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, September 13, 2021

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,

Supply chain refers to the ecosystem of processes, people, organizations, and distributors involved in the creation and delivery of a final solution or product.

In cybersecurity, the supply chain involves a wide range of resources (hardware and software), storage (cloud or local), distribution mechanisms (web applications, online stores), and management software.

We have a new paper from the European Network and Information Security Agency (ENISA) with title "*ENISA threat landscape for supply chain attacks*". According to the paper, supply chain attacks leverage the interconnectedness of the global markets. When multiple customers rely on the same supplier, the consequences of a cyber-attack against this supplier are amplified, potentially resulting in a large-scale national or even cross-border impact.

For some products, such as software and executable code, the existence of a supply chain is opaque or even completely hidden to the end user.

End-user software depends, directly or indirectly, on software provided by the supplier. Such dependencies include packages, libraries, and modules — all of which are used pervasively to lower development costs and accelerate shipping times.

The better protected against cyber-attacks organizations become, the more the attention shifts to suppliers. The math is simple, suppliers are becoming the *weakest link* on the supply chain. At the same time, customers demand products that are more cybersecure but that remain at a low cost, two needs that it is not always possible to reconcile.

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

Best regards,

George Lekatis

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 5)

ENISA threat landscape for supply chain attacks

Number 2 (Page 8)

BIS Bulletin No 45, Regulating big techs in finance

Agustín Carstens, Stijn Claessens, Fernando Restoy and Hyun Song Shin

Number 3 (Page 11)

Risk Dashboard: European insurers' risk levels remain broadly stable

Number 4 (Page 14)

Report on EIOPA Supervisory Activities in 2020

Number 5 (Page 17)

EBA consults on new Guidelines on the role of AML/CFT compliance officers

Number 6 (Page 20)

Committee on Payments and Market Infrastructures publishes work programme for 2021-22

Number 7 (Page 23)

NIST Study on Kids' Passwords Shows Gap Between Knowledge of Password Best Practices and Behavior

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Number 8 (Page 26)

Attackers use Morse code, other encryption methods in evasive phishing campaign

Microsoft 365 Defender Threat Intelligence Team

Microsoft

Number 9 (Page 29)

HOW DID THE NORDIC-BALTIC COUNTRIES HANDLE THE FIRST WAVE OF COVID-19?

A STRATEGIC COMMUNICATIONS ANALYSIS - Published by the NATO Strategic CommunicationsCentre of Excellence

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

Number 10 (Page 33)

Enabling Military Systems to Adapt to the Unexpected

Program aims to provide physical systems with ability to adapt to unexpected events in real-time and effectively communicate system changes to human and AI operators

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

ENISA threat landscape for supply chain attacks

Supply chain attacks have been a security concern for many years, but the community seems to have been facing a greater number of more organized attacks since early 2020.

It may be that, due to the more robust security protection that organizations have put in place, attackers successfully shifted towards suppliers.

They managed to have significant impacts in terms of the downtime of systems, monetary losses and reputational damages, to name but a few.

The importance of supply chains is attributed to the fact that successful attacks may impact a large amount number of customers who make use of the affected supplier.

Therefore, the cascading effects from a single attack may have a widely propagated impact.

This report aims at mapping and studying the supply chain attacks that were discovered from January 2020 to early July 2021.

Based on the trends and patterns observed, supply chain attacks increased in number and sophistication in the year 2020 and this trend is continuing in 2021, posing an increasing risk for organizations.

It is estimated that there will be four times more supply chain attacks in 2021 than in 2020.

With half of the attacks being attributed to Advanced Persistence Threat (APT) actors, their complexity and resources greatly exceed the more common nontargeted attacks, and, therefore, there is an increasing need for new protective methods that incorporate suppliers in order to guarantee that organizations remain secure.

This report presents the Agency's Threat Landscape concerning supply chain attacks, produced with the support of the Ad-Hoc Working Group on Cyber Threat Landscapes.

Table 1: Proposed taxonomy for supply chain attacks. It has four parts: (i) attack techniques used on the supplier, (ii) assets attacked in the supplier, (iii) attack techniques used on the customer, (iii) assets attacked in the customer.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Malware Infection	Pre-existing Software	Trusted Relationship [T1199]	Data
Social Engineering	Software Libraries	Drive-by Compromise [T1189]	Personal Data
Brute-Force Attack	Code	Phishing [T1566]	Intellectual Property
Exploiting Software Vulnerability	Configurations	Malware Infection	Software
Exploiting Configuration Vulnerability	Data	Physical Attack or Modification	Processes
Open-Source Intelligence (OSINT)	Processes	Counterfeiting	Bandwidth
	Hardware		Financial
	People		People
	Supplier		

The main highlights of the report include the following:

- A taxonomy to classify supply chain attacks in order to better analyse them in a systematic manner and understand the way they manifest is described.

- 24 supply chain attacks were reported from January 2020 to early July 2021, and have been studied in this report.

- Around 50% of the attacks were attributed to well-known APT groups by the security community.

- Around 42% of the analysed attacks have not yet been attributed to a particular group.

- Around 62% of the attacks on customers took advantage of their trust in their supplier.

- In 62% of the cases, malware was the attack technique employed.

- When considering targeted assets, in 66% of the incidents attackers focused on the suppliers' code in order to further compromise targeted customers.

- Around 58% of the supply chain attacks aimed at gaining access to data (predominantly customer data, including personal data and intellectual property) and around 16% at gaining access to people.

- Not all attacks should be denoted as supply chain attacks, but due to their nature many of them are potential vectors for new supply chain attacks in the future.

- Organizations need to update their cybersecurity methodology with supply chain attacks in mind and to incorporate all their suppliers in their protection and security verification.

To read more:
https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Table 2: Attack techniques used to compromise the supplier in the chain. Each technique identifies how the attack happened, and not what was attacked. Several techniques may be used in the same attack.

ATTACK TECHNIQUES USED TO COMPROMISE A SUPPLY CHAIN	
Malware Infection	e.g. spyware used to steal credentials from employees.
Social Engineering	e.g. phishing, fake applications, typo-squatting, Wi-Fi impersonation, convincing the supplier to do something.
Brute-Force Attack	e.g. guessing an SSH password, guessing a web login.
Exploiting Software Vulnerability	e.g. SQL injection or buffer overflow exploit in an application.
Exploiting Configuration Vulnerability	e.g. taking advantage of a configuration problem.
Physical Attack or Modification	e.g. modify hardware, physical intrusion.
Open-Source Intelligence (OSINT)	e.g. search online for credentials, API keys, usernames.
Counterfeiting	e.g. imitation of USB with malicious purposes.

Number 2

BIS Bulletin No 45, Regulating big techs in finance

Agustín Carstens, Stijn Claessens, Fernando Restoy and Hyun Song Shin

Key takeaways

- Big tech firms entering financial services can scale up rapidly with user data from their existing business lines in e-commerce and social media, and by harnessing the inherent network effects in digital services.

