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, March 13, 2023

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

I have been studying *all stress testing approaches, challenges and opportunities* at least since January 2009, when the Basel Committee on Banking Supervision released the Consultative Document "Principles for sound stress testing practices and supervision".

The European Systemic Risk Board (ESRB) has just released an excellent paper, the "Advancing macroprudential tools for cyber resilience", where we can read about the *Cyber resilience scenario testing (CyRST)*. This is "an analytical tool for testing the capacity of the financial system to swiftly respond to and recover from a severe but plausible cyber scenario that causes a significant disruption and could affect financial and operational stability."

The ability of the financial system to respond to and recover from such an event determines the extent to which it can support the continuity of key

economic functions in a severe cyber scenario. This is assessed by designing a hypothetical cyber scenario and asking participating firms to:

- document the scenario's impact,
- how they would respond to and recover from it, and
- the extent to which key economic functions could continue to operate under the scenario.

The test is used to evaluate the overall impact of the scenario *on financial and operational stability* and to identify areas where further work is required to mitigate risks.

CyRST can involve financial institutions, financial market infrastructures and other firms that support the operation of the financial system, including information and communications technology (ICT) third party service providers.

CyRST can complement other analytical tools. It should be viewed as one component of the overall framework for assessing system-wide cyber resilience.

In 2017, the Bank of England's Financial Policy Committee (FPC) set out its framework for building and maintaining *cyber resilience*.

Two of the elements of this framework involve setting clear baseline expectations for firms' resilience that reflect their importance for the financial system, and regular resilience testing by firms and supervisors.

Since then, the Bank of England has been working on the development of a new tool known as *"cyber stress testing"* which combines these two elements of the FPC's framework and focuses on the key cyber risks to the stability of the financial system.

The Bank of England is using its test to explore firms' capabilities and the potential impact on financial stability in a hypothetical scenario.

Following a successful pilot in 2019, the Bank of England carried out an exploratory cyber stress test in 2022 with several firms on a voluntary basis. The test had a data integrity incident as the disruption scenario and was intended to test firms' ability to meet the impact tolerance for payments in a severe but plausible scenario involving the retail payments system.

In June 2022, the Danish FSA announced the launch of its programme for strengthened operational resilience in the financial sector. The programme uses cyber stress testing to analyse the consequences of an extensive ICT

disruption. The programme builds, among other things, on the work of the Danish Financial Sector forum for Operational Resilience (FSOR), which is chaired by Danmarks Nationalbank.

The cyber stress test, in which systemic firms will be required to participate, is being led by a team of information and cybersecurity supervisors assisted by core banking and resolution supervisors.

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

Best regards,

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

Number 1 (Page 6)

Advancing macroprudential tools for cyber resilience

ESRB
European Systemic Risk Board
European System of Financial Supervision

Number 2 (Page 10)

BIS Quarterly Review, March 2023 (78 pages)

International banking and financial market developments

BIS

Number 3 (Page 12)

CISA Director Easterly Remarks at Carnegie Mellon University

Number 4 (Page 14)

Statement on the Annual Report 2022

Dr Joachim Nagel, President of the Deutsche Bundesbank, at the press conference presenting the Annual Report 2022, Frankfurt am Main

Number 5 (Page 17)

NBS Working paper 2/2023

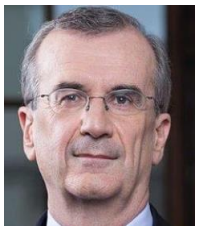
Impact of TLTRO III (Targeted Longer-Term Refinancing Operations) on bank lending: The Slovak experience

Juraj Falath, Alena Kiššová and Adriana Lojschová

NATIONAL BANK OF SLOVAKIA
EUROSYSTEM

Number 6 (Page 19)

Hearing of François Villeroy de Galhau, Governor of the Banque de France, before the Finance Committee and the European Affairs Committee of the National Assembly



Number 7 (Page 24)

NIST Internal Report, NIST IR 8432 ipd, 4 Initial Public Draft

Cybersecurity of Genomic Data

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Number 8 (Page 26)

Social Media Manipulation 2022/2023:

Assessing the Ability of Social Media Companies to Combat Platform Manipulation

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

Number 9 (Page 28)

Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA)

#StopRansomware: Royal Ransomware

JOINT CYBERSECURITY ADVISORY

Coauthored by:

Number 10 (Page 30)

How Digital Twins Could Protect Manufacturers From Cyberattacks

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

Number 1

Advancing macroprudential tools for cyber resilience

ESRB
European Systemic Risk Board
European System of Financial Supervision

The ESRB worked in 2022 within the context of a substantially heightened cyber threat environment across Europe.

The cyber activity resulting from Russia's invasion of Ukraine have affected both Ukraine and EU Member States directly and indirectly.

Furthermore, an increase in cyber attacks and the active sabotage of power and telecommunications infrastructure in EU Member States – which the financial sector relies on – present significant threats to financial stability.

The ESRB responded to this heightened cyber threat environment by:

1. Enhancing the exchange of information across jurisdictions and authorities.

2. Focusing on the tools and elements needed to advance cyber resilience and strengthen preparedness for potential cyber incidents.

3. Advancing a cyber resilience scenario testing (CyRST) approach: the ESRB completed further work on this approach, which could support authorities in:

(i) testing the response and recovery capacity of the financial system against severe but plausible scenarios involving a cyber incident,

(ii) evaluating their impact on financial and operational stability, and

(iii) identifying areas where further work is required to mitigate cyber risks.

4. Developing the concept for a systemic impact tolerance objective (SITO): the ESRB worked on developing SITOs, which can assist in identifying and measuring the impacts of cyber incidents on the financial system, and evaluating when they are likely to breach tolerance levels and cause significant disruption.

5. Reviewing current financial crisis management tools: the ESRB evaluated whether these tools are sufficient for adequately responding to system-wide cyber incidents.

The heightened cyber threat environment across Europe calls for a step change in enhancing system-wide cyber resilience.

The resistance and detection capabilities of individual entities constitute a first layer of defence against cyber incidents.

The Digital Operational Resilience Act (DORA) is part of an ongoing effort at the EU level to improve the cyber resilience of individual entities.

Threat-led penetration tests outlined by DORA, such as the European Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU), provide a way of testing this first layer of defence.

However, further layers of defence are needed to increase the resilience of the financial system as a whole against cyber incidents.

Against this background, the ESRB has three key areas of focus.

1. The ESRB encourages authorities to use the CyRST approach to pilot system-wide cyber resilience scenario testing as soon as possible.

Such pilots can complement other analytical tools that the authorities might be using and deepen their understanding of CyRST and of the risks to system-wide cyber resilience.

This is important and urgent, given the increased likelihood that a cyber attack will strike the European financial sector and because it will take time to pilot CyRST, identify the risks and implement appropriate mitigating measures.

The ESRB will continue to work in this area as a hub for sharing progress and good practice, and will update the conceptual approach based on what the authorities learn from their more detailed work in the pilots.

2. The ESRB advocates the use of SITOs and will continue to transition from a conceptual approach to a practical basis for implementing them.

