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, June 5, 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,

Niccolo Machiavelli believed that “there is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things”.

Niccolo Machiavelli is the proper person to introduce the legal issues and uncertainties related to retail Central Bank Digital Currencies (CBDC). According to the new paper with title *“Central bank digital currencies: ongoing policy perspectives”* from the Bank of Canada, the Swiss National Bank, the European Central Bank, the Bank of England, the Bank of Japan, the Board of Governors Federal Reserve System, the Sveriges Riskbank, and the Bank for International Settlements:

“The legal issues related to a retail CBDC span many different branches of a country’s national law. Some of these issues also arise with traditional forms of money, although the solutions may differ. Legal issues include:

(i) the legal classification of a retail CBDC;

(ii) the authority of the central bank to issue one;

(iii) the concepts of settlement and payment finality in a retail CBDC system;

(iv) data governance, privacy and anonymity in a retail CBDC system;

(v) the potential imposition of restrictions on holdings;

(vi) non-resident access to a retail CBDC; and

(vii) the potential liabilities of participants in a retail CBDC system.

Regulatory issues such as competition and AML/CFT also need to be addressed."

But wait, there is more. At the end of the paper, exactly at the moment I was thinking I had considered enough challenges for one day, I read:

"Quantum computing is developing quickly in addition to the evolving threat of security vulnerabilities. These developments could break current "classical" cryptography that is used by most systems. A new generation of "post-quantum" cryptography (PQC), which is resistant to attacks by quantum computers, is in the process of being developed and standardised. PQC may need to be considered in potential CBDC designs."

Over and out.

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

Best regards,

George Lekatis

George Lekatis
President of the IARCP

Number 6 (Page 17)

Intelligence Advanced Research Projects Activity (IARPA)

IARPA Kicks Off New Research Program to Detect Changes in Movement Patterns

Number 7 (Page 19)

Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

Number 8 (Page 22)

COSMICENERGY operational technology (OT) / industrial control system (ICS)-oriented malware, to Sabotage Power Grids

Number 9 (Page 23)

NIST Team Demonstrates Novel Way to Convert Heat to Electricity

Number 10 (Page 26)

Taking a New Look at Fundamental Tech for Quiet Undersea Propulsion

DARPA sees opportunity to finally make efficient, scalable magnetohydrodynamic drive a reality

Number 1

Central bank digital currencies: ongoing policy perspectives

Bank of Canada	Swiss National Bank
European Central Bank	Bank of England
Bank of Japan	Board of Governors Federal Reserve System
Sveriges Riskbank	Bank for International Settlements

A group of central banks, together with the Bank for International Settlements, are working together to explore central bank digital currencies (CBDCs) for the public ("general purpose" or "retail" CBDC).

Since publishing:

(i) a report in October 2020 setting out the common foundational principles and core features of a CBDC; and

(ii) an executive summary and three detailed reports on system design and interoperability, user needs and adoption and financial stability implications in September 2021, the group has continued to share ideas and perspectives on similar themes, which are summarised in this note.

Central bank digital currencies: ongoing policy perspectives

May 2023

Bank of Canada
European Central Bank
Bank of Japan
Sveriges Riskbank
Swiss National Bank
Bank of England
Board of Governors Federal Reserve System
Bank for International Settlements

Background/motivation

Most central banks are now exploring CBDCs, and more than a quarter of them are developing or running concrete pilots (Kosse and Mattei (2022)).

Many of our jurisdictions are examining whether there is a need to ensure ongoing retail access to central bank money at a time of profound, ongoing changes across finance, technology and society.

The motivation for introducing a retail CBDC may rest primarily on the role of central bank money as a public good.

At the same time, the introduction of a CBDC could be an innovative opportunity for the monetary system.

It is in this context that the central banks contributing to this group have continued their collaboration to deepen the practical policy and technical analysis of CBDC.

Annex 1 draws out some elements of the discussion in 2022. Some of the members of this group are approaching a point where they may decide on whether or not to move to the next stage of their CBDC work.

This may include deeper investment in design decisions relating to technology, end user preferences and business models, while leaving open the decision on whether to issue CBDC.

To date, none of our jurisdictions have yet decided to proceed with the issuance of a retail CBDC. CBDC issuance and design are sovereign decisions for relevant authorities based on their assessments and a jurisdiction's circumstances. However, there has been value in working collectively on common issues.

To read more: https://www.bis.org/publ/othp65.pdf

Number 2

After the crypto-winter, the spring of crypto-assets regulation and supervision

Denis Beau, First Deputy Governor of the Bank of France, at the World Bank Global Payments Week 2023 "The Future of Payments", Marrakesh.