- In addition to traditional policy concerns such as financial risks, consumer protection and operational resilience, the entry of big techs into financial services gives rise to new challenges surrounding the concentration of market power and data governance.

- The current framework for regulating financial services follows an activities-based approach where providers must hold licences for specific business lines. There is scope to address the new policy challenges by developing specific entity-based rules, as proposed in several key jurisdictions – notably the European Union, China and the United States.

The centrality of data in the digital economy has enabled the entry into financial services and rapid growth of big tech firms.

Big techs have existing businesses in e-commerce and social media, among others, from which they can expand into finance.

Their business model revolves around the direct interactions of users and the data generated as an essential by-product of these interactions.

The distinguishing feature of big techs is that they can overcome limits to scale by utilising user data from their existing businesses to scale up rapidly by harnessing the inherent network effects in digital services.

In turn, the greater user activity generates yet more data, reinforcing the advantages that come from network effects.

In this way, big techs can establish a substantial presence in financial services very quickly through the so-called “data-networkactivities” (DNA) loop.

This gives rise to concerns about the emergence of dominant firms with excessive concentration of market power and a possibly systemic footprint in the financial system.

The rapid growth of big tech firms in financial services presents various policy challenges.

Some are variations of familiar themes that lie squarely within the traditional scope of central banks and financial regulators, such as the mitigation of financial risks and the oversight of operational resilience and consumer protection.

Assessing big techs' resilience through a financial cycle will necessitate more systematic monitoring and understanding of big tech business models on the part of the authorities, for instance on whether learning algorithms may inject systematic biases to the detriment of financial stability.

As well as issues that arise from traditional financial stability concerns, there are new and unfamiliar challenges stemming from the potential for excessive concentration of market power, as well as broader issues concerning data governance.

These new challenges lie outside the traditional scope of the central bank's remit, but they can nevertheless impinge on the central bank's core mission of ensuring sound money as well as the integrity and smooth functioning of the payment system.

While some central banks' oversight authority includes the competitive functioning and efficiency of the payment system, their mandates do not normally encompass the broad range of competition and data privacy issues that arise in relation to the activities of big techs in financial services.

Nevertheless, since the central bank issues the unit of account in the economy, trust in the currency rests ultimately on the trust placed in the central bank itself.

Any impact on the integrity of the monetary system arising from the emergence of dominant platforms ought to be a key concern for the central bank.

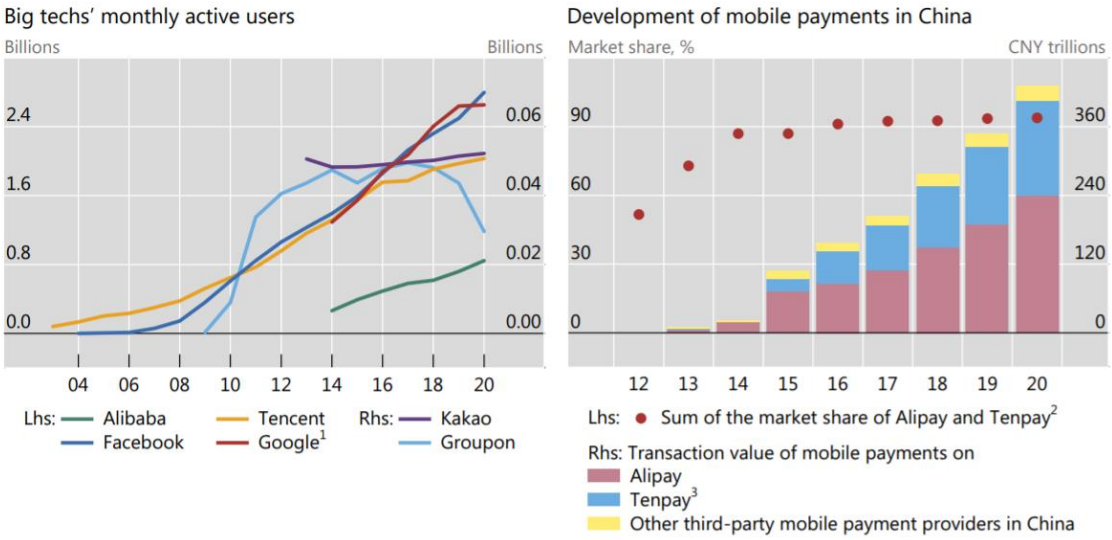
This Bulletin reviews the policy challenges for central banks and financial regulators in their oversight of the activity of big tech firms in financial services, especially as it relates to the payment system.

Traditional demarcations that separate the roles of financial regulators from those of competition authorities and data privacy regulators may become blurred in the case of big techs in finance.

Rules that were formulated with specific financial stability risks in mind (credit and liquidity risk, market risk etc) may be inadequate for addressing the unique combination of policy concerns to which big techs give rise.

These concerns bear on the central bank's core mission to maintain the integrity of the monetary system. In this regard, the central bank should work more closely with competition and data privacy authorities.

Big techs' rapid growth in users underpins their dominance in some markets — Graph 1



[1] The number of Chrome users is used as a proxy for Google's number of active users. [2] Market shares for 2012 are estimated based on market evidence. [3] Tenpay includes WeChat Pay and QQ Wallet.

Sources: BIS (2019); Enfodesk; S&P Capital IQ, company reports, analysys.cn; Statista, Industries; BIS calculations.

To read more: https://www.bis.org/publ/bisbull45.pdf

Number 3

Risk Dashboard: European insurers' risk levels remain broadly stable

The European Insurance and Occupational Pensions Authority (EIOPA) published today its Risk Dashboard based on the first quarter of 2021 Solvency II data.

Risk Dashboard July 2021 (Q1-2021 Solvency II Data)

Risks	Level	Trend (past 3 months)	Outlook (next 12 months)
Macro risks	High	↗	→
Credit risks	Medium	→	→
Market risks	Medium	→	→
Liquidity and funding risks	Medium	→	→
Profitability and solvency	Medium	↘	→
Interlinkages and imbalances	Medium	→	→
Insurance (underwriting) risks	Medium	→	→
Market perceptions	Medium	→	→

Note: The structural break as of Q1 2020 related to the Brexit withdrawal agreement and represented with a dashed line indicates a break in the number of undertakings of the time series and rebalance of the country weights. Additionally, adjusted time series for EU27 before Q1 2020 are also disclosed to reflect potential variations driven by the structural break in the sample.

The results show that insurers' exposures to macro risks remain at high level while all other risk categories remain at medium level.

With regards to macro risk, Gross Domestic Product growth and inflation forecasts registered new upward revisions. The 10 years swap rates have slightly increased across currencies in the second quarter of 2021. Financial markets remain broadly stable, amid fiscal and monetary support.

