Monday, January 29, 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.

Enrico Fermi (the physicist renowned for being the creator of the world's first nuclear reactor, the Chicago Pile-1), had said: "There are two possible outcomes: if the result confirms the hypothesis, then you've made a measurement. If the result is contrary to the hypothesis, then you've made a discovery."

I have just read carefully the Initial Public Draft, NIST SP 800-55v1 ipd, "Measurement Guide for Information Security, Volume 1 — Identifying and Selecting Measures".

We read: "The terms measurement and assessment are often used interchangeably in the information security field. This document provides a lexicon for key terminology and an overview of foundational concepts to those looking to measure and assess information security risk and clarifies the distinction between measurement and assessment.

As described in Sec. 1.4, assessment refers to the process of evaluating, estimating, or judging against defined criteria, and measurement is the process of obtaining quantitative values. Hence, assessment is a broader concept that also includes measurement.

Organizations perform multiple kinds of assessment when evaluating information security risk, such as risk assessments, program assessments, and control assessments. Risk assessments are used to identify the risks that an organization faces and can support decision-making.

Program-level assessments are used for decision-making about the strategies, policies, procedures, and operations that determine the security posture of an information security program.

In control assessments, organizations evaluate whether specific controls are performing the way they were intended and achieving the desired results. Both program assessments and control assessments are in and of themselves a form of risk assessment and provide a different lens for viewing information security risk.

SP 800-55 is intentionally agnostic on specific risk assessment models. However, many identify threat, likelihood, vulnerability, and impact as areas to assess."

Later in the paper, we read: "Measures are numerically expressed data that are gathered through the process of measurement. Measures can be derived from any operations or systems that can be measured with numbers. Quantitative assessments judge measures data against a set criteria or target and can be used to analyze information security risks using frequency, rates, financial impacts, and other numeric indicators."

Ben Bernanke, the economist who served as the 14th chairman of the Federal Reserve, has said: "In many spheres of human endeavor, from science to business to education to economic policy, good decisions depend on good measurement." Well, I do understand that, but I always have doubts about our ability for "good measurement" in areas like economic policy and risk management. Sometimes we follow Galileo Galilei's advice: "Measure what is measurable and make measurable what is not so."

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 1)

NIST SP 800-55 Vol. 1 (Initial Public Draft) Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures

Number 2 (Page 1)

FSB Work Programme for 2024

Number 3 (Page 1)

The path forward for bank capital reform

Michelle W Bowman, Member of the Board of Governors of the Federal Reserve System, at the Protect Main Street, sponsored by the Center for Capital Markets at the US Chamber of Commerce, Washington DC.

Number 4 (Page 1)

Signal versus noise

Ben Broadbent, Deputy Governor for Monetary Policy of the Bank of England, at the London Business School, London.

Number 5 (Page 1)

The EBA publishes its heatmap following scrutiny of the interest rate risk in the banking book

Number 6 (Page 1)

Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

Number 7 (Page 1)

Chinese Espionage Group UNC3886 Found Exploiting CVE-2023-34048 Since Late 2021

Number 8 (Page 1)

Ghidra

NSA's reverse engineering tool that helps cybersecurity professionals analyze malicious code and malware

Number 9 (Page 1)

CISA and ENISA enhance their Cooperation

Number 10 (Page 1)

Voices from DARPA

Podcast Episode 75: The Metamaterial Visionary

Program manager in DARPA's Defense Sciences Office highlights fascinating optics programs made possible by novel engineered materials

Number 1

NIST SP 800-55 Vol. 1 (Initial Public Draft) Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures

The initial public drafts of NIST Special Publication (SP) 800-55, Measurement Guide for Information Security, Volume 1 – Identifying and Selecting Measures and Volume 2 – Developing an Information Security Measurement Program are available for comment after extensive research, development, and customer engagement.

In response to the feedback from the pre-draft call for comment and initial working draft (annotated outline), NIST continued to refine the publications by organizing the guidance into two volumes and developing more actionable and focused guidance in each.

Volume 1 – Identifying and Selecting Measures is a flexible approach to the development, selection, and prioritization of information security measures. This volume explores both quantitative and qualitative assessment and provides basic guidance on data analysis techniques as well as impact and likelihood modeling.

Volume 2 — Developing an Information Security Measurement Program is a methodology for developing and implementing a structure for an information security measurement program.

