Monday, November 9, 2020

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,

Can you hide an espionage operation behind a *revenge porn* story?

Spies are always looking for executives and employees that have access to classified information, and they mainly use two methods to recruit them: Blackmail and bribery. It is not difficult to find compromising information for blackmail, especially when victims do not know they are the targets in an espionage operation.

Revenge porn is a form of sexual abuse that involves the distribution of sexually explicit photos and videos of individuals, without their consent. Ex-lovers and ex-partners from a relationship that seek revenge after the end of a relationship are often the perpetrators. They have the motive, the means, and the opportunity (MMO) to seek revenge, and nobody believes that something else could be behind that, like an espionage operation. Who would believe that spies have released nude photos and videos of a person, and not the ex-partner who owned the material, in an effort to blackmail or discredit the person?

There are perpetrators that use hacking techniques to obtain nude photos and videos from victims, and if this is not possible, they fabricate evidence (anything that an employer, a significant other or a third party might deem inappropriate or offensive).

Love and sex (real or fake) are major factors in the transformation of an employee or an executive that has access to confidential information into a traitor. There are many examples of:

- dedicated professionals, trapped in an unhappy marriage or relationship, who think they have found solace elsewhere.

- lonely professionals, caught in a classic honeytrap and coerced into compromising classified material to satisfy his blackmailers;

- vulnerable professionals, anxious to retain the affection of another person;

- professionals that did nothing wrong, but they cannot deal with the disclosure of even fabricated evidence. I know, this is very hard to believe, but spies can profile persons using the social media and can spot suitable vulnerable persons.

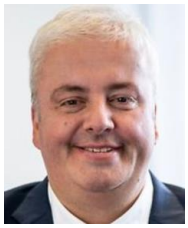
The Nazis institutionalized *sexspionage* by establishing the notorious Salon Kitty in Berlin, a brothel used to blackmail clients. Today in the online world, sexspionage has become so much easier.

Aldrich Ames (a former CIA officer that became a KGB agent, convicted of espionage in 1994), has said: *Espionage, for the most part, involves finding a person who knows something or has something that you can induce them secretly to give to you. That almost always involves a betrayal of trust.*

Welcome to the top 10 list, and always be careful and prepared.

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 6 (Page 25)

Bugs happen, so make sure you're ready to fix them

How a Vulnerability Disclosure Process ensured a bug in the NHS COVID-19 app was fixed quickly and responsibly

National Cyber Security Centre

Number 7 (Page 29)

Financial stability implications of the pandemic

Ignazio Visco, Governor of the Bank of Italy, at the 2nd Bank of Italy and Bocconi University - BAFFI CAREFIN Conference "Financial Stability and Regulation", Rome.

Number 8 (Page 35)

Modernizing and Strengthening CRA Regulations: A Conversation with the Housing Community

Governor Lael Brainard, U.S. Federal Reserve's Board of Governors, at the National Housing Conference National Advisory Council Meeting

Number 9 (Page 41)

Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace

Defendants' Malware Attacks Caused Nearly One Billion USD in Losses to Three Victims Alone; Also Sought to Disrupt the 2017 French Elections and the 2018 Winter Olympic Games

Number 10 (Page 47)

Episode 34: The Orbital Optician

Number 1

When the Nail Fails – Remarks before the National Society of Compliance Professionals

Commissioner Hester Peirce, U.S. Securities and Exchange Commission

It is a pleasure to be speaking to you for the second time, albeit virtually, at your national conference. I would like to thank Lisa Crossley, Holly Orefice, and Kristen Hinz for their work in coordinating the virtual transmission of the thoughts I have to share today.

Of course, I need to include the standard disclaimer: the views I express are my own and do not necessarily reflect those of the Commission or my fellow Commissioners.

Conferences and speeches certainly have changed in the time of COVID, as have the challenges you face as compliance officers. Two years ago, I spoke with you about the important function compliance personnel, including chief compliance officers ("CCOs"), serve in facilitating the work of the Commission.

Since then everything has gotten more complicated. I built that speech around the seasonal activity of trick-or-treating, something the county in which I live now has directed its residents to avoid. A frightening sign of the times.

Nobody could have anticipated such a fraught turn of events, and the difficult conditions now facing compliance professionals, whose compliance programs now often have to operate remotely, also were not foreseen. Compliance professionals, perhaps better than the rest of us, however, adapt to changing circumstances with impressive alacrity and skill.

In an increasingly complex regulatory environment, and with the additional complications caused by the COVID-19 pandemic, a good working relationship between compliance officers at regulated entities and our staff in the Commissions' Office of Compliance Inspections and Examinations (OCIE) is more important than ever.

Under the leadership of Pete Driscoll, OCIE has sought to deepen that relationship. Among other things, recognizing the unique difficulties of compliance during a pandemic in which everyone is being asked to function virtually, OCIE has provided relevant guidance. As new issues arise for which guidance would be useful, please note them for me and the OCIE staff.

Today, though, rather than focusing on compliance during COVID, I would like to focus on a concern that is not new—the question of how to define the parameters of personal liability for compliance officers.

Near the end of my remarks in 2018, I spoke briefly about the role that the Commission's Division of Enforcement plays with respect to compliance functions. I noted that I shared the concerns expressed in some quarters that the increasing specter of personal liability could cause talented individuals to forgo a career in compliance, among other negative effects.

Those concerns have increased over the past two years. Compliance officers' responsibilities are growing, but the nature of the liability they face in executing those responsibilities remains unclear. Indeed, this past February, the New York City Bar published a report that distilled many of the concerns, and offered a number of recommendations.

I hope that my remarks today can help to foster feedback from you and your compliance colleagues, which, in turn, can help me better perceive what useful formal guidance on the topic of individual compliance officer liability might look like.

I want to start with an equine hypothetical, one that I am sure that many of you have heard. It is an old proverb about a nail and a horseshoe—attributed sometimes to a particular person and sometimes to no person in particular, and taking one of a number of forms.

One form goes like this:

For want of a nail the shoe was lost.
For want of a shoe the horse was lost.
For want of a horse the rider was lost.
For want of a rider the message was lost.
For want of a message the battle was lost.
For want of a battle the kingdom was lost.
And all for the want of a horseshoe nail.

Typically, the proverb is used to illustrate that a seemingly inconsequential event can lead to grave consequences. A missing nail from a horseshoe

leads to a series of bad events and ultimately the downfall of an entire kingdom.

I would like to look at this story from a slightly different perspective: who is responsible when the nail fails? Suppose that the farrier trade is a heavily regulated industry, and the regulator comes calling to determine how the nail failure happened and who, precisely, was at fault.

(I know that some of you are thinking "For want of the kingdom, the kingdom's regulator was lost," but we will assume for purposes of this illustration that all that remains standing of the old kingdom is its regulatory bureaucracy.)

So the regulator, the Royal Farrier Commission, comes calling for a cause exam to investigate the wanting nail matter and to determine whether an enforcement action is warranted. What happened? Who is to blame for the missing nail? Why did it happen? Was the farrier whose job it was to secure the nail in place at fault? Did he perform his job badly? What if he did place the nail properly, but the nail was defective? What if the nail was not defective, but it was placed in the horse's hoof in a manner that did not conform to regulatory specifications?

These questions quite naturally lead to second-level questions: did the farrier's employer have adequate policies and procedures with respect to the proper way to place the nail in the shoe? Was there a supervisor regularly checking on the performance of the farrier and his colleagues in the field? Did the employer have compliance surveillance systems adequately designed to detect the use of defective nails and departures from regulatory specifications? Why didn't those systems identify, remediate, and report the nail failure? Were there any red flags? And, of course, where was the CCO? Why didn't the CCO prevent this failure from happening?

I hope that the Royal Farrier Commission, in my hypothetical, had provided more recent and formal guidance on the subject of CCO liability than the Commission has. With respect to the SEC, people still point back to a Keynote Address by the then-Director of the Division of Enforcement at your 2015 National Conference.

In that speech, the Enforcement Director identified three broad categories of cases where the Commission has charged chief compliance officers:

(1) cases where the compliance officer participated in the underlying misconduct unrelated to her compliance duties;

(2) cases where compliance officers obstructed or misled Commission staff; and,

(3) cases where, in the Enforcement Director's words, "the CCO has exhibited a wholesale failure to carry out his or her responsibility."

The first category should not be controversial. After all, serving in a compliance capacity is not a get-out-of-jail free card for clearly unlawful conduct.