Solvency positions for the first quarter of 2021 for all types of undertakings showed an improvement. Life insurers' profitability, measured by annual investments' returns, registered a notable deterioration in 2020.

Insurance risks remain at medium level, in spite of deterioration of some indicators.

The cumulative catastrophe loss ratio and year-on-year premium growth for non-life continued deteriorating.

On the other hand, the loss ratio decreased to one of the lowest values and year-on-year premium growth for life reported a slight recovery after the deterioration in the previous quarters.

Market perceptions remain at medium level with an increasing trend. The life insurance sector underperformed while non-life outperformed the stock market in the second quarter 2021.

Key observations

The results show that insurers' exposures to macro risks remain at high level while all other risk categories remain at medium level.

- With regards to macro risk, Gross Domestic Product growth and inflation forecasts registered new upward revisions. The 10 years swap rates have slightly increased across currencies in the second quarter of 2021.

- Financial markets remain broadly stable, amid fiscal and monetary support. Solvency positions for the first quarter of 2021 for all types of undertakings showed an improvement.

- Life insurers' profitability, measured by annual investments' returns, registered a notable deterioration in 2020.

- Insurance risks remain at medium level, in spite of deterioration of some indicators.

- The cumulative catastrophe loss ratio and year-on-year premium growth for non-life continued deteriorating.

- On the other hand, the loss ratio decreased to one of the lowest values and year-on-year premium growth for life reported a slight recovery after the deterioration in the previous quarters.

- Market perceptions remain at medium level with an increasing trend.

- The life insurance sector underperformed while non-life outperformed the stock market in the second quarter 2021.

To read more:
https://www.eiopa.europa.eu/tools-and-data/risk-dashboard_en

Number 4

Report on EIOPA Supervisory Activities in 2020

EIOPA's supervisory convergence plan for 2021 identifies one of the main goals of the European Insurance and Occupational Pensions Authority (EIOPA) by ensuring a high, effective and consistent level of supervision across Europe, with the aim of guaranteeing a similar level of protection of policyholders and beneficiaries across jurisdictions, preventing supervisory arbitrage and guaranteeing a level playing field.

As a step towards the implementation of the plan, this Report presents how EIOPA contributed during 2020 to enhancing the common European supervisory culture and promoted consistent supervisory practices both from a prudential and conduct of business supervision perspective.

The year of 2020 brought the world a pandemic which has created huge social disruptions and unprecedented economic challenges. EIOPA had adapted its priorities and strategies to support both industry and supervisors to tackle those different challenges.

To maintain supervisory convergence in a pandemic situation required cooperation and timely reaction.

The situation triggered some extraordinary and flexible responses.

In particular, EIOPA encouraged supervisors and insurers to make use of the flexibility embedded in the existing regulatory framework and issued some supervisory statements to deal with the new risks and situations caused by the pandemic.

The need to carry out activities previously not planned inevitably had the consequence to reprioritise some of the planned work.

Anyway, the work on supervisory convergence overall revealed a good degree of progress, covering a variety of areas, from Solvency II related issues such as calculation of technical provisions to further development of supervisory activities in the area of conduct risks and analysis of innovative technologies and how they can improve supervisory practices.

On conduct risks EIOPA finalised a chapter for the Supervisory Handbook containing guidance to supervisors on how to carry out a risk-based, outcome-focused and proportional supervision of Product Oversight and

Governance (POG) requirements. EIOPA also published "EIOPA's approach to the supervision of product oversight and governance" aiming at providing more clarity for insurance manufacturers and distributors on the supervisory approach to POG requirements.

Following up the request of the European Commission to EIOPA for a technical advice on the review of the Solvency II Directive in February 2019, EIOPA finalised its Advice in December 2020 leveraging on a number of activities, originally initiated with the aim to improve supervisory convergence. This led to some proposals from a regulatory perspective.

EIOPA has continued its prudential oversight work during 2020 and strengthened its oversight activities on conduct of business, initiating also in this area bilateral visits to National Competent Authorities (NCAs).

Furthermore, EIOPA has continued its activity to increase the level of supervisory convergence in the area of internal model, including – among others - its consistency projects with a view of tackling some aspects of the calibration of internal model.

Following up the change of EIOPA's regulation, EIOPA has prepared to assist NCAs, upon request, handling requests for new approvals of internal model or model changes.

Since the introduction of this new task, no request for assistance has yet been submitted to EIOPA.

Sound supervision of cross border activities, be it under free provision of services or the right of establishment, has emerged as a compelling priority to enhance trust of consumers in the wellfunctioning of the internal market.

By the end of 2020, six cooperation platforms were operational with the involvement of 21 NCAs.

The cooperation platforms are active as long as the risks identified raise concerns about the appropriate level of protection of policyholders.

Many actions and measures were taken and implemented in 2020 with the aim to conduce to timely supervisory actions to the benefit of consumers.

For some of the platforms the intensive cooperation is continuing into 2021.

Figure 1 presents an overview of the activities EIOPA developed in 2020 to strengthen supervisory convergence in more detail:

1 IMPLEMENTATION OF THE COMMON SUPERVISORY CULTURE AND FURTHER DEVELOPMENT OF SUPERVISORY TOOLS

- As part of the 2020 review of Solvency II, proposed some improvement to the application of the proportionality principle (new process and new measures)
- New Chapters of the Supervisory Handbook on Internal Model Validation
- After re-prioritisation due to COVID-19 close co-operation with NCAs to mitigate the impact of the COVID-19 outbreak and issue supervisory statements and other supervisory measures
- Initiated the thematic review on mortgage life and other credit protection insurance sold through banks
- Seminar on the use of data and SupTech

2 RISKS TO THE INTERNAL MARKET AND TO THE LEVEL PLAYING FIELD

- As part of the 2020 review of Solvency II, proposed some improvement to the application of the proportionality principle with regard to the calculation of best estimate, fit and proper requirements, cooperation in case of complex cross-border cases and use of reinsurance as risk-mitigation techniques
- In the area of supervision of IORPs, published a supervisory statement on the sound supervisory practices for registering or authorising IORPs
- In the area of Internal Models, continued the Non-Life underwriting Comparative Studies (NLCS), market and credit risk comparative study (MCRCS) and study on modelling of diversification benefits

3 SUPERVISION OF EMERGING RISKS

- Supervision of data and IT-related risks, including cyber risk from an operational resilience perspective
- Publication of the draft Guidelines on ICT security and governance

4 OVERSIGHT ACTIVITIES

Next to the cooperative work together with the NCAs, EIOPA performed the following supervisory convergence activities via its oversight function (both prudential and conduct of business) with a focus on:

- 77 Active participations in cross-border Colleges, which also looked at conduct aspects as relevant
- 4 Joint on-site inspections
- 6 Active Cooperation Platforms, covering both conduct and prudential aspects
- 10 Bilateral engagements with NCAs
- 9 Internal-model-specific supervisors meetings
- 3 Technical assistance to a NCA via an Structural Reform Support Service (SRSS) project
- 1 Equivalence monitoring exercise
- 1 Assessment of compliance with the commitments for the non –banking financial sector in the context of ERM II

↑ HIGH, EFFECTIVE AND CONSISTENT LEVEL OF SUPERVISION ↓

To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_bos-21-097-report-on-supervisory-activities.pdf

Number 5

EBA consults on new Guidelines on the role of AML/CFT compliance officers

The European Banking Authority (EBA) has launched a public consultation on new Guidelines on the role, tasks and responsibilities of anti-money laundering and countering the financing of terrorism (AML/CFT) compliance officers.