Table 1. Stevens Scale of Measurement

Scale Level	Definition
Nominal	A nominal scale only looks at classification or identification. Nominal scales are used in surveys and in dealings with either non-numeric variables or numbers that do not have an assigned value. The data collected from a nominal scale can be used for counting, mode, or correlation contingency matrices.
Ordinal	An ordinal scale is similar to a nominal scale in that it primarily uses non-numeric values or numbers that are meant to show ranking. Related statistics include medians and percentiles.
Interval	An interval scale is used when measuring variables with equal intervals between values. When using an interval scale, there is no true zero. Examples of the use of interval scales are temperature or time scales. Interval data allows for quantitative analysis, such as descriptive statistics like frequency, averages, position, and dispersion. Interval statistics include mean, standard deviation, and rank-order correlation.
Ratio	Ratio scales allow for the categorization and ranking of data, similar to an interval scale, but with a true zero and no negative values. Ratio scales allow for numbers to be used for addition, subtraction, multiplication, and division.

*Some organizational motivations may benefit from quantitative assessments, such as trying to determine whether the organization is patching known vulnerabilities in an acceptable amount of time. Knowing the **mean time to remediate a vulnerability** provides more precise insight into patching efficiency than simply knowing the number of vulnerabilities patched in a year. Because the question of **mean time to remediate a vulnerability** deals in non-zero numbers that are attainable to gather, a measurement can be taken, and a mathematically derived answer can be given.*

Type of Assessment	Approach	Example
Risk Assessment	Classical (Value at Risk)	An organization conducting a risk assessment will likely consider their value at risk (VaR) if they were to suffer an adverse information security event. The organization may look at potential losses from downtime, the cost of repairing the environment, or reputational damage.
Risk Assessment	Bayesian	The Bayesian method looks at prior distribution, collected data, and set parameters to make inferences about future outcomes. Using data from SP 800-53 control RA-3(4), Predictive Cyber Analytics, as part of a risk assessment, the inferences found through the Bayesian method allow organizations to make risk-based decisions based on the likelihood of future events.

NIST Special Publication 800
NIST SP 800-55v1 ipd

Measurement Guide for Information Security

Volume 1 — Identifying and Selecting Measures

To read more: https://csrc.nist.gov/pubs/sp/800/55/v1/ipd

Number 2

FSB Work Programme for 2024

The Financial Stability Board's (FSB) work programme for 2024 aims to maximise the value of its work to foster global financial stability while preserving the capacity for the FSB to respond to new issues that may emerge.

The FSB's work priorities reflect the global nature of financial challenges and their ability to affect the financial system as a whole. These challenges include digitalisation, climate change, and the consequences of shifts in the macroeconomic and interest rate environment.

This note summarises ongoing and planned FSB initiatives in 2024. The Annex provides an indicative timeline of the FSB's planned publications in 2024.

Supporting global cooperation on financial stability. Vulnerabilities in the global financial system continue to be elevated, reflecting high interest rates and an uncertain growth outlook, while vulnerabilities from structural change continue to emerge in areas such as climate change, cyber and crypto-asset markets.

These challenges are increasingly affecting the functioning of the financial system through various channels and make global cooperation on financial stability matters as important now as it was after the 2008 global financial crisis.

The FSB, with its broad and diverse membership of national authorities, international standard setters, and international bodies, continues to promote financial stability in a rapidly evolving environment.

As part of this work, the FSB will continue to participate in the joint FSB-IMF Early Warning Exercise. The FSB is constantly updating its monitoring to identify, assess and address new and emerging risks to global financial stability.

The FSB's surveillance framework forms the basis of this monitoring. Work will continue to more fully integrate monitoring of vulnerabilities associated with technological innovation, climate change and non-bank financial intermediation (NBFI).

Completing resolution reforms. The FSB will continue its work to promote the full implementation of the Key Attributes of Effective Resolution Regimes for Financial Institutions across all sectors.

The focus will be to address the lessons learned from the March 2023 banking turmoil, to finalise the work on central counterparty (CCP) financial resources and tools for resolution and to enhance the process for developing the list of insurers subject to resolution planning.

In 2024, the FSB will:

■ conduct follow-up work on public sector backstop funding mechanisms, operationalisation of bail-in, resolution strategies and tools, and the impact of social media and digital innovation on resolution;

■ finalise its toolbox for CCP resolution authorities to have access to a combination of resources and/or tools to use in CCP resolution; and

■ publish the list of insurers subject to the resolution planning standards of the Key Attributes, based on reporting by member authorities.

Other post March 2023 banking turmoil work. Work will continue to address other issues highlighted by the banking turmoil in March 2023.

This includes work on:

■ Deposit behaviour and the role of technology and social media.