If it were, lots of bad actors would want the compliance officer title to shield them from liability. So a compliance officer who, outside of her compliance functions, directly violates provisions of the securities laws is liable the same way anyone else would be.

For example, when a person knows that an investment adviser is misappropriating client funds, does nothing to stop it, and participates in a scheme to hide the theft, she is liable for that conduct no matter her compliance functions.

In cases such as these, compliance personnel are liable on the same terms and to the same extent as any other bad actor. In other words, if you knowingly and intentionally use defective nails or willfully misplace the nails, you are responsible for the thrown shoe, no matter your compliance function.

The second category of cases relates more directly to compliance functions. These cases typically involve facts where a compliance officer obstructs or misleads the Commission's staff.

In a recent example, a compliance officer created and backdated compliance memoranda. When she subsequently provided them to the Commission's examination staff, she described them as a contemporaneous memorialization of the events, an assertion she knew to be false.

I supported this case. The Commission's examination process is essential to its regulatory functions, and conduct that undermines the process must be addressed. In another recent case, a compliance officer similarly misled the Commission's examiners and enforcement staff by producing altered documents.

The alteration was material because it created the appearance that the compliance officer had timely performed certain reviews, when she had not. Again, I supported the case because it evidenced the sort of knowing and

intentional misconduct that materially undermines the examination process.

The third category of cases, the ones involving a wholesale failure of a compliance officer is the one that understandably generates the most controversy and is the most challenging area for me. Typically, in such cases, the Commission charges the compliance officer with aiding and abetting the company's violations, causing the company's violations, or both.

The distinctions between these charges matters a great deal. To establish that a compliance officer aided and abetted the company's violation, the Commission must show that the compliance officer engaged in reckless conduct.

This standard is not simply negligence on steroids; rather, the evidence must show that there was "a danger so obvious that the [compliance officer] must have been aware of the danger."

In contrast, to establish in an administrative cease and desist proceeding that a compliance officer was the cause of a company's violation, it is only necessary to show that the individual committed an "'an act or omission the person knew or should have known would contribute'" to the violation.

The phrase "should have known" is "classic negligence language," and the Commission and courts both have concluded that it sets a negligence standard for liability.

Thus, where a company has committed a violation that does not require scienter—such as failing to have sufficient policies and procedures—a compliance officer can be held to have caused the violation based on her own negligent conduct.

In my example, the Royal Farrier Commission might charge the CCO with causing the company's failure to have reasonably designed policies and procedures to check for defective nails, because the CCO did not put a rigorous enough nail-checking policy in place.

Rule 206(4)-7, the investment adviser compliance rule, exacerbates the problem. It supports negligence-based charges against an adviser's CCO, whom the rule makes "responsible for administering written policies and procedures" that must be "reasonably designed to prevent violation, by you and your supervised persons, of the Act and the rules that the Commission has adopted under the Act."

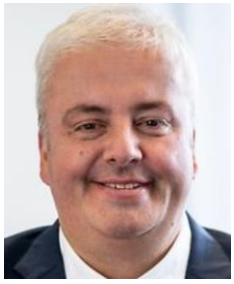
As former Commissioner Dan Gallagher pointed out, in practice, however, the rule's standard has looked more like strict liability.

To read more: https://www.sec.gov/news/speech/peirce-nscp-2020-10-19

Number 2

COVID-19 and cashless payments - has coronavirus changed Europeans' love of cash?

Burkhard Balz, Member of the Executive Board of the Deutsche Bundesbank, at the SME Europe, virtual event.



Ladies and gentlemen,

Thank you very much for inviting me to this conference, and for giving me the opportunity to talk about a very virulent topic: the consequences of COVID-19 for payments.

Do you remember the term "disruption"? If I remember rightly, that was one of the biggest buzz words five years ago, when blockchain, fintech and platformication were the talk of the town.

Disruptive elements are still at play, of course, but we only really saw the true meaning of disruption this year. The threat of the pandemic forced people worldwide to totally change their day-to-day habits.

Many pleasurable activities that people had taken for granted suddenly became impossible: travelling to exciting places all over Europe, going to nice restaurants, or meeting friends or family.

Public life as we knew it ground to a complete halt. This resulted in a dramatic economic downturn, with widespread insolvencies and unemployment cushioned, to a greater or lesser degree, by government support in many countries. This was truly "disruptive" in the worst possible sense of the word.

However, there is a famous saying: every cloud has a silver lining. And indeed, we have observed some "disruption" in the positive sense of the term.

The pandemic has facilitated and driven change. It has turned out to be a catalyst for digital transformation and thus an "innovation accelerator" for the economy.

Apart from getting used to face masks, for many people it was the first time they did their shopping online, the first time they had remote video conversations with colleagues, friends and family, and the first time they started to follow movie series via streaming services.

This quantum leap in digitalisation has also seen a boom in cashless payments. On the one hand, this was a consequence of the uptick in online shopping.

One indicator of this might be the rise in transactions which PayPal registered worldwide in the second quarter of 2020 compared with the first quarter: its transactions increased from about 3.26 billion to around 3.74 billion.

The general decline in shopping activities makes these figures even more impressive. On the other hand, the shift towards cashless payments had something to do with preventing transmission of the virus.

While handling banknotes and coins is not a likely cause of infection, the wish to avoid any contact was still reason enough for many retailers to start offering card payments more actively.

For many payers in Germany, it was the first time they realised that they already had not just a card in their wallet, but a card with contactless payment features.

Acceptance of these payment methods experienced a surge, as even the notoriously conservative German consumer became aware of the advantages this new and easy-to-handle payment instrument has to offer.

Recent figures from girocard - the German debit card system run by the banking sector - seem to confirm this change.

The number of girocard transactions in the first half of 2020 was 21% up on the first two quarters of 2019, climbing to 2.6 billion transactions. About 50% of all girocard transactions were contactless in the first two quarters of 2020, up from 25% in June 2019.

The question now is whether the habits acquired in times of disruption are here to stay.

I think they very well might be. Bundesbank online surveys of April and May 2020 found out that 73% of respondents who changed their payment behaviour during the pandemic said they would probably or even certainly stick to this new behaviour. COVID-19 was just a catalyst.

Because we had already seen in 2019 that cashless payments were becoming more popular and that the shift from cash to cards was stronger than in preceding years. But with a 73% share of transactions, cash is not on the way out, at least not in Germany.

Nevertheless, the changing shape of the payments and settlement landscape raises questions that go to the very heart of a central bank's core functions.

With the onset of COVID-19, talk about digital central bank currency (CBDC) seems to be that much out of scope in the eyes of the average consumer.

Technological advances such as distributed ledger technology (DLT), which opens up fresh opportunities e.g. in the Internet of Things, and also the initiatives pursued by other central banks and private companies to develop new means of payment, like Libra, have triggered debate on the future of payments.

In January 2020, the Governing Council of the ECB established a High-Level Task Force in order to advance joint work on CBDC. Being the Deutsche Bundesbank Executive Board member responsible for the area of payments, I am a member of this group. On 2 October, we published the first results of our analysis.

The main question to be asked is this: under what conditions might it become necessary to introduce CBDC for the general public, or a digital euro?

A structural decline in demand for cash, general support for digital transformation, and potentially competing other offerings of digital money from bigtech firms or other central banks are mentioned as possible motives for issuing a digital euro.

This brings me back to disruption. The debate on the digital euro has just started. My impression is that many stakeholders in the economy have only now begun to understand this thing called CBDC.

Banking sector players who run successful business models for cashless payments, especially, need to grasp what it means to issue a digital euro in the euro area.

Some challenges would need to be overcome in this regard, particularly concerning the potential impact on banking business, financial stability and the central bank balance sheet.

Whether we will issue a digital euro is something which has not yet been decided. I would like to mention the ongoing public consultation which is open until 12 January 2021.

The aim of this consultation is to find out the opinions of individuals, companies and other stakeholders on the digital euro, which we need to take on board when reaching a decision about an imminent "go", a "no-go" or a "go later".

Considering what COVID-19 has taught us about real disruption, I think there needs to be a response to the growing demand in the economy for cheap, quick and convenient means of payment which can also be used in new payment situations, like machine-to-machine payments.

The Bundesbank is deeply engaged in the debate on CBDC. But we are also thinking about alternative solutions, which could avoid disruption and help overcome the existing challenges, reap the benefits of going digital, and support new payment use cases without introducing CBDC.