The Guidelines also include provisions on the wider AML/CFT governance set-up, including at the level of the group. Once adopted, these Guidelines will apply to all financial sector operators that are within the scope of the AML Directive.

This consultation runs until **2 November 2021.**

The draft Guidelines comprehensively address, for the first time at the level of the EU, the whole AML/CFT governance set-up.

They set clear expectations of the role, tasks and responsibilities of the AML/CFT compliance officer and the management body and how they interact, including at group level.

AML/CFT compliance officers need to have a sufficient level of seniority, which entails the powers to propose, on their own initiative, all necessary or appropriate measures to ensure the compliance and effectiveness of the internal AML/CFT measures to the management body in its supervisory and management function.

Without prejudice to the overall and collective responsibility of the management body, the draft Guidelines also specify the tasks and role of the member of the management board, or the senior manager where no management board exists, who are in charge of AML/CFT overall, and on the role of group AML/CFT compliance officers.

As information reaching the management body needs to be sufficiently comprehensive to enable informed decision-making, the draft Guidelines set out which information should be at least included in the activity report of the AML/CFT compliance officer to the management body.

Where a financial services operator is part of a group, the draft Guidelines provide that a Group AML/CFT compliance officer in the parent company

should be appointed to ensure the establishment and implementation of effective group-wide AML/CFT policies and procedures and to ensure that any shortcomings in the AML/CFT framework affecting the entire group or a large part of the group are addressed effectively.

Provisions in the draft Guidelines are designed to be applied in a proportionate manner, taking into account the diversity of financial sector operators that are within the scope of the AML Directive.

They are also in line with existing ESA guidelines, in particular:

- the revised Guidelines on internal governance under the capital requirements Directive (CRD);

- the revised Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body;

- the draft Guidelines on the authorisation of credit institutions; and

- the draft Guidelines for common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing.

Consultation process

Comments to the draft Guidelines can be sent by clicking on the "send your comments" button on the EBA's consultation page. The deadline for the submission of comments is 2 November 2021.

All contributions received will be published following the close of the consultation, unless requested otherwise.

The EBA will hold a virtual public hearing on the draft Guidelines on 28 September 2021 from 10:00 to 12:00 Paris time. The dial-in details will be communicated to those who have registered for the meeting.

Legal basis and background

The EBA drafted these Guidelines in line with its legal mandate to lead, coordinate and monitor the EU financial sector's fight against ML/TF.

In drafting these guidelines, the EBA fulfills a request by the Commission's request in its Supra-National Risk Assessment (SNRA) of 2019 to develop guidance that 'clarifies the role of AML/CFT compliance officers in credit and financial institutions'.

To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2021/Consultation%20on%20draft%20Guidelines%20on%20the%20role%2C%20tasks%20and%20responsibilities%20AML-CFT%20compliance%20officers/1018277/CP%20GLs%20on%20AMLCFT%20compliance%20officer.pdf

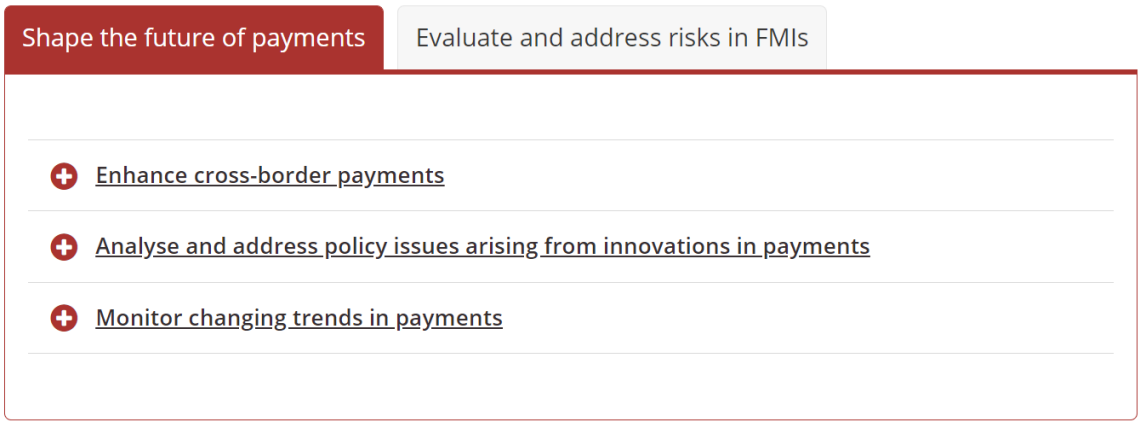
Number 6

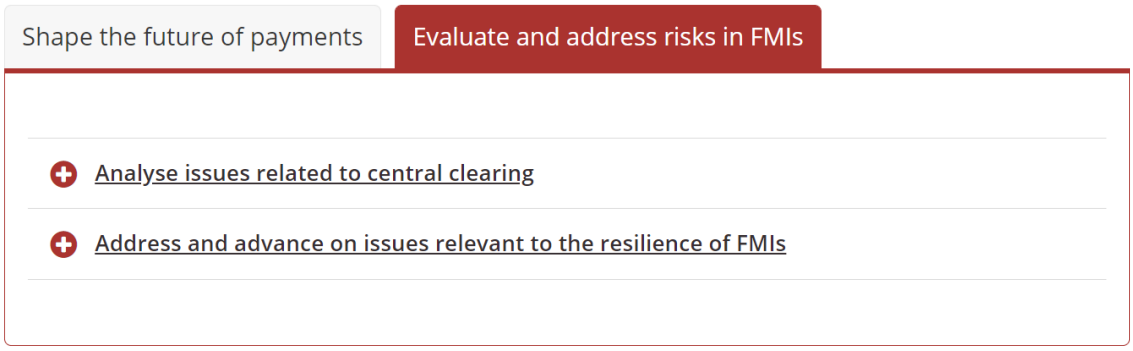
Committee on Payments and Market Infrastructures publishes work programme for 2021-22

- Committee on Payments and Market Infrastructures (CPMI) publishes its work programme for the first time.

- The 2021–22 work programme focuses on shaping the future of payments and addressing risks in financial market infrastructures.