■ Interest rate and liquidity risk in the financial system.

Implementing the systemically important financial institution (SIFI) framework. As part of the FSB framework for SIFIs, the FSB will:

■ Continue its annual review and publication of the list of designated G-SIBs.

■ Monitor insurer systemic risk annually based on the IAIS Holistic Framework reporting.

Enhancing the resilience of NBFI. The NBFI sector has grown faster than the banking sector since the 2008 global financial crisis and has become more diverse. As a result, the importance of NBFI for the financing of the real economy has increased.

The FSB will continue to advance its work programme for enhancing NBFI resilience, which is carried out by the FSB and by standard-setting bodies (SSBs) and international organisations.

This includes:

■ exploring policy recommendations or policy options for non-bank financial leverage,

■ completing the data pilot project to enhance authorities' and the FSB's ability to monitor vulnerabilities associated with open-ended fund liquidity mismatch,

■ enhancing liquidity preparedness of non-bank market participants for margin and collateral calls,

■ conducting new work on the functioning and resilience of repo markets, and

■ publishing its annual Global Monitoring Report on NBFI.

Enhancing cross-border payments. The G20 Roadmap for enhancing cross-border payments, coordinated by the FSB, contains a comprehensive set of actions4 and a framework for monitoring progress toward achieving the quantitative targets that have been set for end2027.

The FSB, working with the Committee on Payments and Market Infrastructures (CPMI) and other SSBs and international organisations, will continue to coordinate taking forward the actions in 2024.

Actions led by the FSB include work on bank and non-bank supervision and work on data frameworks.

The Roadmap places importance on public-private sector partnerships, including the annual Payments Summit and taskforces that were set up in 2023.

To read more: https://www.fsb.org/wp-content/uploads/P240124.pdf

Number 3

The path forward for bank capital reform

Michelle W Bowman, Member of the Board of Governors of the Federal Reserve System, at the Protect Main Street, sponsored by the Center for Capital Markets at the US Chamber of Commerce, Washington DC.

"More is better." This axiom often holds true in many respects, but experience also teaches us that there are limits.

Today, I'm happy to join you here at the U.S. Chamber of Commerce to talk about proposed changes to bank capital rules in the United States and to probe the limits of the notion that "more is better" when regulators seek to apply it to bank capital requirements.

In July 2023, the federal banking agencies proposed changes to implement the Basel III "endgame" capital reforms.

The published capital rulemaking proposal incorporated an expansive scope and a notable shift in approach by pushing down new Basel capital requirements to all banks with over $100 billion in assets, regardless of their international activities.

The proposal would substantially increase regulatory capital buffer and minimum capital requirements for the covered firms.

The comment period closed yesterday, January 16th. We've seen a robust response from commenters, with a large number of comments submitted during the latter part of the comment period.

As a policymaker, I am pleased to see the careful attention stakeholders have paid to this proposal and the thoughtful feedback that has been provided during the comment period.

Public input should help to improve the efficiency and effectiveness of the proposal.

From my perspective, given the significant response from a number of industries and perspectives, as a bank regulatory policymaker, the agencies are obligated to think carefully about the best path forward for this proposal.

This should include making substantive changes to address known deficiencies with the proposal and giving the public an opportunity to comment on any reformulated proposal, to ensure the best possible outcome for the Basel capital reforms.

That path should ensure that sufficient consideration is given to the wide-reaching consequences of capital reform to the U.S. banking industry, the U.S. economy, and, importantly, U.S. businesses.

We should consider tradeoffs in addressing scope, calibration, and tailoring. And we should appropriately adjust the excessive calibrations and eliminate regulatory overreach in the proposed rule.

To read more:
https://www.federalreserve.gov/newsevents/speech/bowman20240117a.htm

Number 4

Signal versus noise

Ben Broadbent, Deputy Governor for Monetary Policy of the Bank of England, at the London Business School, London.

We are all aware that the future is unpredictable. When it comes to gauging the economy, however, it's not just the future that's uncertain: so is the present. For all the time and effort put into its forecasts the MPC also spends a great deal of it getting to understand the here and now.

This isn't straightforward. For one thing, it's not always possible to determine precisely what's causing what – to trace the economy we observe back to the underlying forces that are driving it.

Is output growth being moved around by demand or supply? Ditto employment? To take an example of particular relevance right now, has strong wage growth been the result of exceptional tightness of the labour market, especially last year; or is it the "second-round effect" of very high spot inflation in late 2022 and earlier this year?

