreed by the G20 following the 2008 global financial crisis to strengthen the oversight and regulation of non-bank financial intermediation (NBFI). The implementation status in various NBFI areas is as follows:

1. Jurisdictions have made progress in implementing Basel III reforms to mitigate spillovers between banks and non-bank financial entities, but implementation is not yet complete.

Four jurisdictions have yet to implement applicable risk-based capital requirements for banks' investments in the equity of funds or the supervisory framework for measuring and controlling banks' large exposures.

2. Adoption of the 2012 IOSCO recommendations to reduce the run risk of money market funds (MMFs) is most advanced in the largest MMF markets.

All FSB members adopted the fair value approach for valuation of MMF portfolios, though one jurisdiction does not have in place requirements for use of the amortised cost method only in limited circumstances.

Progress in liquidity management is less advanced. An IOSCO review found that the policy measures in nine jurisdictions representing about 95% of global net MMF assets are generally in line with the IOSCO recommendations.

3. Adoption of the IOSCO recommendations on incentive alignment approaches for securitisation and of the BCBS standard on revised securitisation framework is ongoing.

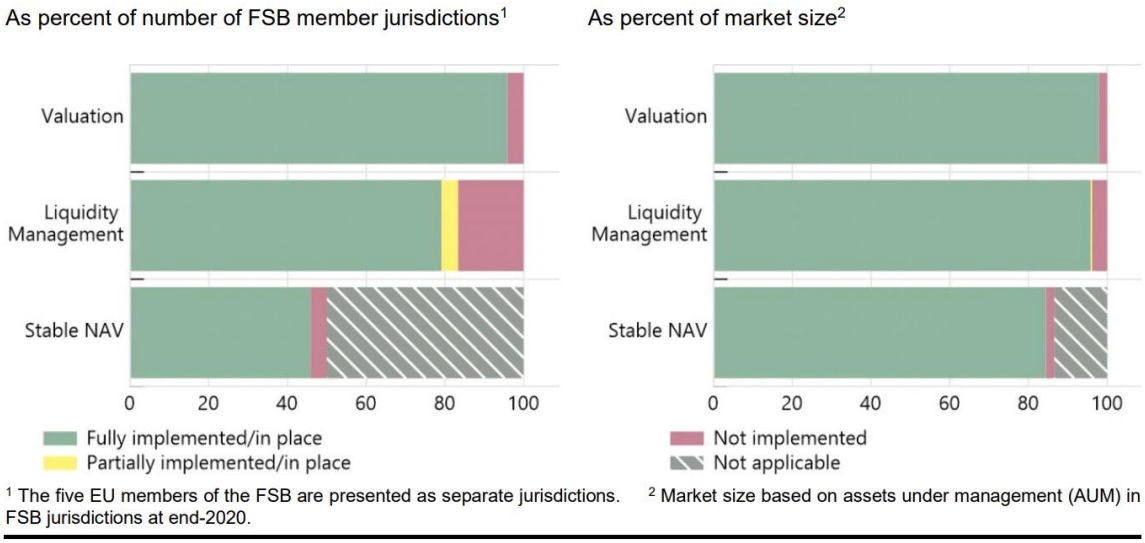
About one-third of FSB jurisdictions (for the IOSCO recommendations) and one-sixth of FSB jurisdictions (for the BCBS standard) have yet to implement them.

4. Implementation of FSB recommendations for dampening procyclicality and other financial stability risks associated with securities financing

transactions (SFTs) is incomplete and continues to face significant delays in most jurisdictions.

On global SFT data collection and aggregation, a few FSB jurisdictions are submitting data to the BIS.

Implementation progress is most advanced in the largest MMF markets Graph 1



[1] The five EU members of the FSB are presented as separate jurisdictions. [2] Market size based on assets under management (AUM) in FSB jurisdictions at end-2020.

5. Implementation of most FSB recommendations to assess and mitigate systemic risks posed by other non-bank financial entities and activities is ongoing.

The FSB and IOSCO assessed the implementation and effectiveness of their respective recommendations to address liquidity mismatch in open-ended funds (OEFs).

The FSB found that authorities have made meaningful progress in implementing the 2017 FSB Recommendations, but that lessons learnt since then have produced new insights into liquidity management challenges in segments of the OEF sector.

While the assessment suggests that the FSB Recommendations remain broadly appropriate, enhancing clarity and specificity on the policy outcomes the FSB Recommendations seek to achieve would make them more effective from a financial stability perspective.