Dear colleagues from the World Bank, Ladies and Gentlemen,

According to some commentators, in a context of cascading bankruptcies (i.e. Terra /Luna, Celsius, Three Arrows, Genesis, BlockFi, FTX), the crypto ecosystem may have entered a so-called **"crypto-winter".**

I don't know if this winter is going to last but I believe that it should be seen as **"spring time"** by regulators and supervisors, whose initiatives should be burgeoning.

Recently, many countries have indeed sped up their regulatory work within their jurisdiction.

However, we have also seen variances in combining three regulatory approaches:

- banning crypto-asset activities;
- containing and isolating them from traditional finance and the real economy, which implies banning certain specific aspects and practices (e.g. advertising);
- regulating the crypto-asset market, either by assimilating crypto-assets to traditional financial assets and applying the corresponding existing regulatory regime, or by adopting a dedicated regulation (e.g. on stablecoins).

With the exception of China, the world's major economies and currency zones have developed or are in the process of adopting a combination of the last two approaches, based on the principle of "same activities, same risks, same rules". As a blunt banning of crypto-asset activities is not seen as an option for most, for a number of reasons, starting for instance with the belief in France that it would most likely lead to regulatory arbitrages between jurisdictions, most of the attention at national and international level has been put on "what?" (what activities and what risks) and "how?" (by which means) to regulate.

In my short introductory remarks today, I would like to share with you my perspective, as the organisers of this Global Payments Week Conference have kindly suggested, speaking from the standpoint of a central bank in charge of ensuring financial stability, on the types of risks associated with crypto-activities that particularly need to be considered for regulation and supervision, and the importance of a convergent and coordinated regulatory approach on crypto-assets at the international level.

To read more:
https://acpr.banque-france.fr/sites/default/files/medias/documents/20230518_gpw2023_keynote_speech_dbeau_en.pdf

Number 3

IOSCO Sets the Standard for Global Crypto Regulation

OICU-IOSCO

International Organization of Securities Commissions

The International Organization of Securities Commissions (IOSCO) has published this Consultation Report with the aim of finalizing IOSCO's policy recommendations to address market integrity and investor protection issues in crypto-asset markets in early-Q4 2023.

In line with IOSCO's established approach for securities regulation, the Crypto and Digital Asset Recommendations (CDA Recommendations) are addressed to relevant authorities and look to support jurisdictions seeking to establish compliant markets for the trading of crypto or 'digital' or 'virtual' assets (hereafter "crypto-assets" and read to include all relevant tokens) in the most effective way possible.

This consultation report proposes 18 policy recommendations that IOSCO plans to finalize in early Q4 this year to support greater consistency with respect to regulatory frameworks and oversight in its member jurisdictions, to address concerns related to market integrity and investor protection arising from crypto-asset activities.

The recommendations have been developed under the stewardship of the IOSCO Board's Fintech Task Force (FTF) in accordance with IOSCO's CryptoAsset Roadmap published in June 2022.

The proposed recommendations are principles-based and outcomes-focused and are aimed at the activities performed by crypto-asset service providers (CASPs).

They apply IOSCO's widely accepted global standards for securities markets regulation to address key issues and risks identified in cryptoasset markets.

The proposed recommendations are activities-based and follow a 'lifecycle' approach in addressing the key risks identified in this report.

They cover the range of activities in crypto-asset markets that involve CASPs from offering, admission to trading, ongoing trading, settlement, market surveillance and custody as well as marketing and distribution (covering advised and non-advised sales) to retail investors.

The proposed recommendations do not cover activities, products or services provided in the so-called "decentralized finance" or "DeFi" area.

Policy Recommendations for Crypto and Digital Asset Markets

Consultation Report

The FTF DeFi workstream is considering issues in relation to DeFi and will publish a consultation report with proposed recommendations later this summer.

One of IOSCO's goals is to promote greater consistency with respect to how IOSCO members approach the regulation and oversight of crypto-asset activities, given the cross-border nature of the markets, the risks of regulatory arbitrage and the significant risk of harm to which retail investors continue to be exposed.

IOSCO is also seeking to encourage optimal consistency in the way cryptoasset markets and securities markets are regulated within individual IOSCO jurisdictions, in accordance with the principle of 'same activities, same risks, same regulatory outcomes'.

The proposed recommendations also cover the need for enhanced cooperation among regulators.

They aim to provide a critical benchmark for IOSCO members to cooperate, coordinate and respond to cross-border challenges in enforcement and supervision, including regulatory arbitrage concerns, that arise from global crypto-asset activities conducted by CASPs that offer their services, often remotely, into multiple jurisdictions.