- CPMI's priorities include: enhancing cross-border payments; addressing policy issues arising from innovations in payments; evaluating and addressing risks in financial market infrastructures that emerged or were accentuated during the pandemic.





The CPMI has published its work programme for 2021–22, which will focus on shaping the future of payments and addressing risks in financial market infrastructures.

The annual work programme has been publicly released for the first time as part of the CPMI's commitment to increased transparency.

The work programme outlines the strategic priorities for its monitoring and analysis, policy, and standard-setting and implementation activities, under its two overarching themes:

Shaping the future of payments will include enhancing cross-border payments and addressing policy issues arising from digital innovations in payments (such as central bank digital currencies and stablecoins), while monitoring changing trends in payments.

Evaluating and addressing risks in financial market infrastructures will work on issues related to central clearing and others that emerged or were accentuated over the course of the Covid-19 pandemic.

The programme was drawn up under the direction of CPMI Chair Sir Jon Cunliffe in consultation with the Governors of the BIS Economic Consultative Committee.

About the Committee's work

The CPMI carries out its mandate through the following activities:

- monitoring and analysing developments to help identify risks for the safety and efficiency of arrangements within its mandate as well as resulting risks for the global financial system;

- sharing experiences related to arrangements within its mandate, to the performance of oversight functions and to the provision of central bank services in order to promote common understanding, and developing policy advice or common policies for central banks;

- establishing and promoting global standards and recommendations for the regulation, oversight and practices of arrangements within its mandate, including guidance for their interpretation and implementation, where appropriate;

- monitoring the implementation of CPMI standards and recommendations with the purpose of ensuring timely, consistent and effective implementation;

- supporting cooperative oversight and cross-border information-sharing, including crisis communication and contingency planning for cross-border crisis management;

- maintaining relationships with central banks which are not members of the CPMI to share experiences and views and to promote the

implementation of CPMI standards and recommendations beyond CPMI member jurisdictions, either directly or by supporting regional bodies as appropriate; and

- coordinating and cooperating with other financial sector standard setters, central bank bodies and international financial institutions.

To read more: https://www.bis.org/cpmi/cpmi_work.htm

Number 7

NIST Study on Kids' Passwords Shows Gap Between Knowledge of Password Best Practices and Behavior

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

When it comes to passwords, the challenges are endless. We must create multiple passwords to manage our many online accounts, from email to shopping sites and social media profiles.

We have to safely keep track of these many passwords and ensure they're strong enough to reduce the risk of cyberattacks.

All of these reasons emphasize why education and training are so important for strengthening passwords and protecting personal accounts.

The problem isn't limited to just adults. Children may seem more technologically savvy because they've grown up in the digital space, but they still face the same cybersecurity threats.

So, to shed light on what kids understand about passwords and their behavior in creating and using them, researchers at the National Institute of Standards and Technology (NIST) conducted a study that surveyed kids from third to 12th grade.

The study found that children are learning best practices, such as memorizing passwords, but are demonstrating a gap between their knowledge of good password practices and their behavior.

The NIST researchers present their findings today at a virtual cybersecurity conference called USENIX Security Symposium 2021.

According to recent data from the Pew Research Center, more than one-third of parents with a child younger than 12 say their child began interacting with a smartphone before the age of 5, and 67% of parents say their child uses or interacts with a tablet computer. You may visit: https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/

"Younger children rely on parents a lot. Their first passwords were either given to them at school or by a parent to open their phone or tablet. So, what kind of guidance can we provide?" said NIST researcher Yee-Yin Choong.

The researchers surveyed more than 1,500 kids from ages 8 to 18 who attended schools across the South, Midwest and Eastern regions of the U.S. Teachers administered two versions of the survey, one for third to fifth graders and the other for sixth to 12th graders. Each survey featured the same questions but had different age-appropriate language.

On the plus side, results from the study showed that kids are learning best practices on passwords, such as limiting their writing of passwords on paper, keeping their passwords private, and logging out after online sessions. They're also not burdened with a lot of passwords as adults are, with kids on average reporting they have two passwords for school and two to four for home.

The passwords that kids created often consisted of concepts reflecting the current state of their lives. Passwords referenced sports, video games, names, animals, movies, titles (such as "princess"), numbers and colors. Examples included "yellow," "doggysafesecure" and "PrincessFrog248."

Password strength increased from elementary to high school students. Examples of stronger passwords among middle and high school students included "dancingdinosaursavrwhoop164" and "Aiken_bacon@28."

But despite the evidence that kids are learning best practices, they also demonstrated bad password habits. They tended to reuse passwords, a habit that increased in frequency from elementary to high school students, and shared their passwords with their friends. "For adolescents, an important part of building friendships is building trust, which is shown with sharing secrets. Their perspective is that sharing passwords is not risky behavior," said Choong.

The study also shed light onto what kids thought about passwords. The survey asked, "Why do people need passwords?" The answers were different for younger and older kids. Elementary students said safety was the primary reason, while for middle and high school students, privacy became more a more dominant answer.

Another notable finding was that younger kids relied on family support for creating and maintaining their passwords at home. This suggests that families play a central role in establishing best practices and that parents affect kids' behavior with passwords.

Not many studies have been performed on kids and cybersecurity, said Choong, which is why this work could be significant in helping researchers understand more about kids' password use.

"This was a very carefully designed study. We had to think carefully about the methodology," said Choong. Researchers contacted the principal of each school first to gain school support for the research, she said. They also worked with the teachers in getting parental consent and administering the surveys.

In future work, the NIST researchers will move outside the scope of passwords to investigate children's and parents' perceptions of online security, privacy and risky behaviors.

"The end goal of this research is to better support children and provide recommendations that can be used to provide guidance to them, parents and educators. Overall, the focus is on providing guidelines and best practices so that they can stay safe and secure online while enjoying the benefits of the internet," said Choong.

Number 8

Attackers use Morse code, other encryption methods in evasive phishing campaign

Microsoft 365 Defender Threat Intelligence Team

Cybercriminals attempt to change tactics as fast as security and protection technologies do. During our year-long investigation of a targeted, invoice-themed XLS.HTML phishing campaign, attackers changed obfuscation and encryption mechanisms every 37 days on average, demonstrating high motivation and skill to constantly evade detection and keep the credential theft operation running.

This phishing campaign exemplifies the modern email threat: sophisticated, evasive, and relentlessly evolving.

The HTML attachment is divided into several segments, including the JavaScript files used to steal passwords, which are then encoded using various mechanisms.

These attackers moved from using plaintext HTML code to employing multiple encoding techniques, including old and unusual encryption methods like Morse code, to hide these attack segments.

Some of these code segments are not even present in the attachment itself. Instead, they reside in various open directories and are called by encoded scripts.

In effect, the attachment is comparable to a jigsaw puzzle: on their own, the individual segments of the HMTL file may appear harmless at the code level and may thus slip past conventional security solutions. Only when these segments are put together and properly decoded does the malicious intent show.