IOSCO's review of its 2018 Recommendations shows a high degree of implementation of regulatory requirements consistent with the Recommendations' objectives, but some areas may warrant further attention.

In addition to these reforms, the FSB is carrying out further analytical and policy work to enhance the resilience of the NBFI sector, building on the lessons from the March 2020 market turmoil.

To read more: https://www.fsb.org/wp-content/uploads/P180123.pdf

Number 3

Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-Service Program and Pay $30 Million to Settle SEC Charges

The Securities and Exchange Commission charged Payward Ventures, Inc. and Payward Trading Ltd., both commonly known as Kraken, with failing to register the offer and sale of their crypto asset staking-as-a-service program, whereby investors transfer crypto assets to Kraken for staking in exchange for advertised annual investment returns of as much as 21 percent.

To settle the SEC's charges, the two Kraken entities agreed to immediately cease offering or selling securities through crypto asset staking services or staking programs and pay $30 million in disgorgement, prejudgment interest, and civil penalties.

According to the SEC's complaint, since 2019, Kraken has offered and sold its crypto asset "staking services" to the general public, whereby Kraken pools certain crypto assets transferred by investors and stakes them on behalf of those investors.

Staking is a process in which investors lock up – or "stake" – their crypto tokens with a blockchain validator with the goal of being rewarded with new tokens when their staked crypto tokens become part of the process for validating data for the blockchain.

When investors provide tokens to staking-as-a-service providers, they lose control of those tokens and take on risks associated with those platforms, with very little protection.

The complaint alleges that Kraken touts that its staking investment program offers an easy-to-use platform and benefits that derive from Kraken's efforts on behalf of investors, including Kraken's strategies to obtain regular investment returns and payouts

"Whether it's through staking-as-a-service, lending, or other means, crypto intermediaries, when offering investment contracts in exchange for investors' tokens, need to provide the proper disclosures and safeguards required by our securities laws," said SEC Chair Gary Gensler.

"Today's action should make clear to the marketplace that staking-as-a-service providers must register and provide full, fair, and truthful disclosure and investor protection."

"In case after case, we've seen the consequences when individuals and businesses tout and offer crypto investments outside of the protections provided by the federal securities laws: investors lack the disclosures they deserve and are harmed when they don't receive them," said Gurbir S. Grewal, Director of the SEC's Division of Enforcement.

"Today, we take another step in protecting retail investors by shutting down this unregistered crypto staking program, through which Kraken not only offered investors outsized returns untethered to any economic realities, but also retained the right to pay them no returns at all. All the while, it provided them zero insight into, among other things, its financial condition and whether it even had the means of paying the marketed returns in the first place."

In addition to ceasing the staking program and the monetary relief, Payward Ventures, Inc. and Payward Trading, Ltd, without admitting or denying the allegations in the SEC's complaint, consented to the entry of a final judgment, subject to court approval, that would permanently enjoin each of them from violating Section 5 of the Securities Act of 1933 and permanently enjoin them and any entity they control from, directly or indirectly, offering or selling securities through crypto asset staking services or staking programs.

The SEC's investigation was conducted by Laura D'Allaird and Elizabeth Goody, under the supervision of Paul Kim, Jorge G. Tenreiro, and David Hirsch, with assistance from Sachin Verma, Eugene Hansen, and James Connor.

To read more: https://www.sec.gov/news/press-release/2023-25

Number 4

Statement

Kraken Down: Statement on SEC v. Payward Ventures, Inc., et al.

SEC Commissioner Hester M. Peirce

Today, the SEC shut down Kraken's staking program and counted it as a win for investors. I disagree and therefore dissent.

Kraken operated a service through which its customers could offer their tokens up for staking. The customers earned returns, and the company earned a fee. The Commission argues that this staking program should have been registered with the SEC as a securities offering.

Whether one agrees with that analysis or not, the more fundamental question is whether SEC registration would have been possible. In the current climate, crypto-related offerings are not making it through the SEC's registration pipeline.

An offering like the staking service at issue here raises a host of complicated questions, including whether the staking program as a whole would be registered or whether each token's staking program would be separately registered, what the important disclosures would be, and what the accounting implications would be for Kraken.

We have known about crypto staking programs for a long time. Although it may not have made a difference, I should have called for us to put out guidance on staking long before now.