While the proposed recommendations are not directly addressed to markets participants, CASPs and all participants in crypto-asset markets are strongly encouraged to carefully consider the expectations and outcomes articulated through the proposed recommendations and the respective supporting guidance in the conduct of registered/licensed, and cross-border activities.

Money Laundering / Fraud / Scams

As with other crypto-assets, stablecoins may appeal to money launderers and criminals who do not wish to subject the proceeds of crime to traditional financial system oversight. Stablecoins are also likely to be perceived as more stable than other crypto-assets, so are more attractive to money launderers and criminals who do not wish to be as exposed to crypto-asset market volatility.

In light of the price instability of crypto-assets, because of their relatively more stable nature scammers have turned to stablecoins, and are soliciting stablecoins from their victims.

To read more:
https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf

Number 4

ESAs launch discussion on criteria for critical ICT third-party service providers and oversight fees

The European Supervisory Authorities (EBA, EIOPA and ESMA - ESAs) published a joint Discussion Paper seeking stakeholders' input on aspects of the Digital Operational Resilience Act (DORA).

This Discussion Paper follows the European Commission's request for technical advice on the criteria for critical ICT third-party providers (CTPPs) and the oversight fees to be levied on them.

Interested stakeholders are invited to provide their input by 23 June 2023.

The Discussion Paper is separated into two parts:

- Proposals covering the criteria to be considered by the ESAs when assessing the critical nature of ICT third-party service providers, in particular, a number of relevant quantitative and qualitative indicators for each of the criticality criteria, along with the necessary information to construct such indicators.

- Proposals in relation to the amount of the fees levied on CTPPs and the way in which they are to be paid, in particular the types of expenditure that shall be covered by fees as well as the appropriate method, basis and information for determining the applicable turnover of the CTPPs, which will form the basis of fee calculation. The ESAs are also seeking input on the fee calculation method and other practical issues regarding the payment of fees.

In light of the two delegated acts envisaged in the Regulation on Digital Operational Resilience for the Financial Sector ("DORA"), the European Commission has requested ('CfA') the ESAs' technical advice to further specify the criteria for critical ICT third-party service providers (CTPPs) and determine the fees levied on such providers.

The ESAs shall deliver their technical advice by 30 September 2023.

The purpose of this discussion paper is to consult market participants, in an open and transparent manner, on the ESAs' proposals towards the specific issues listed in the CfA.

The provided answers during this consultation will be taken into account in the ESAs' advice.

The first part of this discussion paper presents proposals in relation to the elements needed to specify further the criteria referred to in Article 31(2) of the DORA to be considered by the ESAs when assessing the critical nature of ICT third-party service providers.

In particular, a number of relevant quantitative and qualitative indicators are proposed for each of the criticality criteria, along with the necessary information to build up and interpret such indicators.

Moreover, a number of minimum relevance thresholds are proposed for the quantitative indicators, where possible and applicable.

These are thresholds below which the degree to which the factor is in play would not be considered sufficiently relevant to trigger the indicator for inclusion in any criticality assessment methodology.

It is important to note that these proposals relate to the identification of indicators relevant to assessing criticality and not to the methodology for that assessment, including the materiality and interaction of the different criteria.

The expected type and total number of CTPPs, the details of the designation procedure as well as the related methodology, are explicitly excluded from this discussion paper and shall be defined at a later stage in the context of the implementation of the oversight framework.

The second part of this discussion paper presents proposals in relation to the amount of the fees levied on CTPPs and the way in which they are to be paid. In particular, proposals are made on the necessary types of expenditure that shall be covered by fees, the appropriate method, basis and available information for determining the applicable turnover of the CTPPs (which will form the basis of fee calculation) as well as the method of fee calculation and other practical issues regarding the payment of fees. In addition, a proposed financial contribution for voluntary opt-in requests is included in the paper.

Market participants are invited to provide their feedback on the proposals in this discussion paper, which will be considered by the ESAs in finalising the joint technical advice to the European Commission. Responses should be provided through a form available on the ESAs' websites by 23 June 2023 at the latest.

To read more:
https://www.eiopa.europa.eu/esas-launch-discussion-criteria-critical-ict-third-party-service-providers-and-oversight-fees-2023-05-26_en

Number 5

EBA publishes Report on holdings of eligible liabilities issued by G-SIIs and O-SIIs

The European Banking Authority (EBA) published a report on the holdings by EU banks of minimum requirement for own funds and eligible liabilities (MREL) instruments issued by the most systemic European banks.

As of 31 December 2021, these holdings appear small and potential direct contagion risks are, therefore, limited.

