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 28, 2022

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,

I have just read the *Third annual threat assessment* by Mike Burgess, the current Director-General of Security in charge of the Australian Security Intelligence Organisation (ASIO). This is an excellent assessment. We read:

"In the last two years, thousands of Australians with access to sensitive information have been targeted by foreign spies using social media profiles. These spies are adept at using the internet for their recruitment efforts.

On any of the popular social media or internet platforms, they make seemingly innocuous approaches—such as job offers. This then progresses to direct messaging on different, encrypted platforms, or in-person meetings, before a recruitment pitch is made.

I've previously highlighted our concerns about approaches on professional networking sites, but during the pandemic we've seen this threat spread.

There's been a jump in suspicious approaches on messaging platforms like WhatsApp, for example.

It's an easy way for foreign intelligence services to target employees of interest.

ASIO is also tracking suspicious approaches on dating platforms such as Tinder, Bumble and Hinge. My message for any potential victims on these sites is a familiar one—if it seems too good to be true, it probably is!

While espionage is one of the most insidious security threats we are dealing with online, it is not the most concerning trend.

The internet is the world's single most potent and powerful incubator of extremism.

Online radicalisation is nothing new, but COVID-19 sent it into overdrive. Isolated individuals spent more time online, exposed to extremist messaging, misinformation and conspiracy theories.

Social media platforms, chat rooms, and algorithms are designed to join up people who share the same views, and push them material they will 'like'. It's like being in an echo chamber where the echo gets louder and louder, generating cycles of exposure and reinforcement.

More time in those online environments—without some of the circuit breakers of everyday life, like family and community engagement, school and work—created more extremists. And in some cases, it accelerated extremists' progression on the radicalisation pathway towards violence."

This is a great presentation. In a few words, Mike Burgess explains a major problem in all countries. In 5 minutes, employees and managers with access to sensitive information can understand better the modus operandi of foreign intelligence services.

Mike Burgess continues:

"I can confirm that ASIO recently detected and disrupted a foreign interference plot in the lead-up to an election in Australia.

I'm not going to identify the jurisdiction because we are seeing attempts at foreign interference at all levels of government, in all states and territories.

But it is important to explain what political interference actually looks like.

This case involved a wealthy individual who maintained direct and deep connections with a foreign government and its intelligence agencies.

This agent of interference has roots in Australia but did the bidding of offshore masters, knowingly and covertly seeking to advance the interests of the foreign power and, in the process, undermine Australia's sovereignty.

I'll call this person 'the puppeteer', although it's important to remember that while the puppeteer pulled the strings, the foreign government called the shots.

The puppeteer hired a person to enable foreign interference operations and used an offshore bank account to provide hundreds of thousands of dollars for operating expenses.

Secretly shaping the jurisdiction's political scene to benefit the foreign power was considered a key performance indicator. It was like a foreign interference start-up.

The employee hired by the puppeteer began identifying candidates likely to run in the election who either supported the interests of the foreign government or who were assessed as vulnerable to inducements and cultivation.

The employee used existing relationships with politicians, staffers and journalists to select potential targets, without revealing the secret intent, the foreign connection or the puppeteer's involvement.

The puppeteer and the employee plotted ways of advancing the candidates' political prospects through generous support, placing favourable stories in foreign language news platforms and providing other forms of assistance.

They investigated hiring political consultants, advertising agencies and PR specialists to help individual campaigns.

The aim was not just to get the candidates into positions of power, but also to generate a sense of appreciation, obligation and indebtedness that could subsequently be exploited.

The political candidates had no knowledge of the plot. Even if the plan had proceeded, they would not have known who was pulling the strings.

The puppeteer used the employee as a cut-out. This deliberate deceit and secrecy about the foreign government connection is what took the case into the realm of foreign interference.

At this point, ASIO acted. Our intervention ensured the plan was not executed, and harm was avoided."

Read more at number 10 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 7)

Justice Department Announces First Director of National Cryptocurrency Enforcement Team

Number 2 (Page 10)

Preparing for the Financial System of the Future

Governor Lael Brainard, at the 2022 U.S. Monetary Policy Forum, New York, New York

Number 3 (Page 17)

BIS Working Papers No 1000

Dollar beta and stock returns

Valentina Bruno, Ilhyock Shim and Hyun Song Shin - Monetary and Economic Department

Number 4 (Page 19)

Why Security Concerns Drive Customers Towards Public DNS Resolvers

The European Union Agency for Cybersecurity (ENISA) analyses the security pros and cons of using public DNS resolvers.

Number 5 (Page 22)

2021 CONSUMER TRENDS REPORT

Number 6 (Page 25)

FSB Chair's letter to G20 Finance Ministers and Central Bank Governors: February 2022

Klaas Knot, Chair of FSB

Number 7 (Page 28)

A repository of free tools and services, from the U.S. Cybersecurity and Infrastructure Security Agency (CISA)

Number 8 (Page 31)

ESRB issues new warnings and recommendations on medium-term residential real estate vulnerabilities

Number 9 (Page 35)

Largest South Korean Telecommunications Co. Agrees to Pay the SEC to Settle FCPA Charges

Number 10 (Page 37)

Third annual threat assessment

Mike Burgess, Director-General of Security, in charge of the Australian Security Intelligence Organisation (ASIO).

Number 1

Justice Department Announces First Director of National Cryptocurrency Enforcement Team

The Justice Department announced the selection and appointment of Eun Young Choi to serve as the first Director of the National Cryptocurrency Enforcement Team (NCET).

Ms. Choi is a seasoned prosecutor with nearly a decade of experience within the department, and most recently served as Senior Counsel to the Deputy Attorney General. She will assume her duties full-time effective today.

"With the rapid innovation of digital assets and distributed ledger technologies, we have seen a rise in their illicit use by criminals who exploit them to fuel cyberattacks and ransomware and extortion schemes; traffic in narcotics, hacking tools and illicit contraband online; commit thefts and scams; and launder the proceeds of their crimes," said Assistant Attorney General Kenneth A. Polite Jr. of the Justice Department's Criminal Division. "The NCET will serve as the focal point for the department's efforts to tackle the growth of crime involving these technologies.

Eun Young is an accomplished leader on cyber and cryptocurrency issues, and I am pleased that she will continue her service as the NCET's inaugural Director, spearheading the department's efforts in this area."

The NCET was established to ensure the department meets the challenge posed by the criminal misuse of cryptocurrencies and digital assets, and comprises attorneys from across the department, including prosecutors with backgrounds in cryptocurrency, cybercrime, money laundering and forfeiture.

The NCET will identify, investigate, support and pursue the department's cases involving the criminal use of digital assets, with a particular focus on virtual currency exchanges, mixing and tumbling services, infrastructure providers, and other entities that are enabling the misuse of cryptocurrency and related technologies to commit or facilitate criminal activity.

The NCET will set strategic priorities regarding digital asset technologies, identify areas for increased investigative and prosecutorial focus, and lead the department's efforts to coordinate with domestic and international law

enforcement partners, regulatory agencies and private industry to combat the criminal use of digital assets.

Finally, the NCET will enhance the Criminal Division's existing efforts to provide support and training to federal, state, local, and international law enforcement to build capacity to aggressively investigate and prosecute serious crimes involving cryptocurrency and digital assets in the United States and around the world.

The NCET's work will be furthered through close collaboration with components across the department, including the Criminal Division's Computer Crime and Intellectual Property Section and Money Laundering and Asset Recovery Section; the U.S. Attorneys' offices; the National Security Division; and the FBI, including the FBI's new Virtual Asset Exploitation Unit, a specialized team of cryptocurrency experts dedicated to providing analysis, support, and training across the FBI, as well as innovating its cryptocurrency tools to stay ahead of future threats.

"The department has been at the forefront of investigating and prosecuting crimes involving digital currencies since their inception," said Director Choi. "The NCET will play a pivotal role in ensuring that as the technology surrounding digital assets grows and evolves, the department in turn accelerates and expands its efforts to combat their illicit abuse by criminals of all kinds.

I am excited to lead the NCET's incredible and talented team of attorneys, and to get to work on this important priority for the department. I would like to thank Assistant Attorney General Polite and the Criminal Division's leadership for this opportunity."

Prior to her service as Senior Counsel to Deputy Attorney General Lisa O. Monaco, Director Choi began her career at the department as an Assistant U.S. Attorney for the Southern District of New York, where she served as the office's Cybercrime Coordinator and investigated and prosecuted cyber, complex fraud and money laundering crimes, with a particular focus on network intrusions, digital currency, the dark web and national security investigations.

She served as lead prosecutor in a variety of cases, including the investigation of a transnational organization responsible for the hacking of J.P. Morgan Chase and a dozen other financial companies; the operation of Coin.mx, an unlicensed virtual currency exchange; and the only U.S. prosecution brought in connection with the "Panama Papers."

In addition, she successfully argued the appeal before the Second Circuit in the case against Ross Ulbricht, the founder and chief administrator of the Silk Road, the first darknet marketplace.

Earlier in her career, she served as a law clerk to the Honorable Naomi Reice Buchwald of the U.S. District Court for the Southern District of New York, and the Honorable Reena Raggi of the U.S. Court of Appeals for the Second Circuit. She is a graduate of Harvard College and Harvard Law School.