Instead of taking the path of thinking through staking programs and issuing guidance, we again chose to speak through an enforcement action, purporting to "make clear to the marketplace that staking-as-a-service providers must register and provide full, fair, and truthful disclosure and investor protection."

Using enforcement actions to tell people what the law is in an emerging industry is not an efficient or fair way of regulating.

Moreover, staking services are not uniform, so one-off enforcement actions and cookie-cutter analysis does not cut it.

Most concerning, though, is that our solution to a registration violation is to shut down entirely a program that has served people well. The program will no longer be available in the United States, and Kraken is enjoined from ever offering a staking service in the United States, registered or not.

A paternalistic and lazy regulator settles on a solution like the one in this settlement: do not initiate a public process to develop a workable registration process that provides valuable information to investors, just shut it down.

More transparency around crypto-staking programs like Kraken's might well be a good thing. However, whether we need a uniform regulatory solution and if that regulatory solution is best provided by a regulator that is hostile to crypto, in the form of an enforcement action, is less clear.

To read more:
https://www.sec.gov/news/statement/peirce-statement-kraken-020923

Number 5

BIS Working Papers, No 1070

Theory of supply chains: a working capital approach

by Se-Jik Kim and Hyun Song Shin, Monetary and Economic Department

BIS

Abstract

This paper presents a time-to-build theory of supply chains which implies a key role for the financing of working capital as a determinant of supply chain length. We apply our theory to offshoring and trade, where firms strike a balance between the productivity gain due to off-shoring against the greater financial cost due to longer supply chains. In equilibrium, the ratio of trade to GDP, inventories and productivity are procyclical and closely track financial conditions.

Introduction

Production takes time, especially when conducted through long supply chains.

Working capital in the form of inventories and receivables bridges the timing mismatch between incurring costs and receiving cash from sales. To the extent that the financing cost of working capital matters, the length of supply chains is not only a matter of the economic fundamentals (such as the production technology or trade barriers) but is also shaped by financial conditions.

In this paper, we lay out a theory of supply chains where financial conditions play a pivotal role in the determination of the length of supply chains.

Through this theory, we highlight a novel channel for macro fluctuations through investment in working capital, which bears a strong analogy with investment in physical capital, but which operates across groups of firms, rather than at the individual firm level.

We highlight the associated repercussions of financing conditions on productivity and the volume of international trade.

By highlighting the analogy between physical capital and working capital on the firms balance sheet, our theory suggests a reorientation in the way that economists think of inventories.

Rather than being a buffer stock that smooths shocks, inventories in transit reflect the choice in working capital investment underpinning global supply chains.

Tom Friedman's (2005) popular book on globalization ("The World is Flat") has an apt quote from the chief executive of UPS in this respect. The UPS CEO is quoted as saying:

"When our grandfathers owned shops, inventory was what was in the back room. Now it is a box two hours away on a package car, or it might be hundreds more crossing the country by rail or jet, and you have thousands more crossing the ocean" [Friedman (2005, p. 174)]

To read more: https://www.bis.org/publ/work1070.pdf

Number 6

How Cybersecurity Standards Support the Evolving EU Legislative Landscape

The European Union Agency for Cybersecurity (ENISA) joined forced with the European Standards Organisations (ESOs), CEN, CENELEC and ETSI, to organise their 7th annual conference. The hybrid conference focused on "European Standardisation in support of the EU cybersecurity legislation".

Given the latest developments in cybersecurity policy, the hybrid conference focused once more on European Standardisation in support of EU cybersecurity legislation. Building on the effective contributions of past editions, the high-level event attracted over 1600 attendees from the European Union and from the international sphere.

The conference was organised around four panels, which discussed ongoing standardisation work and future requirements. The event opened by the European Standards Organisations, Ms. Elena Santiago Cid, Director General of CEN and CENELEC, Mr. Wolfgang Niedziella, President of CENELEC, Mr. Luis Jorge Romero, ETSI Director-General and Mr.

Andreas Mitrakas, head of unit "Market Certification and Standardisation" at ENISA, as well as Ms. Christiane Kirketerp de Viron, head of unit Cybersecurity and Digital Privacy Policy at the European Commission.

The first panel addressed the future of EU standardisation with the "regional versus international" angle.

The second panel dealt with the Cyber Resilience Act (CRA) as a game changer and how standards can support it.

The Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (or eIDAS) V2 and digital identities were the topics of the third panel, while the final panel gave an overview of the landscape of the EU cybersecurity legislation.