In particular, more than half of the resolution banks in the sample have exposures to eligible liabilities issued by global systemically important institutions (G-SIIs) and other systemically important institutions (O-SIIs) below 2% of MREL and 0.6% of the total risk exposure amount (TREA).

In addition, the report finds that, overall, the largest EU banks do not rely on other banks to place their MREL instruments. As of December 2021, G-SIIs and O-SIIs had placed a limited 3.7% of their eligible liabilities with banks in the sample, with seven banks out of 72 placing more than 20%.

As a consequence of these limited exposures, direct spill over effects from a possible bail-in appear limited.

The Report considered systemic crisis under two scenarios:

(i) the failure of G-SIIs and O-SIIs rated below investment grade and

(ii) the failure of the largest issuers of the sample. Under both scenarios, the contagion via direct exposures would not lead to a failure of any of the holders.

None of the banks would breach their Pillar 2 Requirement (P2R) under any of the two scenarios.

Yet, it should be noted that the Report does identify some outliers with higher-than-average exposure.

In particular, twenty-five banks report exposures above 8% of their MREL and six institutions report exposures above 20% of their MREL.

Furthermore, the Report neither captures issuances by non-systemic banks nor considers the impact on banks with balance sheets below EUR 5bn – which limits its conclusions.

To read more:
https://www.eba.europa.eu/eba-publishes-report-holdings-eligible-liabilities-issued-g-siis-and-o-siis

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2023/1055437/Report%20on%20holdings%20of%20eligible%20liabilities%20%28Art.%20504a%20CRR%20II%29_final.pdf

Number 6

Intelligence Advanced Research Projects Activity (IARPA)

IARPA Kicks Off New Research Program to Detect Changes in Movement Patterns

The Intelligence Advanced Research Projects Activity (IARPA) — the advanced research and development arm of the Office of the Director of National Intelligence — recently announced the launch of a research program to develop systems capable of modeling population movement patterns around the globe and providing alerts when concerning anomalies emerge.

The Hidden Activity Signal and Trajectory Anomaly Characterization (HAYSTAC) program aims to establish "normal" movement models across times, locations, and populations and determine what makes an activity atypical.

Expansive data from the Internet of Things and Smart City infrastructures provides opportunities to build new models that understand human dynamics at unprecedented resolution and creates the responsibility to understand privacy expectations for those moving through this sensor-rich world.

"An ever-increasing amount of geospatial data is created every day," said HAYSTAC Program Manager Dr. Jack Cooper.

"With HAYSTAC, we have the opportunity to leverage machine learning and advances in artificial intelligence to understand mobility patterns with exceptional clarity. The more robustly we can model normal movements, the more sharply we can identify what is out of the ordinary and foresee a possible emergency."

Through a competitive Broad Agency Announcement, IARPA awarded HAYSTAC research contracts to the following lead organizations, which together bring 27 additional academic institutions, non-profits, and businesses into the program:

Raytheon Technologies Research Center
L3Harris Technologies, Inc.

STR
Kitware, Inc.
Leidos, Inc.
Novateur Research Solutions
Deloitte Consulting LLP
Raytheon BBN

The HAYSTAC test and evaluation team consists of Johns Hopkins Applied Physics Laboratory, MITRE, and Oak Ridge National Laboratory.

To read more:
https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2023/item/2381-iarpa-kicks-off-new-research-program-to-detect-changes-in-movement-patterns

Number 7

Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

Microsoft

Microsoft has uncovered stealthy and targeted malicious activity focused on post-compromise credential access and network system discovery aimed at critical infrastructure organizations in the United States.

The attack is carried out by Volt Typhoon, a state-sponsored actor based in China that typically focuses on espionage and information gathering.

Microsoft assesses with moderate confidence that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises.

Volt Typhoon has been active since mid-2021 and has targeted critical infrastructure organizations in Guam and elsewhere in the United States. In this campaign, the affected organizations span the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors.