This campaign's primary goal is to harvest usernames, passwords, and—in its more recent iteration—other information like IP address and location, which attackers use as the initial entry point for later infiltration attempts.

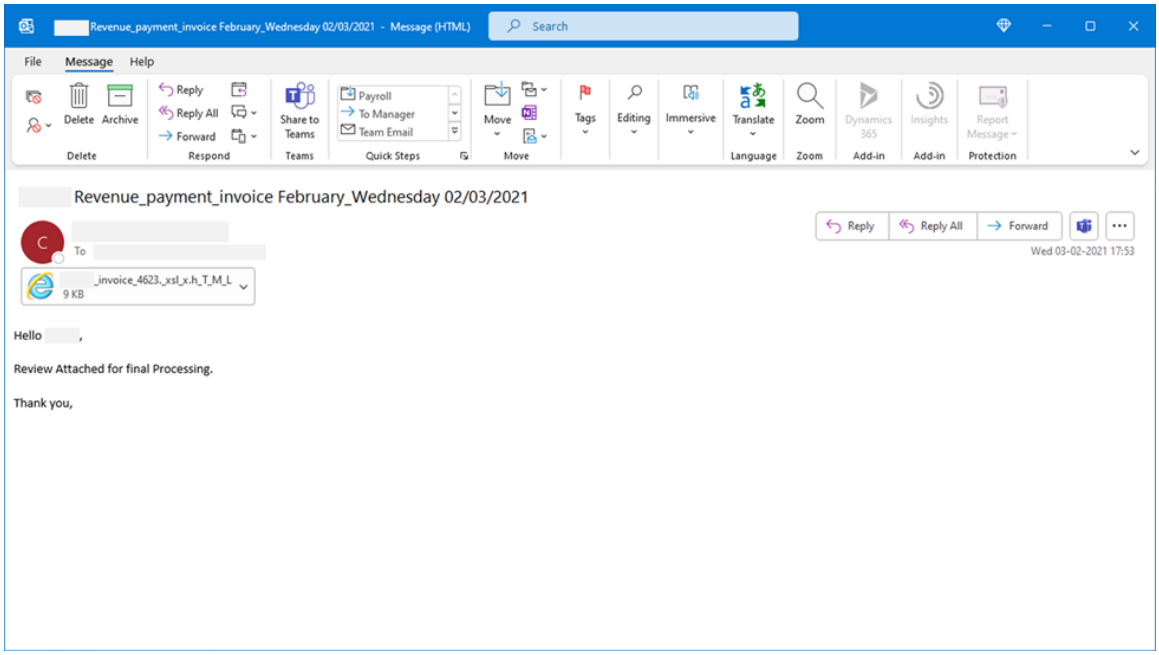
As we previously noted, the campaign components include information about the targets, such as their email address and company logo. Such details enhance a campaign's social engineering lure and suggest that a prior reconnaissance of a target recipient occurs.

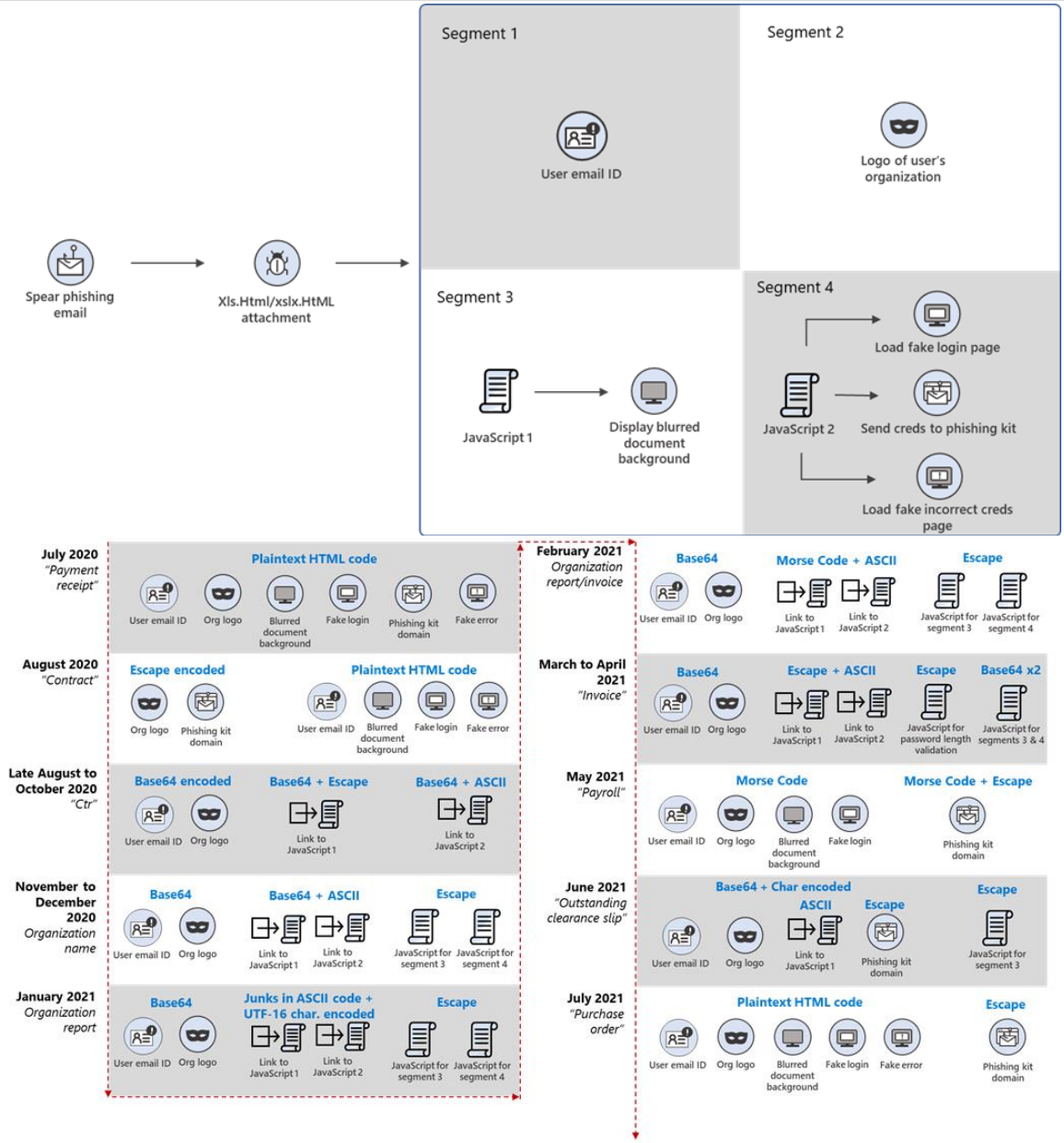
Email-based attacks continue to make novel attempts to bypass email security solutions. In the case of this phishing campaign, these attempts include using multilayer obfuscation and encryption mechanisms for known existing file types, such as JavaScript. Multilayer obfuscation in HTML can likewise evade browser security solutions.