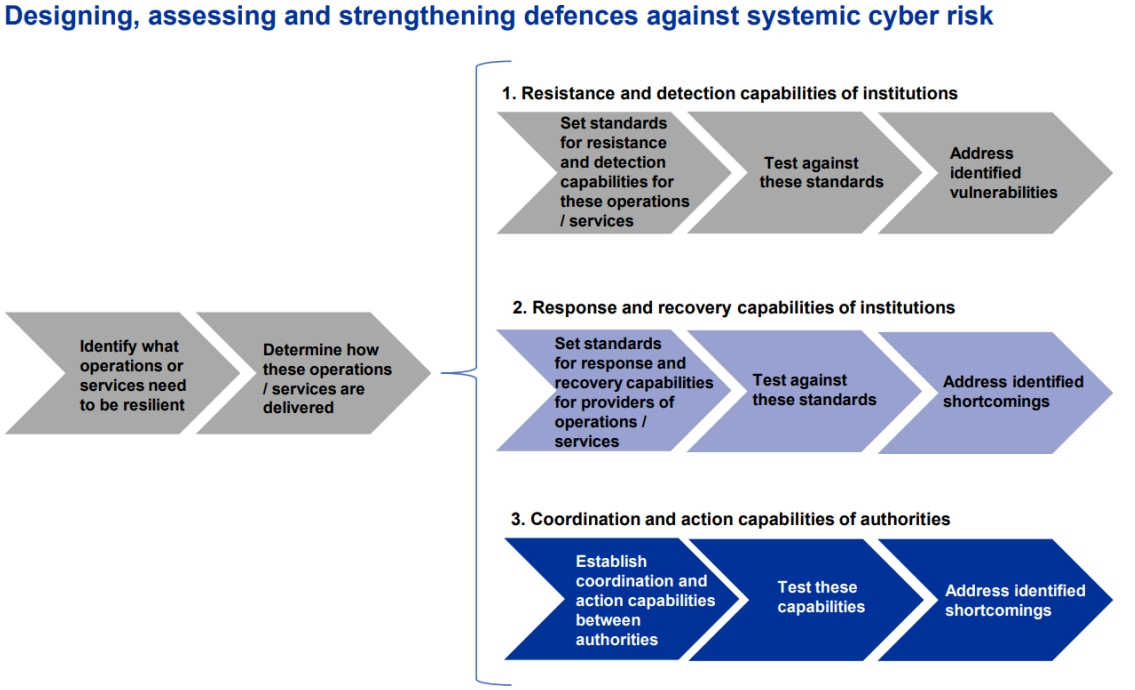
Specifically, the ESRB will identify a key economic function3 where disruptions have cross-border implications and define appropriate SITOs at EU level so as to ensure consistency across the region/sector and authorities.

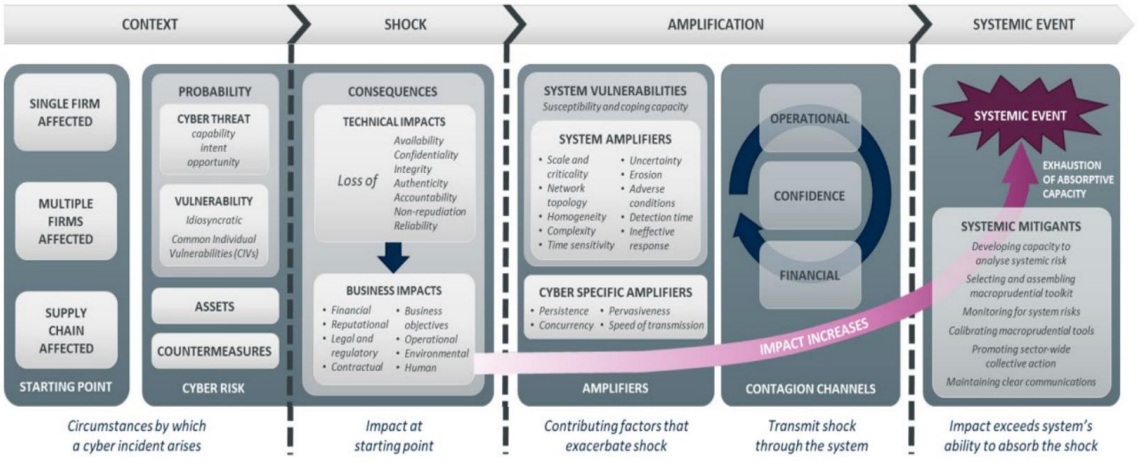
The ESRB will work with authorities across the EU to identify where a consistent approach is required and to decide on the approach for setting SITOs where there are crossborder implications.

The ESRB recognises that where disruptions have no or few cross-border implications, SITOs may differ across jurisdictions to reflect national specificities.

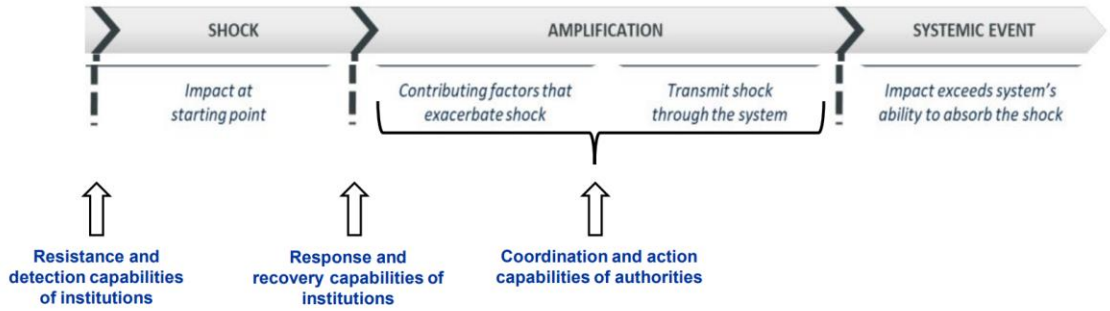
3. The ESRB will consider which operational policy tools are most effective in responding to a system-wide cyber incident and identify gaps across operational and financial policy tools.

This work will build on the analysis of financial crisis management tools described in this report.

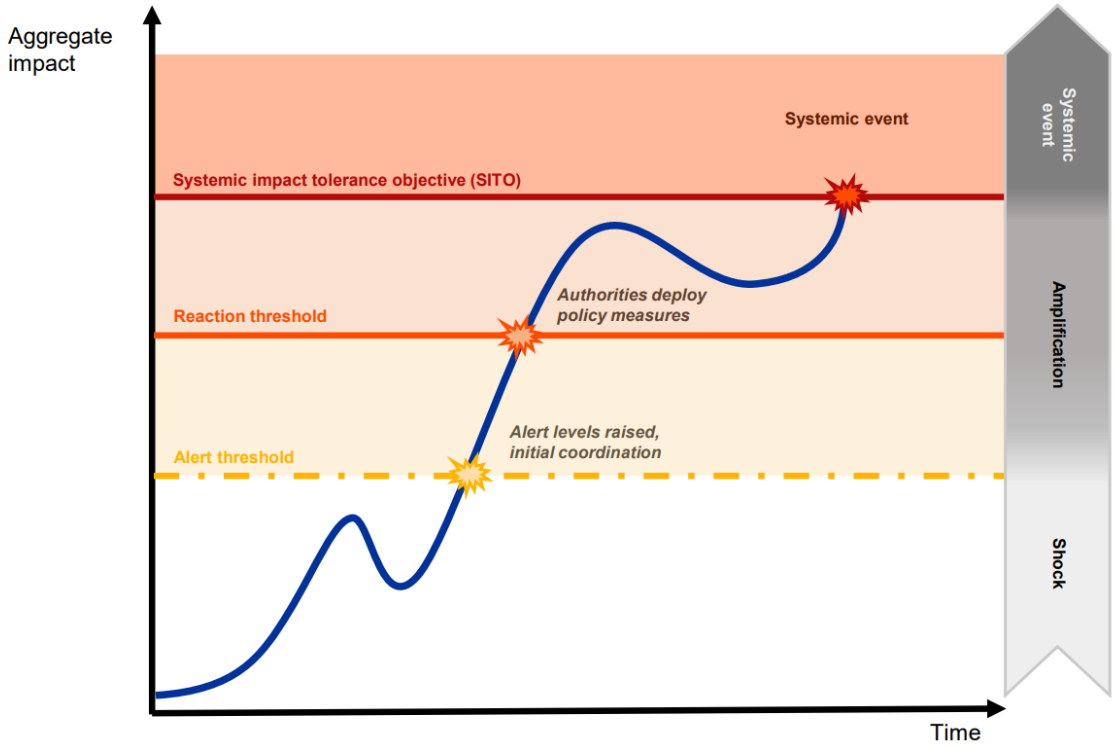




Stylised representation of the layers of defence



Cyber incident impact and tolerance for different impact levels



To read more:
https://www.esrb.europa.eu/pub/pdf/reports/esrb.macroprudentialtoolscyberresilience220214~984a5ab3a7.en.pdf?888a06fcb36d2c1ce41594efd67a4c88

Number 2

BIS Quarterly Review, March 2023 (78 pages)

International banking and financial market developments

BIS

Perceptions of risk and policy outlook drive markets

Financial markets extended previous gains during the review period. As inflation readings gradually fell and the pace of policy tightening slowed early in the period, financial conditions eased and risky asset valuations generally rose on the back of perceptions of declining risks.