To read more:
https://www.justice.gov/opa/pr/justice-department-announces-first-director-national-cryptocurrency-enforcement-team

Number 2

Preparing for the Financial System of the Future

Governor Lael Brainard, at the 2022 U.S. Monetary Policy Forum, New York, New York

The financial system is undergoing fast-moving changes associated with digitalization and decentralization. Some of these innovations hold considerable promise to reduce transaction costs and frictions, increase competition, and improve financial inclusion, but there are also potential risks.

With technology driving profound change, it is important we prepare for the financial system of the future and not limit our thinking to the financial system of today.

The Evolving Digitalization and Decentralization of Finance

In recent years, there has been explosive growth in the development and adoption of new digital assets that leverage distributed ledger technologies and cryptography.

The market capitalization of cryptocurrencies grew from less than $100 billion five years ago to a high of almost $3 trillion in November 2021 and is currently around $2 trillion.

In parallel, we have seen rapid growth in the platforms that facilitate the crypto finance ecosystem, including decentralized finance (DeFi) platforms.

These crypto platforms facilitate a variety of activities, including lending, trading, and custodying crypto-assets, in some cases outside the traditional regulatory guardrails for investor and consumer protection, market integrity, and transparency.

The growth in the crypto finance ecosystem is fueling demand for stablecoins—digital assets that are intended to maintain stable value relative to reference assets, such as the U.S. dollar. Stablecoin supply grew nearly sixfold in 2021, from roughly $29 billion in January 2021 to $165 billion in January 2022.

There is a high degree of concentration among a few dollar-pegged stablecoins: As of January 2022, the largest stablecoin by market capitalization made up almost half of the market, and the four largest stablecoins together made up almost 90 percent.

Today, stablecoins are being used as collateral on DeFi and other crypto platforms, as well as in facilitating trading and monetization of cryptocurrency positions on and between crypto and other platforms.

In the future, some issuers envision that stablecoins will also have an expanded reach in the payment system and be commonly used for everyday transactions, both domestic and cross-border. So it is important to have strong frameworks for the quality and sufficiency of reserves and risk management and governance.

As noted in a recent report on stablecoins by the President's Working Group on Financial Markets, it is important to guard against run risk, whereby the prospect of an issuer not being able to promptly and adequately meet redemption requests for the stablecoin at par could result in a sudden surge in redemption demand.

It is also important to address settlement risk, whereby funds settlement is not certain and final when expected, and systemic risk, whereby the failure or distress of a stablecoin provider could adversely affect the broader financial system.

The prominence of crypto advertisements during the Super Bowl highlighted the growing engagement of retail investors in the crypto ecosystem. In late 2021, Pew Research found that 16 percent of survey respondents reported having personally invested in, traded, or otherwise used a cryptocurrency—up from less than 1 percent of respondents in 2015. There is also rising interest among institutional investors.

So it is perhaps not surprising that established financial intermediaries are undertaking efforts to expand the crypto services and products they offer. If the past year is any guide, the crypto financial system is likely to continue to grow and evolve in ways that increase interconnectedness with the traditional financial system.

As a result, officials in many countries are undertaking efforts to understand and adapt to the transformation of the financial system. Many jurisdictions are making efforts to ensure statutory and regulatory frameworks apply like rules to like risks, and some jurisdictions are issuing or contemplating issuing central bank currency in digital form.

Preparing for the Payment System of the Future

The Federal Reserve needs to be preparing for the payment landscape of the future even as we continue to make improvements to meet today's needs. In light of the rapid digitalization of the financial system, the Federal Reserve has been thinking critically about whether there is a role for a potential U.S. central bank digital currency (CBDC) in the digital payment landscape of the future and about its potential properties, costs, and benefits.

Our financial and payment system delivers important benefits today and is continuing to improve with developments like real-time payments. Nonetheless, certain challenges remain, such as a lack of access to digital banking and payment services for some Americans and expensive and slow cross-border payments.

Growing interest in the digital financial ecosystem suggests that technology is enabling potential improvements that merit consideration.

In addition, it is important to consider how new forms of crypto-assets and digital money may affect the Federal Reserve's responsibilities to maintain financial stability, a safe and efficient payment system, household and business access to safe central bank money, and maximum employment and price stability.

It is prudent to explore whether there is a role for a CBDC to preserve some of the safe and effective elements of the financial system of the present in a way that is complementary to the private sector innovations transforming the financial landscape of the future.

The public and private sector play important complementary roles within the financial system in the United States. From Fedwire to FedNow, the Federal Reserve has over a century of experience working to improve the infrastructure of the U.S. payment system to provide a resilient and adaptable foundation for dynamic private sector activity.

In parallel, private sector banks and nonbanks have competed to build the best possible products and services on top of that foundation and to meet the dollar-denominated needs of consumers and investors at home and around the world. The result is a resilient payment system that is responsive to the changing needs of businesses, consumers, and investors.

While the official sector provides a stable currency, operates some important payment rails, and undertakes regulation and oversight of financial intermediaries and critical financial market infrastructures, the

private sector brings competitive forces encouraging efficiency and new product offerings and driving innovation.

Responsible innovation has the potential to increase financial inclusion and efficiency and to lower costs within guardrails that protect consumers and investors and safeguard financial stability.

As we assess the range of future states of the financial system, it is prudent to consider how to preserve ready public access to government-issued, risk-free currency in the digital financial system—the digital equivalent of the Federal Reserve's issuance of physical currency.

The Board recently issued a discussion paper that outlines the Federal Reserve's current thinking on the potential benefits, risks, and policy considerations of a U.S. CBDC.

The paper does not advance any specific policy outcome and does not signal that the Board will make any imminent decisions about the appropriateness of issuing a U.S. CBDC.

It lays out four CBDC design principles that analysis to date suggests would best serve the needs of the United States if one were created.

Those principles are that a potential CBDC should be privacy-protected, so consumer data and privacy are safeguarded; intermediated, such that financial intermediaries rather than the Federal Reserve interface directly with consumers; widely transferable, so the payment system is not fragmented; and identity-verified, so law enforcement can continue to combat money laundering and funding of terrorism.

Financial Stability

Given the Federal Reserve's mandate to promote financial stability, any consideration of a CBDC must include a robust evaluation of its impact on the stability of the financial system—not only as it exists today but also as it may evolve in the future.

In consideration of the financial system today, it would be important to explore design features that would ensure complementarity with established financial intermediation.

A CBDC—depending on its features—could be attractive as a store of value and means of payment to the extent it is seen as the safest form of money.

This could make it attractive to risk-averse users, perhaps leading to increased demand for the CBDC at the expense of other intermediaries during times of stress. So it is important to undertake research regarding the tools and design features that could be introduced to limit such risks, such as offering a non-interest bearing CBDC and limiting the amount of CBDC an end user could hold or transfer.

As I noted at the start, the digital asset and payment ecosystem is evolving at a rapid pace. Thus, it is also important to contemplate the potential role of a CBDC to promote financial stability in a future financial system in which a growing range of consumer payment and financial transactions would be conducted via digital currencies such as stablecoins. If current trends continue, the stablecoin market in the future could come to be dominated by just one or two issuers.

Depending on the characteristics of these stablecoins, there could be large shifts in desired holdings between these stablecoins and deposits, leading to large-scale redemptions by risk-averse users at times of stress that could prove disruptive to financial stability.

In such a future state, the coexistence of CBDC alongside stablecoins and commercial bank money could prove complementary, by providing a safe central bank liability in the digital financial ecosystem, much like cash currently coexists with commercial bank money.

It is essential that policymakers, including the Federal Reserve, plan for the future of the payment system and consider the full range of possible options to bring forward the potential benefits of new technologies, while safeguarding stability.

International Considerations

Analysis of the potential future state of the financial system is not limited to the domestic implications. The dollar is important to global financial markets: It is not only the predominant global reserve currency, but the dollar is also the most widely used currency in international payments.

Decisions by other major jurisdictions to issue CBDCs could bring important changes to global financial markets that may prove more or less disruptive and that could influence the potential risks and benefits of a U.S. CBDC.

Thus, it is wise to consider what the future states of global financial markets and transactions would look like both with and without a Federal Reserve-issued CBDC. For example, the People's Bank of China has been

piloting the digital yuan, also known as e-CNY, in numerous Chinese cities over the past two years.

The substantial early progress on the digital yuan may have implications for the evolution of cross-border payments and payment systems. And it may influence the development of norms and standards for cross-border digital financial transactions.

It is prudent to consider how the potential absence or issuance of a U.S. CBDC could affect the use of the dollar in payments globally in future states where one or more major foreign currencies are issued in CBDC form.

A U.S. CBDC may be one potential way to ensure that people around the world who use the dollar can continue to rely on the strength and safety of U.S. currency to transact and conduct business in the digital financial system.

More broadly, it is important to consider how the United States can continue to play a lead role in the development of standards governing international digital financial transactions involving CBDCs consistent with norms such as privacy and security.

Given the dollar's important role as a payment instrument across the world, it is essential that the United States be on the frontier of research and policy development regarding CBDC, as international developments related to CBDC can have implications for the global financial system.

Technology Research and Experimentation

Given the range of possible future states with significant digitization of the financial system, it is important that the Federal Reserve is actively engaging with the underlying technologies.

Our work to build 24x7x365 instant payments rails leverages lessons from some of today's most resilient, high-performing, and large-scale technology platforms across the globe.

It is providing important insights on the clearing and settlement models associated with real time payments as well as on fraud, cyber resilience, cloud computing, and related technologies.

