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, October 3, 2022

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

Dear members and friends,

Year after year, the human element of cyber security is still the weakest link. I remember Alan Greenspan who had said: "Corruption, embezzlement, fraud, these are all characteristics which exist everywhere. It is regrettably the way human nature functions, whether we like it or not. What successful economies do is keep it to a minimum. No one has ever eliminated any of that stuff."

I have just read the new paper from the Bank for International Settlements (BIS Working Paper No 1039) with title "Cyber risk in central banking". We can read that, again, *three types* of attack stand out:

1. Phishing remains by far the most common initial attack vector. Traditionally, phishing emails have been used to trick a user to run a malicious attachment so that malware could be installed to take over the user's actual device.

Credential phishing has a different goal. It is the practice of stealing a user's login and password combination by masquerading as a reputable or known entity in an email, instant message, or another communication channel. Attackers then use the victim's credentials to carry out attacks on additional targets to gain further access.

The frequency of phishing attacks is increasing: for example, between January and June 2021, the monthly average of phishing emails targeting cloud services almost doubled. Attackers rely on ever more targeted and tailored malicious emails, through which they can either compromise end-user devices or gain an entry point for privileged access to local infrastructure or cloud-based services. Such unauthorised access can result in large damages.

2. Supply chain attacks occur when a threat actor infiltrates a legitimate software vendor's network and uses malicious code to compromise the software before the vendor sends it to their customers.

Such attacks take advantage of established relationships of trust and the machine-to-machine communications used to provide essential software updates.

They are thus difficult to mitigate and target both service providers (eg the 2020 SolarWinds Attack) and key technologies (eg Microsoft Exchange servers in 2021). Supply chain attacks are less frequent, but they can have great and potentially systemic consequences.

3. Ransomware is a type of malware deployed by attackers on a victim's computer network to encrypt their files and hold them for ransom. It typically propagates from a compromised end-user device through the entire organisation's IT environment.

It can compromise not only the availability of information and IT assets, but also their confidentiality and integrity.

The use of ransomware has grown massively over the past few years and incidences have tripled over the past year alone. Ransomware is mostly used by organised crime.

The type of attacker can vary. Beyond outright criminal and terrorist organisations, there can be industrial spies, "hacktivists", or state and state-sponsored players.

In consequence, the motive of a cyber attack can be to simply earn a profit (eg ransomware, industrial spying), but can also be geopolitical concerns

(statesponsored attacks on critical infrastructures) or general discontent (hacktivism).

Cyber incidents can have monetary and/or reputational consequences. Business disruptions and IT system failures can damage integrity and availability. Data breaches compromise confidentiality, with financial and reputational losses.

Fraud and theft include the loss of funds or any information (eg intellectual property) that may or may not be personally identifiable.

Read more at number 7 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)

The Economic Outlook: Time to Let the Data Do the Talking

Governor Christopher J. Waller, Board of Governors of the Federal Reserve System, 17th Annual Vienna Macroeconomics Workshop, Vienna, Austria

Number 2 (Page 15)

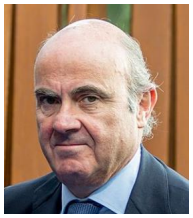
Governors and Heads of Supervision reaffirm expectation to implement Basel III in full and as fast as possible; provide direction on future work on climate-related financial risks and cryptoassets

BIS

Number 3 (Page 18)

Euro area current policy challenges

Luis de Guindos, Vice-President of the European Central Bank, at the CIRSF (Research Centre on Regulation and Supervision of the Financial Sector) Annual International Conference 2022 "The future of the EU financial system in a new geo-economic context", Lisbon



Number 4 (Page 24)

MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone

Microsoft Threat Intelligence Center (MSTIC), Microsoft Detection and Response Team (DART), Microsoft 365 Defender Research Team

Microsoft

Number 5 (Page 28)

Agencies reaffirm commitment to Basel III standards

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency

Number 6 (Page 29)

ESAs warn of rising risks amid a deteriorating economic outlook

EBA EUROPEAN BANKING AUTHORITY | eiopa European Insurance and Occupational Pensions Authority | esma European Securities and Markets Authority | JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Number 7 (Page 32)

BIS Working Paper No 1039

Cyber risk in central banking

by Sebastian Doerr, Leonardo Gambacorta, Thomas Leach, Bertrand Legros and David Whyte - Monetary and Economic Department

BIS

Number 8 (Page 35)

Consultation outcome

Proposals for new telecoms security regulations and code of practice - government response to public consultation

GOV.UK

Number 9 (Page 41)

NIST and Google to Create New Supply of Chips for Researchers and Tech Startups

Cooperative research agreement aims to unleash innovation in the semiconductor and nanotechnology industries.

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

Number 10 (Page 43)

Revolutionizing Infrared Sensing Could Transform Imaging Applications

New DARPA program seeks to enable quantum-level IR detection

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

The Economic Outlook: Time to Let the Data Do the Talking

Governor Christopher J. Waller, Board of Governors of the Federal Reserve System, 17th Annual Vienna Macroeconomics Workshop, Vienna, Austria

Thank you, Klaus, and thank you for the invitation to speak at this workshop, which I have been attending since its very beginning in 2004.