Expectations of significant rate cuts in the near term appeared to firm up, despite cautious central bank communication about the policy outlook. The US dollar depreciated further, lending additional support to assets in emerging market economies (EMEs).

Towards the end of the period, however, market developments proved sensitive to news that challenged investors' sanguine attitude. Investors' expectations about future policy rate paths stood in contrast to central bank communications.

While several major central banks slowed the pace of monetary tightening, they remained cautious about the interest rate path going forward, particularly in view of the persistent strength of labour markets.

Nevertheless, interest rate futures continued to relay market participants' expectation that rate hikes will end this year, followed by steep rate cuts stretching well into 2024.

Conditions in government bond markets remained sensitive to perceptions of growth, inflation and the attendant policy response.

In Japan, tensions remained in fixed income markets, as investors reassessed the yield curve control (YCC) policy.

Broad-based and recurrent open market operations by the central bank smoothed market functioning and contained upward pressure on bond yields.

Risky assets registered gains and the US dollar depreciated through most of the review period, before news tempered markets' optimism about the policy outlook. Stock markets experienced bouts of selling pressure but registered positive returns, despite a still subdued earnings outlook.

The concurrent fall in forward-looking gauges of market volatility suggested that valuations were boosted by benign risk perceptions. In a similar vein, credit spreads narrowed further, on the heels of declines in perceived default risks, and corporate bond issuance showed signs of recovery in January.

US data releases in February steered investors towards anticipating stronger policy headwinds. This led to a slight dollar appreciation and some reversal of risky asset gains, halting their divergence from subdued bank lending in major advanced economies (AEs).

Financial conditions eased moderately in EMEs, largely mirroring those in AEs. Bond yields fell, amid an upbeat backdrop of resilient growth and falling inflation. Equity markets saw wider fluctuations, swayed by the gyrations of the US dollar.

The abrupt end to the zero-Covid policy in China reinvigorated its equity market and contributed to the strong performance of risky assets in economies with close links to China. Yet it failed to turn around the lethargic portfolio flows to the country, while such flows did stabilise or even rebounded for most other EMEs.

Key takeaways

- Perceptions of the future path of monetary policy shaped markets as central banks continued their fight against inflation.
- A benign assessment of the risk landscape supported risky asset valuations, notwithstanding subdued earnings forecasts.
- EME asset performance was generally strong but was also sensitive to AE financial conditions and to the ebb and flow of the US dollar.

To read more:
https://www.bis.org/publ/qtrpdf/r_qt2303.pdf

Number 3

CISA Director Easterly Remarks at Carnegie Mellon University

Good morning. Thank you to President Jahanian for that warm introduction and to everyone for joining me today on this Monday morning. It's wonderful to start the week off with this incredible community.

I can't think of a more fitting location for this discussion than Pittsburgh, a city built on innovation, imagination, and technological transformation; and Carnegie Mellon University, one of the world's most renowned educational institutions, home to one of our nation's top undergraduate computer science programs and top engineering programs, but also, to so much more. Let me share a few of my own favorites:

- The first smile in an email was created by research Professor Scott Fahlman, which launched the emoticon craze

- CAPTCHAs—or completely automated public Turing tests to tell computers and humans apart— (how many of you knew what that stood for?) were developed here by Professor Luis von Ahn and his colleagues, used to help prevent cybercrime

- Wireless research conducted at CMU laid the foundation for now ubiquitous wi-fi

- CMU is home to the nation's first robotics lab; and of course, home to the Software Engineering Institute, the first Federal Lab dedicated to software engineering. SEI established the first Computer Emergency Response Team, or CERT, in response to the Morris worm—that became the model for CERTs around the globe, and of course was a key partner in the creation of US-CERT in 2003, the precursor to CISA's Cybersecurity Division.

But the partnership between CMU and CISA goes well beyond technical capability – to what I consider the most important aspect of technology – People.

The CISA team is full of amazing CMU alumni like Karen Miller who leads our vulnerability evaluation work and Dr. Jono Spring, who is on the front lines of our vulnerability management work – both are here with me today.

Finally, I wanted to come here because CISA and CMU share a common set of values—collaboration, innovation, inclusion, empathy, impact, and service. And of course, a shared passion for our work.

So, now that you know why I am here, I want to start with a story.

At 2:39 pm on a chilly but sunny Saturday, just six miles off the coast of South Carolina, an F-22 fighter jet from Langley Air Force Base fired a Sidewinder air-to-air missile to take down a balloon—the size of three school buses—that had drifted across the United States.

The deliberate action came after a tense public standoff with Beijing and intense media scrutiny about the Chinese "spy balloon."

The response and surrounding attention to the issue, reinforced for me a major challenge we face in the field of cybersecurity—raising national attention to issues much less visible but in many ways far more dangerous.

Our country is subject to cyber intrusions every day from the Chinese government, but these intrusions rarely make it into national news.

Yet these intrusions can do real damage to our nation—leading to theft of our intellectual property and personal information; and even more nefariously: establishing a foothold for disrupting or destroying the cyber and physical infrastructure that Americans rely upon every hour of every day—for our power, our water, our transportation, our communication, our healthcare, and so much more.

China's massive and sophisticated hacking program is larger than that of every other major nation – combined. This is hacking on an enormous scale, but unlike the spy balloon, which was identified and dealt with, these threats more often than not go unidentified and undeterred.

The Speech:
https://www.cisa.gov/cisa-director-easterly-remarks-carnegie-mellon-university

Watch the Speech:
https://www.kaltura.com/index.php/extwidget/preview/partner_id/2612992/uiconf_id/49325582/entry_id/1_s80j6080/embed/dynamic

Number 4

Statement on the Annual Report 2022

Dr Joachim Nagel, President of the Deutsche Bundesbank, at the press conference presenting the Annual Report 2022, Frankfurt am Main

1 Words of welcome

Ladies and gentlemen, I would like to welcome you to the presentation of the Bundesbank's Annual Report 2022. I would also like to extend a warm welcome to those of you attending our livestream.

After a three-year break, our balance sheet press conference is now a fully in-person event once again. It is being held for the first time at the Bundesbank's Regional Office in Hesse. This is because we have cleared out our main building on Wilhelm-EpsteinStrasse so that, after 50 years of use, it can be refurbished and modernised from top to bottom.

The lineup greeting you today is likewise a first. Ms Ingrid Herden has been head of Directorate General Communications since October 2022. And Mr Joachim Wuermeling of our Executive Board assumed responsibility for Directorate General Controlling, Accounting and Organisation at the start of this year.

Later on, he will present and discuss details of our annual accounts. However, I would like to begin by taking a look at economic and price developments as well as monetary policy decisions.

2 Looking back, looking ahead

2.1 Economic developments

Ladies and gentlemen, For one year now, Russia's terrible war of aggression against Ukraine has been raging. The extent of devastation and destruction, as well as the human suffering, are unspeakable.

The war and its side effects have left a mark on economic developments as well, especially due to the energy crisis they have triggered.

For example, Germany's recovery from the COVID-19 pandemic was throttled to a considerable extent.