In parallel with the Board's public consultation on CBDC, the Federal Reserve Bank of Boston, in collaboration with the Massachusetts Institute of Technology, has developed a theoretical high-performance transaction processor for CBDC.

They recently published the resulting software under an open-source license as a way of engaging with the broader technical community and promoting transparency and verifiability.

Moreover, the Board is studying how innovations, such as distributed ledger technology, could improve the financial system. This work includes experimentation with stablecoin interoperability and testing of retail payments across multiple distributed payment ledger systems. The Federal Reserve Bank of New York recently established an Innovation Center, focused on validating, designing, building, and launching new financial technology products and services for the central bank community.

These technology research and development initiatives are vital to our responsibilities to promote a safe and efficient payment system and financial stability, whatever the future may bring.

Conclusion

The financial system is not standing still, and neither can we. The digital financial ecosystem is evolving rapidly and becoming increasingly connected with the traditional financial system.

It is prudent for the Board to understand the evolving payment landscape, the technological advancements and consumer demands driving this evolution, and the consequent policy choices as it seeks to fulfill its congressionally-mandated role to promote a safe, efficient, and inclusive system for U.S. dollar transactions.

To prepare for the financial system of the future, the Federal Reserve is engaging in research and experimentation with these new technologies and consulting closely with public and private sector partners.

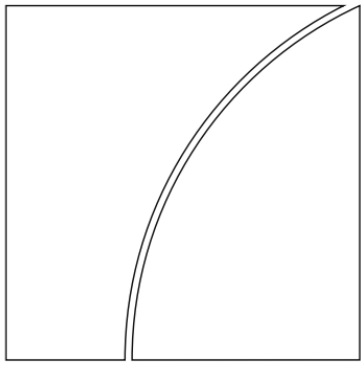
Number 3

BIS Working Papers No 1000

Dollar beta and stock returns

Valentina Bruno, Ilhyock Shim and Hyun Song Shin - Monetary and Economic Department

BIS



BIS Working Papers

No 1000

Dollar beta and stock returns

by Valentina Bruno, Ilhyock Shim and Hyun Song Shin

Monetary and Economic Department

February 2022

Abstract

The financial channel of exchange rates operates through changes in risk-taking by investors and is reflected in the response of financial conditions to exchange rate movements.

We show that stock returns also reflect the financial channel of exchange rates, with higher local currency stock returns associated with a weaker dollar.

The broad dollar index emerges as a global factor, consistent with the financial channel operating through swings in risk-taking by global investors.

We introduce the *dollar beta* as the sensitivity of stock returns to swings in the broad dollar index, and show that emerging market stock indices that have a higher dollar beta tend to have higher average returns, implying that the dollar beta is a cross-section risk factor that is priced.

Introduction

Exchange rates affect the economy through both real and financial channels. Deeper global integration of banking and capital market activity

has meant that the financial channel of exchange rates has taken on an increasingly important role in recent decades.

The financial channel of exchange rates operates through changes in the risk capacity of market participants and is reflected in the response of financial conditions to exchange rate movements.

There is an active and accumulating series of studies (to be reviewed below) that show how capital flows and market conditions fluctuate with swings in exchange rates, where an appreciating local currency is associated with more accommodative local financial conditions.

To read more: https://www.bis.org/publ/work1000.pdf

Number 4

Why Security Concerns Drive Customers Towards Public DNS Resolvers

The European Union Agency for Cybersecurity (ENISA) analyses the security pros and cons of using public DNS resolvers.

A core part of the internet is the Domain Name System (DNS) mechanism. All computers, internet browsers and other applications use DNS resolvers to translate the human readable website names to machine readable IP addresses of computers.

Traditionally, these DNS resolvers are provided by the telecom provider, as part of the internet access connection. However, customers are increasingly turning away from private DNS resolvers and going for large cloud-based public DNS resolvers instead.

Carried out by ENISA, this project supports the work of the NIS Cooperation group in the area of core internet. The 22nd meeting of the NIS Cooperation group is taking place today in a virtual format. The meeting is chaired by France, currently holding the presidency of the Council of the EU.

What are the security concerns driving customers to public DNS resolvers?

Better security and privacy are identified as key drivers for this shift to public DNS resolvers.

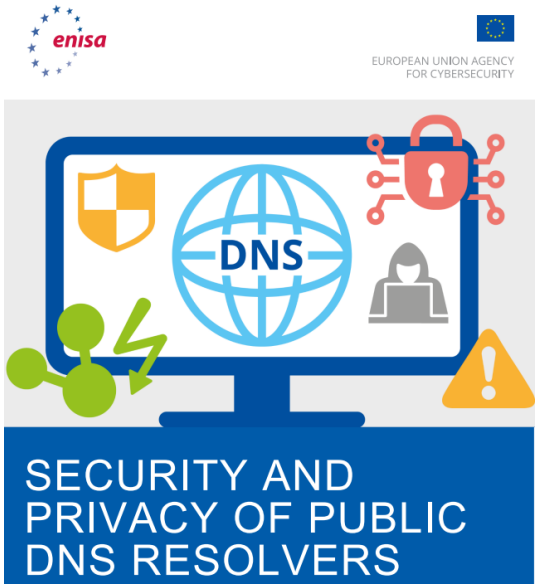
The public DNS resolvers typically support the newest DNS protocols, which encrypt DNS queries for instance. Some public DNS resolvers also offer additional security and protection features such as the blocking of malicious domains.

On the contrary, traditional private DNS resolvers use older protocols, and do not encrypt DNS queries, which translates into risks for the end-user.

Blocking of content by private DNS resolvers and service outages by the private DNS resolvers are other important reasons why consumers make the configuration change. An outage or a website block can lead consumers to temporarily configure their computer to use a public DNS resolver.

Outcome of the security analysis

In the ENISA Report - Security and privacy of Public DNS resolvers, ENISA assesses the shift in the DNS resolution market toward public DNS resolution and assesses the cybersecurity impact. You may visit: https://www.enisa.europa.eu/publications/security-and-privacy-for-public-dns-resolvers



Additional encryption is an example of those clear security benefits driving the change in consumers' behaviour. On the other hand, security and privacy concerns remain. For instance, enterprise network security controls do not always work when computers use public DNS resolution with encrypted DNS queries.

Although encryption is an improvement in general, it is important to underline that even with encrypted DNS resolution like DNS over HTTPS, computers still send a lot of unencrypted information over the network. Such information can then be used to track the websites visited. An example of this would be the IP addresses of the website or the domain name in the Transport Layer Security (TLS).

Other concerns also relate to dependencies, resilience and the lack of diversification. Well established and well known DNS resolvers are few and those most widely used resolvers are enjoy a dominant market position.

Implementation of the NIS Directive

The objective of this report is to help national authorities in the EU Member States supervise this part of the DNS resolution market. Supervision of DNS

is required under Article 14 of the Network and Information Security (NIS) Directive. ENISA supports the NIS cooperation group in developing technical cybersecurity guidelines and in the cybersecurity analysis of new technologies, as this is the case of the report published today on DNS resolution.

DNS4EU

The EU's Cybersecurity Strategy, published at the end of 2020, also addresses the topic of public DNS resolution. DNS4EU is a European Commission initiative that aims to offer an alternative to the public DNS resolvers currently dominating the market. The objective of DNS4EU is to implement the latest security and privacy standards and thus ensure a high level of security for customers and end-users.

You may visit:
https://www.enisa.europa.eu/publications/security-and-privacy-for-public-dns-resolvers

Number 5

2021 CONSUMER TRENDS REPORT

Executive summary

The insurance sector has shown resilience by continuing to smoothly serve consumers amidst the shocks caused by the lasting global pandemic. This has fast-forwarded digitalisation highlighting opportunities but also showing possible concerns.

› Continued issues relating to unit-linked (hybrid) products

The decrease (-10%) in with proft participation gross-written premium (GWP), led to an overall decrease in life insurance GWP. This is the result of the continued low for long interest rate environment which is accelerating the shift from traditional products with guarantees towards unit-linked insurance (+2%).

While this shift allows consumers to seek higher returns, a number of conduct issues continue being observed. In particular, consumers continue having limited understanding of these products and some of the products are highly complex.

Moreover, a number of unit-linked products showing high costs and complex structures with high commissions further increase concerns relating to possible mis-selling and value for money.

› Fast-forwarded digitalisation bringing opportunities but also raising Challenges

The acceleration in digitalisation observed at the on-set of the pandemic continued. NCAs reported an increase in innovations across the product lifecycle, with sales and distribution remaining the most digitalised stages:

- Sales through e-channels remain steadily strong in the non-life business, while they materially grew in the life business. 13 Member States reported that sales through e-channels either increased or signifcantly increased in the last 3 years;

- Digital transformation also impacted pricing and underwriting with undertakings allowing consumers to use digital platforms to personalise

their products whilst also increasingly using price optimisation practices;

- While the risk of digital exclusion should not be under-estimated, most consumers surveyed by EIOPA as part of its consumer research, stated they prefer and appreciate digital tools which allow them to have on-demand engagement with their intermediary and their insurer;

- Issues relating to conficts of interest and limited product choices on digital platforms, require further monitoring;

- Moreover, NCAs reported increased evidence of fraud and scams targeting both consumers and insurance undertakings.

› Consumer detriment due to poor claims handling albeit positive developments being observed thanks to digitalisation

Improvements in the claims handling process have been observed.