These things aren't mutually exclusive: almost certainly, both have played a part. But the balance of the two matters. As the direct effects of the pandemic and the war dissipate, wholesale prices of energy and other traded goods have been declining.

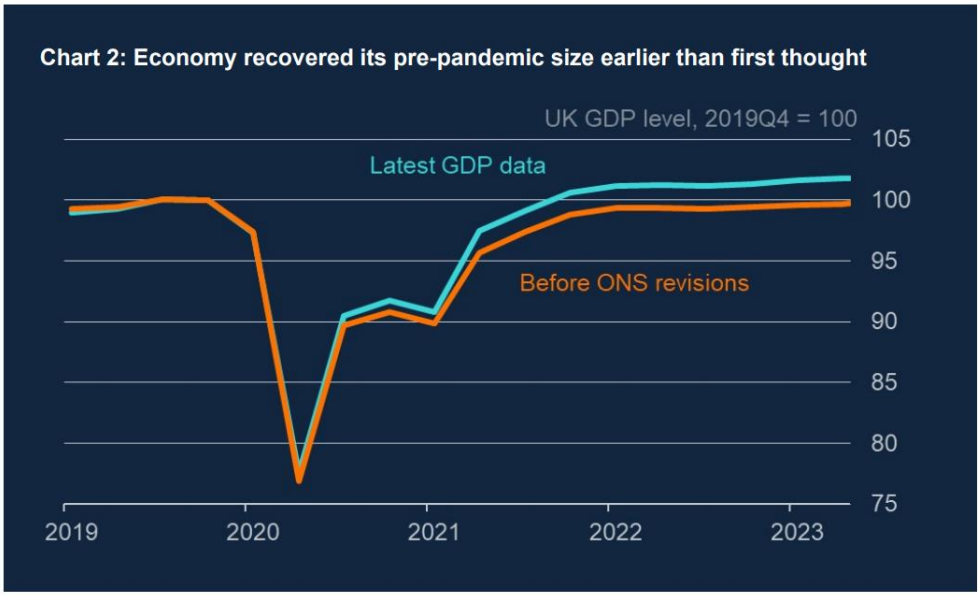
Sources: ONS and Bank calculations. Core output PPI is for manufactured products excluding non-core items. Core output PPI annual inflation is advanced by two months, which maximises correlation with CPI core goods inflation.

This is now feeding through to inflation rates for retail goods prices and the aggregate CPI itself (Chart 1 plots core goods inflation against its wholesale counterpart; there have been similar trends in food and energy markets).

As this happens, one might expect these second-round effects on wage growth and broader domestic inflation to weaken as well, quite independently of the stance of monetary policy.

To the extent the tight labour market is the cause of strong domestic inflation, however, then the economy would need a longer period of below-trend growth – possibly with corresponding consequences for monetary policy – to bring it back into a more sustainable position.

At any rate, the more general point is that it's not always easy to infer the deeper, unobserved causes of economic fluctuations from the directly observable information.



Sources: ONS and Bank calculations. ONS 2023 Blue Book revisions. See Box C in the November Monetary Policy Report for more details.

Second, even what we do get to observe – GDP, employment, wages and the like – may not be perfectly measured.

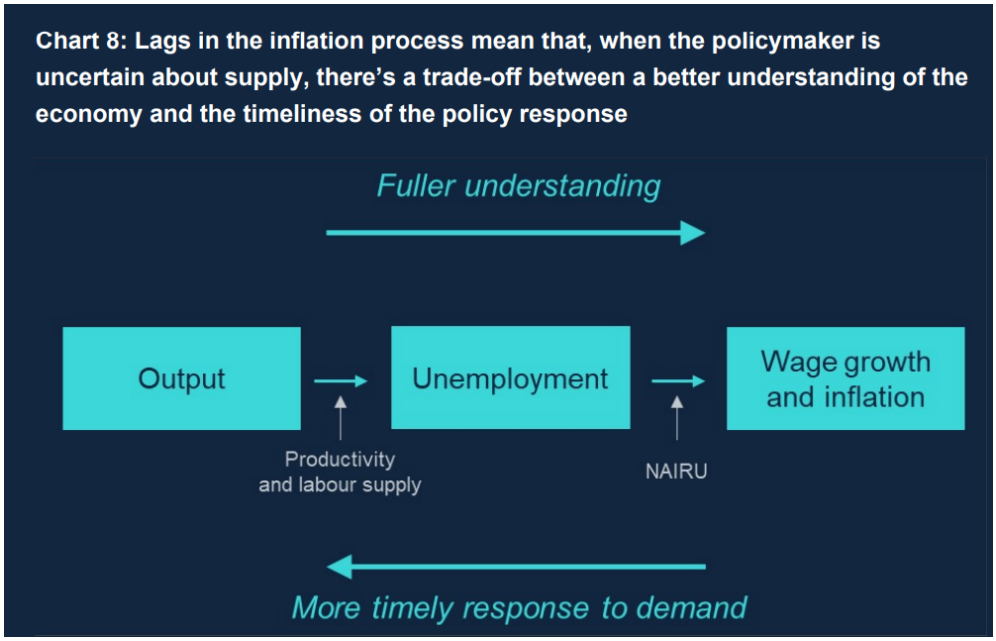
For some things (notably GDP) the relevant information comes in only over time and, as a result, the data are subject to revision.