A reminder: at the beginning of 2022, the Federal Government had been expecting the German economy to grow at an annual rate of 3.6%. Actual real growth then clocked in at 1.9% (after calendar adjustment). So thus roughly half the figure expected at the beginning of the year, but considerably better than had been feared at times.

It was not only the energy crisis and the strong price increases they triggered that weighed on the German economy.

Supply bottlenecks, too, continued to apply pressure. At times, they were exacerbated by the Ukraine war.

The business climate and consumer sentiment deteriorated massively. Uncertainty began to spread: owing to surging consumer prices, for one thing, and to energy supply, for another.

But private consumption still increased. This was thanks, first and foremost, to the catchup effects following the lifting of coronavirus restrictions. This easing boosted activity in consumer-related services sectors, in particular.

Exports and investment in machinery and equipment likewise supported economic growth over the past year.

On the other hand, construction activity contracted as a result of higher financing costs, reduced household purchasing power and high construction prices.

Economic output exceeded its pre-pandemic levels for the first time in the summer. Towards the end of the year, however, the positive effects from the lifting of the coronavirus mitigation measures tailed off. In addition, the global economy slowed down further.

This put a damper on export demand. And, in particular, uncertainty surrounding energy supply and its costs weighed heavily on enterprises and households. The situation in the energy markets eased over the course of this winter half-year.

On top of that, the feared gas shortage was successfully averted thanks to efforts to save energy as well as to mild temperatures.

Nevertheless, economic output in the final quarter of 2022 was still down by 0.4% on the quarter.

German economic output is likely to contract in the first quarter of 2023, too. Although there could be a gradual pick-up in the second quarter, there is still no sign of any major improvement for now.

As before, our experts are not expecting there to be a visible economic recovery until the second half of the year.

From today's vantage point, gross domestic product is likely to decline slightly for the full year, which would be less of a drop than projected in December, however.

To read more:
https://www.bundesbank.de/en/service/media-library/videos/statement-by-joachim-nagel-on-the-annual-report-2022-905822

Number 5

NBS Working paper 2/2023

Impact of TLTRO III (Targeted Longer-Term Refinancing Operations) on bank lending: The Slovak experience

Juraj Falath, Alena Kiššová and Adriana Lojschová

Abstract

We investigate the impact of the TLTRO III operations introduced by the European Central Bank in 2020 on the bank lending activity of Slovak banks, using unique bank-level data on the program.

We deploy a difference-in-difference approach on monthly data covering the time period from January 2012 to December 2021 with 34 banks included in the analysis.

Our findings suggest that the credit easing measures had a positive effect on bank lending to non-financial corporations and negative effect on lending rates, even when controlling for possible confounding factors.

We also explore other possible uses of TLTRO III liquidity by banks besides increased lending.

Although inconclusive, there is some evidence of banks improving their profitability via holding cheap liquidity in their deposit accounts and to a lesser extent via increasing their holdings of debt securities.

Introduction

Central banks have taken several swift and powerful steps to keep the economy afloat during the COVID-19 crisis. In the euro-area, the European Central Bank (ECB) has put in place a set of monetary policy and banking supervision measures to mitigate the impact of the coronavirus pandemic on the euro area economy.

Since March 2020 the Eurosystem has provided long-term loans to banks at very favourable rates, on the condition that banks lend this money on to people and businesses (targeted longer-term refinancing operations – TLTROs). Under this program, banks could borrow at a rate as low as -1% and for the first time in its history the Eurosystem lent at a rate lower than the remuneration of banks' reserves.

In this paper, we study whether Slovak banks used the liquidity obtained from TLTRO III operations to increase lending volumes and/or decrease lending rates, using difference-indifference methodology.

For this purpose we construct a unique bank-level dataset with monthly frequency covering the time period from January 2012 to December 2021.

We also explore other possible uses of TLTRO III liquidity by banks besides increased lending, for example earning profit by investing it into higher-yielding assets (carry trade), substituting other market funding sources or helping fulfil some regulation requirements.

Answering the question whether common monetary policy can operate effectively through unconventional targeted instruments supporting lending to the economy in a small open economy dominated by foreign-owned bank finance is important for two reasons.

First, it is an issue of monetary policy design. If viewed from the perspective of the ECB, it is important to understand if monetary policy decisions transmit in a similar way in all of its juristictions.

Second, it is also an aspect of monetary policy regime choice from the perspective of the small open economy involved.

Our paper has two main findings.

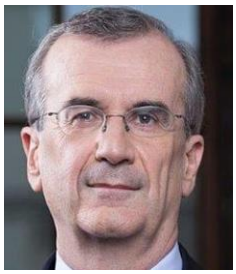
First, we find evidence for an unambiguously positive effect of TLTRO III uptake on loan supply. Slovak banks that participated in the operations boosted their total lending by roughly 17% on average in comparison with control banks during the time of the TLTRO. We also find positive and economically sizable impact on volumes for sectoral lending.

Second, we estimate that the banks which participated in the TLTRO III operations decreased their lending rates for non-financial corporations (NFCs) by around 0.6% relative to other banks.

To read more:
https://nbs.sk/dokument/b6528586-2679-4245-a850-cca84c5a9ca6/stiahnut/?force=false

Number 6

Hearing of François Villeroy de Galhau, Governor of the Banque de France, before the Finance Committee and the European Affairs Committee of the National Assembly



Mr President, Madam President, Mr Rapporteur-General, ladies and gentlemen,

I would like to thank you for welcoming me this afternoon, virtually and exceptionally, before the two Committees. The Banque de France regularly "reports" to you, the elected representatives of the Nation, but this task is even more essential during this unprecedented crisis.

I will begin with a few words on the economic situation; I will then address the strong mobilisation of the Banque de France and the ECB during the crisis, before outlining the conditions for economic recovery.

I. The economic situation during the lockdown

As regards the economic effects of the lockdown, we are converging towards a loss of activity of about one third. The figure for the first quarter published by INSEE last Thursday confirms this order of magnitude, in line with the -6% we had forecast as early as 8 April: -5.8% of GDP over three months corresponding to -32% over a fortnight in March.

These effects will be mechanically more pronounced in the second quarter because they will be longer-lasting. We will estimate them for April in our next monthly business survey to be published on 12 May. However, it is still too early for us to forecast the recession in 2020 and the expected rebound in 2021.

A word on the first comparison with other European economies, which should be taken with much caution: all have slowed significantly, but France more so than Germany; even Spain and Italy have seen their construction sector less affected than in France, and recourse to short-time work appears to be much stronger in our country, with the most generous compensation package.

There may be several useful lessons to be learned for exiting the lockdown; it is essential for our economic health that France now returns to work at full capacity, while of course ensuring the protection of all employees.

II. The mobilisation of the Banque de France and the ECB during the crisis

During this crisis, the Banque de France immediately focused its activities on five key fronts:

(i) supporting households in difficulty as well as VSEs and SMEs through the Bank's network across France – I would like to stress the essential role played by Credit Mediation, under the aegis of the Banque de France, in each département – the number of daily requests for mediation has reached 200, the vast majority of which are from VSEs: in one week, this figure is higher than in the whole of last year, but it is less than 1.5% of the requests for State-guaranteed loans;

(ii) responding to needs for cash – we have not experienced any supply problems;

(iii) economic analysis and monetary policy; (iv) careful monitoring of the markets;

(v) and supervision of the financial soundness of banks and insurance companies via the ACPR.

We are also on the front line of the European response, that of the ECB Governing Council. It was rapid – within six days, as early as 12 and 18 March – and massive – in terms of potential liquidity for businesses and governments.

And, so far, it has been effective in financing the sharp increase in corporate loans (+7.5% in one year in France at end-March) and stabilising their cost. But, as we just said last Thursday, we will be as flexible as required – in particular to avoid the fragmentation of the euro area, with unjustified interest rate increases in some countries; and we will be as innovative as necessary regarding instruments.