Participants came from a diverse community of associations representing small and medium enterprises and vertical sectors, industry, and included several speakers from the European Commission.

To read more:
https://www.enisa.europa.eu/news/how-cybersecurity-standards-support-the-evolving-eu-legislative-landscape

Number 7

Predicting pandemics through museum animal collections

Coalition studies UNM museum samples to explore pathogens

Zoonotic pathogens, those that spill over from animals to humans such as SARS-CoV-2 and hantavirus, present a challenge for scientists in terms of how the diseases evolve and spread in animal populations.

Now, a broad coalition of institutions, including Los Alamos National Laboratory and the University of New Mexico, seeks to shed light on the evolution and spread of these pathogens before they make the jump into human populations.

“Our understanding of pathogens with high spill-over potential is limited by our preference for sampling human cases after a spill-over has already happened,” said Ethan Romero-Severson, a Los Alamos co-lead on the project. “This type of reactive data collection limits our ability to see the clues as to what was going on in the animal populations before the spill-over occurred.”

The central innovation behind the coalition — called the Pathogen Informatics Center for Analysis, Networking, Translation & Education (PICANTE) — directly addresses this deficiency by using the extensive frozen animal-tissue biorepositories housed at natural history museums around the globe. In fact, the most extensive collection of cryopreserved mammalian tissue known to date is housed at UNM’s Museum of Southwestern Biology (MSB).

PICANTE is currently funded through a Phase 1 Predictive Intelligence for Pandemic Preparedness (PIPP) grant from the National Science Foundation.

Premier datasets allow scientists to study host-pathogen relationships

Using the preserved tissues at MSB and those from collaborating biorepositories, scientists in PICANTE can develop screening and genetic sequencing methods to isolate pathogens from these extensive collections.

Because the data has been curated and vouchsafed by museums such as MSB over a period of decades, scientists have access to datasets spanning both space and time, resources that would be impossible to collect without the foresight of the collaborators at MSB.

The Los Alamos team includes Romero-Severson and Emma Goldberg, whose role in PICANTE is to develop methods for studying the evolutionary relationships among hosts and pathogens. They will also use pathogen sequence data coming from these biorepositories to document the history of pathogens such as hantavirus jumping between different rodent species.

“If we can understand what allows or inhibits pathogens to move between different animal species, we can better understand the risk animal pathogens pose to human health and global security,” said Romero-Severson.

“Despite being a small state, we have a golden opportunity here in New Mexico: UNM has the world’s largest collection of cryopreserved mammalian tissues coupled to an extensive network of international biorepositories, and Los Alamos has decades-long experience developing the methodology to model the evolution, epidemiology and control of pathogens and the computational power to actually implement those methods.”

Romero-Severson added, “PICANTE offers a new way for Los Alamos and UNM scientists to collaborate on some of the most pressing questions that will dominate the intersection of public health and global security in the coming decades.”

To read more: https://discover.lanl.gov/news/0210-picante/

Number 8

U.S. Department of Justice Disrupts Hive Ransomware Variant

FBI Covertly Infiltrated Hive Network, Thwarting Over $130 Million in Ransom Demands

The Justice Department announced today its months-long disruption campaign against the Hive ransomware group that has targeted more than 1,500 victims in over 80 countries around the world, including hospitals, school districts, financial firms, and critical infrastructure.

Since late July 2022, the FBI has penetrated Hive's computer networks, captured its decryption keys, and offered them to victims worldwide, preventing victims from having to pay $130 million in ransom demanded.

Since infiltrating Hive's network in July 2022, the FBI has provided over 300 decryption keys to Hive victims who were under attack. In addition, the FBI distributed over 1,000 additional decryption keys to previous Hive victims.

Finally, the department announced today that, in coordination with German law enforcement (the German Federal Criminal Police and Reutlingen Police Headquarters-CID Esslingen) and the Netherlands National High Tech Crime Unit, it has seized control of the servers and websites that Hive uses to communicate with its members, disrupting Hive's ability to attack and extort victims.

"Last night, the Justice Department dismantled an international ransomware network responsible for extorting and attempting to extort hundreds of millions of dollars from victims in the United States and around the world," said Attorney General Merrick B. Garland.