Technological innovation appears to be the most relevant driver, leading to the automation and simplification of some parts of claims handling processes, in particular in relation to low value high frequency claims.

Nevertheless, some issues continue being reported, with 9 NCAs having highlighted claims management issues as an area of concern. In particular, NCAs reported issues relating to: lower payments than expected, long and complicated liquidation processes, a lack of adequate justifcation for claim refusals. This is mostly in relation to motor insurance, travel insurance and household insurance products.

› Emerging risks surfacing existing structural problems on exclusions and protection gaps

The ongoing pandemic and an increase in natural catastrophe risks surfaced problems in relation to contract complexity for some products whilst also bringing new challenges for the sector and consumers.

Following the signifcant increase in both claims ratios and expense ratios for business interruption and travel insurance many insurers have further introduced exclusions to certain products or have withdrawn such products from the market, widening protection gaps.

This is counterbalanced by the fact that consumers in the aftermath of the pandemic have sought to buy more travel insurance products, and new products advertised as ofering COVID-19 coverage have emerged.

The increase in systemic risks highlighted that issues relating to a lack of clarity in exclusions, limited consumer understanding of exclusions, and instances of unilateral changes to terms and conditions persist and go beyond travel and business interruption products.

NCAs reported issues with household and health insurance and particularly high increases in the total claims rejected have been observed for the medical expense (over 25 percentage points) and fre and other damage to property lines of business (almost 30 percentage points).

› *Increased use of price optimisation practices*

While this trend is not yet widespread across Europe, more than 50% of NCAs observed that more and more insurance product manufacturers adjust premiums using a number of diferent techniques which are largely independent from the risk profle of the consumers.

These are known as price optimisation practices and mostly relate to motor insurance products (59% of the cases reported) and household insurance products (29% of the cases reported).

These practices are mainly the result of high levels of market competition coupled to the emergence of new techniques enabled by modern data processing and analytics.

The major consequence stemming out of these practices is an increase in premiums for old/loyal consumers and vulnerable consumers. Instances of unlawful indirect discrimination have also been observed and this, in the longer term, could lead to an increase in financial exclusion.

To read more:
https://www.eiopa.europa.eu/sites/default/files/working_groups/reports/eiopa_2021_consumer_trends_report.pdf

Number 6

FSB Chair's letter to G20 Finance Ministers and Central Bank Governors: February 2022

Klaas Knot, Chair of FSB

Two years after its onset, the COVID-19 pandemic continues to weigh on the global economy.

New waves of infections have led to further rounds of containment measures, and have contributed to an uneven recovery across regions, higher inflation and record-high debt levels globally.

The global financial system has been able to support the recovery to date, thanks to the greater resilience of banks and market infrastructures – supported by the G20's post-2008 crisis reforms – and a determined policy response to the pandemic.

A resilient, well-functioning global financial system remains key for leaving the pandemic behind us and for achieving strong, inclusive and sustainable growth over the long term.

However, promoting global financial resilience during the transition to a post-pandemic world poses its own challenges.

Heightened economic uncertainty and potentially lasting changes in the global economy may significantly affect interest rates and asset prices.

The financial system also needs to harness the benefits of digital innovation while managing the risks, not least in the form of rapidly developing crypto-assets, and play its part in the transition to reduced, and eventually, net zero carbon emissions.

The move into a post-pandemic world brings with it a demand for more sustainable and innovative forms of finance, which promise to deliver tangible benefits to citizens and societies.

But it may also give rise to vulnerabilities, which must be addressed if their benefits are to be fully realised.

The FSB and G20 will play key roles in ensuring that these transitions happen smoothly.

This letter lays out how I see the FSB's policy work to promote global financial resilience during the coming year.
An annex provides a complete list of FSB deliverables to the G20 in 2022.

Supporting financial market adjustment to a post-COVID world

The transition path to a post-pandemic economy remains highly uncertain. Accommodative financial conditions have kept debt servicing costs low and supported asset prices, amid a continued search for yield.

But, in the current environment, embedded leverage in some parts of the financial system as well as rising real estate and other asset valuations across a number of jurisdictions have become vulnerabilities.

A rapid or disorderly tightening of financial conditions and a greater divergence of these conditions between advanced and emerging market economies could pose risks to financial stability, including through volatile capital flows.

The FSB will continue to monitor and analyse these risks closely and update the G20 on relevant issues.

Increasing divergences in growth across regions mean that an asynchronous unwinding of pandemic support measures is becoming more likely, with the potential for cross-border spillovers.

In many jurisdictions, limited remaining policy space constrains the ability to counter such spillovers.

Supporting an even, sustainable and inclusive recovery requires careful consideration of both these potential spillovers as well as the residual policy space.

As part of the exit and recovery process, it is also important to guard against the risk of longer term scarring of the real economy.

Financial sector policies should address factors that could impair the ability of the financial system to provide financing to the economy over the medium term, including on a cross-border basis.

These factors include corporate debt overhang in the aftermath of the pandemic.

The FSB will report to the G20 on policy considerations to support a more even, sustainable and inclusive global recovery, and on effective financial sector practices for national authorities to consider for addressing the effects of COVID-19 scarring. This will comprise an interim report in July and a final report in October.

To read more: https://www.fsb.org/wp-content/uploads/P170222.pdf

Yours sincerely,

Klaas Knot

Number 7

A repository of free tools and services, from the U.S. Cybersecurity and Infrastructure Security Agency (CISA)

As part of our continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and state, local, tribal, and territorial governments, CISA has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities.

This living repository includes cybersecurity services provided by CISA, widely used open source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community.

CISA will implement a process for organizations to submit additional free tools and services for inclusion on this list in the future.

The list is not comprehensive and is subject to change pending future additions.

CISA applies neutral principles and criteria to add items and maintains sole and unreviewable discretion over the determination of items included.

CISA does not attest to the suitability or effectiveness of these services and tools for any particular use case.

CISA does not endorse any commercial product or service. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA.

Foundational Measures

All organizations should take certain foundational measures to implement a strong cybersecurity program:

- Fix the known security flaws in software. Check the CISA Known Exploited Vulnerabilities (KEV) Catalog for software used by your organization and, if listed, update the software to the latest version according to the vendor's instructions.

Note: CISA continually updates the KEV catalog with known exploited vulnerabilities.

- Implement multifactor authentication (MFA). Use multifactor authentication where possible. MFA is a layered approach to securing your online accounts and the data they contain.

  When you enable MFA in your online services (like email), you must provide a combination of two or more authenticators to verify your identity before the service grants you access.

  Using MFA protects your account more than just using a username and password. Why? Because even if one factor (like your password) becomes compromised, unauthorized users will be unable to meet the second authentication requirement, ultimately stopping them from gaining access to your accounts.

- Halt bad practices. Take immediate steps to:

  (1) replace end-of-life software products that no longer receive software updates;

  (2) replace any system or products that rely on known/default/unchangeable passwords; and

  (3) adopt MFA (see above) for remote or administrative access to important systems, resources, or databases.

- Sign up for CISA's Cyber Hygiene Vulnerability Scanning. Register for this service by emailing vulnerability@cisa.dhs.gov. Once initiated, this service is mostly automated and requires little direct interaction.

  CISA performs the vulnerability scans and delivers a weekly report. After CISA receives the required paperwork, scanning will start within 72 hours and organizations will begin receiving reports within two weeks. Note: vulnerability scanning helps secure internet-facing systems from weak configurations and known vulnerabilities and encourages the adoption of best practices.

- Get your Stuff Off Search (S.O.S.). While zero-day attacks draw the most attention, frequently, less complex exposures to both cyber and physical security are missed. Get your Stuff Off Search–S.O.S.–and reduce internet attack surfaces that are visible to anyone on web-based search platforms.

Service	Skill Level	Owner	Description	Link
CISA Cybersecurity Publications	Basic	CISA	CISA provides automatic updates to subscribers via email, RSS feeds, and social media. Subscribe to be notified of CISA publications upon release.	https://www.cisa.gov/subscribe-updates-cisa
CISA Vulnerability Scanning	Basic	CISA	This service evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. It provides weekly vulnerability reports and ad-hoc alerts. See https://www.cisa.gov/cyber-resource-hub for details.	Email: vulnerability@cisa.dhs.gov
CISA Web Application Scanning	Basic	CISA	This service evaluates known and discovered publicly accessible websites for potential bugs and weak configuration to provide recommendations for mitigating web application security risks. See https://www.cisa.gov/cyber-resource-hub for details.	Email: vulnerability@cisa.dhs.gov
CISA Phishing Campaign Assessment	Basic	CISA	This service provides an opportunity for determining the potential susceptibility of personnel to phishing attacks. This is a practical exercise intended to support and measure the effectiveness of security awareness training. See https://www.cisa.gov/cyber-resource-hub for details.	Email: vulnerability@cisa.dhs.gov
CISA Remote Penetration Test	Basic	CISA	This test simulates the tactics and techniques of real-world adversaries to identify and validate exploitable pathways. This service is ideal for testing perimeter defenses, the security of externally available applications, and the potential for exploitation of open	Email: vulnerability@cisa.dhs.gov

To read more: https://www.cisa.gov/free-cybersecurity-services-and-tools

Number 8

ESRB issues new warnings and recommendations on medium-term residential real estate vulnerabilities

ESRB
European Systemic Risk Board
European System of Financial Supervision

The European Systemic Risk Board (ESRB) has published five warnings and two recommendations on medium-term residential real estate vulnerabilities. It has also published an assessment of compliance with recommendations issued in 2019.