Our Governing Council took note yesterday of the judgement by the German Federal Constitutional Court in Karlsruhe: as the Court of Justice of the European Union (CJEU) has said, our past actions are indeed proportionate to our mandate, and our determination for the future to deliver on that mandate is total.

Allow me to express a broader consideration, at a time when some voices are being raised in various quarters to call into question the independence of the central bank and its mandate focused on price stability. Criticising these two pillars seems to me not only unnecessary, but also dangerous.

Unnecessary because the ECB has demonstrated its ability to innovate and to act swiftly while remaining within its mandate. But it is also dangerous because these two pillars, which are enshrined in the democratically voted Treaty, are the legal basis for our action.

Even more so, they are the basis for Europeans' confidence in their currency. We cannot cancel the public debts we hold today, neither legally, nor from a "fiduciary" point of view: a suspicion of fiscal dominance would cause mistrust in the currency. Independence and price stability do in no way stand in the way of powerful action by the ECB, on the contrary.

Our definition of price stability is an inflation rate below but close to 2% over the medium term, and this target is a symmetric target, not a ceiling. In comparison, inflation is currently low: it stands at 0.4% in the euro area and 0.5% in France; our estimate is that it should remain below 1% overall, contrary to the fears of our fellow citizens, who have seen a temporary rise in food prices.

The current shock is disinflationary, with low oil prices and, more broadly, demand that is likely to recover more slowly than supply. And so, in the very name of our mandate, we will be able to go further, and we will most likely have to go further, and thus support the recovery through low interest rates and abundant liquidity for a long time.

III. The conditions for a recovery: a "triangle of reassurances"

Initial hopes were for a rapid "V-shaped" recovery. It is clear today that it will take time, and that, beyond the Act 1 emergency phase, patient and selective measures will be needed to guide the recovery.

Getting back onto a better economic footing will require what I call a "triangle of reassurances": household confidence, the solvency of businesses and the sustainability of public debt.

1/ Unfortunately, some households have been made more vulnerable by the crisis, and it is crucial that they be helped through solidarity. But on the whole, household consumption will have fallen to a much greater extent than household income during this lockdown, leading to a significant build-up of "forced savings" – at least EUR 15 billion in March, and probably EUR 60 billion by the end of May.

Going forward, these reserves will need to be converted rapidly into spending and hence growth. To ensure economic confidence, it will be preferable in the short-term to avoid the recessionary impact of higher household taxes.

More than purchasing power, therefore, the priority regarding households is their confidence. If a tax measure for all households were to be envisaged, it would be better to focus on temporary and targeted incentives to encourage households to consume their savings.

2/ For businesses and the self-employed, the exit from lockdown will potentially prove risky. Despite major liquidity support, the irrecoverable losses in revenue will have damaged their solvency. Their overall debt has already increased sharply, by 2% or EUR 32 billion in March alone.

Support for businesses will therefore need to be redirected in part from the loans seen in Act 1 towards quasi-equity. But to avoid any windfall effects or ruinous failures, the scheme will have to be both efficient and selective. Act 1 was broadspread; the next acts will need to set priorities. Another idea would be to allow companies to offset their 2020 losses immediately against their corporation tax for 2019 and previous years.

Those sectors subject to a long-term shutdown will have to be provided with ad-hoc support. Among other measures, the Ministry of the Economy has proposed injecting public capital into listed companies, provided they are viable. For SMEs, however, a system of crowdlending will be more appropriate.

One interesting suggestion from several economists is that we should set up a temporary European business recapitalisation fund, which could be linked to the EIB. This would have the dual advantage of (i) levelling the playing field between countries, by ensuring that those least in debt today do not provide more help to their own national companies; and (ii) potentially bringing Northern and Southern Europe into agreement, so that we can end the somewhat sterile debate over loans and subsidies.

3/ The cushioning mechanism put in place by the government is playing a massive role, which is good news: it is absorbing around 60% of the current shock, with the balance mainly being absorbed by companies and, to a more marginal extent – around 5% – by employees.

The price of this mechanism is that public debt will have increased by at least 17 percentage points to 115% of GDP by end-2020. The post-lockdown period will therefore be a delicate balancing act for public finances, between fostering a rapid recovery and ensuring long-term sustainability.

Supporting the recovery could mean dealing with the debt inherited from the crisis separately, by partially "ring-fencing" it – the only advantage of which would be to push back its repayment further into the future.

Conversely, for future debt associated with the financing of the recovery, the idea of pooling it with more financially sound countries was what inspired the post-war Marshall Plan. The French proposal for a common European fund to finance new investment programmes, for the climate for example, would be the best way of showing European solidarity.

But there is no magic bullet: in the long run, this debt will need to be financed through growth and through our work – which is why a balance needs to be found in fiscal policy. It is up to the government and parliament to make the necessary adjustments, but I would just like to raise two points:

In the short run, it is normal – and even desirable – to have a high deficit, in order to counter the recession. But we need to prioritise spending that is temporary, and even reversible debt – such as investment in firms' quasi-equity – and avoid permanent spending or tax cuts which would place an unjustified burden on the post-crisis period. Again in the short run, we will need to avoid tightening fiscal policy too soon into the recovery.

Conversely, in the medium term, once growth is firmly established, we will need to come back to a more selective fiscal policy, and to more efficient public spending. This is the structural challenge that France faces, while at the same time prioritising investment in the future, which means in education, professional training and a more qualified workforce.

In the four years from 2016 to 2019, we notched up some impressive collective successes in terms of employment; we will need to pick up where we left off. In this way, I hope we will be able to overcome this harsh challenge for our country.

Thank you for your attention and I am happy to answer any questions.

To read more:
https://www.banque-france.fr/en/intervention/hearing-francois-villeroy-de-galhau-governor-banque-de-france-finance-committee-and-european-affairs

Number 7

NIST Internal Report, NIST IR 8432 ipd, 4 Initial Public Draft
Cybersecurity of Genomic Data

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Genomic data has enabled the rapid growth of the U.S. bioeconomy and is valuable to the individual, industry, and government due to intrinsic properties that, in combination, make it different from other types of high-value data which possess only a subset of these properties.

The characteristics of genomic data compared to other high value datasets raises some correspondingly unique cybersecurity and privacy challenges that are inadequately addressed with current policies, guidance, and technical controls.

This report describes current practices in risk management, cybersecurity, and privacy management for protecting genomic data, as well as the associated challenges and concerns.

It identifies gaps in protection practices across the genomic data lifecycle and proposes solutions to address real-life use cases occurring at various stages of the genomic data lifecycle.

This report also is intended to provide areas for regulatory/policy enactment or further research.

Cybersecurity and Privacy Concerns

Cyber attacks targeted at genomic data include attacks against the confidentiality of the data, its integrity, and its availability.

Cyber attacks against the confidentiality of the data can threaten our economy through theft of the intellectual property owned by the U.S. biotechnology industry, allowing competitors to gain an unfair economic advantage by accessing U.S. held genomic data.

Attacks against the integrity of the data can disrupt biopharmaceutical output, agricultural food production, and bio-manufacturing activity.

Attacks against the availability of the data include encrypting for ransom, deletion of data, and disabling critical automated equipment used in research, development, and manufacturing.

The potential harms of cyber attacks on genomic data threaten our national security as well, including enabling the development of biological weapons and the surveillance, oppression, and extortion of our citizens, military, and intelligence personnel based on their genomic data.

Cyber attacks targeted at genomic data can also harm individuals by enabling blackmail, discrimination based on disease risk, and privacy loss from the revealing of hidden consanguinity or phenotypes including health, emotional stability, mental capacity, appearance, and physical abilities.

In addition to the privacy risks that can arise because of a cyber attack, privacy risks unrelated to cybersecurity can arise when processing genomic data. These risks can arise when there is insufficient predictability, manageability, and disassociability in the genomic data processing.