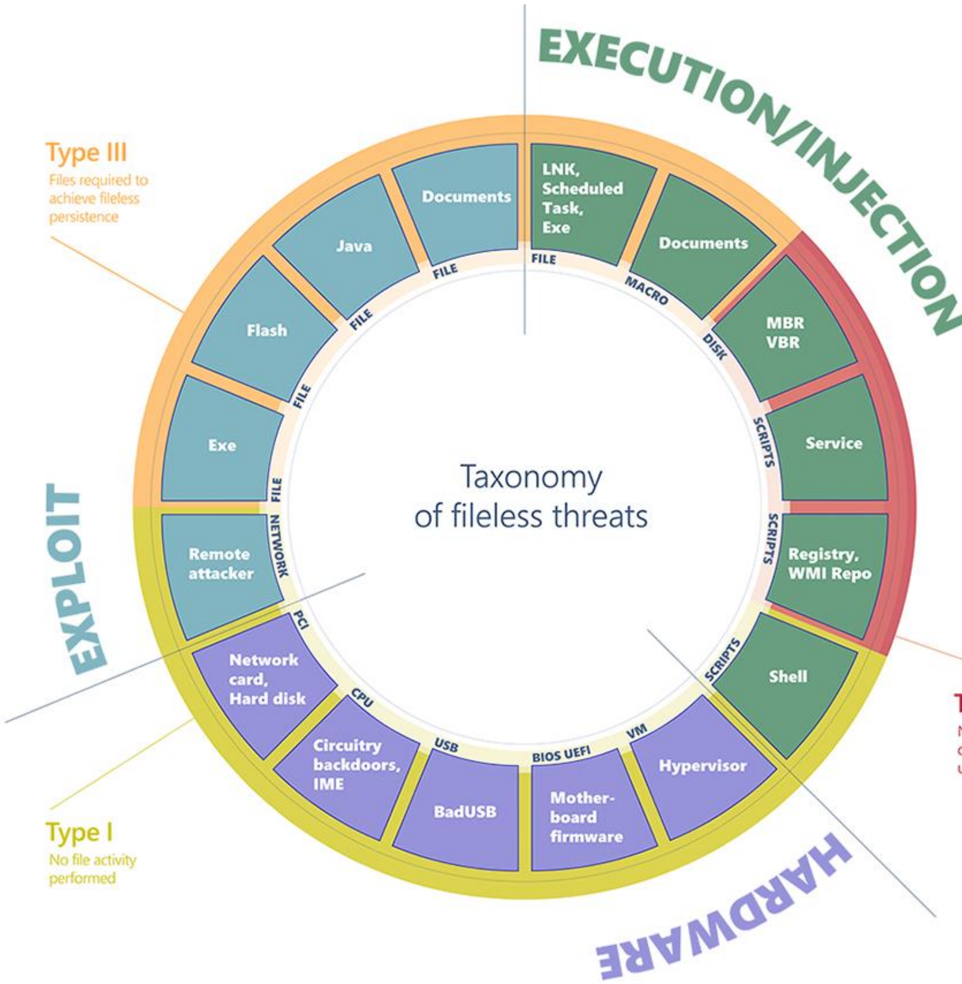
Observed behavior suggests that the threat actor intends to perform espionage and maintain access without being detected for as long as possible.

Microsoft is choosing to highlight this Volt Typhoon activity at this time because of our significant concern around the potential for further impact to our customers.

Although our visibility into these threats has given us the ability to deploy detections to our customers, the lack of visibility into other parts of the actor's activity compelled us to drive broader community awareness and further investigations and protections across the security ecosystem.

To achieve their objective, the threat actor puts strong emphasis on stealth in this campaign, relying almost exclusively on living-off-the-land techniques and hands-on-keyboard activity.

They issue commands via the command line to (1) collect data, including credentials from local and network systems, (2) put the data into an archive file to stage it for exfiltration, and then (3) use the stolen valid credentials to maintain persistence.



In addition, Volt Typhoon tries to blend into normal network activity by routing traffic through compromised small office and home office (SOHO) network equipment, including routers, firewalls, and VPN hardware.

They have also been observed using custom versions of open-source tools to establish a command and control (C2) channel over proxy to further stay under the radar.

In this blog post, we share information on Volt Typhoon, their campaign targeting critical infrastructure providers, and their tactics for achieving and maintaining unauthorized access to target networks. Because this activity relies on valid accounts and living-off-the-land binaries (LOLBins), detecting and mitigating this attack could be challenging.

Compromised accounts must be closed or changed. At the end of this blog post, we share more mitigation steps and best practices, as well as provide details on how Microsoft 365 Defender detects malicious and suspicious activity to protect organizations from such stealthy attacks.

The National Security Agency (NSA) has also published a Cybersecurity Advisory which contains a hunting guide for the tactics, techniques, and procedures (TTPs) discussed in this blog. You may visit: https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF

Joint Cybersecurity Advisory

TLP:CLEAR

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

As with any observed nation-state actor activity, Microsoft has directly notified targeted or compromised customers, providing them with important information needed to secure their environments. To learn about Microsoft's approach to threat actor tracking, read Microsoft shifts to a new threat actor naming taxonomy.

To read more:
https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

Number 8

COSMICENERGY operational technology (OT) / industrial control system (ICS)-oriented malware, to Sabotage Power Grids

The discovery of COSMICENERGY illustrates that the barriers to entry for developing offensive OT capabilities are lowering as actors leverage knowledge from prior attacks to develop new malware.