These changes can be sizeable. Recently, for example, estimated growth during 2020 and 2021 was revised up by almost two percentage points (Chart 2).

As a result the economy is now thought to have reached its pre-pandemic size nearly two years earlier than was previously thought.

To read more:

https://www.bankofengland.co.uk/speech/2023/december/ben-broadbent-speech-at-london-business-school#:~:text=In%20this%20speech%20Ben%20talks,the%20economy%20and%20incoming%20data.



Number 5

The EBA publishes its heatmap following scrutiny of the interest rate risk in the banking book

Interest rate risk in the banking book (IRRBB) is by nature a complex risk to assess. It is part of an 'enhanced' Pillar 2 framework, generally relying on modelling approaches that can be quite heterogeneous depending on jurisdictions markets' structures.

In addition, contrary to internal models used under a Pillar 1 framework, the use of IRRBB internal models is not subject to prior approval from supervisors.

Supervisory assessment of IRRBB must be supported by an appropriate regulatory toolkit, given the materiality of this risk for institutions and the impact of non-maturity deposits (NMDs) modelling assumptions calibration after more than a decade of low interest rates, considering the materiality of this risk for large and small institutions.

The dedicated attention to the enhanced IRRBB supervision forms a key part of the 2024 European Supervisory Examination Programme.

The implementation into EU rules of the Basel standards on IRRBB published by the Basel Committee on Banking Supervision in April 2016 started with the EBA Guidelines (GL) on the management of interest rate risk arising from non-trading book activities.

These GL, published on the EBA website in July 2018, introduced supervisory requirements regarding the management of IRRBB, encompassing the identification, measurement, monitoring and control of IRRBB.

The GL also included the revised supervisory outlier tests (SOT) on the Economic Value of Equity (EVE) as an early warning signal and high-level guidance on credit spread risk in the banking book (CSRBB).

In a second step the implementation of the Basel IRRBB standards into EU has taken place by means of the publication in October 2022 of the EBA mandates stemming from the Directive 2013/36/EU and issuing an IRRBB regulatory package.

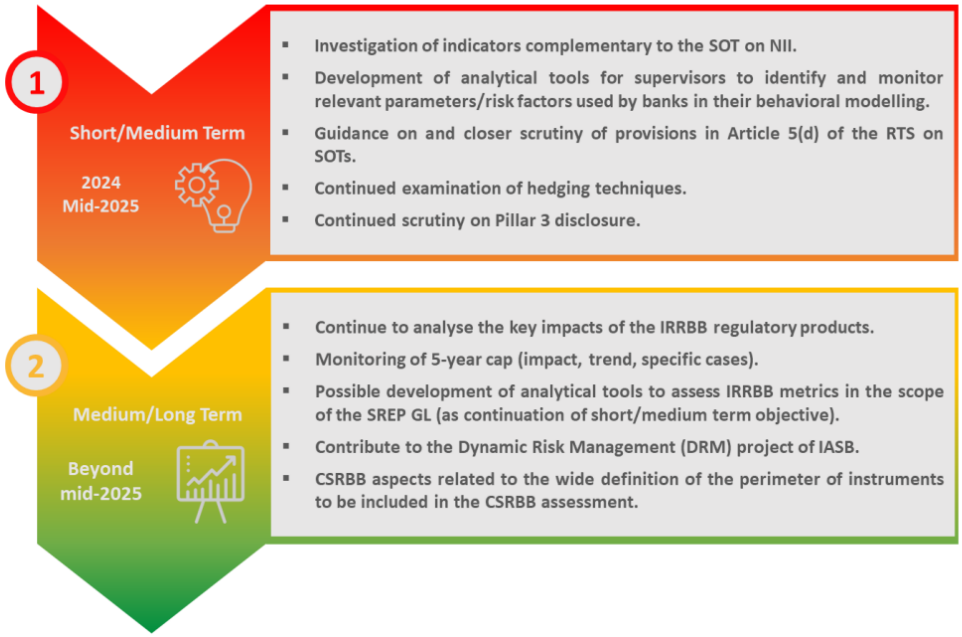
This package included draft Regulatory Technical Standards (RTS) on the SOT, draft RTS on the standardised approach (SA) and revised GL on IRRBB and CSRBB.