Insufficient predictability in data processing can result in privacy problems if individuals are surprised by what is happening with their genomic data.

Insufficient manageability in data processing can arise when the capabilities are not in place to allow for appropriately granular administration of genomic data, for example, individuals may need to be able to have some or all their genomic data deleted from a dataset.

Permitting access to raw genomic data, instead of using appropriate privacy-enhancing technologies to extract only the necessary insights (without revealing the raw data), introduces privacy risks from insufficient disassociability in data processing.

Each of these areas of privacy risks can disrupt the ability to realize the benefits of processing genomic data.

To read more:
https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8432.ipd.pdf

Number 8

Social Media Manipulation 2022/2023:

Assessing the Ability of Social Media Companies to Combat Platform Manipulation

In this report—the fourth version of our social media manipulation experiment—we show that social media companies remain unable to prevent commercial manipulators from undermining platform integrity.

Overall, no platform has improved compared to 2021 and, taken together, their ability to prevent manipulation has decreased.

Buying manipulation remains cheap. The percentage of accounts identified and removed by the platforms dropped. We demonstrate that the manipulation providers have circumvented sanctions imposed in response to Russia's full-scale invasion of Ukraine.

It remains easy to pay for manipulation services with both Visa and Apple Pay. The platforms' ability to combat manipulation by slowing the speed of delivery has declined.

Today, 89 per cent of purchased inauthentic behaviour is delivered within one day. The vast majority of the inauthentic engagement remained active across all social media platforms four weeks after purchasing.

Thus, the platforms' moderation decisions appear to be only minimally responsive to user notifications.

Social media manipulation services hence continue to outperform social media platforms. With the quality of transparency reporting unchanged, the gap between platform performance in countering inauthentic engagement and the quality of platform reporting is widening.

Platforms have found it expedient to focus less on preventing commercial manipulators from accessing the platform, and more on reducing the reach and impact of their posts.

However, our research shows that commercial accounts are exploiting flaws in platforms, and pose a structural threat to the integrity of platforms.

More data is required to assess whether the platforms' approach adequately mitigates the systemic risk posed by platform manipulators.

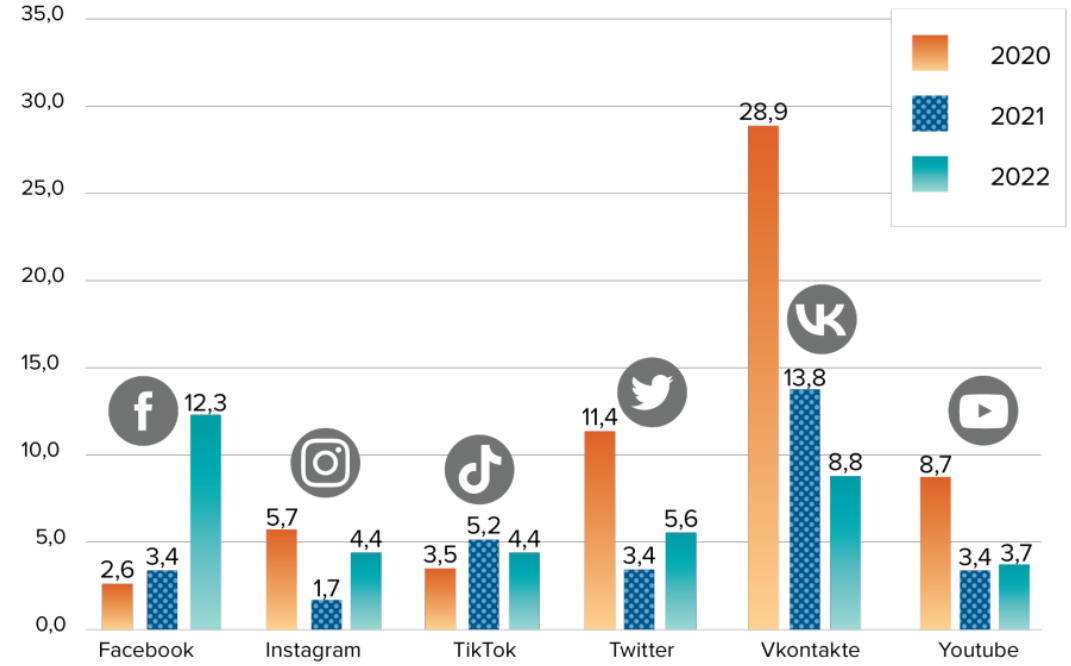


Figure 1: Cost (euro cents) of purchasing fake accounts by platform over time

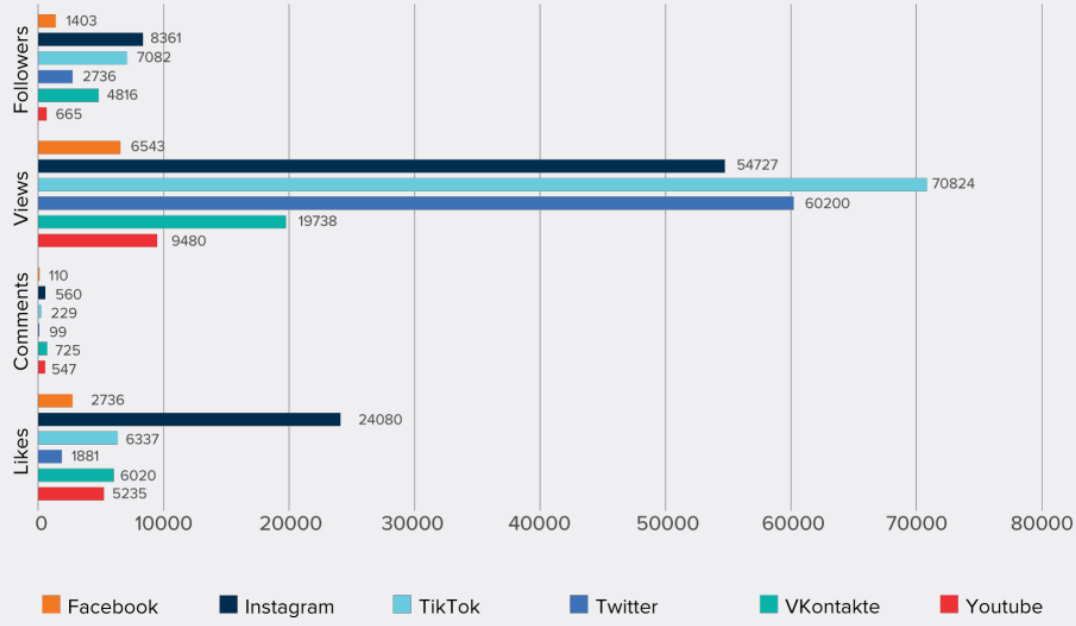


Figure 4. The amount of manipulation that can be bought for €10

To read more:
https://stratcomcoe.org/publications/social-media-manipulation-2022202323-assessing-the-ability-of-social-media-companies-to-combat-platform-manipulation/272