Something that I love about this conference that has kept me coming back almost every year is its tradition of open inquiry and even some fun, on the one hand, combined with rigorous, critical analysis, on the other.

I am a supporter, and I guess a practitioner, of rigorous criticism, because, as you may have heard, the conference award given each year for "outstanding critic" was named for me.

Based on the standard I set, the person who wins the award is also known as the "most annoying participant." I suppose it was only karma that a guy like me who likes to dish out the criticism would end up in a job that receives plenty of it.

Kidding aside, I do consider being the namesake for this award a great honor, and just to make sure I don't get too much of a swelled head, by tradition the conference organizers purposefully misspell my name.

My subject today is the outlook for the U.S. economy and the Federal Reserve's ongoing campaign to bring down inflation and achieve our 2 percent objective.

There are three takeaways from my speech today. First, inflation is far too high, and it is too soon to say whether inflation is moving meaningfully and persistently downward.

The Federal Open Market Committee (FOMC) is committed to undertake actions to bring inflation back down to our 2 percent target. This is a fight we cannot, and will not, walk away from.

The second takeaway is that the fears of a recession starting in the first half of this year have faded away and the robust U.S. labor market is giving us the flexibility to be aggressive in our fight against inflation.

For that reason, I support continued increases in the FOMC's policy rate and, based on what I know today, I support a significant increase at our next meeting on September 20 and 21 to get the policy rate to a setting that is clearly restricting demand.

The final takeaway is that I believe forward guidance is becoming less useful at this stage of the tightening cycle.

Future decisions on the size of additional rate increases and the destination for the policy rate in this cycle should be solely determined by the incoming data and their implications for economic activity, employment, and inflation.

Based on all of the data that we have received since the FOMC's last meeting, I believe the policy decision at our next meeting will be straightforward.

Because of the strong labor market, right now there is no tradeoff between the Fed's employment and inflation objectives, so we will continue to aggressively fight inflation.

Inflation is widespread, driven by strong demand that has only begun to moderate, by an ongoing lag in labor force participation, and by supply chain problems that may be improving in some areas but are still considerable.

For these reasons, I expect it will take some time before inflation moves back to our 2 percent goal, and that the FOMC will be tightening policy into 2023. But the answers to questions of "how high?" and "for how long?" will depend solely on incoming data.

Since I last spoke in July, I think the argument that we entered a recession in the first half of 2022 has pretty much ended—we didn't. With each passing week, the absence of any indication of a recession in spending or employment data buries that recession argument a little deeper.

We understand some of the factors that lowered the gross domestic product (GDP) numbers in the first half, and a debate continues about other possible factors, such as mismeasurement, potentially underreporting GDP.

What we can say is that after the Fed telegraphed its policy pivot to tightening in the latter months of 2021 and began raising rates in the first quarter of this year, demand and economic activity slowed in the first half of 2022 from the strong pace of 2021.

Data suggest an uptick in consumption growth in the third quarter. Meanwhile, the Atlanta Fed's GDPNow model forecasts real GDP will grow 2.6 percent this quarter, though other estimates are a touch below this prediction.

Spending data are supportive of continued expansion. Nominal retail sales overall were flat in July, but that is mainly because falling gasoline and auto prices—which is good news—held back sales in those sectors.

Excluding that, retail sales rose 0.7 percent, suggesting that discretionary spending grew solidly. Businesses also continued to expand production and spending. Total industrial production increased 0.6 percent in July, standing 3.9 percent above its level a year ago.

Forward-looking indicators of manufacturing activity, such as new orders indexes in various manufacturing surveys, are softer than earlier in the year, but most (and in particular the positive August reading from the ISM) are not suggestive of a material pullback in manufacturing activity.

Meanwhile, the non- manufacturing ISM report suggests continuing growth, with its new orders index rising to a solid level last month.

But there are signs of moderation in economic activity, which is what the FOMC is trying to achieve by tightening monetary policy. Not surprisingly, higher interest rates this year are slowing activity in the housing market.

There have been declines in construction of single-family homes for a number of months, with permits and home starts both decreasing in July.

Sales of existing and new single-family homes have also slowed. Existing home sales fell by 5.9 percent to a seasonally adjusted annual rate of 4.8 million homes in July.

While the imbalance between housing supply and demand remains significant, it has meaningfully improved. The inventory of unsold new and existing homes has more than doubled since January.

While the three months supply of existing home is still below levels before the pandemic, the eleven months of new home inventory is the highest since the spring of 2009.

This latter statistic has raised concerns by some about a significant downturn looming in the housing market, but an important caveat is that much of the current elevated inventory reflects the recent low rate of housing completion due to continued supply constraints.

Many of these new homes for sale are still under construction, and as supply constraints ease, builders will be able deliver more completed homes to a market where the supply of existing homes remains tight. All that said, the housing market is a significant channel for monetary policy, and I will be watching this sector carefully.

The FOMC's goal is that the tightening in monetary policy slows aggregate demand so that it is in better alignment with supply across all sectors of the economy.

My expectation is that strong household savings, the tight labor market, and additional availability of manufactured goods as supply chains constraints continue to resolve will allow households to make long-awaited purchases, which will provide a partial offset to tighter policy. That will support a slowing, rather than a contraction, in demand.

Turning to the very strong labor market, private payroll employment has been increasing at an average of nearly 400,000 a month over the last several months.