To defend organizations against this campaign and similar threats, Microsoft Defender for Office 365 uses multiple layers of dynamic protection technologies backed by security expert monitoring of email campaigns.

Rich email threat data from Defender for Office 365 informs Microsoft 365 Defender, which provides coordinated defense against follow-on attacks that use credentials stolen through phishing.

Microsoft 365 Defender does this by correlating threat data from email, endpoints, identities, and cloud apps to provide cross-domain defense.





To read more:
https://www.microsoft.com/security/blog/2021/08/12/attackers-use-morse-code-other-encryption-methods-in-evasive-phishing-campaign/

Number 9

HOW DID THE NORDIC-BALTIC COUNTRIES HANDLE THE FIRST WAVE OF COVID-19?

A STRATEGIC COMMUNICATIONS ANALYSIS - Published by the NATO Strategic CommunicationsCentre of Excellence

What is this project?

When the Covid-19 virus struck Europe in 2020 with the full force of a pandemic, eight countries allied in the Nordic-Baltic region immediately faced a challenge to their hard-won partnership.

For three decades Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway, and Sweden had been building a common purpose.

How would that friendship respond to the greatest health scare in a hundred years?

This report aims to answer this question by looking at developments in the Nordic-Baltic Eight (NB8) through a Strategic Communications lens.

Why a Strategic Communications lens?

To understand fully the pandemic that gripped these eight partner states is to paint a picture that goes beyond the number of human lives lost or the rise in unemployment, fall in national economic growth, and assumption of state debt so punitive to their taxpayers.

Any complete picture would also tell the story of how governments chose to speak to their electorates, and how civil society would respond to unprecedented measures imposed in peace time: curbing individual freedoms, it may be assumed, would elicit a consequent questioning of trust between government and governed.

All states communicate strategically. But that is not to say they engage in Strategic Communications. Which is understood as the shifting and shaping of significant discourses in societies.

It aspires to change the way people think and behave; in other words, to achieve a strategic effect. Inevitably, such an ambitious task requires separating out diverse audiences and honing particular approaches to appeal to those audiences' attitudes and grievances.

In trying to achieve a strategic effect – inshort, change – the strategic dimension of the term Strategic Communications sees strategy as focused on the long term; more specifically, its proponents play the long game.

However, the NB8 members in early 2020 would find themselves facing a national crisis on a scale they had not experienced since the Second World War.

Uneven levels of preparedness, despite repeated warnings from global health officials that dated back to the early years of this century, would suddenly demand governments act in ways for which their populations had not yet been prepared.

By the time the scale of the pandemic had been recognised by scientists and politicians, governments could be excused for having resorted to short term reactions expressed through crisis communications.

The latter, however necessary, live in constant tension with long term communications.

The aim, after all in Strategic Communications, is to ensure consistency and coherence between the demands of today and the ambitions of tomorrow.

How did the NB8 fare? The answer is not simple, especially when faced with the conundrum brought about by the Covid-19 pandemic.

From the outset, it was clear that the pandemic was as much political, economic, and social in its effect as it was bio-medical in its nature.

Governments across the world have since faced hard choices in balancing these threats against the well-being of their citizens while retaining friendly relations and long-term objectives in international politics.

The Nordic governments started from a strong position. The Nordic countries (Denmark, Finland, Iceland, Norway, Sweden) make up the world'seleventh largest economy.

Their populations show high levels of trust in government structures and law enforcement, and demonstrate a high degree of confidence in their partner states.

The same cannot be said of the Baltic countries. By comparison, trust in government is low and their economies are less prosperous.

Consequently, the Nordic countries spend above the European average on healthcare, whereas the Baltic countries allocate significantly less.

This context would influence the decisions of governments and the subsequent debate.

The Baltic countries would find themselves trapped between trying to maintain their under-funded health systems throughout stricter lock-downs, while at the same time fearing for the consequences for their economies.

Disinformation in the Baltics

From the beginning of the pandemic, the Baltic countries were concerned with the potential spread of disinformation, particularly emanating from the Kremlin.

Although the concern with disinformation was apparent in all Nordic-Baltic countries, Estonia, Latvia and Lithuania were particularly wary.

Since the restoration of Baltic independence, the Kremlin has worked to shape public opinion and politics in the Baltic countries by driving wedges between ethnic groups, sowing distrust in media outlets and governments, and undermining NATO and the EU.

Historical experience and large Russian-speaking minorities who consume Russian language media make Baltic governments particularly cautious.

Understandably perhaps, since investigative reports show Russian government officials, media outlets, proxy news sites, and social media accounts to have engaged in coordinated campaigns to spread disinformation on Covid-19 and Western-manufactured vaccines.

At a meeting in June 2020, the Presidents of Latvia and Estonia discussed how to manage the pandemic and remarked that the levels of disinformation had increased significantly, posing a threat to their societies.

In a recent meeting between the Foreign Ministers of the Baltic countries and the UK, the lack of resilience shared by democratic societies against Covid-19 related disinformation was raised as a major concern.

It was proposed that transatlantic partners pursue joint solutions to the threat posed by disinformation operations.

Baltic countries have been strong advocates for EU-level regulation to fight disinformation.

At the same time, Latvia has initiated a resolution since adopted by the United Nations in March 2021 to fight the spread of disinformation and misinformation, particularly in the context of the continuing pandemic.

Faced with the Covid-19 crisis, populations around the world have become more vulnerable. They face fear at the level of the individual, and instability at the community level.

Fear hinders rational judgement, rendering society more susceptible to disinformation and talk of conspiracies.

As research shows, emotionally packaged stigmas – unjustified disapproval of something or someone shared by a group – exert a particularly strong effect on people.

Consequently, it was perhaps to be anticipated that Moscow would leverage the stigma it has been creating and attaching to NATO and its Enhanced Forward Presence in the Baltics.

The pandemic has provided a new storyline for the Russian government to discredit NATO and its forces.

To read more:
https://stratcomcoe.org/pdfjs/?file=/cuploads/pfiles/Nato-Covid19-Nordic-Baltic-d6933.pdf?zoom=page-fit

Number 10

Enabling Military Systems to Adapt to the Unexpected

Program aims to provide physical systems with ability to adapt to unexpected events in real-time and effectively communicate system changes to human and AI operators

Many complex, cyber-physical military systems are designed to last for decades but their expected functionality and capabilities will likely evolve over time, prompting a need for modifications and adaptation.

High Mobility Multipurpose Wheeled Vehicles (HMMWV), for example, had a design life of 15 years, but are now undergoing modernization to extend the average age of the fleet to 37+ years.

At design time, these systems are built to handle a range of expected operating environments and parameters.