One way could be to enhance conventional payment systems, both at a domestic and a global level. In this respect, we urge the market to develop a pan-European payment solution with full deployment of the new instant payments infrastructure.

In addition, we believe that the roadmap developed by the Financial Stability Board (FSB) provides an excellent plan to enhance cross-border payments.

In this respect, it also becomes clear that CBDC is not a panacea; the challenges we face are multi-faceted, and we need to find a whole array of tailor-made solutions to them.

We are also examining the possibilities of interlinking blockchain-based solutions with conventional payment systems - like our real-time gross settlement system TARGET2.

For example, a technical link between a smart contract on a blockchain could automatically trigger a payment in TARGET2.

This would have the benefit that the existing payment infrastructure could be used in a tokenised economy without any potential disruption to the division of labour between central banks and the financial sector.

Let me summarise: introducing CBDC is not just a technical decision - it's a policy stance. Therefore, to prevent disruption, a comprehensive

conceptual analysis and assessment of CBDC compared to the alternatives needs to be carried out - especially with a view to the fulfilment of our mandate, but also regarding its impact on society.

Thank you for your attention.

Number 3

EBA published final draft regulatory technical standards specifying the prudential treatment of software assets

The European Banking Authority (EBA) has published its final draft Regulatory Technical Standards (RTS) specifying the prudential treatment of software assets.

As the banking sector is moving towards a more digital environment, the aim of these draft RTS is to replace the current upfront full deduction prudential regime so as to strike an appropriate balance between the need to maintain sufficient conservatism in the prudential treatment of software assets and their relevance from a business and an economic perspective.

The final draft RTS keep a simple approach based on a prudential amortisation of software assets calibrated over a period of maximum three years.

These final draft RTS specify the methodology to be adopted by institutions for the purpose of the prudential treatment of software assets, following the amendments introduced as part of the Risk Reduction Measures (RRM) package adopted by the European legislators. You may visit: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:150:FULL&from=END

In particular, these draft RTS envisage the application of a prudential treatment based on software amortisation, which is deemed to strike an appropriate balance between the need to maintain a certain margin of conservatism in the treatment of software assets as intangibles, and their relevance from a business and an economic perspective.

Following the feedback received during the public consultation, the calibration of the maximum prudential amortisation period of software has

been extended to three years. Moreover, the final draft RTS have been revised in order to envisage that prudential amortisation shall be calculated starting from the date on which the software asset is available for use.

This would result in a better alignment between the starting date of the accounting and the prudential amortisation, facilitating the implementation of the new prudential treatment of software.

Finally, in line with the recent targeted 'quick fix' amendments to the Capital Requirements Regulation (CRR) aimed at bringing forward the date of application of the new prudential treatment for software assets, the date of entry into force of the draft RTS has been anticipated to the day following that of its publication in the Official Journal of the European Union.

The EBA will closely monitor the evolution of the investments in software assets going forward, including the link between the proposed prudential treatment and the need for EU institutions to make some necessary investments in IT developments in areas like cyber risk or digitalisation.

Legal basis and next steps

These draft RTS have been developed according to Article 36(4) of Regulation (EU) No 575/2013 (CRR), which mandates the EBA to "specify the application of the deductions referred to in point (b) of paragraph 1 of Article 36, including the materiality of negative effects on the value which do not cause prudential concerns".

The final standards have been sent to the European Commission for their adoption as EU Regulations that will be directly applicable throughout the EU.

Number 4

Focus on the future of banking supervision in a changing world

International banking supervisory community meets virtually

- At the 21st International Conference of Banking Supervisors, senior banking supervisors and central bankers discussed issues related to the future of banking supervision in a changing world.

- Discussions covered the digitalisation of finance and the evolution of banking models, operational resilience, climate-related financial risks and remote working arrangements.

- This was the first time the Basel Committee has worked with a host country to offer a completely virtual conference.

The 21st International Conference of Banking Supervisors (ICBS), hosted virtually by the Office of the Superintendent of Financial Institutions (OSFI) and the Bank of Canada, was held on 19-22 October 2020. Approximately 450 senior banking supervisors and central bankers representing close to 100 countries took part.

Delegates discussed a wide range of issues related to the future of banking supervision in a changing world. The discussions covered the digitalisation of finance and the evolution of banking models, operational resilience, climate-related financial risks and remote working arrangements.

Participants also exchanged views on the challenges for central banks and bank supervisors in advanced and emerging market economies during the Covid-19 pandemic, as well as adapting to the changing operating environment for central banks and supervisors.

The event included several panel discussions and keynote speeches by Pablo Hernández de Cos, Chair of the Basel Committee on Banking Supervision and Governor of the Bank of Spain, and Prithwiraj Choudhury, Associate Professor at Harvard Business School.

This successful event marks the first time that the Basel Committee has worked with a host country to offer a completely virtual conference.

The ICBS, which has been held every two years since 1979, brings together bank supervisors and central bankers from around the world as well as representatives of international financial institutions.

The conference promotes the discussion of key supervisory issues and fosters the continuing cooperation in the oversight of international banking.

With its wide membership of senior supervisors and policymakers, the ICBS presents a unique opportunity for a broad-based discussion on issues that are timely and relevant to supervisors in both advanced and emerging market economies.

Number 5

Is home working good for you?

Andrew G Haldane, Executive Director and Chief Economist of the Bank of England, at the Engaging Business Summit and Autumn Lecture.

I am delighted to be speaking at this "Engaging Business" Summit, at such a critical time for business, for workers and for the wider economy.

The focus of today, and the excellent background report, is happiness in the workplace. This is an issue in which everyone has a stake.

It is particularly pertinent with many people having had to adapt their ways of working as a result of the Covid crisis.

Indeed, this year may well have seen the largest shift in working practices ever seen, certainly the largest in modern times.

That begs a host of questions about the impact of these changes in working practices on workers, businesses, communities and the wider economy.

For economists like me, it raises questions about the impact on productivity and output in the workplace.

As arid as these concepts can sometimes sound, they are crucial for shaping how this crisis will affect incomes and living standards over the medium-term.

Equally important are issues of well-being, not least given understandable concerns about how the virus and lockdown are affecting our mental health.

The background report for this event is timely in providing some early answers to these questions.

Taken at face value, its conclusions are encouraging.

Workplace happiness is, in general, higher and many are feeling a greater sense of workplace empowerment.

At the same time, it is too early to be reaching definitive conclusions on what the long-term effects of these seismic shifts in how we work will be.

It is also crucial to recognise that these changes have affected individuals in very different ways.

For many frontline workers - from health and social care, to public transport and police – home-working has simply not been an option.

Those jobs, and many others like them, have become both harder and more hazardous as a result of the Covid crisis.

The report captures some of those important distributional differences, with happiness lowest among young people, black people, females and those in the worst-affected sectors whose jobs and incomes are most at risk.

Even for those who are currently content home-working, there is a question about whether the benefits will persist.

Some of the potential costs of home-working, including the loss of social engagement, are only now being felt and may grow with time, in ways which affect both our well-being and productivity at work.

In what follows, I will try to navigate through some of these issues, drawing on evidence where possible.

There are both positives and negatives from the shift in working practices that has taken place this year and the balance of these is likely itself to shift over time.

If you'll forgive the indulgence, I'll try and weave in some of my own work experiences to add some personal colour.

The Changing World of Work

Even before the Covid crisis struck, there was evidence of a secular shift towards more flexible forms of working.

Analysis of working trends by the Association of Professional Staffing Companies in 2019 found that, over the past two decades, the number of people working 'flexible hours' has increased five-fold, from less than 10% to more than half the workforce.

As with many other things, the Covid crisis brought about an overnight transformation and acceleration of those trends.

ONS data suggests that, prior to the pandemic, around 5% of people worked from home as their main location.

Around 12% had worked from home in the previous week and a little more than a quarter said they had worked from home at some point in the recent past.

At the peak of lockdown in April, almost half of the workforce was working from home in any given week, either exclusively or partially.

Over the summer that fraction began falling as restrictions were loosened, before beginning to rise again gradually following government announcements in September.

The fraction of the workforce home-working currently stands at around a third, multiples of its pre-Covid level.

Of course, these averages obscure some sharp differences across sectors and occupations.

Even before the pandemic, there was a high incidence of home-working in sectors such as information and communication (over 50%), professional and scientific (around 45%) and real estate and finance (about 40%).

During lockdown, all of these sectors headed towards a 100% model of home-working.