While providing continuity to the previous GL on the management of interest rate risk arising from non-trading book activities, the updated GL include new aspects,

particularly the criteria to identify non-satisfactory IRRBB internal systems and criteria to assess and monitor CSRBB.

These GL apply from 30 June 2023, except for the part on CSRBB, which apply from 31 December 2023.

Annex I: Heatmap following the EBA scrutiny on the IRRBB



To read more:
https://www.eba.europa.eu/sites/default/files/2024-01/4eff856e-650f-4080-9dcb-7e03fbb6f1d1/Heatmap%20following%20the%20EBA%20scrutiny%20on%20the%20IRRBB%20Standards%20implementation%20in%20the%20EU.pdf

Number 6

Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

Microsoft

The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024, and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access.

Microsoft has identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as Nobelium. As part of our ongoing commitment to responsible transparency as recently affirmed in our Secure Future Initiative (SFI), we are sharing this update.

Beginning in late November 2023, the threat actor used a password spray attack to compromise a legacy non-production test tenant account and gain a foothold, and then used the account's permissions to access a very small percentage of Microsoft corporate email accounts, including members of our senior leadership team and employees in our cybersecurity, legal, and other functions, and exfiltrated some emails and attached documents.

The investigation indicates they were initially targeting email accounts for information related to Midnight Blizzard itself. We are in the process of notifying employees whose email was accessed.

The attack was not the result of a vulnerability in Microsoft products or services. To date, there is no evidence that the threat actor had any access to customer environments, production systems, source code, or AI systems. We will notify customers if any action is required.

This attack does highlight the continued risk posed to all organizations from well-resourced nation-state threat actors like Midnight Blizzard.

As we said late last year when we announced Secure Future Initiative (SFI), given the reality of threat actors that are resourced and funded by nation states, we are shifting the balance we need to strike between security and business risk – the traditional sort of calculus is simply no longer sufficient.

For Microsoft, this incident has highlighted the urgent need to move even faster. We will act immediately to apply our current security standards to Microsoft-owned legacy systems and internal business processes, even when these changes might cause disruption to existing business processes.

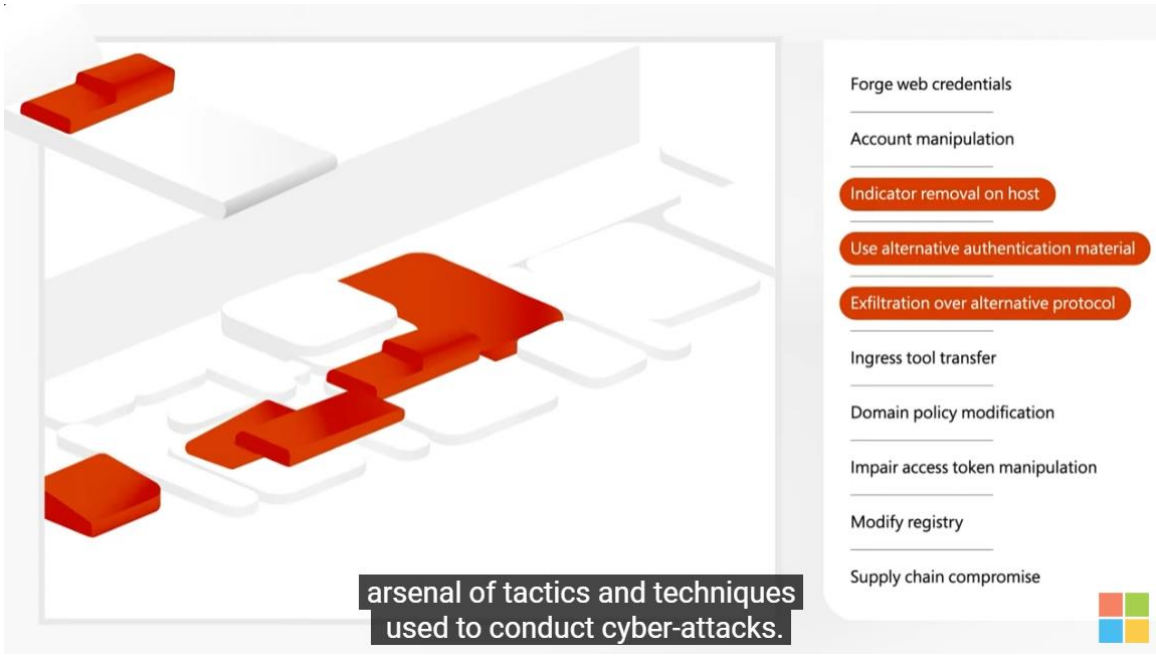
This will likely cause some level of disruption while we adapt to this new reality, but this is a necessary step, and only the first of several we will be taking to embrace this philosophy.