Adapting them is currently done in an improvisational manner – often involving custom-tailored aftermarket remedies, which are not always commonly available, require a skilled technician to install, and can take months or even years to procure.

Further, as they evolve and are placed outside of their original design envelop these systems can fail unexpectedly or become unintentionally dangerous.

"Today, we start with exquisitely built control systems but then someone needs to add something or make a modification – all of which results in changes to the safe operating limits," said DARPA program manager John-Francis Mergen. "These changes are done in a way that wasn't anticipated – or more likely couldn't have been anticipated – by the original designers. Knowing that military systems will undoubtedly need to be altered, we need greater adaptability."

In response, DARPA developed the Learning Introspective Control (LINC) program. The program aims to develop machine learning (ML)-based introspection technologies that enable systems to adapt their control laws as they encounter uncertainty or unexpected events.

The program also seeks to develop technologies to communicate these changes to a human or AI operator while retaining operator confidence and ensuring continuity of operations.

"When a system 'wakes up' in a different space, it needs to be able to realize there are things it can't do anymore or new things it can, and 'learn' how to adapt to its new operating reality," noted Mergen. "With LINC, we want to provide physical systems with the ability to figure out what is still feasible, alert the operator, and then help them operate in that new space."

Developing LINC technologies will require addressing a specific set of challenges related to learning control and communicating situational awareness to the operator.

Current state of the art (SOTA) ML approaches are not robust to unknown or unstructured parameter uncertainty, owing largely to the bounds set on their operation at design time as well as their reliance on fixed assumptions about their operating model.

Further, complex systems – like drone swarms – are unable to rapidly converge on a common solution.

When damage occurs to a single drone, the swarm is unable to uniformly adapt, potentially resulting in a failed operator or unsafe operating conditions.

LINC's first research area will seek to overcome existing limitations in learning models and ML techniques that currently hamper system adaptation.

The program will explore how to provide a system with the ability to sense change and then reconstitute control using only onboard sensors and actuators.

LINC aims to develop new control regimes that detect and characterize changes in the system's operations in real-time, rapidly find solutions for reconstituting control under these changing conditions, and then calculate operating limits to identify a safe operating envelope.

"The idea is that you have a plethora of indigenous sensors on the system, and you can use these to determine and define a new set of control laws. With those new laws, you can then calibrate the system," said Mergen.

Another challenge area LINC seeks to address is around operator communications.

Today, operators are not often provided with sufficient explanations or guidance around a system's behavior or it's situation-specific operating limits.

Existing cues to operators about system dynamics don't always provide options, making it difficult for an operator to appropriately trust the information its receiving.

Further, interpreting current system diagnostics displays, which are not always intuitive, creates additional cognitive load for human operators.

This further erodes operator trust and can lead to misunderstanding, confusion, and incorrect actions.

A second research area will focus on improving how situational awareness and guidance are shared with the operator. This area will explore ways of translating and effectively communicating the operational information generated by the dynamic model developed under the first research area.

The resulting technologies must be able to provide the operator – whether human or AI – with updates on the operating status of the system as well as cues for safe actions. Further, they must be able to help retain operator trust by providing optionality and explainability around what's happening "under the hood."

A third research area will focus on testing and evaluating the resulting technologies. LINC expects to use demonstration platforms that will evolve in sophistication and complexity throughout the life of the program – starting with a realistic physical model and progressing to a military-relevant system in the program's final phase.

Interested proposers will have an opportunity to learn more about the Learning Introspective Control (LINC) program during a Proposers Day, which will be held on August 26, 2021, from 9:00 AM to 2:00 PM (ET) both at the DARPA Conference Center, located at 675 N. Randolph Street, Arlington, Virginia, 22203, and virtually through Zoom. Advance registration is required to attend. To learn more: https://sam.gov/opp/69db6bff225344f481f229edc1e2b97a/view

The LINC Broad Agency Announcement is forthcoming and will be published on the System for Award Management (SAM) website at https://beta.sam.gov/

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.

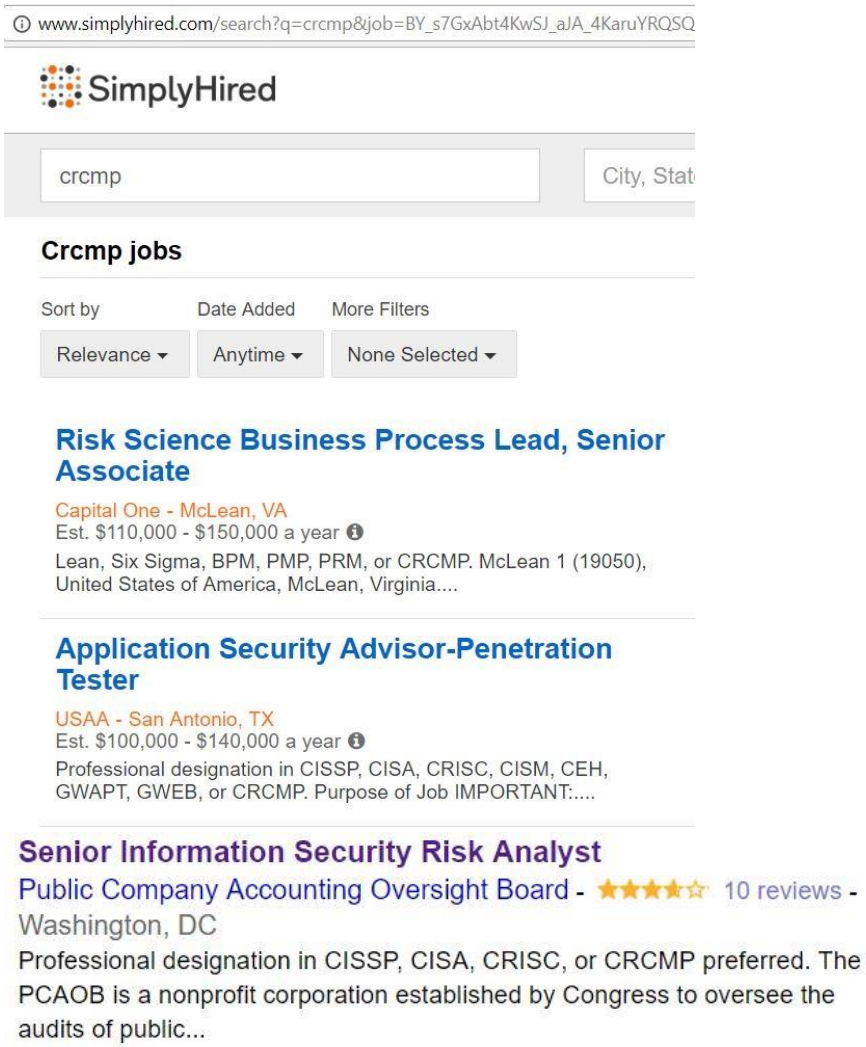
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

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

- 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.