That was not the case, either pre or post-Covid, among a range of other occupations representing between half and two-thirds of the workforce.

Many of those were key workers, including in health and social care, dealing with the effects of the pandemic.

In this respect, Covid has not only accelerated pre-existing trends towards home-working; it has also widened pre-existing occupational divides between those who can and cannot exercise the option of home-working.

Surveys of workers and businesses suggest increased home-working is likely to persist, albeit not on the same scale.

Around a fifth of businesses say they intend using home-working as a permanent business model.

Interestingly, the main reason cited is improved staff well-being.

Among workers the picture is much the same, with surveys suggesting more than a quarter expect to spend more time home-working after the pandemic has abated.

My own experience since March has mirrored trends in the wider economy.

I am one of the lucky ones who has been able to work from home, as have virtually all other Bank of England staff.

I have been back into the office only twice in the past six months. Full-time home-working has, for me, been a radical shift.

For the past 30, my working week has been 5-0, office versus home.

Nonetheless, like many others, if you asked me how my future working week might look, I think it unlikely I will revert back to the 5-0 model.

To read more: https://www.bis.org/review/r201026a.pdf

Number 6

Bugs happen, so make sure you're ready to fix them

How a Vulnerability Disclosure Process ensured a bug in the NHS COVID-19 app was fixed quickly and responsibly

National Cyber Security Centre

Bugs happen. It's unrealistic to expect software (and hardware) to be bug free. So when designing a system (such as the NHS COVID-19 App), it's important to build in multiple layers of defence so that when bugs are found (which they will be), you can quickly respond to them, and fix the system.

One such layer is a vulnerability disclosure programme (VDP). When set up, a VDP makes it easy for anyone to report a security vulnerability they find in your system, as there's an established process in place to triage and fix the bug.

I've been working with the NHS COVID-19 app team from the early stages of development, and asked them to establish a VDP early on.

This meant that internal processes could be put in place and tested to ensure when a bug is discovered, the team can respond efficiently.
You may visit:
https://www.ncsc.gov.uk/blog-post/nhs-test-and-trace-securing-the-nhs-covid-19-app

Recently, James "zofrex" Sanderson reported a bug which affected the Android version of the app. The bug allowed a venue check-in QR code poster to be scanned, despite not being generated by the NHS venue poster generation service. In a nutshell, the app would accept a QR code without a valid signature.

Complex software is comprised of an intricate web of libraries and interdependencies. This means it can be hard to get complete coverage of misuse cases.

The NHS COVID-19 has been thoroughly reviewed and tested, including specifically around this bug.

But it still managed to slip through. Luckily the bug was spotted by James, one of the many independent researchers who took a closer look at the app and its source code. Once the team received the vulnerability report, the challenge is now to respond to the report.

Here's a timeline that describes what happened:

- 30th September 2:22pm: The bug report is submitted via HackerOne.

- 2:33pm: The issue is confirmed and the triage process initiated. A new Slack channel is created to bring all the relevant people together to discuss and agree the next steps.

- 3:43pm: The lead Android developer creates a pull request which patches the bug. After the pull request was accepted and merged into the main branch, a build is kicked off which is then passed on to the testing team.

- 6:51pm: End-to-end testing completed. Given the severity of the bug and to ensure the proper change request process is followed, the team decides to release the next day.

- 1st October 7:55am: The team updates the reporter on progress so far.

- 9:03am: A ticket is created to start the release processes. The new build is submitted to the Google Play Store for review.

- 1:43pm: The release ticket is reviewed and approved by all the relevant parties.

- 3:58pm: After final checks, the new version of the app is made available to download. Devices that are set to automatically update start to download the new version over the next few days.

To summarise, within 24 hours the team had triaged, fixed, tested, and approved a patch for the bug. At the time of writing, the new update has been installed by over 93% of the apps Android users.

Of course, not all the bugs will get triaged and fixed this quickly, but a VDP allows us to quickly triage and prioritise vulnerabilities effectively which I think demonstrates the benefits of setting up a VDP.

The NCSC has recently launched its own Vulnerability Disclosure Toolkit to help organisations create their own vulnerability disclosure process, and I'd encourage all organisations who want to improve the security of their systems to do the same.
You may visit:
https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit

Even if your organisation already has a process in place, please download the toolkit (pdf) as it may help you to improve on what you already have in place.
You may visit:
https://www.ncsc.gov.uk/files/NCSC_Vulnerability_Toolkit.pdf

National Cyber Security Centre
a part of GCHQ

Vulnerability Disclosure Toolkit

Contents

Plenty of government departments have established their own VDP. However, it's still a relatively new concept so if you do spot an issue and there isn't a reporting process, you can report it to the NCSC via our Vulnerability Reporting Service (which has already resolved 19 of the 27

vulnerabilities reported). We'll help you to make contact with the system owner, and if possible, get it fixed.
You may visit:
https://www.ncsc.gov.uk/information/vulnerability-reporting

Stuart H
NCSC Senior Security Architect and acting Chief Information Security Officer (CISO) for the NHS COVID-19 app

Number 7

Financial stability implications of the pandemic

Ignazio Visco, Governor of the Bank of Italy, at the 2nd Bank of Italy and Bocconi University - BAFFI CAREFIN Conference "Financial Stability and Regulation", Rome.

It is a pleasure for me to open the second conference on "Financial Stability and Regulation" organised by Banca d'Italia and the Baffi Centre for Applied Research on International Markets, Banking, Finance and Regulation.

This event could not take place in March in Rome as we had all wished. But it is taking place today with its original programme, albeit in a virtual format.

I want to thank the organisers at Bocconi and at the Bank for their efforts, the contributors to the five sessions, and the keynote speakers. The papers that will be presented today and tomorrow will cover financial stability and regulatory issues that have been hotly debated over recent years.

The keynote lectures will address forward-looking issues on the implications of Fintech competition on payment systems, the determinants of the low price-to-book ratios observed in the banking sector, and the challenges to central banking and financial stability created by climate change.

In these brief remarks I will focus on the financial stability implications of the outbreak of the current pandemic. This is of course a topic not explicitly covered in the sessions of this conference.

Last November, when the call for papers was closed, nobody could have anticipated the events that would then unfold. But this does not mean that the discussions that will take place during this event will have no relevance to current financial and policy developments.

On the contrary, many of the topics that will be covered in this conference - like the pro-cyclicality of loan loss provisioning requirements, the challenges associated with the rapid adoption of new technologies in the

banking sector, the effects of bank dividend pay-out policies, or the implications of rising corporate solvency risk on banks' balance sheets - have been and will continue to be at the heart of the debate on the policy response to the Covid-19 crisis in the coming months.

The spread of the Covid-19 disease and the necessary lockdown and social distancing measures adopted to contain it have triggered a contraction of the global economy of unparalleled magnitude.

The reaction to the uncertainty and risks surrounding the initial stages of the Covid-19 outbreak led to serious liquidity strains in global financial markets.

The traditional flight-to-quality behaviour among investors during stress episodes was followed by an unprecedented "dash for cash" in which even US Treasuries became illiquid.

The lockdown measures adopted in many countries in the following weeks halted economic activity in several sectors, triggering massive increases in (observed and disguised) unemployment and plummeting corporate sales. Without policy intervention, a credit crunch would have unfolded and households' and firms' cash shortfalls would most likely have led to a large wave of defaults.

The prompt and massive response of monetary and fiscal authorities prevented an immediate liquidity crisis, which would have had profound economic and financial stability consequences.

Central banks reacted swiftly to market turmoil in March by deploying a wide array of emergency liquidity facilities and new asset purchase programmes.

Further lending support was also provided through the introduction of funding facilities for banks conditional on them granting new loans to the real economy.

Most governments introduced measures to assuage firms' and households' liquidity needs, such as debt moratoriums and temporary lay-off assistance, and to facilitate their access to new financing, such as loan guarantee programmes.

Bank supervisors in turn used the flexibilities embedded in Basel III regulation and accounting standards to increase banks' headroom to absorb losses and continue financing the economy.

The policy response has been effective in achieving its short-term objectives. Markets have stabilised.

Credit is flowing to firms and households, sustained to a large extent by exceptionally generous loan guarantee schemes.

Economic activity is recovering. Growth forecasts have improved slightly, although there is still substantial uncertainty, driven mostly by the evolution of the global health crisis.

But, while this crisis is not over, it has already created some "legacies" of its own, which could threaten financial stability in the medium term.