"Cybercrime is a constantly evolving threat. But as I have said before, the Justice Department will spare no resource to identify and bring to justice, anyone, anywhere, who targets the United States with a ransomware attack. We will continue to work both to prevent these attacks and to provide support to victims who have been targeted. And together with our international partners, we will continue to disrupt the criminal networks that deploy these attacks."

“The Department of Justice’s disruption of the Hive ransomware group should speak as clearly to victims of cybercrime as it does to perpetrators,” said Deputy Attorney General Lisa O. Monaco.

“In a 21st century cyber stakeout, our investigative team turned the tables on Hive, swiping their decryption keys, passing them to victims, and ultimately averting more than $130 million dollars in ransomware payments. We will continue to strike back against cybercrime using any means possible and place victims at the center of our efforts to mitigate the cyber threat.”

“The coordinated disruption of Hive’s computer networks, following months of decrypting victims around the world, shows what we can accomplish by combining a relentless search for useful technical information to share with victims with investigation aimed at developing operations that hit our adversaries hard,” said FBI Director Christopher Wray.

“The FBI will continue to leverage our intelligence and law enforcement tools, global presence, and partnerships to counter cybercriminals who target American business and organizations."

“Our efforts in this case saved victims over a hundred million dollars in ransom payments and likely more in remediation costs,” said Assistant Attorney General Kenneth A. Polite, Jr. of the Justice Department’s Criminal Division.

“This action demonstrates the Department of Justice’s commitment to protecting our communities from malicious hackers and to ensuring that victims of crime are made whole. Moreover, we will continue our investigation and pursue the actors behind Hive until they are brought to justice.”

“Cybercriminals utilize sophisticated technologies to prey upon innocent victims worldwide,” said U.S. Attorney Roger Handberg for the Middle District of Florida.

“Thanks to the exceptional investigative work and coordination by our domestic and international law enforcement partners, further extortion by HIVE has been thwarted, critical business operations can resume without interruption, and millions of dollars in ransom payments were averted.”

Since June 2021, the Hive ransomware group has targeted more than 1,500 victims around the world and received over $100 million in ransom payments.

Hive ransomware attacks have caused major disruptions in victim daily operations around the world and affected responses to the COVID-19 pandemic.

In one case, a hospital attacked by Hive ransomware had to resort to analog methods to treat existing patients and was unable to accept new patients immediately following the attack.

Hive used a ransomware-as-a-service (RaaS) model featuring administrators, sometimes called developers, and affiliates. RaaS is a subscription-based model where the developers or administrators develop a ransomware strain and create an easy-to-use interface with which to operate it and then recruit affiliates to deploy the ransomware against victims.

Affiliates identified targets and deployed this readymade malicious software to attack victims and then earned a percentage of each successful ransom payment.

Hive actors employed a double-extortion model of attack. Before encrypting the victim system, the affiliate would exfiltrate or steal sensitive data. The affiliate then sought a ransom for both the decryption key necessary to decrypt the victim's system and a promise to not publish the stolen data.

Hive actors frequently targeted the most sensitive data in a victim's system to increase the pressure to pay. After a victim pays, affiliates and administrators split the ransom 80/20. Hive published the data of victims who do not pay on the Hive Leak Site.

According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), Hive affiliates have gained initial access to victim networks through a number of methods, including: single factor logins via Remote Desktop Protocol (RDP), virtual private networks (VPNs), and other remote network connection protocols; exploiting FortiToken vulnerabilities; and sending phishing emails with malicious attachments.

To read more:
https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant

Number 9

Screentime: Sometimes It Feels Like Somebody's Watching Me

proofpoint.

Since October 2022 and continuing into January 2023, Proofpoint has observed a cluster of evolving financially motivated activity which we are referring to as "Screentime".

The attack chain starts with an email containing a malicious attachment or URL and leads to malware that Proofpoint dubbed WasabiSeed and Screenshotter. In some cases, Proofpoint observed post-exploitation activity involving AHK Bot and Rhadamanthys Stealer.

Proofpoint is tracking this activity under threat actor designation TA866. Proofpoint assesses that TA866 is an organized actor able to perform well thought-out attacks at scale based on their availability of custom tools; ability and connections to purchase tools and services from other vendors; and increasing activity volumes.