Warnings were sent to the competent ministers of five countries with newly identified vulnerabilities that have not been addressed sufficiently: Bulgaria, Croatia, Hungary, Liechtenstein and Slovakia.

Recommendations were sent to the competent ministers of two countries, Austria and Germany, which had already received ESRB warnings in 2016 and 2019, respectively, and whose vulnerabilities have not been addressed sufficiently.

After these recommendations were issued, the authorities in Austria and Germany announced new measures to address vulnerabilities in the residential real estate sector.

The ESRB assesses vulnerabilities in the residential real estate sector because of its importance for financial and macroeconomic stability. In 2016 and 2019, the ESRB conducted systematic, forward-looking assessments of such vulnerabilities in the European Economic Area (EEA).

Recently, the ESRB concluded another assessment of this sector in the EEA, which formed the basis for the latest set of country-specific warnings and recommendations. The ESRB has a mandate to issue such warnings when significant systemic risks are identified and to make recommendations for remedial action.

The assessment covered all EU Member States, Iceland, Liechtenstein and Norway and analysed the main trends in various real estate indicators as well as the macroprudential policy actions that countries have taken to mitigate the financial stability risks identified.

The outcome of this analysis shows that financial stability risks related to residential real estate have continued to increase in several countries in the context of macroeconomic risks related to the coronavirus (COVID-19) pandemic and continued strong dynamics in housing markets, housing credit and household indebtedness.

The key vulnerabilities highlighted by the ESRB assessment are of a medium-term nature and, depending on the country, relate to rapid house price growth and possible overvaluation of residential real estate, the level and dynamics of household indebtedness, the growth of housing credit and signs of a loosening of lending standards.

The specific vulnerabilities vary from country to country, and the details can be found in the individual warnings and recommendations.

Beyond macroprudential policy considerations, in a number of countries, some underlying vulnerabilities would be mitigated more efficiently with the help of reforms of housing and tax policies.

In view of the economic uncertainty during the pandemic, any policy action should be carefully assessed to ensure that it contributes to mitigating residential real estate vulnerabilities, while aiming to avoid procyclical effects on the overall performance of the real economy and the financial system.

Residential real estate vulnerabilities have remained elevated in the countries that received ESRB recommendations in 2019.

In a number of these countries, vulnerabilities have persisted in spite of recent measures introduced to address them.

The latter countries are Denmark, Finland, Luxembourg, the Netherlands and Sweden.

In most cases, house prices have continued rising or have grown even faster than before, resulting in unchanged or increased house price overvaluation.

The risk related to household indebtedness has also remained unchanged or increased in several countries, partly as a result of strong mortgage credit growth. In most cases, lending standards for new mortgage loans have not significantly improved or have shown signs of deterioration.

For the remaining EEA countries, either the ESRB has not identified a build-up of material vulnerabilities in the residential real estate sector, or such vulnerabilities have been identified but the current policy stance is assessed as sufficient in addressing them.

Full details of the ESRB’s assessment are included in the ESRB report "Vulnerabilities in the residential real estate sectors of the EEA countries", which has been published today alongside the warnings and

recommendations. The assessment of vulnerabilities is based on available data and covers developments up to mid-November 2021.

The ESRB has also published a compliance report on the countries that received ESRB recommendations in 2019 concerning medium-term vulnerabilities in their residential real estate sectors. You may visit: https://www.esrb.europa.eu/pub/pdf/recommendations/esrb.Country-specific_Recommendations202201~816f54bbf7.en.pdf


Compliance report

February 2022

Country-specific Recommendations of the European Systemic Risk Board of 27 June 2019 on medium-term vulnerabilities in the residential real estate sector in Belgium (ESRB/2019/4), Denmark (ESRB/2019/5), Luxembourg (ESRB/2019/6), the Netherlands (ESRB/2019/7), Finland (ESRB/2019/8) and Sweden (ESRB/2019/9), respectively

The report reviews the policy responses aimed at mitigating the vulnerabilities in Belgium, Denmark, Finland, Luxembourg, the Netherlands and Sweden.

The ESRB monitors and assesses compliance with its recommendations via an “act or explain” mechanism.

The ESRB recommendations issued in 2019 have a specific timeline for implementation (ranging from 2020 to 2022).

Overall, the compliance assessment findings are as follows: one addressee is assessed as fully compliant (Luxembourg), three addressees are assessed as largely compliant (Belgium, Denmark and Sweden) and two addressees are assessed as partially compliant (Finland and the Netherlands).

Going forward, the ESRB will continue exercising its mandate of macroprudential oversight of the financial system in the EU Member

States, Iceland, Liechtenstein and Norway, including identifying financial stability vulnerabilities related to real estate.

The ESRB will continue to issue warnings if a significant systemic risk to financial stability is identified and, where appropriate, will issue recommendations for remedial action.

To read more:
https://www.esrb.europa.eu/news/pr/date/2022/html/esrb.pr220211~9393d5e991.en.html

Number 9

Largest South Korean Telecommunications Co. Agrees to Pay the SEC to Settle FCPA Charges

The Securities and Exchange Commission announced that Seoul-based KT Corporation (KT Corp.) will pay $6.3 million to resolve charges that it violated the *Foreign Corrupt Practices Act (FCPA)* by providing improper payments for the benefit of government officials in Korea and Vietnam.

According to the SEC's order, KT Corp., South Korea's largest telecommunications operator, engaged in multiple schemes to make improper payments in Korea and Vietnam.

KT Corp. lacked sufficient internal accounting controls over charitable donations, third-party payments, executive bonuses, and gift card purchases.

As a result, KT Corp. employees, including high-level executives, were able to generate slush funds that were used for gifts and illegal political contributions to government officials in Korea who had influence over KT Corp.'s business.

Other employees were able to make payments in connection with seeking business from government customers in Vietnam.

"For nearly a decade, KT Corp. failed to implement sufficient internal accounting controls with respect to key aspects of its business operations, while at the same time lacking relevant anti-corruption policies or procedures. Issuers must be sure to devote appropriate attention to meeting their obligations under the FCPA," said Charles Cain, Chief of the SEC Enforcement Division's FCPA Unit.

In November 2021, South Korean authorities indicted KT Corp. and 14 executives for criminal violations related to illegal political contributions from the slush funds.

KT Corp. consented to the SEC's order without admitting or denying the findings that it violated the books and records and internal accounting controls provisions of the Securities Exchange Act of 1934, and agreed to pay approximately $3.5 million in civil penalties and $2.8 million in disgorgement.

The SEC's investigation was conducted by Ilana Z. Sultan, Steven Susswein, and M. Shahriar Masud and supervised by Tracy L. Price.

UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 94279 / February 17, 2022

ADMINISTRATIVE PROCEEDING
File No. 3-20780

In the Matter of **KT CORPORATION,** **Respondent.**	**ORDER INSTITUTING CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTION 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING A CEASE-AND-DESIST ORDER**

You may visit: https://www.sec.gov/news/press-release/2022-30

https://www.sec.gov/litigation/admin/2022/34-94279.pdf

Number 10

Third annual threat assessment

Mike Burgess, Director-General of Security, in charge of the Australian Security Intelligence Organisation (ASIO).

Australian Government
Australian Security Intelligence Organisation

Good evening. Welcome to ASIO and to my Annual Threat Assessment.

I'd like to recognise our partners and colleagues represented here tonight – Excellencies, MP's and Senators, the Inspector-General, Directors-General, Secretaries, Military Chiefs, Commissioners, ladies and gentlemen.

Can I start with an admission? While I am pleased to host this event and welcome you to the Ben Chifley Building, a lectern is not my happy place. I loathe public speaking.

So you might be thinking, why would someone like me choose to do something like this?

There are three key reasons, and I'd like to explain them.

The first is trust.

ASIO protects Australia and Australians from threats to their security. Our ability to deliver our mission requires us to maintain the confidence and trust of our stakeholders, including the Australian people.

A vibrant liberal democracy requires a Security Service that is transparent and trusted.

I believe this imposes a responsibility on ASIO to be as open as possible about what the Organisation does, and why we do it.

Giving this address, and inviting you into our building, is a tangible expression of how seriously I take that responsibility.

It's why I was one of the first intelligence leaders anywhere in the world to have a personal, identifiable Twitter account; why I give speeches and do occasional media interviews; why ASIO is on social media; and why I've declassified operations and case studies to give a clearer picture of the threats we face.

None of that was easy. Some of it was controversial. But all of it was important.

Transparency matters. Transparency is a precursor for trust.

My thinking on transparency crystallised at a time in my career when the Defence Signals Directorate was accused of an illegal act.

The allegations were proved to be completely unfounded, but damage was done, reputations were stained, and confidence was bruised.

The affair taught me how difficult it can be for a secret organisation to defend itself, even when it's done nothing wrong—it's assumed that if you're in the shadows, you're shadowy.

We can dispel this with sunlight—by explaining who we are, what we do, and why we matter.

Not long after that incident, a journalist put a salacious and inaccurate claim to a certain intelligence agency—I won't say which one, or even in which country. Instead of saying, 'that's ridiculous'—or 'hell no', which would have been my response—the brains trust replied with, 'no comment—and that's off the record'.