First, authorities will soon have to make difficult decisions about the extension or phasing-out of some lending support measures. On the one hand, an early removal of lending support could have a destabilising cliff effect on credit supply conditions, holding back the pace of economic recovery.

Even viable firms, especially those with high leverage, could face credit rationing problems. On the other hand, the extension of support measures could give rise to an undesirable allocation of credit towards unviable firms, which will eventually weigh on growth prospects. This is a dynamic trade-off.

At the current juncture, where uncertainty is high and recovery still weak, downside risks from an early removal loom large and would call for a cautious extension of expiring measures.

Going forward, the appropriate modulation of exit strategies must take careful account of the evolution of underlying sanitary, economic and financial developments.

Second, non-financial firms' indebtedness is expected to increase significantly, giving rise to debt overhang problems. In the wake of the first stage of the crisis, it had to be ensured that firms were able to obtain financing to cover cash shortfalls created by lockdowns.

Speed in the delivery of funds to hundreds of thousands of cash-strapped small firms - as we observed in Italy - was key. In several jurisdictions this was achieved by designing policies, such as loan guarantees, that made use of the existing bank lending "infrastructure".

Yet, as corporate revenue losses are unlikely to be recouped entirely, this bridge financing may lead to a permanent increase in leverage for some

firms. This creates challenges in the medium term; it could lead to generalised debt overhang problems that would reduce firms' investment, weaken competitiveness and hamper economic growth.

Therefore, capital-strengthening measures by governments to reduce non-financial firms' leverage and increase their debt servicing capacity seem to be necessary.

Several options have been proposed and, in some countries, already implemented, such as direct cash transfers, purchase of equity stakes or subordinated debt instruments by special purpose vehicles with public capital, and fiscal incentives to favour private equity injections into firms.

The challenges are nevertheless substantial. An efficient use of public funds calls for the establishment of procedures which effectively separate, in a fast-moving environment, those firms deserving of support from the non-viable ones.

This will undoubtedly be a demanding task; at the same time policy measures should be tailored to account for the differences between the governance of (often very) small firms, mostly managed by their owners, and larger firms (often joint stock companies), run by managers on behalf of shareholders.

Losses from public investment in firms' equity should be minimised, if not completely fended off, while at the same time avoiding excessive and intrusive interventions in business governance and decisions.

Third, how to ensure the resilience of the banking system in the face of a likely surge in credit losses is a crucial question. Banks entered the pandemic crisis with much stronger capital and liquidity positions than before the global financial crisis, not least because of the regulatory reforms in the aftermath of the latter.

As a result, there has been some room for supervisory authorities to release macroprudential buffers and to provide a flexible interpretation of microprudential requirements, with the aim of allowing banks to absorb losses and sustain the flow of credit to all borrowers, including the most vulnerable ones; an important contribution to banks' resilience has come also from supervisors' recommendations to abstain from paying out dividends or undertaking share buybacks.

As further credit losses are expected to materialise over the coming months, several banks have already started to increase their provisions substantially.

A prudent approach to provisioning in the current phase is certainly desirable. Looking ahead, it is crucial that supervisors and regulators reach a difficult balance between avoiding pro-cyclical credit restrictions and maintaining safe and forward-looking risk management practices.

That said, the scale of the current crisis could nevertheless require extraordinary interventions in the banking sector. Banks have to continue to manage non-performing loans (NPLs) effectively, so that they do not build up in balance sheets, hindering efforts to strengthen capital and undermining market and consumer confidence.

In Europe there is a discussion around initiatives aimed at setting up or improving the functioning of special purpose vehicles focused on the management of NPLs (asset management companies, or "bad banks").

Proposals that also include the possibility of private investors participating in the capital of these companies could be looked upon favourably.

Moreover, this unprecedented shock could potentially have some banks among its victims. Unresolved issues with the crisis management framework in Europe, then, should be addressed promptly.

This comprises harmonising the liquidation procedures for small and medium-sized intermediaries, including through the possibility of using common funds to conduct orderly liquidations, and finalising the creation of a backstop to the Single Resolution Fund as part of the crisis management framework.

Finally, we are left with the need to address the moral hazard, in particular on non-bank financial intermediation, created by the expectation of a "central bank put".

With the outbreak of the Covid-19 pandemic, investor risk aversion has increased rapidly, leading to a surging demand for cash and to the exit from equity and fixed income markets in search of short-term, risk-free assets.

Large price swings have been observed in many asset classes, volatility has increased enormously and redemptions in open-end funds have been at record high levels.

Central banks have had to introduce extraordinary asset purchase programmes, special liquidity operations and US dollar funding facilities to restore market functioning and maintain the efficient transmission of monetary policy measures.

These interventions have been effective, but the expectation of public intervention in the event of systemic market disruption could create moral hazard, and subsequently result in making further disruption more likely.

As a consequence, progress needs to be made to introduce or reinforce the macroprudential framework for non-bank financial intermediaries (NBFIs), in particular investment funds and insurers.

Macroprudential stress testing, which aims at identifying possible transmission channels and feedback effects among financial firms and markets, is still at a preliminary stage in the non-bank sector. It could represent a useful tool to assess how shocks originating in one part of the financial system can spread to other components.

Further NBFI areas that need additional investigation include: minimum liquidity buffers; rules to reduce structural liquidity transformation; possible additional requirements for synthetic and traditional leverage; concentration and interconnectedness.

To conclude, the extreme macroeconomic shock triggered by the Covid-19 outbreak is testing the resilience of the global financial system and the ability of policy makers to respond to tail events, highlighting the strengths of the current regulatory framework but also some of its vulnerabilities.

It is also accelerating trends that are likely to reshape the financial industry in the future. The coming months will be challenging for our societies, and the following years will see substantial structural transformations.

Complex decisions with far reaching consequences will have to be taken by authorities and intermediaries all over the world.

Experience in the use of existing policies is growing, but new risks are also emerging. Research and discussion fora like this conference, in which fresh ideas and experiences are exchanged among academics and policymakers, will be ever more important. Therefore, I wish you all two very fruitful and constructive days of open discussion.

Number 8

Modernizing and Strengthening CRA Regulations: A Conversation with the Housing Community

Governor Lael Brainard, U.S. Federal Reserve's Board of Governors, at the National Housing Conference National Advisory Council Meeting

I want to thank David Dworkin for inviting me to participate in this discussion. I am pleased to be with you to talk about Community Reinvestment Act (CRA) modernization and how this process can help address the housing challenges facing minority and low- and moderate-income (LMI) communities around the country. The National Housing Conference (NHC) is an important voice in housing and community development policy, so I look forward to hearing from you.

During the mortgage foreclosure crisis, many families around the country suffered the devastating loss of their home through no fault of their own, and homeownership rates have not recovered to pre-crisis levels for the affected groups. Now, the COVID-19 pandemic is raising a new set of housing challenges for renters and the rental market.

The current crisis is hitting LMI households with limited financial resources the hardest, and this is especially true for Black and Latinx households. Data from the Census Household Pulse Survey indicate that 25 percent of Black renters and 22 percent of Hispanic renters were behind on their rent payments as of September, along with 12 percent of White renters.

Among homeowners, Black and Hispanic households have been "significantly more likely to miss or defer monthly mortgage payments and experience uncertainty about making next month's payment than white households" during the pandemic.

Coronavirus Aid, Relief, and Economic Security (CARES) Act emergency payments and supplemental unemployment benefits provided vital support to households in the initial stages of the crisis, and the mortgage forbearance period of up to 360 days in the Act and eviction moratoriums at the federal, state, and local level have provided vital stop-gap stability for many families.

There is growing concern about what will happen to individuals who may be behind on their rent or mortgage payments as a result of job loss or reduced hours when eviction moratoriums and mortgage forbearance programs come to an end, especially given uncertainty about whether there will be further fiscal support.

The housing challenges resulting from the COVID-19 pandemic are layered on top of existing challenges in both the homeownership and rental markets. Affordable housing is essential to providing low-income households the stability necessary to engage in employment and schooling, provide for essential needs, and accumulate some financial cushion for emergencies. However, the need for affordable housing has grown at a faster pace than the supply.

With limited supply of lots and other challenges, new construction in many places has been oriented to higher-end units, leaving more limited supply for households with lower incomes, especially in higher cost cities. Many households have been unable to purchase a home since the last financial crisis due to a confluence of factors, including higher home prices and stricter lending standards.