Given that threat actors use red team tools and public exploitation frameworks for targeted threat activity in the wild, COSMICENERGY poses a plausible threat to affected electric grid assets.

To read more:
https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response

Number 9

NIST Team Demonstrates Novel Way to Convert Heat to Electricity

Researchers at the National Institute of Standards and Technology (NIST) have fabricated a novel device that could dramatically boost the conversion of heat into electricity.

If perfected, the technology could help recoup some of the heat energy that is wasted in the U.S. at a rate of about $100 billion each year.

The new fabrication technique — developed by NIST researcher Kris Bertness and her collaborators — involves depositing hundreds of thousands of microscopic columns of gallium nitride atop a silicon wafer.

Layers of silicon are then removed from the underside of the wafer until only a thin sheet of the material remains.

The interaction between the pillars and the silicon sheet slows the transport of heat in the silicon, enabling more of the heat to convert to electric current.

Bertness and her collaborators at the University of Colorado Boulder reported the findings online March 23 in Advanced Materials.

Once the fabrication method is perfected, the silicon sheets could be wrapped around steam or exhaust pipes to convert heat emissions into electricity that could power nearby devices or be delivered to a power grid. Another potential application would be cooling computer chips.

The NIST-University of Colorado study is based on a curious phenomenon first discovered by German physicist Thomas Seebeck.

In the early 1820s, Seebeck was studying two metal wires, each made of a different material, that were joined at both ends to form a loop.

He observed that when the two junctions connecting the wires were kept at different temperatures, a nearby compass needle deflected.

Other scientists soon realized that the deflection occurred because the temperature difference induced a voltage between the two regions, causing current to flow from the hotter region to the colder one. The current created a magnetic field that deflected the compass needle.

In theory, the so-called Seebeck effect could be an ideal way to recycle heat energy that would otherwise be lost. But there's been a major obstacle. A material must conduct heat poorly in order to maintain a temperature difference between two regions yet conduct electricity extremely well to convert the heat to a substantial amount of electrical energy.

For most substances, however, heat conductivity and electrical conductivity go hand in hand; a poor heat conductor makes for a poor electrical conductor and vice versa.

In studying the physics of thermoelectric conversion, theorist Mahmoud Hussein of the University of Colorado discovered that these properties could be decoupled in a thin membrane covered with nanopillars — standing columns of material no more than a few millionths of a meter in length, or about one-tenth the thickness of a human hair. His finding led to the collaboration with Bertness.

Using the nanopillars, Bertness, Hussein and their colleagues succeeded in uncoupling the heat conductivity from electrical conductivity in the silicon sheet — a first for any material and a milestone for enabling efficient conversion of heat to electrical energy.

The researchers reduced the heat conductivity of the silicon sheet by 21% without lowering its electrical conductivity or changing the Seebeck effect.

In silicon and other solids, atoms are constrained by bonds and cannot move freely to transmit heat. As a consequence, the transport of heat energy takes the form of phonons — moving collective vibrations of the atoms.

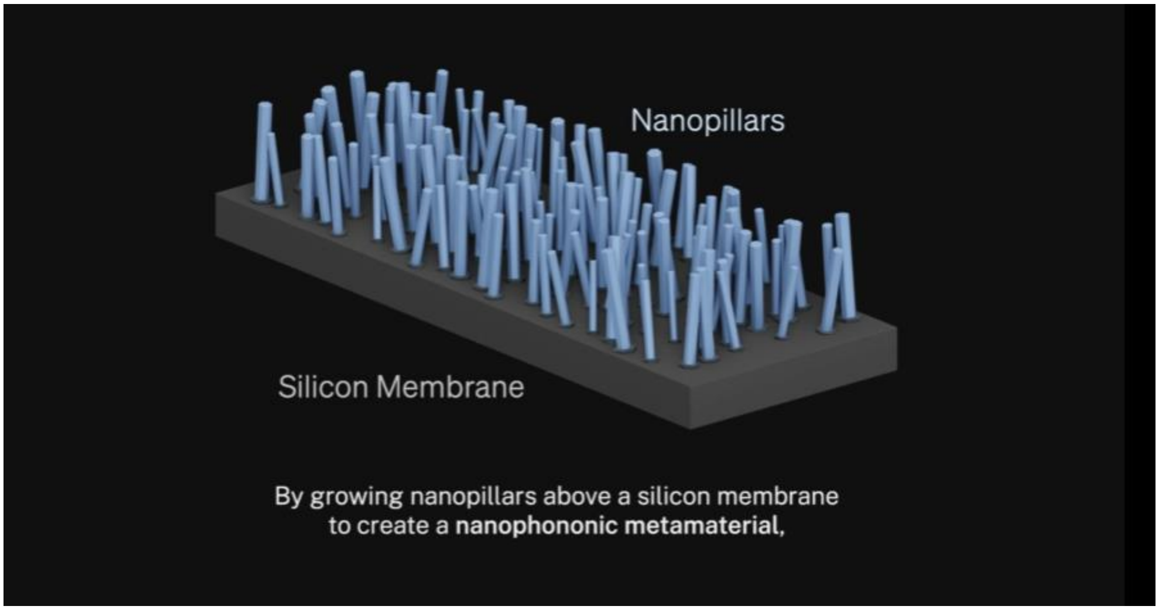
Both the gallium nitride nanopillars and the silicon sheet carry phonons, but those within the nanopillars are standing waves, pinned down by the walls of the tiny columns much the way a vibrating guitar string is held fixed at both ends.