Unemployment rose two tenths of a percent in August to 3.7 percent, in part reflecting an increase in the labor force participation rate, but still stands at a very low level.

The increase in participation was welcome news, but this rate is still far below that achieved before the pandemic, when unemployment was roughly as low as today.

We are facing worker shortages in many sectors of the economy. Job openings have started to decline a bit but remain very elevated. These data confirm that the Fed is hitting its full employment mandate, so all my attention is on bringing inflation down.

Inflation slowed in July, which was a very encouraging development. Headline inflation for both the consumer price index and the index derived from personal consumption expenditures (PCE)—the Fed's preferred measure—slowed, largely due to continuing declines in prices for gasoline and other petroleum products.

Excluding volatile energy and food prices, core inflation for these two indexes also stepped down from the rapid increases of earlier this year, but it is still too early to say that inflation is moving meaningfully and persistently downward.

Inflation is still widespread. For both headline and core inflation, at least 60 percent of the underlying categories of different goods and services increased by 3 percent or more.

Prices for housing services are elevated and still rising. Core goods inflation continues to run well above its pre-pandemic level.

Inflation for services excluding housing has moved up this past year in part due to consumers shifting back to more normal activities outside the household as social distancing has eased.

Looking ahead, I will be focusing on a number of factors that will influence inflation. On housing services—rent and the so-called owners' equivalent rent —I expect to see sizable increases in this component of inflation for a while as the recent rise in new rentals makes its way into aggregate price measures.

In a speech in March, I noted that, based on various measures of asking rents, some analysts were predicting that the rate of rent inflation in the consumer price index could double in 2022, and so far it is on pace to more than double.

Owners-equivalent rent is similarly on pace to nearly double this year. Sometime early next year, though, I expect to see the upward pressure on inflation from these forces to ease as future increases in new or renewed leases moderate and the full effects of monetary policy tightening make their way to housing services prices.

Beyond housing, I expect goods price inflation to continue to moderate as monetary policy now and going forward slows the pace of increase in aggregate demand, supply problems ease, and supply and demand come into better balance.

There is some evidence that goods supply production and delivery problems tied to the pandemic are improving, with supplier delivery times and reports of items in short supply continuing to drop.

In terms of service price inflation, we saw a step-down in airfares and other travel-related services last month, but I am uncertain about how these

services, as well as food services, and nonmarket services prices will evolve going forward.

Nominal wages have been growing quickly, and I'll be watching closely to see how wage growth evolves and feeds into inflation.

The Atlanta Fed's Wage Growth Tracker hit another record in July for its 24 years of data, a 12-month rate of 6.7 percent wage growth.

I don't expect wage increases to ease up much unless and until there is a significant softening in the labor market.

One way to anticipate future wage growth is through quit rates. Most people who quit their jobs are moving to others that pay significantly better, so I take quits as one signal about where wages are headed in the near term.

Quits are near their highest level over the 22 years that the government has tracked them, but they have come down from the start of this year, and further decreases would bring them closer to the level they were at immediately before the pandemic, when wages were growing much more slowly than today.

Another factor that I will be watching closely is longer-term inflation expectations, which I believe significantly influence inflation.

As inflation moved higher over the past year and a half, measures of short-term inflation expectations moved up notably, but measures of longer-term expectations rose only a little and generally stand near levels seen in the years before the pandemic, when inflation was low.

In fact, several measures of longer-term expectations have edged lower over the past couple of months. To me, this means that the public retains confidence that the Fed will be able to rein in inflation in the medium term.

To sum up, while I welcome promising news about inflation, I don't yet see convincing evidence that it is moving meaningfully and persistently down along a trajectory to reach our 2 percent target.

I keep in mind that a year ago we saw similarly promising evidence of inflation moderating for several months before it jumped up to a high and then very high level.

Those earlier inflation readings probably delayed our pivot to tightening monetary policy by a few months.

The consequences of being fooled by a temporary softening in inflation could be even greater now if another misjudgment damages the Fed's credibility.

So, until I see a meaningful and persistent moderation of the rise in core prices, I will support taking significant further steps to tighten monetary policy.

Now let me lay out the implications of this outlook for monetary policy. Since March, the FOMC has raised our policy target range from near zero to between 2-1/4 and 2-1/2 percent.

That puts the upper bound of the current target range at the median of FOMC participants' longer-run projection for the policy rate, as recorded in the June Summary of Economic Projections (SEP).

This long-run rate is effectively where participants think the policy rate would settle when the economy is growing at its potential and inflation is at our 2 percent target.

This is a good definition of success when employment and inflation are near our goals and no help is needed from monetary policy. But that isn't the case now; inflation is far from our goal, so more action is needed.

The policy rate will have to move meaningfully above this neutral level to further restrain aggregate demand and put more downward pressure on prices.

Looking ahead to our next meeting, I support another significant increase in the policy rate. But, looking further out, I can't tell you about the appropriate path of policy. The peak range and how fast we will move there will depend on data we will receive about the economy.

Earlier this year, when we were ending asset purchases, inflation was quite elevated, and we were lifting the target range off the effective lower bound, so it made sense to provide forward guidance to help convey the urgency the FOMC felt about tightening monetary policy.