The story got published and the next morning there was much head-shaking and tut-tutting as spy chiefs wondered how the newspaper could get it so wrong. The journalist got it so wrong because the agency ignored an opportunity to make it right!

Obviously there are things a spy agency cannot talk about—especially one where human sources and technical capabilities are critical to its success.

We need to be able to do things our adversaries think are impossible. But as I rose through the ranks, it became increasingly clear that there is much more we can say than 'no comment'.

We don't talk about our operations but we can reveal their outcomes.

We must be secretive about our capabilities, but we can be open about our values.

We cannot identify our undeclared staff, but we can celebrate the difference they make.

That brings me to the second principle of my transparency push— ASIO's people. Transparency is a powerful recruitment tool. People won't work for an agency if they don't know what it does and what it values; they can't apply for jobs they don't know exist.

I want more people to choose ASIO, and I want ASIO to be able to choose more people from more diverse backgrounds. This is a challenge intelligence agencies around the world are grappling with.

We need to do better. We should reflect the community we protect.

It's never too early to start planning a career at ASIO.

I recently received a letter from seven-year-old Ava, who wants to be a surveillance officer. She told me she's good at spying because she is small and nobody notices her.

Ava volunteered her mum to drive her around on her surveillance shifts. Clearly, young Ava already possesses some of the skills we're looking for—she's creative, shows initiative, and can communicate. But hide-and-seek isn't just for kids, and surveillance isn't just hide and seek. We are actually hiring surveillance officers right now.

While surveillance is a traditional spy role, we have many other roles too. Many of the jobs we are advertising, or are about to advertise, are not usually associated with spy agencies, but are integral to our success:

- Trades professionals such as electricians and plumbers.

- Technology graduates who can design, build and deliver systems, access data and help our analysts make sense of data.

- Business analysts and project managers to drive our capability uplift.

- Intelligence officers and analysts to collect the dots and connect the dots.

- And legal graduates to ensure our covert operations are conducted lawfully, and to work on litigation and corporate matters.

There is no ASIO type. ASIO needs people from all walks of life and I invite you to find your fit.

So that's what an annual threat assessment delivers for ASIO.

The final—and perhaps most important—factor is what's in it for you, ASIO's partners and stakeholders. It's critically important to explain the threats we are seeing so you are armed with the awareness and advice you need to counter those threats.

Security is a shared responsibility. ASIO cannot stop every terrorist and catch every spy. The scale, persistence and sophistication of the threats Australia is facing demands a broader approach to security. I'll return to this later.

Australia's security outlook remains complex, challenging and changing. COVID-19 and its associated lockdowns added considerable volatility to the mix.

While, thankfully, the time of lockdowns seems to have come to an end, the impacts of the lockdowns are continuing to influence the security environment.

We all spent a lot more time online during the pandemic. This was positive in many respects. During difficult times, the internet helped us maintain connections with families and friends, allowed many of you to work from home, and, of course, enabled plenty of online shopping!

But like many things online, for every benefit the internet delivered, a related downside was created.

More online shopping meant more cyber-crime. More online engagement provided greater opportunities for radicalisation. More working from home increased the risk of cyber-enabled espionage.

I'd like to dive into the last two a little more deeply because they fall squarely within ASIO's remit, and are exerting a significant influence on Australia's security environment.

In the last two years, thousands of Australians with access to sensitive information have been targeted by foreign spies using social media profiles. These spies are adept at using the internet for their recruitment efforts.

On any of the popular social media or internet platforms, they make seemingly innocuous approaches—such as job offers. This then

progresses to direct messaging on different, encrypted platforms, or in-person meetings, before a recruitment pitch is made.

I've previously highlighted our concerns about approaches on professional networking sites, but during the pandemic we've seen this threat spread. There's been a jump in suspicious approaches on messaging platforms like WhatsApp, for example.

It's an easy way for foreign intelligence services to target employees of interest.

ASIO is also tracking suspicious approaches on dating platforms such as Tinder, Bumble and Hinge. My message for any potential victims on these sites is a familiar one—if it seems too good to be true, it probably is!

While espionage is one of the most insidious security threats we are dealing with online, it is not the most concerning trend.

The internet is the world's single most potent and powerful incubator of extremism.

Online radicalisation is nothing new, but COVID-19 sent it into overdrive. Isolated individuals spent more time online, exposed to extremist messaging, misinformation and conspiracy theories.

Social media platforms, chat rooms, and algorithms are designed to join up people who share the same views, and push them material they will 'like'. It's like being in an echo chamber where the echo gets louder and louder, generating cycles of exposure and reinforcement.

More time in those online environments—without some of the circuit breakers of everyday life, like family and community engagement, school and work—created more extremists. And in some cases, it accelerated extremists' progression on the radicalisation pathway towards violence.

Back in 2007, ASIO produced an assessment warning about the implications of a pandemic. We did that not because we're health experts, but because it's our job to identify and analyse phenomena that might have security impacts for our country. We assessed that a pandemic would result in an increase in anti-government behaviours, and we have certainly seen that with COVID.

While ASIO's overall terrorism caseload has decreased since this time last year, there's been a distinct increase in radicalisation and specific-issue grievances.

Some Australians believe the government's approach to vaccinations and lockdowns infringed their freedoms. And in a small number of cases, grievance turned to violence.
Obvious examples are the violent incidents at COVID-related protests fuelled by anti-vaccination, anti-lockdown and anti-government agendas.

We have also seen threats against public office holders, an attack on a vaccination clinic, and several physical assaults on healthcare workers.

We assess that these tensions and the associated possibility of violence will persist.

While lockdowns and mandatory quarantine requirements are being eased, the introduction of vaccination requirements for some forms of employment, social engagement and travel will continue to drive anger, uncertainty and fear within a small section of society.

This cohort views the restrictions as an attack on their rights, the creation of a two-tier society and confirmation of their perceived persecution.

ASIO does not have any issue with people who have opinions they want to express. This is a critical part of a vibrant democracy. We do not—and cannot—investigate peaceful protest or dissent. Our concern is where opinions tip into the promotion of violence, or actual acts of violence.

So I should stress that the vast majority of people who choose not to be vaccinated will not engage in violence in response to vaccine mandates. The vast majority of protestors are not violent extremists, and the vast majority of the protests are not violent. ASIO's focus is on a small number of angry and alienated Australians.

This is precisely the concern I identified in this speech last year, and precisely why we changed the language we use to describe violent extremism. As I warned back then:

We are seeing a growing number of individuals and groups that don't fit on the left–right spectrum at all; instead, they're motivated by a fear of societal collapse or a specific social or economic grievance or conspiracy. The behaviours we are seeing in response to COVID ockdowns and vaccinations are not specifically left or right wing. They are a cocktail of views, fears, frustrations and conspiracies. Individuals who hold these views, and are

willing to support violence to further them, are best and most accurately described as ideologically motivated violent extremists.

Some of the alleged violent acts at the recent Old Parliament House protest are a case in point. The individuals involved were driven by a diverse range of grievances, including anti-vaccination agendas, conspiracy theories and anti-government sovereign citizen beliefs.
Assigning the protesters to a specific point on the political spectrum is neither accurate nor helpful.

Of course, this does not mean that people who hold, say, racist and nationalist beliefs never participate in these activities—sometimes they do—but they are just one relatively small part of a much wider and looser group.

This is an important point to make, because we expect to see more of this behaviour in Australia in the medium term. Protests driven by diverse specific-issue grievances will be part of our security environment for the foreseeable future. In some cases, protesters will advocate the use of violence, and in a smaller number of cases, they may use violence.

In this uptick in specific-issue or grievance-motivated violent extremism, many of the actors are newcomers, so it's harder to get a sense of what is simply big talk—and what is genuine planning for violence.

Making the call about which statements indicate a genuine plan for violence, and which are purely sounding off or wishful thinking, is one of the greatest challenges our analysts have. Our information is often incomplete—and the stakes are high.

Every judgement our analysts make affects another: when they decide to continue one investigation they are, in effect, deciding not to continue or launch a different one. With finite resources, it is a zero-sum game.

The most likely terrorist attack scenario in Australia over the next 12 months continues to be a lone-actor attack—and that fact weighs heavily on my mind and the minds of our staff.

While there were no terrorist attacks domestically last year, there were two major disruptions of violent extremist attacks. Globally, violent extremist attacks remain a frequent occurrence. And the transnational nature of terrorism means that events in distant places, such as the fall of the government in Afghanistan, can reverberate much closer to home. We are monitoring this carefully.

While we do not assess it has increased the immediate threat in Australia, we remain concerned that, in the longer term, violent extremists from our region may travel to Afghanistan for militant training.

Two years ago, in my first threat assessment, I noted that ASIO was seeing an increase in the radicalisation of young Australians.

Unfortunately and alarmingly, this trend is continuing. The number of minors being radicalised is getting higher and the age of the minors being radicalised is getting lower.

Most of the radicalisation occurs online, reflecting the dynamic I raised earlier, but some of it also happens in person, face to face. Children as young as 13 are now embracing extremism, and this is happening with religiously motivated violent extremism and ideologically motivated violent extremism.

And unlike past experience, many of these young people do not come from families where a parent or sibling already holds extreme views.