For those who have purchased a home, higher home prices have translated into higher debt levels relative to household income.

For renters, available subsidies or programs for affordable housing have fallen short of the need, particularly in higher cost cities, while new higher-end rental housing has increased significantly since the financial crisis. The high cost of renting leaves many families paying a higher share of their income for housing. American Community Survey data from 2019 show that 45 percent of renter households spend more than 30 percent of their monthly income on rent.

While 22 percent of renters pay more than half of their income toward rent, this figure jumps to nearly 38 percent for renters earning below $50,000. This leaves families with little to no room to save for emergencies, such as the COVID-19 pandemic.

This growing shortage underscores the importance of the incentives provided by the CRA for the production and rehabilitation of affordable housing. With the demand for affordable units significantly exceeding supply, it is essential to strengthen the incentives for these loans and investments as part of CRA modernization.

Increasing access to affordable housing is critical to creating opportunities for homeownership for LMI households and with it the chance to build

wealth through home equity. Here too, CRA plays a role, not only in providing incentives for the provision of affordable housing, but also in encouraging access to credit for homeownership for LMI households and communities. Indeed, mortgage lending has long been at the center of evaluating CRA performance.

The challenges facing LMI and minority renters and would-be homeowners underscore the importance of getting CRA modernization right. The Federal Reserve Board unanimously voted to approve an Advance Notice of Proposed Rulemaking (ANPR) about CRA modernization on September 21, 2020.

The ANPR was published yesterday in the Federal Register, and the comment period will end on February 16, 2021.

By providing a 120-day comment period, we hope to receive comments from a wide range of stakeholders and build on the already robust feedback that informed the development of the ANPR.

Throughout this process, NHC has provided the Federal Reserve with valuable insights into the unique role and needs of affordable housing providers. Your members support community development projects in communities throughout the country, and we have benefited from the engagement of NHC and its members both in the form of detailed comment letters and through meetings to discuss different aspects of CRA reform.

The CRA is a critical law, enacted along with other complementary federal civil rights laws during the late 1960s and 1970s. The intent of these laws was to address redlining and systemic inequities in access to credit and other financial services for LMI and minority communities.

The core purpose of CRA remains as important as ever, especially given the national conversation we are having about racial equity in our society and the disproportionate impact that COVID-19 is having on LMI and minority communities.

Even with these critical laws, the wealth gap remains stubbornly wide. The Survey of Consumer Finances for 2019 found that the typical White family has eight times the wealth of the typical Black family.

For many American families, homeownership is the single most important component of their wealth. In 2019, the homeownership rate for Black households was 42.1 percent, as compared to the 73.3 percent for White households. This homeownership gap of 31.2 percent is 3.1 percentage points wider than a decade ago.

The Board's ANPR seeks to advance the law's core purpose of addressing unequal access to credit for LMI and minority communities and disinvestment in underserved communities. A modernized CRA should help move the needle on credit access, wealth building, and the availability of community development financing.

This includes strengthening the regulations to ensure that a wide range of low-income and minority banking needs are being met. It also includes promoting financial inclusion by proposing incentives for further bank investments in Minority Depository Institutions, Community Development Financial Institutions (CDFIs), and community development activity in designated areas of need outside of assessment areas, such as Indian Country.

The ANPR also seeks to provide greater certainty, tailor regulations based on bank size and business model, and minimize burden. For example, the ANPR introduces a metrics-based approach that would separately evaluate retail lending and community development financing activity.

The use of standardized metrics would provide greater clarity and transparency on how lending and investment activity is evaluated. These proposed metrics would also use thresholds that are tailored to local market conditions, while also retaining a focus on targeted performance context factors.

Lastly, we hope the ANPR will provide a foundation for the agencies to converge on a consistent approach that has broad support among stakeholders. Stakeholders, including the NHC, have expressed strong support for the agencies to work together to modernize CRA.

By reflecting stakeholder views and providing a long public comment period, we believe that the ANPR provides the basis for the agencies to establish a consistent approach that has broad support.

Before concluding, I want to highlight a few proposals in the ANPR that have particular relevance to affordable housing. First, the ANPR proposes two separate tests for evaluating the CRA performance of large retail banks—a Retail Test and a Community Development Test—in response to the overwhelming stakeholder feedback we heard about the vital importance of both retail and community development activities.

In the ANPR, each of these tests would have a subtest that focuses on financing and a subtest that focuses on services, resulting in four overall subtests for large retail banks.

Second, the ANPR proposes evaluating a bank's retail lending in its major product lines using metrics that measure the number of loans a bank makes, not the dollar-value of these loans. As a result, a larger mortgage loan would count the same as a smaller-dollar mortgage under the proposed metrics.

We think this is important to avoid providing incentives to serve borrowers seeking to finance higher-priced homes at the expense of lower-income borrowers seeking finance for lower-priced homes.

Third, the ANPR proposes combining consideration of community development loans and qualified investments, including originations and purchases, into one metrics-based Community Development Financing Subtest.

We believe this could encourage the provision of patient capital because both new originations and those already on the balance sheet would be included in the evaluation metric.

Fourth, stakeholders have emphasized the critical importance of CRA-motivated capital as a source of funding for affordable rental and single-family housing for LMI populations.

Given the significant unmet need for affordable housing, the ANPR provides an opportunity to carefully reconsider how we define affordable housing in the CRA regulations and how we can strengthen existing provisions for the creation and preservation of affordable housing, both rental and owner-occupied.

The ANPR proposes new regulatory language that would specify that a housing unit would be considered affordable if it is purchased, developed, rehabilitated, or preserved in conjunction with a federal, state, local, or tribal government affordable housing program or subsidy, with the bona fide intent of providing affordable housing.

This definition is intended to capture a wide variety of subsidies, including tax credit programs (such as the Low-Income Housing Tax Credit), federal government direct subsidies, and state and local government direct subsidies for the production or preservation of affordable housing. These programs could be for rental housing or homeownership.

The suggested language is also intended to capture programs that do not provide monetary subsidies, but that have the express intent of producing or preserving affordable housing, such as a loan in support of a land bank program.

In addition, many stakeholders have noted the importance of preserving unsubsidized housing that is affordable to LMI households and ensuring units retain their affordability in gentrifying areas.

In response to these concerns, the ANPR seeks to clarify the criteria under which banks can receive CRA consideration for investing in unsubsidized, or naturally-occurring, affordable housing.

We are also considering other options to ensure that housing-related community development financing activities maintain long-term affordability, limit displacement, and encourage affordable housing located in all communities.

As experts in this field, we look forward to receiving your feedback on what specific data sources and criteria we should consider to promote the preservation of naturally-occurring, affordable housing.

Fifth, the ANPR seeks feedback on the appropriate CRA treatment of mortgage-backed securities (MBS) that are backed by loans that finance subsidized multifamily rental housing, loans for mixed-income housing that includes affordable housing for LMI families, or loans to LMI borrowers.

While issuance of qualifying MBS can improve liquidity, and thereby increase capacity for lenders that make home mortgage loans to LMI borrowers, some stakeholders have expressed concern that MBS purchases may be undertaken in lieu of other more impactful community development financing activities that may require greater effort.

Finally, the ANPR seeks feedback on extending to CDFIs the status that is extended to Minority Depository Institutions, women-owned financial institutions, and low-income credit unions. Such an approach would effectively give banks CRA consideration for loans, investments, or services in conjunction with a CDFI anywhere in the country.

Additionally, the ANPR discusses granting automatic CRA community development consideration for qualified activities in conjunction with U.S. Department of the Treasury-certified CDFIs for activities in a bank's assessment area(s).

We hope that you will provide us with feedback on how to modernize the CRA in a way that supports affordable housing and promotes housing-related credit and investments to LMI and minority individuals and communities. We thank you for your engagement and look forward to hearing more from you and your members through the rulemaking process.

Number 9

Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace

Defendants' Malware Attacks Caused Nearly One Billion USD in Losses to Three Victims Alone; Also Sought to Disrupt the 2017 French Elections and the 2018 Winter Olympic Games

THE UNITED STATES DEPARTMENT of JUSTICE

On Oct. 15, 2020, a federal grand jury in Pittsburgh returned an indictment charging six computer hackers, all of whom were residents and nationals of the Russian Federation (Russia) and officers in Unit 74455 of the Russian Main Intelligence Directorate (GRU), a military intelligence agency of the General Staff of the Armed Forces.