Forward guidance was useful in helping the public understand how quickly we expected to tighten, and we saw longer-term interest rates move up quite rapidly as a result of these communications. And additional hikes should lead to further restraint in aggregate demand.

As we continue to raise rates, we need to see, month by month, how households and businesses are adjusting to the tighter financial conditions,

and how that adjustment is affecting inflation. We shouldn't be estimating what the peak level of the target range will be and how quickly we will get there, because those details are much more dependent on what new economic data tell us than was the case when the only direction for the federal funds rate to go was up—and up by a lot.

This is not to suggest that I anticipate rate increases stopping very soon. I expect that getting inflation to fall meaningfully and persistently toward our 2 percent target will require increases in the target range for the federal funds rate until at least early next year.

But don't ask me about the policy path because I truly don't know—it will depend on the data.

Six months ago, I would not have thought that we would be where we are today, with inflation so far from our target, after significantly tightening policy with a series of large rate increases and by shrinking the balance sheet.

There are a range of possibilities for how the economy will perform, however, and we can talk about the implications of that range. Say, for example, that inflation follows the path laid out in the June SEP, which has core PCE inflation falling to 4.3 percent in the fourth quarter of 2022 and then moving toward 2 percent over 2023 and 2024. In that case, I would support our policy rate peaking near 4 percent.

But based on the experience of the past year and half, it would be foolish to express great confidence that this plausible path will come to pass. Instead, it is important to consider the range of possibilities and the appropriate policy responses.

For example, if inflation does not moderate or rises further this year, then, in my view, the policy rate will probably need to move well above 4 percent. Alternatively, if inflation suddenly decelerates, then, in my view, the policy rate might peak at less than 4 percent.

One thing that is more predictable and has a significant effect on tightening policy over time is the shrinking of the Fed's holdings of assets as maturing securities run off our balance sheet. Starting this month, the Fed is shedding $60 billion a month in Treasury securities and up to $35 billion a month in agency mortgage-backed securities.

This action effectively increases the supply of securities in the hands of private investors and will thus put upward pressure on interest rates, as private investors must now be enticed to hold these assets.

All told, the FOMC has taken unprecedented and decisive policy actions this year to quickly increase the policy rate in response to high inflation. But where we stand now is not good enough. Though the labor market is strong, inflation is too elevated.

So I support another significant hike in two weeks. After that, the tightening path will continue until we see clear and convincing evidence that inflation is moving meaningfully and persistently down to our 2 percent target.

The pace of tightening is uncertain; it will depend on the data. No matter what, I am ready and willing to do what it takes to bring inflation down.

To read more:
https://www.federalreserve.gov/newsevents/speech/waller20220909a.htm

Number 2

Governors and Heads of Supervision reaffirm expectation to implement Basel III in full and as fast as possible; provide direction on future work on climate-related financial risks and cryptoassets

- The Basel Committee's oversight body reiterates its expectation to implement all aspects of the Basel Framework consistently and as fast as possible.

- Provides direction to the Basel Committee on its work on *climate-related financial risks and cryptoassets*.

- Reviews the Committee's work programme and reaffirms the importance of a stable regulatory framework to facilitate implementation.

The Group of Central Bank Governors and Heads of Supervision (GHOS), the oversight body of the Basel Committee on Banking Supervision, met on 12 September to reaffirm its expectations on implementing Basel III and to provide direction on key areas of work by the Committee.

The resurgence of inflation in many jurisdictions, coupled with a deteriorating macroeconomic outlook and tighter financial conditions, may expose vulnerabilities accumulated in the financial system.

While the global banking system has remained broadly resilient to date, thanks in part to the Basel III reforms implemented after the Great Financial Crisis, GHOS members underlined the importance of banks and supervisors continuing to closely monitor, assess and mitigate emerging risks and vulnerabilities.

The unwinding of public support measures – which were critical in shielding banks from losses over the past two years – places greater importance on the resilience of the banking sector to absorb potential shocks.

Basel III implementation

Against that backdrop, GHOS members took stock of the implementation status of the outstanding Basel III reforms.

These standards, finalised in 2017, seek to strengthen the resilience of bank capital by addressing some of the weaknesses in the regulatory framework that were exposed by the Great Financial Crisis, including by reducing excessive variability in risk-weighted assets and improving the comparability and transparency of banks' risk-based capital ratios.

Addressing these weaknesses remains as important today as it was pre-pandemic.

More than two thirds of jurisdictions plan to implement all, or the majority of, the standards in 2023 or 2024, with the remaining jurisdictions planning to implement Basel III in 2025.

There are only a limited set of technical standards that are particularly subject to an implementation delay.

GHOS members unanimously reaffirmed their expectation of implementing all aspects of the Basel III framework in a full and consistent manner, and as soon as possible, in order to provide a regulatory level playing field for internationally active banks.

These banks should continue preparing for the forthcoming implementation of the standards.

Basel Committee work priorities

The GHOS also reviewed the Committee's work on climate-related financial risks and cryptoassets.

On the former, GHOS members reaffirmed the scope of the Committee's work – which currently focuses on climate-related financial risks – and endorsed the Committee's holistic approach to developing and assessing potential measures related to disclosure, supervision and/or regulation.

On cryptoassets, members reiterated the importance of designing a robust and prudent regulatory framework for banks' exposures to cryptoassets that promotes responsible innovation while preserving financial stability.