As the Director-General of Security, this trend is deeply concerning. As a parent, it is deeply distressing. As a nation, we need to reflect on why some teenagers are hanging Nazi flags and portraits of the Christchurch killer on their bedroom walls, and why others are sharing beheading videos. And just as importantly, we must reflect on what we can do about it.

A few years ago, minors represented around two to three per cent of our new counter-terrorism investigations. In the last year, though, the figure's been closer to fifteen per cent. And perhaps more disturbingly, these young people are more intense in their extremism.

Where once minors tended to be on the fringe of extremist groups, we are now seeing teenagers in leadership positions, directing adults, and willing to take violent action themselves.

At the end of last year, on average, minors represented more than half of our priority counter-terrorism investigations each week.

This should concern us all. Again, minors made up 15 per cent of our new counter-terrorism investigations, and more than half of our highest priority investigations each week.

ASIO is aware of minors preying on other minors, seeking to turn them to their violent ideology and using grooming techniques similar to those used by paedophiles.

We have seen cases involving young, radicalised violent extremists systematically targeting vulnerable associates who were lonely or going through tough times.

The targeting took place online, and face to face in a variety of settings, even schools. The tactics used by the extremists in these cases involved a combination of attention, flattery and friendship, which shifted to bullying and manipulation. We've seen young ringleaders deliberately desensitise their targets, gradually exposing them to more extreme and more violent propaganda, until the most graphic material imaginable was normalised.

Believe me when I tell you that ASIO finds these kinds of cases challenging — we do not belong in the schoolyard — and while we act when there is a threat of violence, the broader trend of teenage radicalisation demands a different response, one where ASIO and law enforcement are not the answer.

It is very hard to deradicalise an adult extremist, but there are many more options to redirect young people who are experimenting with extremism in response to unhappiness or insecurity.

As a society, we have to recognise the signs and step in early. Radicalisation in young people can happen quickly—in days and weeks, not months and years—and kids are most vulnerable when they are under stress.

In these situations, ASIO's role is at the end—at the point where there is an active threat to security. But before this point there are nearly always off-ramps: opportunities to redirect behaviour.

Government plays a key role in helping to counter violent extremism. Our colleagues in policy agencies, law enforcement and community organisations are doing important work in this space.

But the community can play a pivotal part identifying signs a teenager isn't just going through adolescence, but is heading towards radicalisation. Without knowing about these indicators it is much harder for us to divert them from a dangerous path.

Schools and sports clubs—notice and ask questions if the young people you know are acting antisocially and out of character.

Parents and carers—notice and ask questions if your children are receiving or circulating inappropriate material online. Children often start with moderately objectionable material, which then becomes worse and worse—identifying it early can be critical.

Community leaders—notice and ask questions if young people you know are showing marked changes in their demeanour or views.

Security is a shared responsibility.

While threat to life will always be a priority for ASIO, our attention and resourcing is increasingly being directed towards threats to Australia's way of life.

The first and perhaps most significant thing to say is that espionage and foreign interference has supplanted terrorism as our principal security concern.

This is not to downplay the significance of terrorism.

In terms of scale and sophistication, though, espionage and foreign interference threats are outpacing terrorism threats, and therefore demanding more attention and more resources.

The threat is pervasive, multifaceted and, if left unchecked, could do serious damage to our sovereignty, values and national interest.

Multiple countries are seeking to conduct espionage against us—and not just those countries that might be considered our traditional adversaries. In some instances, espionage is conducted by countries we consider friends—friends with sharp elbows and voracious intelligence requirements.

For decades, foreign spies have been seeking information about Australia's strategic capabilities, economic and policy priorities, world-class research and development, and defence technologies.

Obviously the capabilities and decision-making around AUKUS fall squarely into that category. Foreign intelligence agencies will have already added them to their collection requirements—just as ASIO is already working to thwart them. That should surprise no one; it's one of the reasons I'm flagging a more proactive approach to our security advice and engagement.

Following my previous address, our disruption of a 'nest of spies' got a lot of attention. But dismantling spy networks is business as usual for ASIO. We did it again last year.

Over a series of months, we painstakingly mapped out a foreign intelligence service's onshore network of sources and contacts. And then we picked it apart.

Australians who were targeted by the foreign intelligence service included current and former high-ranking government officials, academics, members of think-tanks, business executives and members of a diaspora community.

When we interviewed members of the network, some of the contacts suspected they'd engaged with spies, but most had no idea—and were shocked when we knocked on their doors.

As a sting in the tail, after we removed the spies, we laid trip wires—just in case the foreign country ever tries to reactivate this network. And this was just one of a number of disruptions we undertook in the past year.

As well as espionage, we've also seen an increase in foreign interference. I want to take a moment to draw out how this is different from foreign influence.

The confusion about where legitimate influence stops and foreign interference begins is understandable. We see our targets engaging in both things, and foreign interference is clandestine, and therefore difficult to discern.

Publicly praising a foreign regime—even an odious one—is not interference.

Transparently lobbying on behalf of a foreign government is not interference.

Diplomacy is not interference. These things are routine acts of statecraft.

But any and all of these acts could become foreign interference if they involve the hidden hand of a foreign state and are contrary to Australia's interests. If the person publicly praising another country is doing so because they've received discreet instructions from an overseas government, it could constitute foreign interference if it's detrimental to Australia's interests or done to affect our political processes.

So what does foreign interference look like in practice? There are two manifestations I'd like to focus on.

One is the harassment of Australia's diaspora communities. This is something ASIO's been warning about for some time. Foreign governments

will often monitor and intimidate members of diaspora communities who are critics of the foreign government or express views at odds with the regime's policies. It's unacceptable that people who live in your street—and mine—might be subjected to the strongarm—and long arm—of a foreign state.

Again, it's important to understand exactly what is, and is not, foreign interference in this context. Just as it is perfectly legal to criticise a foreign regime in this country, it is perfectly legal to stage a counter-protest. That is not necessarily foreign interference, it may just be nationalist zeal.

But if a foreign government is clandestinely directing the counter-protest, then my Organisation will be very interested.

Some of the foreign governments we've dealt with seem to think that this sort of community harassment is OK. They think wrong. It's not OK.

One of the most insidious things about foreign interference is that it uses our strengths against us. The perpetrators exploit our values, freedoms and trust, to undermine our values, freedoms and trust.

Foreign interference in our politics is a case in point. The governments—and I emphasise governments—involved in these activities take advantage of the open and accessible nature of our political system.

Attempts at political interference are not confined to one side of politics, and you'd be surprised by the range of countries involved.

It's also important to put it in context. While attempts to interfere in our democratic processes are common, successful interference is not.

Our democracy remains robust, our parliaments remain sovereign, our elections remain free and the overwhelming majority of our politicians remain thoroughly resistant to even the most sophisticated and subtle approaches.

It is critical we do not let fear of foreign interference undermine stakeholder engagement or stoke community division. Were this to happen, it would perversely have the same corrosive impact on our democracy as foreign interference itself.

This year—a federal election year—we need to be particularly on guard against foreign political interference.

I can confirm that ASIO recently detected and disrupted a foreign interference plot in the lead-up to an election in Australia. I'm not going to identify the jurisdiction because we are seeing attempts at foreign interference at all levels of government, in all states and territories.

But it is important to explain what political interference actually looks like.

This case involved a wealthy individual who maintained direct and deep connections with a foreign government and its intelligence agencies. This agent of interference has roots in Australia but did the bidding of offshore masters, knowingly and covertly seeking to advance the interests of the foreign power and, in the process, undermine Australia's sovereignty.

I'll call this person 'the puppeteer', although it's important to remember that while the puppeteer pulled the strings, the foreign government called the shots.

The puppeteer hired a person to enable foreign interference operations and used an offshore bank account to provide hundreds of thousands of dollars for operating expenses. Secretly shaping the jurisdiction's political scene to benefit the foreign power was considered a key performance indicator. It was like a foreign interference start-up.

The employee hired by the puppeteer began identifying candidates likely to run in the election who either supported the interests of the foreign government or who were assessed as vulnerable to inducements and cultivation. The employee used existing relationships with politicians, staffers and journalists to select potential targets, without revealing the secret intent, the foreign connection or the puppeteer's involvement.

The puppeteer and the employee plotted ways of advancing the candidates' political prospects through generous support, placing favourable stories in foreign language news platforms and providing other forms of assistance.

They investigated hiring political consultants, advertising agencies and PR specialists to help individual campaigns. The aim was not just to get the candidates into positions of power, but also to generate a sense of appreciation, obligation and indebtedness that could subsequently be exploited.

The political candidates had no knowledge of the plot. Even if the plan had proceeded, they would not have known who was pulling the strings. The puppeteer used the employee as a cut-out. This deliberate deceit and secrecy about the foreign government connection is what took the case into the realm of foreign interference.

At this point, ASIO acted. Our intervention ensured the plan was not executed, and harm was avoided.

It's impossible to know exactly what would have happened without ASIO's disruption but I can offer an informed scenario. Some of the candidates get elected. The puppeteer's employee then recommends they hire certain other associates as political staffers. These people are also agents or proxies of the foreign government, and will try to influence the politician, shape decision-making and help identify other political figures who can be influenced and recruited.

Down the track, the new parliamentarians might be asked for information about the party's position on defence policy, human rights, foreign investment or trade.

This information will be sent to the foreign power without the knowledge of the parliamentarian. At some point, the politicians might be prevailed upon to vote a particular way on a contentious issue, or lobby colleagues to vote a certain way.