We are continuing our investigation and will take additional actions based on the outcomes of this investigation and will continue working with law enforcement and appropriate regulators.

We are deeply committed to sharing more information and our learnings, so that the community can benefit from both our experience and observations about the threat actor. We will provide additional details as appropriate.

To read more:
https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

https://www.youtube.com/watch?v=wFtGD7p58cQ



Number 7

Chinese Espionage Group UNC3886 Found Exploiting CVE-2023-34048 Since Late 2021

While publicly reported and patched in October 2023, Mandiant and VMware Product Security have found UNC3886, a highly advanced China-nexus espionage group, has been exploiting CVE-2023-34048 as far back as late 2021.

These findings stem from Mandiant's continued research of the novel attack paths used by UNC3886, which historically focuses on technologies that are unable to have EDR deployed to them. UNC3886 has a track record of utilizing zero-day vulnerabilities to complete their mission without being detected, and this latest example further demonstrates their capabilities.

When covering the discovery of CVE-2023-20867 in VMware's tools, the attack path in Figure 1 was presented describing the flow of attacker activity within the VMware ecosystem (i.e. vCenter, ESXi Hypervisors, Virtualized Guest Machines). At the time, with the evidence available, Mandiant continued researching how backdoors were being deployed to vCenter systems.

To read more:
https://www.mandiant.com/resources/blog/chinese-vmware-exploitation-since-2021

Number 8

Ghidra

You can download NSA's reverse engineering tool that helps cybersecurity professionals analyze malicious code and malware like viruses and gives them a better understanding of potential vulnerabilities in their networks and systems.

Ghidra is one of many open-source software (OSS) projects developed within the National Security Agency. Complete source code for Ghidra along with build instructions have been added to the repository. Please read the updated CONTRIBUTING guide to find out more about how you can join the community.

To read more:
https://www.nsa.gov/Cybersecurity/Cybersecurity-Products-Services/

Number 9

CISA and ENISA enhance their Cooperation

Geopolitics have shaped the cyber threat landscape, bringing like-minded partners closer together in the wake of common cyber challenges and advances in digital technologies.

At the EU-US Cyber Dialogue, ENISA and CISA announced the signing of their Working Arrangement as an important milestone in the overall cooperation between the United States and the European Union in the field of cybersecurity, also following the Joint Statement of European Commissioner Thierry Breton and U.S. Secretary for Homeland Security Alejandro Mayorkas of January 2023.

ENISA's International Strategy directs the Agency to be selective in engaging with international partners and to limit its overall approach in international cooperation to those areas and activities that will have high and measurable added value in achieving the Agency's strategic objectives.

CISA is a key partner to ENISA in achieving these objectives and by extension the EU in achieving a higher common level of cybersecurity.

The Working Arrangement is both a consolidation of present areas of cooperation, as well as opening the door to new ones.

Current examples are the organisation and promotion of the International Cybersecurity Challenge (ICC), exchanging best practices in the area of incident reporting or ad hoc information exchanges on basic cyber threats.

This arrangement is broad in nature and covers both short-term structured cooperation actions, as well as paving the way for longer-term cooperation in cybersecurity policies and implementation approaches.

Cooperation will be sought in the areas of:

1. Cyber Awareness & Capacity Building to enhance cyber resilience: including facilitating the participation as third country representatives in specific EU-wide cybersecurity exercises or trainings and the sharing and promotion of cyber awareness tools and programmes.

2. Best practice exchange in the implementation of cyber legislation; including on key cyber legislation implementation such as the NIS Directive, incident reporting, vulnerabilities management and the approach to sectors such as telecommunications and energy.

3. Knowledge and information sharing to increase common situational awareness: including a more systematic sharing of knowledge and information in relation to the cybersecurity threat landscape to increase the common situational awareness to the stakeholders and communities and in full respect of data protection requirements.