The GHOS tasked the Committee with finalising such a framework around the end of this year.

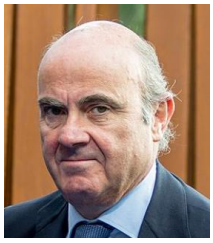
GHOS members also took note of the ongoing work by the Committee to evaluate the impact of Basel III standards already implemented on the resilience and behaviour of the banking system.

Members emphasised the importance of focusing on the implementation of outstanding Basel III reforms before considering any policy or supervisory implications related to findings of the Committee's evaluation work.

Number 3

Euro area current policy challenges

Luis de Guindos, Vice-President of the European Central Bank, at the CIRSF (Research Centre on Regulation and Supervision of the Financial Sector) Annual International Conference 2022 "The future of the EU financial system in a new geo-economic context", Lisbon



I am very pleased to be taking part in this event again and to be back to Lisbon in person.

Following our monetary policy decisions last week, I would like to start with an overview of the euro area economic outlook that underpinned the Governing Council's deliberations. I will then share our assessment of the stability of the euro area financial system at the current juncture – the core focus of today's conference –and outline the ways in which recent economic developments are affecting financial stability in the euro area.

The euro area economic outlook

After the rebound in the first half of 2022, the euro area is now facing a challenging outlook. The economy grew by 0.8% in the second quarter of the year on the back of strong consumer spending on services. Buoyant tourism has been supporting growth also during the third quarter, even as businesses struggle with high energy costs and continued supply bottlenecks. However, we expect output growth to slow down substantially.

The robust consumer demand that came with the loosening of pandemic restrictions will lose steam in the coming months. Global demand is falling and euro area terms of trade have been worsening. Moreover, uncertainty remains high and confidence is falling sharply. Finally, the very high inflation is dampening spending and production, and these headwinds are reinforced by gas supply disruptions.

As a result, the latest ECB staff projections for growth have been revised down markedly, with the euro area economy now set to expand by less than 1% next year. Russia's unjustified aggression towards Ukraine remains the key risk factor for the growth outlook. In a downside scenario reflecting a complete and long-lasting cut-off of Russian gas flows, ECB staff project a recession in 2023.

The slowdown in economic activity is set against a deteriorating inflation outlook. Inflation rose further to 9.1% in August, marking the tenth consecutive month of record-high inflation rates. Energy prices are still the dominant driver of overall inflation. But price pressures have continued to strengthen and broaden, in part owing to the impact of high energy costs across more and more sectors.

Even when excluding food and energy, almost half of the items in the inflation basket have recently recorded annual inflation rates above 4%. While supply bottlenecks have been easing, they continue to gradually feed through to consumer prices. The depreciation of the euro also adds to these inflationary pressures.

These factors also explain the upward revisions to the staff projections for inflation. HICP inflation is projected to be unacceptably high this year and next. Even in 2024, the final year of the projection horizon, inflation is projected to stand at 2.3%, both for headline and core inflation, excluding the more volatile energy and food components.

While most measures of longer-term inflation expectations currently stand at around 2%, they warrant continued monitoring for any signs of material above-target revisions. This is particularly important because the risks to the inflation outlook are primarily on the upside. In the downside scenario with a more severe energy crisis, headline inflation is projected to be even higher, reaching 6.9% next year and 2.7% in 2024.

The ECB's recent monetary policy decisions

This outlook for growth and inflation leaves monetary policymakers with no easy choices. Some might ask why the ECB is normalising its interest rates in the face of an economic slowdown and high inflation that are largely driven by a cost-push shock.

It is true that we are not in a classic demand-driven overheating episode, and that energy remains the dominant driver of rising inflation and slowing growth.

But at the current low level of interest rates, monetary policy is still accommodative, thus supporting demand and ultimately also contributing to price pressures.

With inflation at record-high levels, such an accommodative monetary policy stance is no longer appropriate. Moreover, we need to ensure that inflation expectations remain well anchored until the current shocks have passed so as to facilitate the return of inflation to our medium-term target.

Against this background, we decided to raise interest rates by 0.75 percentage points at our Governing Council meeting last week. This major step frontloaded the transition from a highly accommodative level of policy rates towards levels that will ensure the return of inflation to our 2% medium-term target.

We will regularly re-evaluate our policy path in light of incoming information and the evolving inflation outlook. Our future policy rate decisions will continue to be data-dependent and follow a meeting-by-meeting approach. Importantly, we need to guard against second-round effects such as the risk of a persistent upward shift in inflation expectations.

At the same time, we are carefully monitoring the smooth transmission of our monetary policy stance throughout the euro area. The lasting vulnerabilities caused by the pandemic still pose a risk in this regard. Therefore, we also decided to continue applying flexibility in reinvesting redemptions coming due in the pandemic emergency purchase programme (PEPP) portfolio.

Moreover, our new Transmission Protection Instrument (TPI) is available to counter unwarranted, disorderly market dynamics that pose a serious threat to the transmission of monetary policy across all euro area countries.

Financial stability in the euro area

Turning to the impact on the financial sector, overall financial stability conditions have deteriorated this year.