These GRU hackers and their co-conspirators engaged in computer intrusions and attacks intended to support Russian government efforts to undermine, retaliate against, or otherwise destabilize:

(1) Ukraine;
(2) Georgia;
(3) elections in France;
(4) efforts to hold Russia accountable for its use of a weapons-grade nerve agent, Novichok, on foreign soil; and
(5) the 2018 PyeongChang Winter Olympic Games after Russian athletes were banned from participating under their nation's flag, as a consequence of Russian government-sponsored doping effort.

Their computer attacks used some of the world's most destructive malware to date, including: KillDisk and Industroyer, which each caused blackouts in Ukraine; NotPetya, which caused nearly $1 billion in losses to the three victims identified in the indictment alone; and Olympic Destroyer, which disrupted thousands of computers used to support the 2018 PyeongChang Winter Olympics. The indictment charges the defendants with conspiracy, computer hacking, wire fraud, aggravated identity theft, and false registration of a domain name.

According to the indictment, beginning in or around November 2015 and continuing until at least in or around October 2019, the defendants and their co-conspirators deployed destructive malware and took other disruptive actions, for the strategic benefit of Russia, through unauthorized access to victim computers (hacking).

As alleged, the conspiracy was responsible for the following destructive, disruptive, or otherwise destabilizing computer intrusions and attacks:

- Ukrainian Government & Critical Infrastructure: December 2015 through December 2016 destructive malware attacks against Ukraine's electric power grid, Ministry of Finance, and State Treasury Service, using malware known as BlackEnergy, Industroyer, and KillDisk;

- French Elections: April and May 2017 spearphishing campaigns and related hack-and-leak efforts targeting French President Macron's "La République En Marche!" (En Marche!) political party, French politicians, and local French governments prior to the 2017 French elections;

- Worldwide Businesses and Critical Infrastructure (NotPetya): June 27, 2017 destructive malware attacks that infected computers worldwide using malware known as NotPetya, including hospitals and other medical facilities in the Heritage Valley Health System (Heritage Valley) in the Western District of Pennsylvania; a FedEx Corporation subsidiary, TNT Express B.V.; and a large U.S. pharmaceutical manufacturer, which together suffered nearly $1 billion in losses from the attacks;

- PyeongChang Winter Olympics Hosts, Participants, Partners, and Attendees: December 2017 through February 2018 spearphishing campaigns and malicious mobile applications targeting South Korean citizens and officials, Olympic athletes, partners, and visitors, and International Olympic Committee (IOC) officials;

- PyeongChang Winter Olympics IT Systems (Olympic Destroyer): December 2017 through February 2018 intrusions into computers supporting the 2018 PyeongChang Winter Olympic Games, which culminated in the Feb. 9, 2018, destructive malware attack against the opening ceremony, using malware known as Olympic Destroyer;

- Novichok Poisoning Investigations: April 2018 spearphishing campaigns targeting investigations by the Organisation for the Prohibition of Chemical Weapons (OPCW) and the United Kingdom's Defence Science and Technology Laboratory (DSTL) into the nerve agent poisoning of Sergei Skripal, his daughter, and several U.K. citizens; and

- Georgian Companies and Government Entities: a 2018 spearphishing campaign targeting a major media company, 2019 efforts to

compromise the network of Parliament, and a wide-ranging website defacement campaign in 2019.

Cybersecurity researchers have tracked the Conspirators and their malicious activity using the labels “Sandworm Team,” “Telebots,” “Voodoo Bear,” and “Iron Viking.”

The charges were announced by Assistant Attorney General John C. Demers; FBI Deputy Director David Bowdich; U.S. Attorney for the Western District of Pennsylvania Scott W. Brady; and Special Agents in Charge of the FBI’s Atlanta, Oklahoma City, and Pittsburgh Field Offices, J.C. “Chris” Hacker, Melissa R. Godbold, and Michael A. Christman, respectively.

“No country has weaponized its cyber capabilities as maliciously or irresponsibly as Russia, wantonly causing unprecedented damage to pursue small tactical advantages and to satisfy fits of spite,” said Assistant Attorney General for National Security John C. Demers. “Today the department has charged these Russian officers with conducting the most disruptive and destructive series of computer attacks ever attributed to a single group, including by unleashing the NotPetya malware. No nation will recapture greatness while behaving in this way.”

“The FBI has repeatedly warned that Russia is a highly capable cyber adversary, and the information revealed in this indictment illustrates how pervasive and destructive Russia’s cyber activities truly are,” said FBI Deputy Director David Bowdich. “But this indictment also highlights the FBI’s capabilities. We have the tools to investigate these malicious malware attacks, identify the perpetrators, and then impose risks and consequences on them. As demonstrated today, we will relentlessly pursue those who threaten the United States and its citizens.”

“For more than two years we have worked tirelessly to expose these Russian GRU Officers who engaged in a global campaign of hacking, disruption and destabilization, representing the most destructive and costly cyber-attacks in history,” said U.S. Attorney Scott W. Brady for the Western District of Pennsylvania. “The crimes committed by Russian government officials were against real victims who suffered real harm. We have an obligation to hold accountable those who commit crimes – no matter where they reside and no matter for whom they work – in order to seek justice on behalf of these victims.”

“The exceptional talent and dedication of our teams in Pittsburgh, Atlanta and Oklahoma City who spent years tracking these members of the GRU is unmatched,” said FBI Pittsburgh Special Agent in Charge Michael A.

Christman. "These criminals underestimated the power of shared intelligence, resources and expertise through law enforcement, private sector and international partnerships."

The defendants, Yuriy Sergeyevich Andrienko (Юрий Сергеевич Андриенко), 32; Sergey Vladimirovich Detistov (Сергей Владимирович Детистов), 35; Pavel Valeryevich Frolov (Павел Валерьевич Фролов), 28; Anatoliy Sergeyevich Kovalev (Анатолий Сергеевич Ковалев), 29; Artem Valeryevich Ochichenko (Артем Валерьевич Очиченко), 27; and Petr Nikolayevich Pliskin (Петр Николаевич Плискин), 32, are all charged in seven counts: conspiracy to conduct computer fraud and abuse, conspiracy to commit wire fraud, wire fraud, damaging protected computers, and aggravated identity theft.

Each defendant is charged in every count. The charges contained in the indictment are merely accusations, however, and the defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt.

The defendants and their co-conspirators caused damage and disruption to computer networks worldwide, including in France, Georgia, the Netherlands, Republic of Korea, Ukraine, the United Kingdom, and the United States.

The NotPetya malware, for example, spread worldwide, damaged computers used in critical infrastructure, and caused enormous financial losses.

Those losses were only part of the harm, however. For example, the NotPetya malware impaired Heritage Valley's provision of critical medical services to citizens of the Western District of Pennsylvania through its two hospitals, 60 offices, and 18 community satellite facilities.

The attack caused the unavailability of patient lists, patient history, physical examination files, and laboratory records. Heritage Valley lost access to its mission-critical computer systems (such as those relating to cardiology, nuclear medicine, radiology, and surgery) for approximately one week and administrative computer systems for almost one month, thereby causing a threat to public health and safety.

The conspiracy to commit computer fraud and abuse carries a maximum sentence of five years in prison; conspiracy to commit wire fraud carries a maximum sentence of 20 years in prison; the two counts of wire fraud carry a maximum sentence of 20 years in prison; intentional damage to a protected computer carries a maximum sentence of 10 years in prison; and

the two counts of aggravated identity theft carry a mandatory sentence of two years in prison.

The indictment also alleges false registration of domain names, which would increase the maximum sentence of imprisonment for wire fraud to 27 years in prison; the maximum sentence of imprisonment for intentional damage to a protected computer to 17 years in prison; and the mandatory sentence of imprisonment for aggravated identity theft to four years in prison.

These maximum potential sentences are prescribed by Congress, however, and are provided here for informational purposes only, as the assigned judge will determine any sentence of a defendant.

Defendant Kovalev was previously charged in federal indictment number CR 18-215, in the District of Columbia, with conspiring to gain unauthorized access into the computers of U.S. persons and entities involved in the administration of the 2016 U.S. elections.

Trial Attorney Heather Alpino and Deputy Chief Sean Newell of the National Security Division's Counterintelligence and Export Control Section and Assistant U.S. Attorneys Charles Eberle and Jessica Smolar of the U.S. Attorney's Office for the Western District of Pennsylvania are prosecuting this case.