The interaction between the phonons traveling in the silicon sheet and the vibrations in the nanopillars slow the traveling phonons, making it harder for heat to pass through the material.

This reduces the thermal conductivity, thus increasing the temperature difference from one end to the other. Just as importantly, the phonon interaction accomplishes this feat while leaving the electrical conductivity of the silicon sheet unchanged.

The team is now working on structures fabricated entirely of silicon and with a better geometry for thermoelectric heat recovery.

The researchers expect to demonstrate a heat-to-electricity conversion rate high enough to make their technique economically viable for industry.



To read more:
https://www.nist.gov/news-events/news/2023/05/nist-team-demonstrates-novel-way-convert-heat-electricity

Number 10

Taking a New Look at Fundamental Tech for Quiet Undersea Propulsion

DARPA sees opportunity to finally make efficient, scalable magnetohydrodynamic drive a reality

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Since the 1960s, academic, commercial, and military researchers have attempted to realize a novel form of maritime propulsion involving no moving parts – no propeller, no drive shaft, no seals – just magnets and an electric current that silently propel a boat or submarine through water.

Developers have had some success over the decades demonstrating magnetohydrodynamic (MHD) drive technology on a small scale, but it has been inefficient and impractical for full-scale systems due to a couple big tech hurdles.

The first challenge has been inability to generate powerful enough magnetic fields to enable high-efficiency pumps.

The second has been lack of electrode materials that can withstand corrosion, hydrolysis, and erosion caused by the interaction of magnetic fields, electrical current, and saltwater.

In recent years, breakthroughs in generating high magnetic fields have been demonstrated, but the electrode materials problem remains.

To address the materials challenge, DARPA announced the Principles of Undersea Magnetohydrodynamic Pumps (PUMP) program that seeks to create novel electrode materials suitable for a militarily significant MHD drive.

The program will assemble and validate multi-physics modeling and simulation tools including hydrodynamics, electrochemistry, and magnetics for scaling MHD designs.

The goal of the program is to determine an electrode material system and prototype an MHD drive that could be scaled up.

“The best efficiency demonstrated in a magnetohydrodynamic drive to date was 1992 on the Yamato-1, a 30m vessel that achieved 6.6 knots with an efficiency of around 30% using a magnetic field strength of approximately 4 Tesla,” said Susan Swithenbank, PUMP program manager in DARPA’s Defense Sciences Office.

“In the last couple years, the commercial fusion industry has made advances in rare-earth barium copper oxide (REBCO) magnets that have demonstrated large-scale magnetic fields as high as 20 Tesla that could potentially yield 90% efficiency in a magnetohydrodynamic drive, which is worth pursuing. Now that the glass ceiling in high magnetic field generation has been broken, PUMP aims to achieve a breakthrough to solve the electrode materials challenge.”

A major problem when electric current, magnetic field, and saltwater interact is the development of gas bubbles over the electrode surfaces. The bubbles reduce efficiency and can collapse and erode the electrode surfaces.

PUMP will address different approaches to reduce the effect of hydrolysis and erosion. The program also will enable modeling of interactions between the magnetic field, the hydrodynamic, and the electrochemical reactions, which all happen on different time and length scales.

“We’re hoping to leverage insights into novel material coatings from the fuel cell and battery industries, since they deal with the same bubble generation problem,” Swithenbank said.

“We’re looking for expertise across all fields covering hydrodynamics, electrochemistry, and magnetics to form teams to help us finally realize a militarily relevant scale magnetohydrodynamic drive.”

PUMP is a 42-month program. There are multiple potential approaches to the MHD system including conductive and inductive approaches.

The conductive approach involves a conductive current between a pair of electrodes within a magnetic field. The inductive approach uses a time-varying magnetic field and electric current.