Number 9

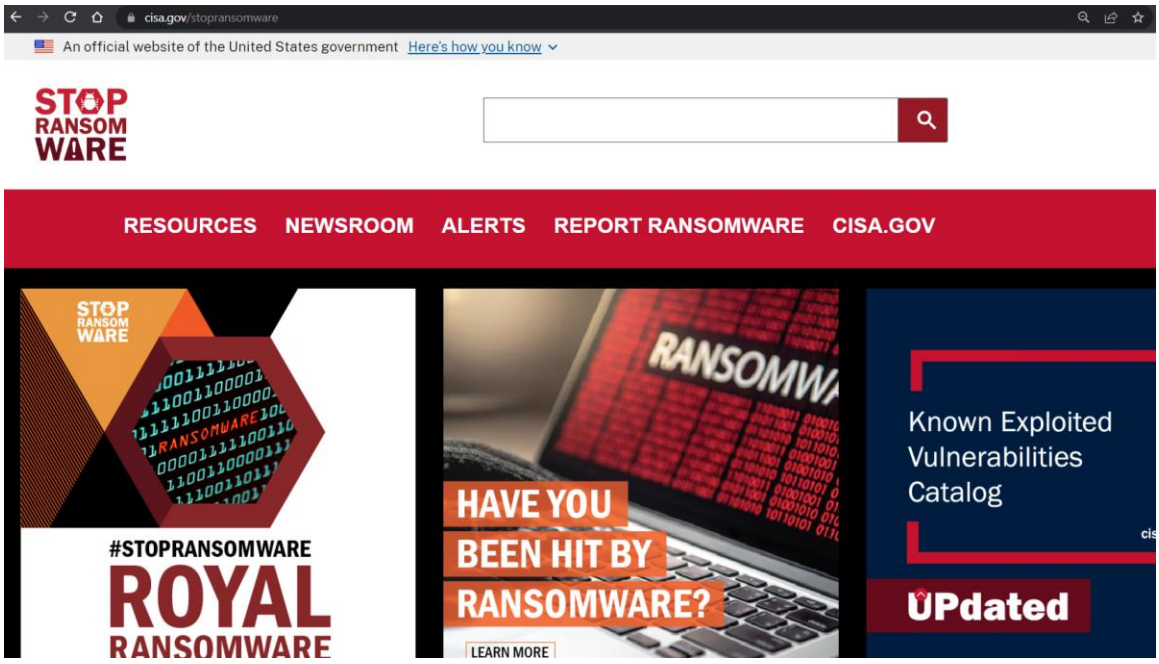
Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA)

#StopRansomware: Royal Ransomware

This joint Cybersecurity Advisory (CSA) is part of an ongoing effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors.

These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware.

Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.



The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint CSA to disseminate known Royal ransomware IOCs and TTPs identified through FBI threat response activities as recently as January 2023.

Since approximately September 2022, cyber criminals have compromised U.S. and international organizations with a Royal ransomware variant.

FBI and CISA believe this variant, which uses its own custom-made file encryption program, evolved from earlier iterations that used "Zeon" as a loader.

After gaining access to victims' networks, Royal actors disable antivirus software and exfiltrate large amounts of data before ultimately deploying the ransomware and encrypting the systems.

Royal actors have made ransom demands ranging from approximately $1 million to $11 million USD in Bitcoin.

In observed incidents, Royal actors do not include ransom amounts and payment instructions as part of the initial ransom note.

Instead, the note, which appears after encryption, requires victims to directly interact with the threat actor via a .onion URL (reachable through the Tor browser).

Royal actors have targeted numerous critical infrastructure sectors including, but not limited to, Manufacturing, Communications, Healthcare and Public Healthcare (HPH), and Education.

Initial Access

Royal actors gain initial access to victim networks in a number of ways including:

- **Phishing.** According to third-party reporting, Royal actors most commonly (in 66.7% of incidents) gain initial access to victim networks via successful phishing emails [T1566].
  - According to open-source reporting, victims have unknowingly installed malware that delivers Royal ransomware after receiving phishing emails containing malicious PDF documents [T1566.001], and malvertising [T1566.002].[2]
- **Remote Desktop Protocol (RDP).** The second most common vector Royal actors use (in 13.3% of incidents) for initial access is RDP compromise.
- **Public-facing applications.** FBI has also observed Royal actors gain initial access through exploiting public-facing applications [T1190].
- **Brokers.** Reports from trusted third-party sources indicate that Royal actors may leverage brokers to gain initial access and source traffic by harvesting virtual private network (VPN) credentials from stealer logs.

To read more:
https://www.cisa.gov/sites/default/files/2023-03/aa23-061a-stopransomware-royal-ransomware.pdf

Number 10

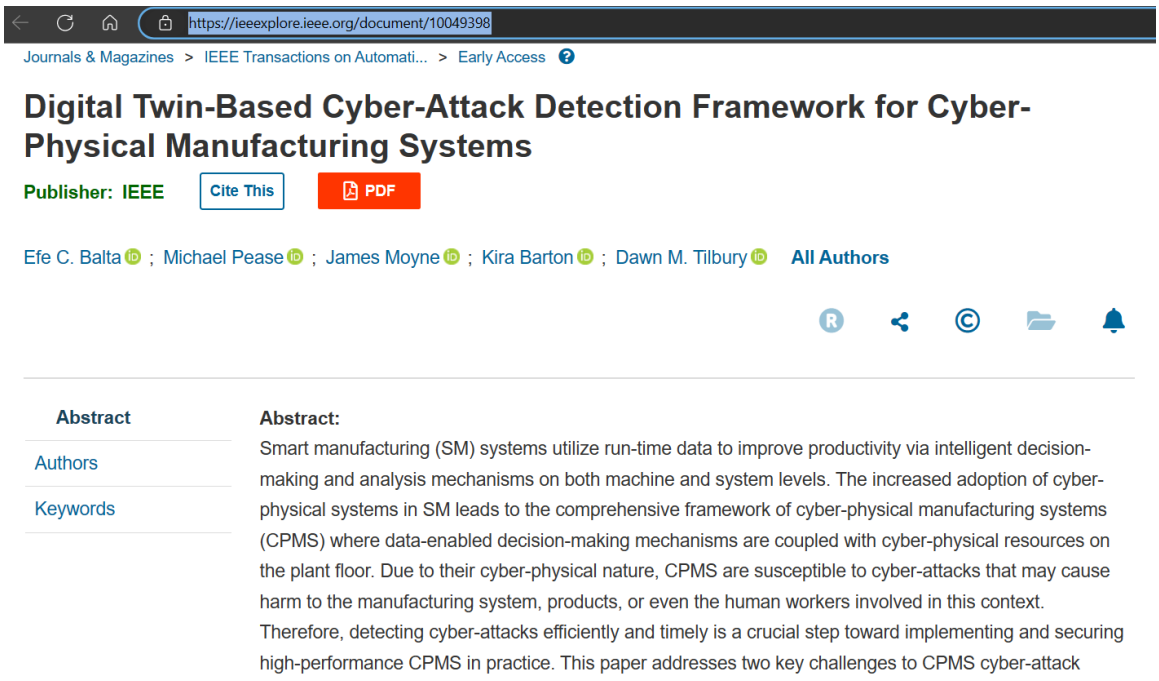
How Digital Twins Could Protect Manufacturers From Cyberattacks

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

Detailed virtual copies of physical objects, called digital twins, are opening doors for better products across automotive, health care, aerospace and other industries. According to a new study, cybersecurity may also fit neatly into the digital twin portfolio.

As more robots and other manufacturing equipment become remotely accessible, new entry points for malicious cyberattacks are created. To keep pace with the growing cyber threat, a team of researchers at the National Institute of Standards and Technology (NIST) and the University of Michigan devised a cybersecurity framework that brings digital twin technology together with machine learning and human expertise to flag indicators of cyberattacks.

In a paper published in IEEE Transactions on Automation Science and Engineering, the NIST and University of Michigan researchers demonstrated the feasibility of their strategy by detecting cyberattacks aimed at a 3D printer in their lab. They also note that the framework could be applied to a broad range of manufacturing technologies. You may visit: https://ieeexplore.ieee.org/document/10049398



Cyberattacks can be incredibly subtle and thus difficult to detect or differentiate from other, sometimes more routine, system anomalies.

Operational data describing what is occurring within machines — sensor data, error signals, digital commands being issued or executed, for instance — could support cyberattack detection. However, directly accessing this kind of data in near real time from operational technology (OT) devices, such as a 3D printer, could put the performance and safety of the process on the factory floor at risk.