Rising inflation and the worsened economic outlook in combination with tighter financing conditions are aggravating pre-existing vulnerabilities in both the non-financial and non-bank financial sectors – while in the banking sector profitability is, at least partly, supported by higher interest rates.

Financial markets are vulnerable to changes in expectations about growth and inflation, as well as to changes in the monetary policy outlook.

Tighter financial conditions have already resulted in a significant market correction in the first half of the year amid rising cross-asset correlations, notably between equity and bonds, two segments in which investors suffered the largest losses.

Some market segments are still pricing in rapidly declining inflation and a mild growth slowdown, an assessment which could turn out to be too

benign. In addition, investors do not expect the growth slowdown to significantly challenge corporate solvency or profitability.

Over the next 12 months, corporate earnings are still expected to grow, while speculative-grade default rates are forecasted to pick up only slightly.

But euro area corporates are facing continued headwinds from high input prices, higher borrowing costs and lower sales. Industrial producer price inflation in the euro area exceeded 40% in June.

The resulting margin squeezes could limit firms' debt servicing capacity, particularly in the case of firms that are highly indebted and are still suffering from the repercussions of the pandemic.

Moreover, high input costs affect production, especially for manufacturing firms, whose heavy reliance on natural gas makes them more vulnerable to high energy prices.

Higher inflation is also squeezing households' disposable income. Families have to divert a larger fraction of their income towards everyday consumption, reducing their debt servicing capacity.

As low-income households allocate a higher share of their income to food and energy, they are especially vulnerable to increases in these expenses.

Vulnerabilities in euro area residential real estate markets are also rising in light of continued price increases and vigorous mortgage lending growth.

In the first quarter of 2022 euro area residential real estate price growth stood at 9.8%, the highest nominal growth rate since the early 1990s.

However, since the beginning of the year, household survey responses on the intention to buy a house have declined, and banks have lowered their expectations regarding mortgage loan demand, pointing to a greater potential for house price corrections.

Turning to financial institutions, vulnerabilities in the non-bank financial sector have also increased this year.

The risk that forced selling by investment funds could amplify a market correction remains high, amid low liquidity buffers.

Duration risk has started to materialise and remains elevated, and further bond portfolio revaluation losses may arise in the context of rising yields.

On a better note, systemic vulnerabilities in the banking sector are assessed as moderate. Bank profitability has improved owing partly to higher longer-term interest rates. This should, however, not overshadow rising fragilities related to the worsening macroeconomic outlook.

Higher probabilities of default on corporate exposures and a related increase in provisioning, point to some early signs of higher bank credit risk due to high energy prices.

While the situation is stable overall, with little sign of fragmentation in funding markets, bank funding costs have increased, with weaker banks remaining more vulnerable to further rises in their funding costs.

Before concluding, let me recall the topic of transmission. As already mentioned, flexibility in redemptions coming due in the PEPP portfolio and TPI are important tools for addressing possible fragmentation from the monetary policy side.

But monetary policy would be greatly facilitated if the banking union were complete. The lack of a common deposit insurance scheme remains an obstacle on our pathway towards a genuine Economic and Monetary Union.

Conclusion

A period of heightened uncertainty is here to stay for a while, rendering decision-making more complex.

Output growth is slowing down substantially and is expected to stagnate around year-end and remain low next year at less than 1%, while risks have intensified on the downside.

This is set against a deteriorating inflation outlook with record-high inflation rates expected to stay elevated, well above our target, with risks primarily on the upside.

In this challenging environment, monetary policy needs to walk a fine line to get it right.

The same applies to the policy mix. Complementary actions of fiscal and monetary policy in their respective fields of responsibility were effective during the pandemic and continue to be of the essence in dealing with the current inflation shock.

But the scope and nature of fiscal measures should be different now.

Measures need to be focused, selective and targeted to the most vulnerable firms and households, who are hardest hit by the high inflation levels. Fiscal policy must be designed in a way that does not give rise to inflationary effects.

Monetary policy needs to be focused on price stability and on delivering our inflation target over the medium term. Determined action is essential to keep inflation expectations anchored, which in itself contributes to delivering price stability and avoids second-round effects in inflation.

The main asset that central banks have is credibility, and this asset becomes even more important in times of high uncertainty.

Thank you for your attention.

Number 4

MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone

Microsoft Threat Intelligence Center (MSTIC), Microsoft Detection and Response Team (DART), Microsoft 365 Defender Research Team