The FBI's Atlanta, Oklahoma City, and Pittsburgh field offices conducted the investigation, with the assistance of the FBI's Cyber Division.

The Criminal Division's Office of International Affairs provided critical assistance in this case.

The department also appreciates the significant cooperation and assistance provided by Ukrainian authorities, the Governments of the Republic of Korea and New Zealand, Georgian authorities, and the United Kingdom's intelligence services, as well as many of the FBI's Legal Attachés and other foreign authorities around the world.

Numerous victims cooperated and provided valuable assistance in the investigation.

The department is also grateful to Google, including its Threat Analysis Group (TAG); Cisco, including its Talos Intelligence Group; Facebook; and Twitter, for the assistance they provided in this investigation. Some private sector companies independently disabled numerous accounts for violations of the companies' terms of service.

To read more:
https://www.fbi.gov/news/pressrel/press-releases/fbi-deputy-director-david-bowdichs-remarks-at-press-conference-announcing-cyber-related-indictment-of-six-russian-intelligence-officers

https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

Number 10

Episode 34: The Orbital Optician

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

In this episode of the Voices from DARPA podcast, Stacie Williams, a program manager since 2019 in the agency's Tactical Technology Office, reveals how a lifelong love of optical and photonic phenomena, beginning with fireflies during her childhood, is now unfolding in her stewardship of ambitious light-and-optics-centric programs at DARPA.

One of these, the Deformable Mirror (DeMi) program, recently reached a milestone with the placement from the International Space Station of a dime-sized deformable mirror on a loaf-sized CubeSat platform.

The goal of DeMi is to deliver cheaper, lighter, smaller telescope mirrors—in the form of a microelectromechanical system (MEMS)—that could open unprecedented options for space-based ISR (intelligence, surveillance, reconnaissance) technology that, in Stacie's words, "helps us understand what's going on with a space eyeview."

In another optics-tech effort under Stacie's wing, researchers are learning how to design so-called metamaterials—with engineered microstructures that manipulate electromagnetic wavelengths—that also could greatly simplify, lighten, and cheapen far more massive, complex, and expensive conventional telescopes.

In the podcast, Stacie also recounts her work beyond technology as a champion of science, technology, engineering, and math (STEM) education for economically disadvantaged communities.

You may visit:

- Blubrry (podcast host): https://blubrry.com/voices_from_darpa/69016999/episode-34-the-orbital-optician/

- YouTube: https://youtu.be/RYlPFCFfhTA

- iTunes: https://itunes.apple.com/us/podcast/voices-from-darpa/id1163190520

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.

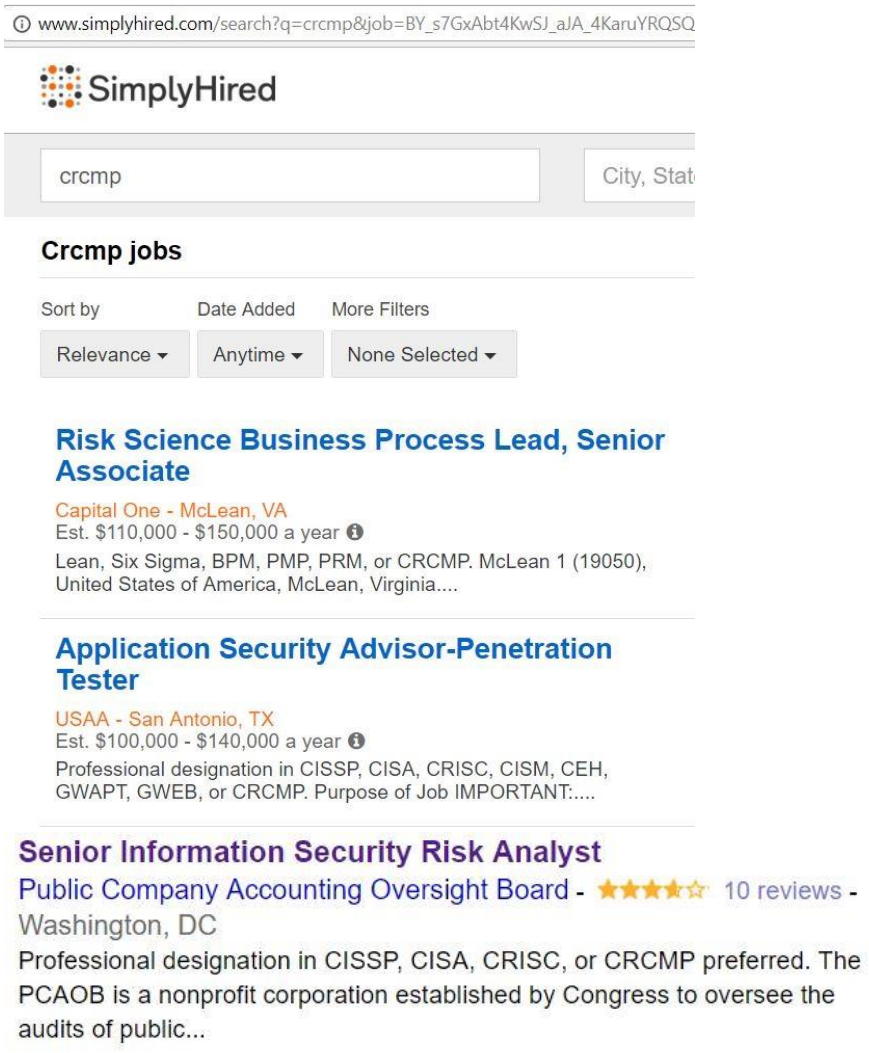
International Association of Risk and Compliance Professionals

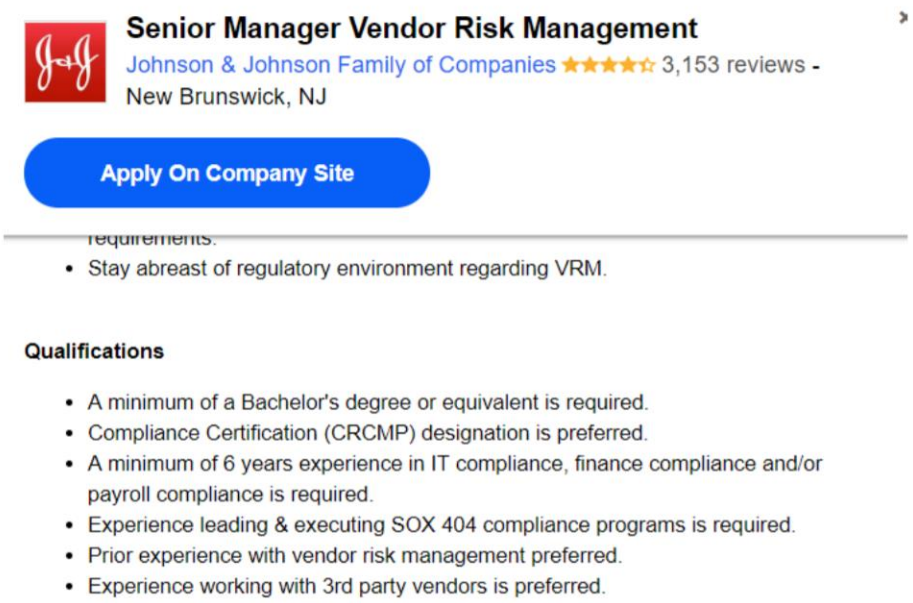
You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.
You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

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

3. *Training and Certification* – Become a Certified Risk and Compliance Management Professional (CRCMP), a Certified Information Systems Risk and Compliance Professional (CISRCP), a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, and / or a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I.





Senior Manager Vendor Risk Management

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

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

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

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

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

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

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

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

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

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

4. *IARCP Authorized Certified Trainer (IARCP-ACT) Program* - This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

To learn more, you may visit:
https://www.risk-compliance-association.com/IARCP_ACT.html

5. *Approved Training and Certification Centers (IARCP-ATCCs)* - In response to the increasing demand for CRCMP training, the International Association of Risk and Compliance Professionals is developing a world-wide network of Approved Training and Certification Centers (IARCP-ATCCs).

This will give the opportunity to risk and compliance managers, officers, and consultants to have access to instructor led training at convenient locations that meet international standards.

ATCCs use IARCP approved course materials and have access to IARCP Authorized Certified Trainers (IARCP-ACTs).

To learn more:
https://www.risk-compliance-association.com/Approved_Centers.html