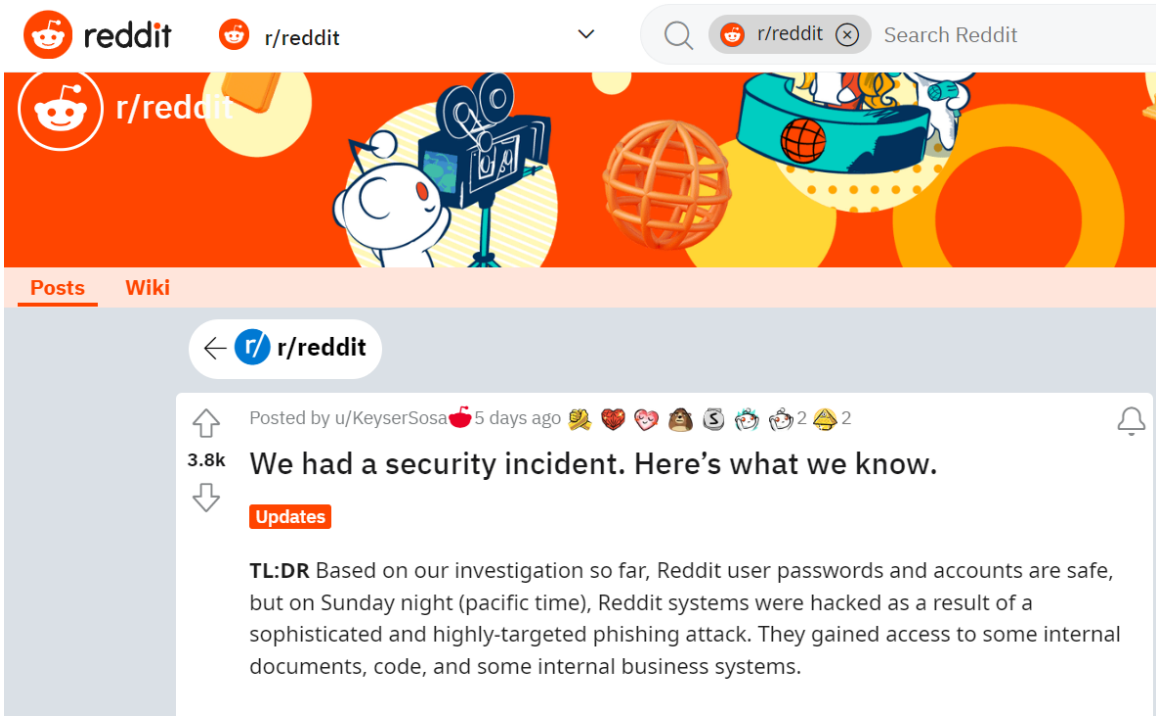
To read more:
https://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me

Number 10

We had a security incident. Here's what we know.

reddit

TL:DR Based on our investigation so far, Reddit user passwords and accounts are safe, but on Sunday night (pacific time), Reddit systems were hacked as a result of a sophisticated and highly-targeted phishing attack. They gained access to some internal documents, code, and some internal business systems.



What Happened?

On late (PST) February 5, 2023, we became aware of a sophisticated phishing campaign that targeted Reddit employees. As in most phishing campaigns, the attacker sent out plausible-sounding prompts pointing employees to a website that cloned the behavior of our intranet gateway, in an attempt to steal credentials and second-factor tokens.

After successfully obtaining a single employee's credentials, the attacker gained access to some internal docs, code, as well as some internal dashboards and business systems. We show no indications of breach of our primary production systems (the parts of our stack that run Reddit and store the majority of our data).

Exposure included limited contact information for (currently hundreds of) company contacts and employees (current and former), as well as limited

advertiser information. Based on several days of initial investigation by security, engineering, and data science (and friends!), we have no evidence to suggest that any of your non-public data has been accessed, or that Reddit's information has been published or distributed online.

How Did We Respond?

Soon after being phished, the affected employee self-reported, and the Security team responded quickly, removing the infiltrator's access and commencing an internal investigation.

Similar phishing attacks have been recently reported. We're continuing to investigate and monitor the situation closely and working with our employees to fortify our security skills. As we all know, the human is often the weakest part of the security chain.

Our goal is to fully understand and prevent future incidents of this nature, and we will use this post to provide any additional updates as we learn and can share more. So far, it also appears that many of the lessons we learned five years ago have continued to be useful.

User Account Protection

Since we're talking about security and safety, this is a good time to remind you how to protect your Reddit account. The most important (and simple) measure you can take is to set up 2FA (two-factor authentication) which adds an extra layer of security when you access your Reddit account. Learn how to enable 2FA in Reddit Help. And if you want to take it a step further, it's always a good idea to update your password every couple of months – just make sure it's strong and unique for greater protection.