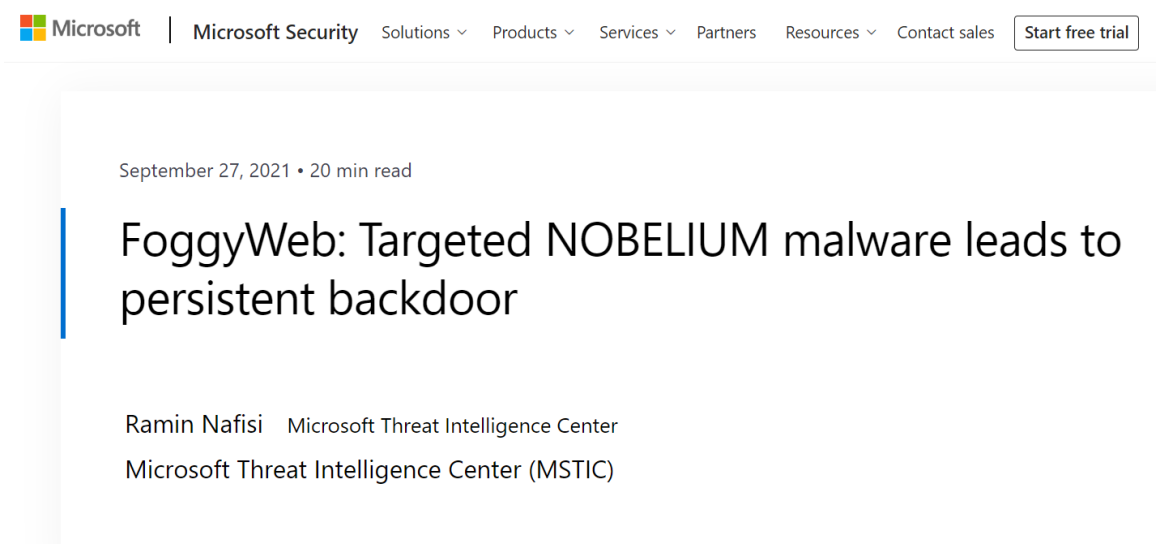
Microsoft

Microsoft security researchers have discovered a post-compromise capability we're calling MagicWeb, which is used by a threat actor we track as NOBELIUM to maintain persistent access to compromised environments.

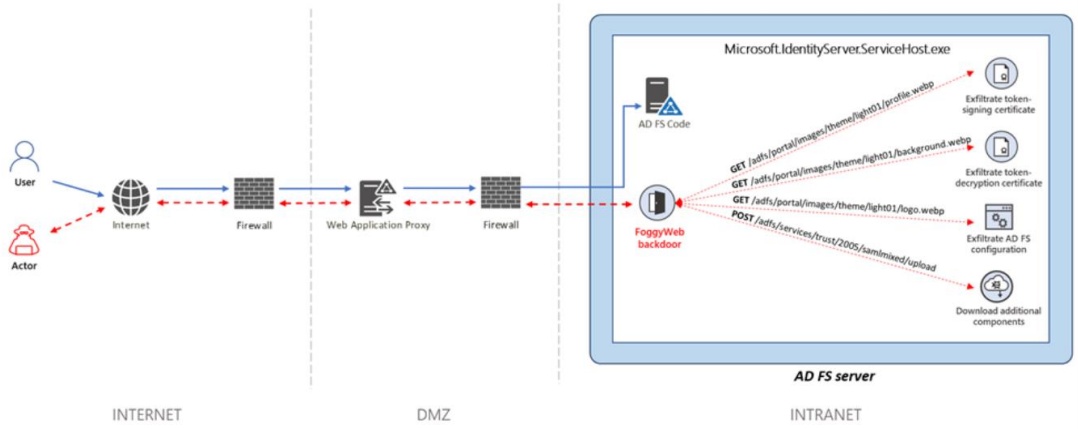
NOBELIUM remains highly active, executing multiple campaigns in parallel targeting government organizations, non-governmental organizations (NGOs), intergovernmental organizations (IGOs), and think tanks across the US, Europe, and Central Asia.

The Microsoft Threat Intelligence Center (MSTIC) assesses that MagicWeb was likely deployed during an ongoing compromise and was leveraged by NOBELIUM possibly to maintain access during strategic remediation steps that could preempt eviction.

NOBELIUM has used abuse of identities and credentialed access as a method for maintaining persistence, and a specialized capability like MagicWeb is not novel for the actor: in September 2021, Microsoft disclosed a post-exploitation capability named FoggyWeb with methods and intent similar to MagicWeb. You may visit: https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/



The diagram below illustrates the methodology used by the actor to communicate with the FoggyWeb backdoor located on a compromised internet-facing AD FS server.



FoggyWeb was capable of exfiltrating the configuration database of compromised AD FS servers, decrypting token-signing certificates and token-decryption certificates, and downloading and executing additional malware components.

MagicWeb goes beyond the collection capabilities of FoggyWeb by facilitating covert access directly.

MagicWeb is a malicious DLL that allows manipulation of the claims passed in tokens generated by an Active Directory Federated Services (AD FS) server.

It manipulates the user authentication certificates used for authentication, not the signing certificates used in attacks like Golden SAML.

NOBELIUM was able to deploy MagicWeb by first gaining access to highly privileged credentials and moving laterally to gain administrative privileges to an AD FS system. This is not a supply chain attack.

The attacker had admin access to the AD FS system and replaced a legitimate DLL with their own malicious DLL, causing malware to be loaded by AD FS instead of the legitimate binary.

The backdoor was discovered by Microsoft's Detection and Response Team (DART) in coordination with MSTIC and Microsoft 365 Defender Research during an ongoing incident response investigation.

Microsoft is sharing this information with consent from the client. At the time of this investigation, MagicWeb appears to be highly targeted.

Like domain controllers, AD FS servers can authenticate users and should therefore be treated with the same high level of security.

Customers can defend against MagicWeb and other backdoors by implementing a holistic security strategy including the AD FS hardening guidance. In the case of this specific discovery, MagicWeb is one step of a much larger intrusion chain that presents unique detection and prevention scenarios.