“Typically, I have observed that manufacturing cybersecurity strategies rely on copies of network traffic that do not always help us see what is occurring inside a piece of machinery or process,” said NIST mechanical engineer Michael Pease, a co-author of the study. “As a result, some OT cybersecurity strategies seem analogous to observing the operations from the outside through a window; however, adversaries might have found a way onto the floor.”

Without looking under the hood of the hardware, cybersecurity professionals may be leaving room for malicious actors to operate undetected.

Taking a Look in the Digital Mirror

Digital twins aren’t your run-of-the-mill computer models. They are closely tied to their physical counterparts, from which they extract data and run alongside in near real time. So, when it’s not possible to inspect a physical machine while it’s in operation, its digital twin is the next best thing.

In recent years, digital twins of manufacturing machinery have armed engineers with an abundance of operational data, helping them accomplish a variety of feats (without impacting performance or safety), including predicting when parts will start to break down and require maintenance.

In addition to spotting routine indicators of wear and tear, digital twins could help find something more within manufacturing data, the authors of the study say.

“Because manufacturing processes produce such rich data sets — temperature, voltage, current — and they are so repetitive, there are opportunities to detect anomalies that stick out, including cyberattacks,” said Dawn Tilbury, a professor of mechanical engineering at the University of Michigan and study co-author.

To seize the opportunity presented by digital twins for tighter cybersecurity, the researchers developed a framework entailing a new strategy, which they tested out on an off-the-shelf 3D printer.

The team built a digital twin to emulate the 3D printing process and provided it with information from the real printer. As the printer built a part (a plastic hourglass in this case), computer programs monitored and analyzed continuous data streams including both measured temperatures from the physical printing head and the simulated temperatures being computed in real time by the digital twin.

The researchers launched waves of disturbances at the printer. Some were innocent anomalies, such as an external fan causing the printer to cool, but others, some of which caused the printer to incorrectly report its temperature readings, represented something more nefarious.

So, even with the wealth of information at hand, how did the team's computer programs distinguish a cyberattack from something more routine? The framework's answer is to use a process of elimination.

The programs analyzing both the real and digital printers were pattern-recognizing machine learning models trained on normal operating data, which is included in the paper, in bulk. In other words, the models were adept at recognizing what the printer looked like under normal conditions, also meaning they could tell when things were out of the ordinary.

If these models detected an irregularity, they passed the baton off to other computer models that checked whether the strange signals were consistent with anything in a library of known issues, such as the printer's fan cooling its printing head more than expected. Then the system categorized the irregularity as an expected anomaly or a potential cyber threat.

In the last step, a human expert is meant to interpret the system's finding and then make a decision.

"The framework provides tools to systematically formalize the subject matter expert's knowledge on anomaly detection. If the framework hasn't seen a certain anomaly before, a subject matter expert can analyze the collected data to provide further insights to be integrated into and improve the system," said lead-author Efe Balta, a former mechanical engineering graduate student at the University of Michigan and now a postdoctoral researcher at ETH Zurich.

Generally speaking, the expert would either confirm the cybersecurity system's suspicions or teach it a new anomaly to store in the database. And then as time goes on, the models in the system would theoretically learn more and more, and the human expert would need to teach them less and less.

In the case of the 3D printer, the team checked its cybersecurity system's work and found it was able to correctly sort the cyberattacks from normal anomalies by analyzing physical and emulated data.

But despite the promising showing, the researchers plan to study how the framework responds to more varied and aggressive attacks in the future, ensuring the strategy is reliable and scalable. Their next steps will likely also include applying the strategy to a fleet of printers at once, to see if the expanded coverage either hurts or helps their detection capabilities.

"With further research, this framework could potentially be a huge win-win for both maintenance as well as monitoring for indications of compromised OT systems," Pease said.

To read more:
https://www.nist.gov/news-events/news/2023/02/how-digital-twins-could-protect-manufacturers-cyberattacks

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

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

International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.

You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

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

3. *Training and Certification* – Become:

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

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

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

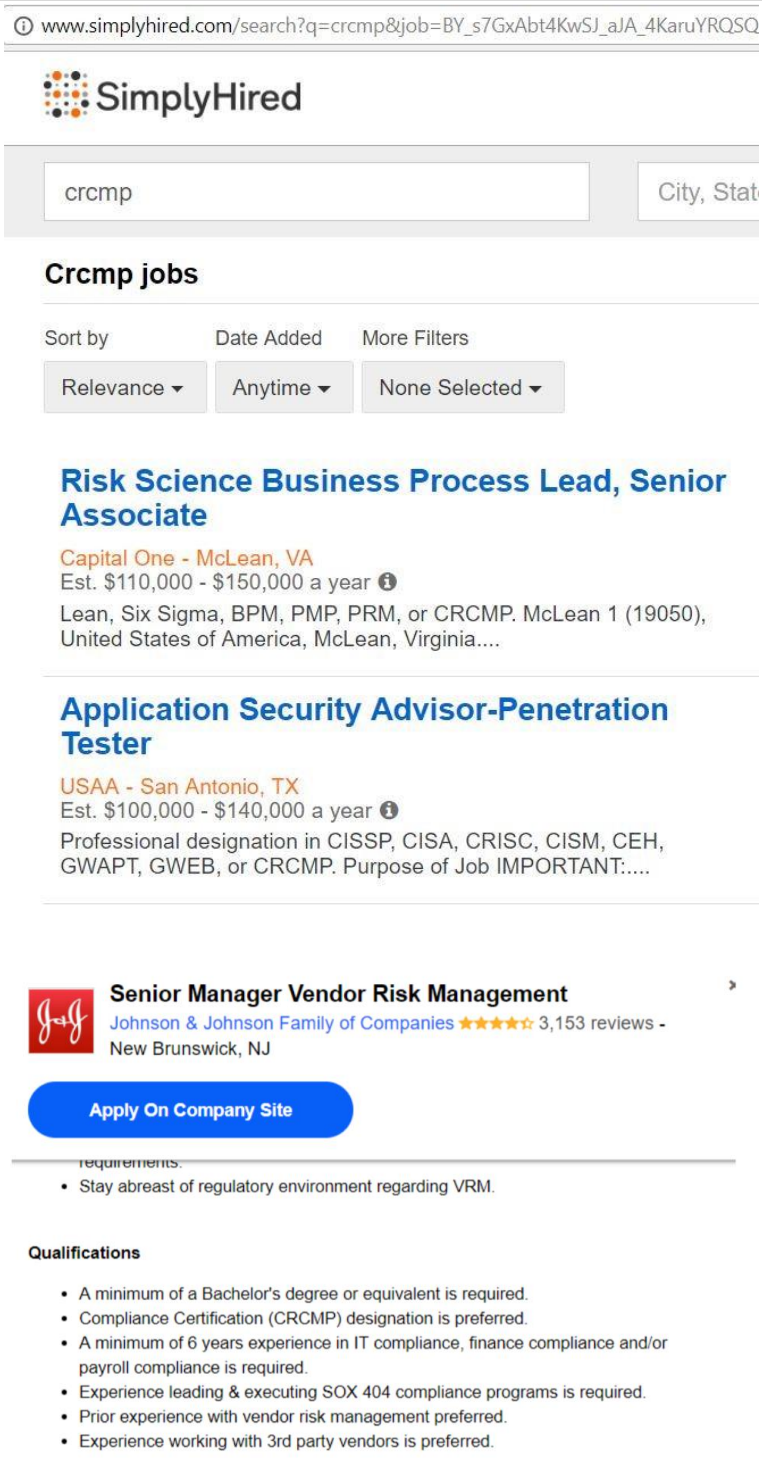
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- a Travel Security Trained Professional (TSecTPro).

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 32 countries.

Companies and organizations around the world consider the CRCMP a preferred certificate:

Senior Information Security Risk Analyst
Public Company Accounting Oversight Board - ★★★★☆ 10 reviews - Washington, DC
Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...



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

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

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

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

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

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

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

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

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