Also: use a password manager! Besides providing great complicated passwords, they provide an extra layer of security by warning you before you use your password on a phishing site… because the domains won't match!

To read more:
https://www.reddit.com/r/reddit/comments/10y427y/we_had_a_security_incident_heres_what_we_know/

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

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

International Association of Risk and Compliance Professionals (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

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

3. *Training and Certification* – Become:

- a Certified Risk and Compliance Management Professional (CRCMP),

- a Certified Information Systems Risk and Compliance Professional (CISRCP),

- a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P,

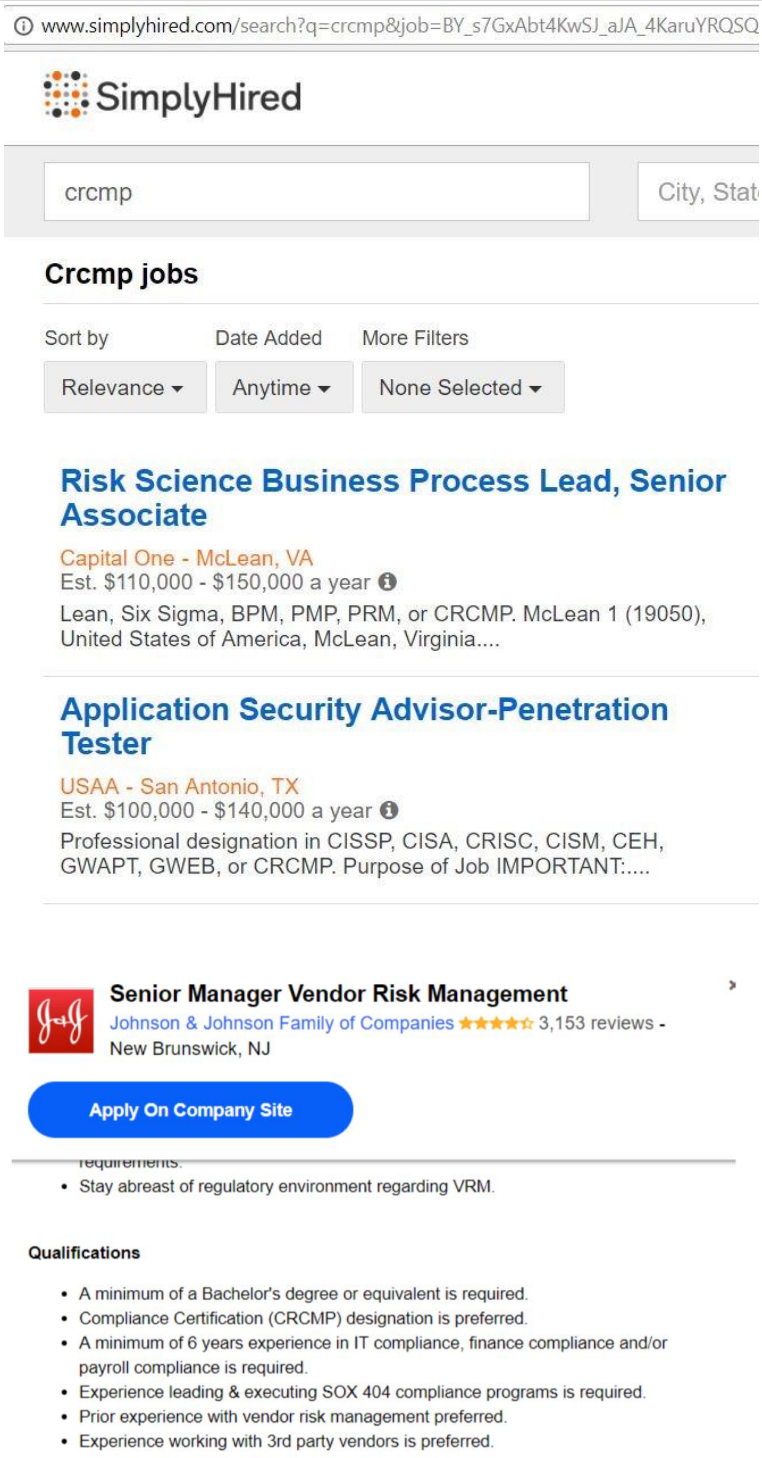
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- 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...



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.