A work plan will operationalise the Working Arrangement and regular reporting at the EU-US Cyber Dialogues is foreseen.

To read more:
https://www.enisa.europa.eu/news/cisa-and-enisa-enhance-their-cooperation

Number 10

Voices from DARPA

Podcast Episode 75: The Metamaterial Visionary

Program manager in DARPA's Defense Sciences Office highlights fascinating optics programs made possible by novel engineered materials

We usually think of materials based on our experience in the natural world. For example, something that's light is usually fragile (like a feather) or something heavy is usually strong (like a brick).

But what if we could engineer a material that had completely new characteristics that defied properties found in nature?

Engineered materials, also known as metamaterials, allow us to do just that. DARPA Program Manager Dr. Rohith Chandrasekar in DARPA's Defense Sciences Office has led programs designing metamaterials that revolutionize how light interacts with matter.

His programs are enabling new concepts for improving Warfighter effectiveness and health on the battlefield with new optics and materials.

In this episode, Dr. Chandrasekar discusses several of these programs including Enhanced Night Vision in Eyeglass Form (ENVision), which has developed metamaterials to replace heavy and bulky binocular-like night-vision goggles lenses with lightweight lenses providing more infrared information and near eyesight field of view, in a form factor like a pair of glasses.

He also discusses his Coded Visibility program, which focused on developing novel obscurants (aka smoke) used on the battlefield to provide friendly forces with visibility of the environment, while simultaneously hiding them from detection by an adversary.

The catch, however, is that the smoke particles needed to be safe to breathe and potentially even tunable using active sources. Finally, he talks about the Accelerating discovery of Tunable Optical Materials (ATOM) program.

This effort seeks to identify new materials whose properties could be rapidly changed to enable different functions.

Imagine a massive telephoto camera on the sideline of a sporting event replaced with a planar imaging system that could zoom, or a thin filter that can rapidly collect critical data across infrared bands for spectroscopy, all with no moving parts.

Sounds like magic, but it's not! Enjoy listening to DARPA's Metamaterial Visionary.

To find more: https://www.youtube.com/watch?v=FK15MTLfY5w

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.

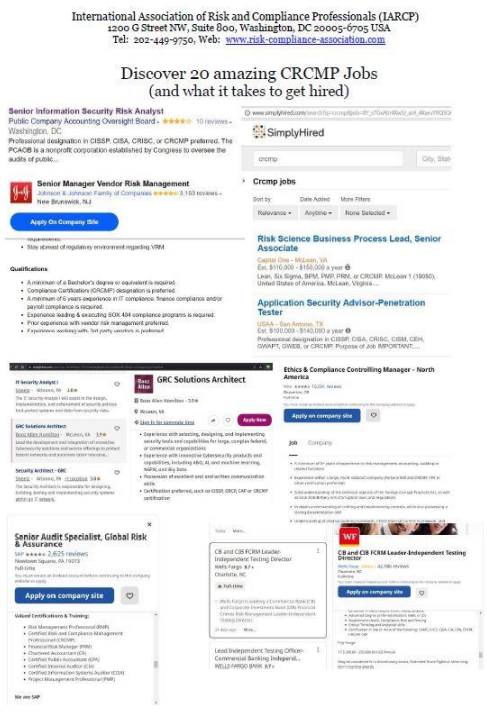
International Association of Risk and Compliance Professionals (IARCP)

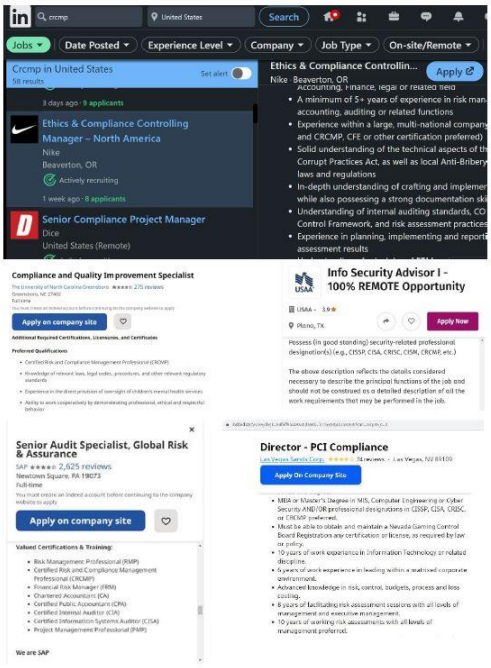
Our training and certification programs:

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