A Broad Agency Announcement (BAA) solicitation with full program details will be posted on www.SAM.gov

To read more:
https://www.darpa.mil/news-events/-2023-05-18

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,

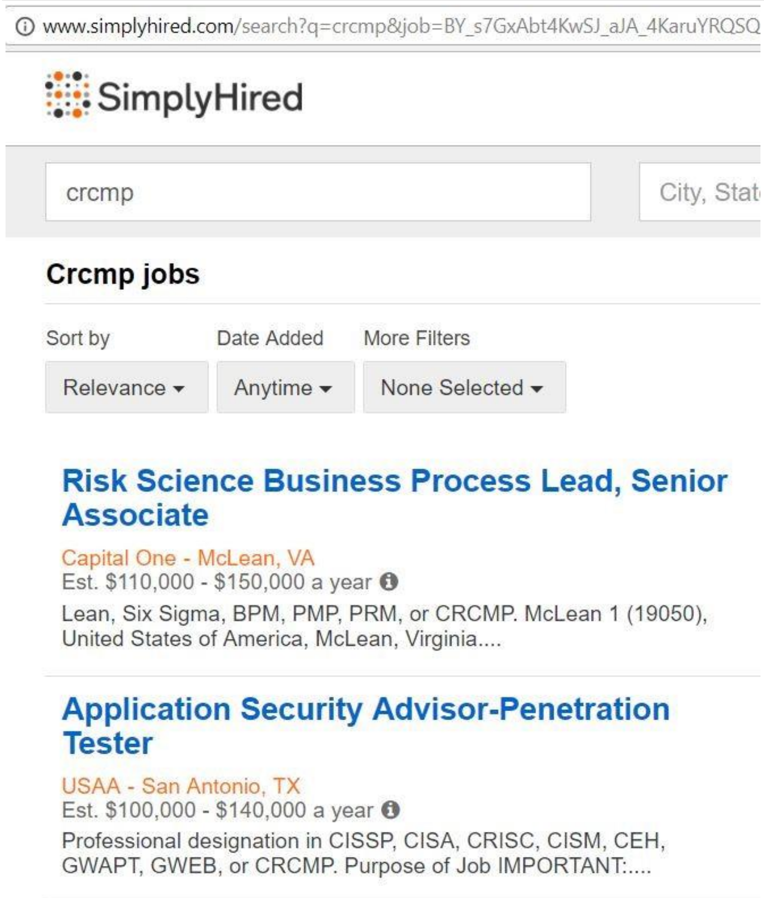
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- 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...



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

SimplyHired

crcmp

City, Stat

Crcmp jobs

Sort by | Date Added | More Filters

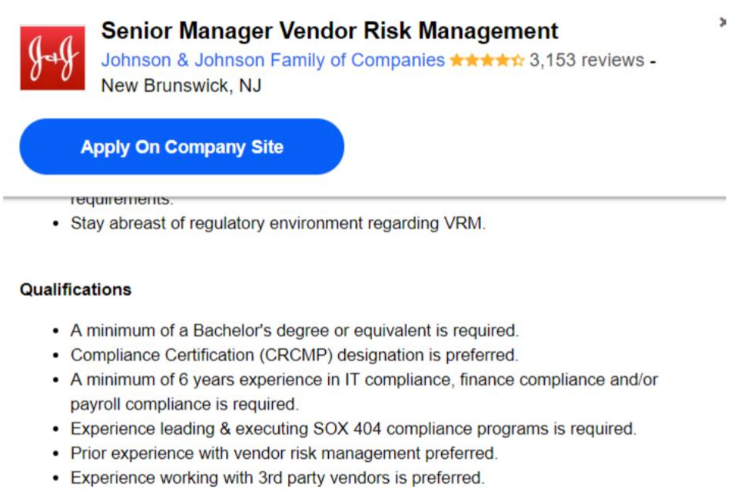
Relevance | Anytime | None Selected

Risk Science Business Process Lead, Senior Associate

Capital One - McLean, VA
Est. $110,000 - $150,000 a year
Lean, Six Sigma, BPM, PMP, PRM, or CRCMP. McLean 1 (19050), United States of America, McLean, Virginia....

Application Security Advisor-Penetration Tester

USAA - San Antonio, TX
Est. $100,000 - $140,000 a year
Professional designation in CISSP, CISA, CRISC, CISM, CEH, GWAPT, GWEB, or CRCMP. Purpose of Job IMPORTANT:....



Senior Manager Vendor Risk Management

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

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

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

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

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

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

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

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

For the Travel Security Trained Professional (TSecTPro), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm

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

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

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