I know that this is how it plays out because we've seen it happen in situations where we uncovered the foreign interference at a later stage. These cases are much more serious.

This is why ASIO's role is crucial. We and our partners use a suite of measures to disrupt foreign interference plots. The tools include defensive briefings to potential victims; interviews of perpetrators and other targeted intelligence activities; visa cancellations if we are dealing with foreign nationals and, of course, law enforcement action.

The first and most effective defence against all forms of foreign interference is awareness. Know who you are dealing with and why. That's why I've given you a level of detail that we would normally not reveal in public.

I want to improve your understanding of what foreign interference is—and, just as importantly, what it is not. The case study I've described makes it clear that foreign interference in our political system is far removed from lobbying, diplomacy or other open and transparent attempts to influence decision-making.

And as I mentioned earlier, I do not want misunderstandings about foreign interference to undermine democratic processes, community engagement or our multicultural society, which I firmly believe is a national asset.

The perpetrators of foreign interference carefully hide their true motivations. But that does not mean politicians are powerless to protect themselves.

The instincts, values and transparency that guide other elements of political engagement are powerful shields against foreign interference. If a supporter wants to provide significant levels of assistance or install a certain staffer in your office, do your due diligence. If business operators want to donate significant resources to your campaign, ask what's in it for them. If a media proprietor promises unlimited positive coverage, query their motives.

To be clear, I'm not suggesting people should reflexively turn down these types of assistance; just that they should be aware of the risks, pose the appropriate questions, and be transparent and accountable about what's received. And, most critically, stay alert to the backers calling in their favours by asking for something that conflicts with Australia's interests.

Security is a shared responsibility.

That's the message I want to leave you with tonight.

I want to assure you of two things: good security is achievable, and good security works.

I find it infuriating when companies say they were done over by an adversary so powerful there was no way to defend against it. That's what I call the Borg defence—'resistance is futile'.

In my experience, resistance is rarely futile.

Certainly, in the cyber field, the overwhelming majority of compromises are foreseeable and avoidable.

While some of these are seriously damaging, many others that are breathlessly called 'cyber-attacks' in the media are not compromises at all—they are reconnaissance missions; if the digital doors are locked, the intruder moves on and tries somewhere else.

At the same time, I'm the first to admit ASIO is not all-seeing or all-knowing—we don't want to be—and while ASIO is part of the answer to the challenges I've outlined, we are not the whole answer.

The acceleration of radicalisation, online propaganda and misinformation, single-issue extremism and minors embracing violent extremism all require a whole-of-government, whole-of-system and whole-of-nation approach.

That's why teamwork is critical.

Our work with law enforcement, the national intelligence community, Home Affairs and our international counterparts is well known—all of you are represented in the room tonight and I want to thank and commend you for being such effective mission enablers, leaders and force multipliers. But ASIO can do more. The scale and scope of Australia's adversaries requires a broader approach to security intelligence, its influence and impact.

The threat environment demands we take our engagement to a new strategic level. It's what we call 'hardening the environment'; making our economy, institutions and political system more difficult and resilient targets for those seeking to undermine them.

I started this address with a personal admission, so I might as well conclude with one, too.

The Director-General of Security is not always the most welcome visitor. All too often when I knock on a door the person who opens it looks like they are thinking, 'Uh oh—here comes the bad news.'

It's time to improve that.

Obviously, ASIO will continue to identify and communicate threats, but I want to put more emphasis on what you can do about them.

How you can protect your people, places, technology and information.

How a good security strategy addresses physical security, IT security and personal security.

As I said before, good security is achievable, and good security works.

The threats facing Australia are serious, but not insurmountable. Our adversaries are sophisticated, but not unstoppable.

In all the case studies I presented this evening—the online radicalisers, the teenage extremists, the nation-state conducting political interference—in all of them, the adversary made a mistake that brought its activities to ASIO's attention and led to the threat being mitigated.

And just in case our adversaries are listening, I should point out that you don't need to make a mistake to come to our attention. ASIO can catch you even if your tradecraft is perfect. I'll back my people any day.

ASIO will always play its part. We will protect Australia's security and safeguard its sovereignty. We will detect and defeat Australia's adversaries, and we will work with our partners to defend our nation's interests.

Thank you.

The video: https://www.youtube.com/watch?v=IL2xZhN1vnM

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.

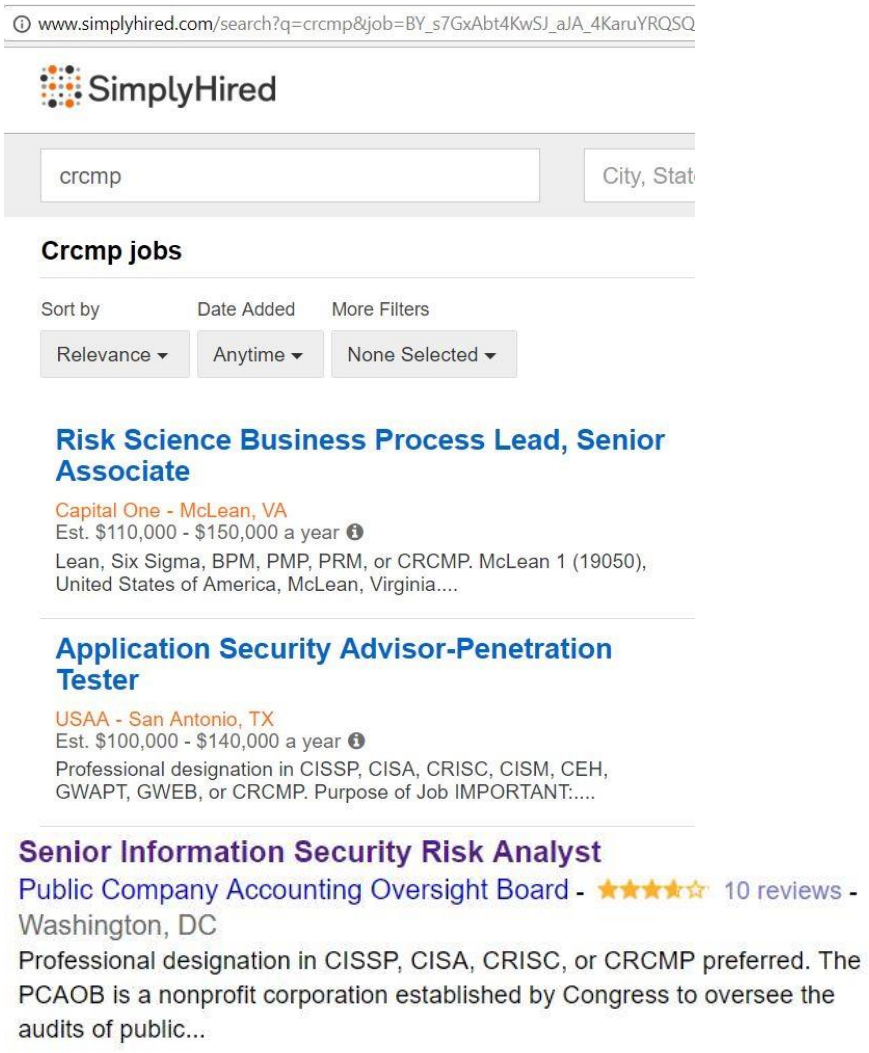
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

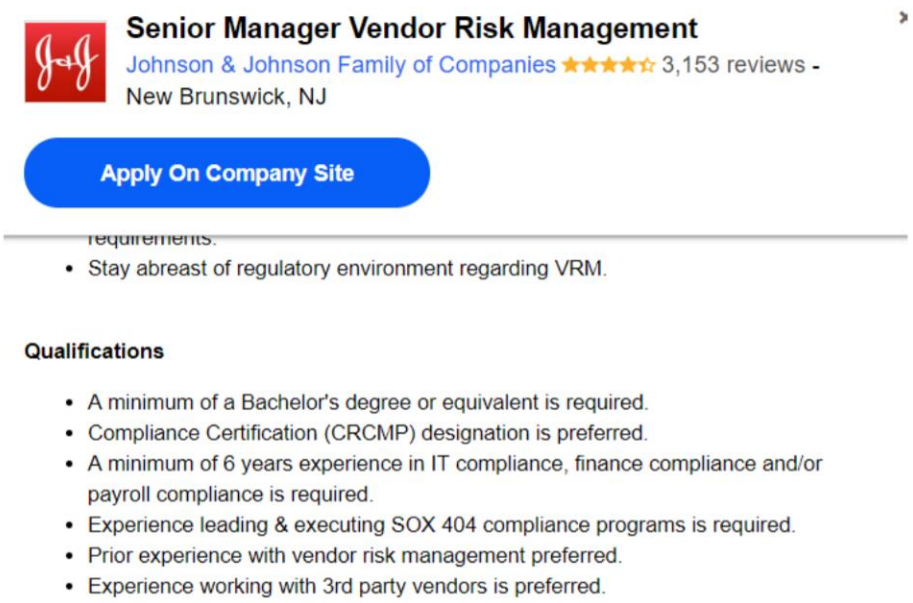
You can explore what we offer to our members:

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





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.

Companies and organizations like Accenture, American Express, USAA etc. consider the Certified Risk and Compliance Management Professional (CRCMP) program a preferred certificate. There are CRCMPs in 32 countries.

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

Our Reading Room:
https://www.risk-compliance-association.com/Reading_Room.htm