With all critical infrastructure such as AD FS, it is important to ensure attackers do not gain administrative access.

Once attackers gain administrative access, they have many options for further system compromise, activity obfuscation, and persistence.

We recommend that any such infrastructure is isolated, accessible only by dedicated admin accounts, and regularly monitored for any changes.

Other security measures that can prevent this and other attacks include credential hygiene to prevent lateral movement. AD FS is an on-premises server, and as with all on-premises servers, deployments can get out of date and/or go unpatched, and they can be impacted by local environment compromises and lateral movement.

For these reasons, migration to a cloud-based identity solution such as Azure Active Directory for federated authentication is recommended for the robust security it provides.

See the mitigation section below for more information.

Though we assess the capability to be in limited use, Microsoft anticipates that other actors could adopt similar methodologies and therefore recommends customers review hardening and mitigation guidance provided in this blog.

How MagicWeb subverts authentication

MagicWeb is a post-compromise malware that can only be deployed by a threat actor after gaining highly privileged access to an environment and moving laterally to an AD FS server.

To achieve their goal of maintaining persistent access to an environment by validating authentication for any user account on the AD FS server, NOBELIUM created a backdoored DLL by copying the legitimate Microsoft.IdentityServer.Diagnostics.dll file used in AD FS operations.

The legitimate version of this file is catalog signed by Microsoft and is normally loaded by the AD FS server at startup to provide debugging capabilities. NOBELIUM's backdoored version of the file is unsigned.

The threat actor's highly privileged access that allowed them to access the AD FS server meant they could have performed any number of actions in the environment, but they specifically chose to target an AD FS server to facilitate their goals of persistence and information theft during their operations.

After gaining administrative access to an AD FS server via elevation of privilege and lateral movement, the loading of NOBELIUM's malicious Microsoft.IdentityServer.

To read more:
https://www.microsoft.com/security/blog/2022/08/24/magicweb-nobeliums-post-compromise-trick-to-authenticate-as-anyone/

Number 5

Agencies reaffirm commitment to Basel III standards

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency

Federal bank regulatory agencies reaffirmed their commitment to implementing enhanced regulatory capital requirements that align with the final set of "Basel III" standards issued by the Basel Committee on Banking Supervision in December 2017. The implementation of these standards for large banking organizations would strengthen the resilience of the domestic banking system and is a priority for the agencies.

Strong capital requirements have proven to be a critical element of the bank regulatory framework, allowing the banking industry during times of economic stress to serve as a source of strength for the U.S. economy and to lend to creditworthy households and businesses.

The agencies plan to seek public input on the new capital standards for large banking organizations and are **currently developing a joint proposed rule** for issuance as soon as possible. Community banking organizations, which are subject to different capital requirements, would not be impacted by the proposal.

Number 6

ESAs warn of rising risks amid a deteriorating economic outlook

The three European Supervisory Authorities (EBA, EIOPA and ESMA - ESAs) issued today their Autumn 2022 joint risk report.

JOINT COMMITTEE REPORT ON
RISKS AND VULNERABILITIES IN THE EU FINANCIAL SYSTEM
SEPTEMBER 2022

The report highlights that the deteriorating economic outlook, high inflation and rising energy prices have increased vulnerabilities across the financial sectors.

The ESAs advise national supervisors, financial institutions and market participants to prepare for challenges ahead.

The post-pandemic economic recovery in Europe has dwindled as a result of the Russian invasion of Ukraine.

Russia's war on Ukraine and the disruptions in trade caused a rapid deterioration of the economic outlook.

It adds to pre-existing inflationary pressures by strongly raising energy- and commodity prices, exacerbates imbalances in supply and demand, and weakens the purchasing power of households.

The risk of persistent inflation and stagflation has risen.

These factors, coupled with the deteriorated economic outlook, have significantly impacted the risk environment of the financial sector.

Financial market volatility has increased across the board given high uncertainties.

After a long period of low interest rates, central banks are tightening monetary policy.

The combination of higher financing costs and lower economic output may put pressure on government, corporate and household debt refinancing while also negatively impacting the credit quality of financial institutions' loan portfolios.

The reduction of real returns through higher inflation could lead investors to higher risk-taking at a time when rate rises are setting in motion a far-reaching rebalancing of portfolios.

Financial institutions also face increased operational challenges associated with heightened cyber risks and the implementation of sanctions against Russia.

The financial system has to date been resilient despite the increasing political and economic uncertainty.

In light of the above risks and vulnerabilities, the Joint Committee of the ESAs advises national competent authorities, financial institutions and market participants to take the following policy actions:

Financial institutions and supervisors should continue to be prepared for a deterioration in asset quality in the financial sector and monitor developments including in assets that benefitted from temporary measures related to the pandemic and those that are particularly vulnerable to a deteriorating economic environment, to inflation as well as to high energy and commodity prices.

The impact of further increases in policy rates and of potential sudden increases in risk premia on financial institutions and market participants at large should be closely monitored.

Financial institutions and supervisors should closely monitor the impact of inflation risks.

Supervisors should continue to monitor risks to retail investors, in particular with regard to products where consumers may not fully realise the extent of the risks involved, such as crypto-assets.

Financial institutions and supervisors should continue to carefully manage environmental risks and cyber risks to address threats to information security and business continuity.

The report:
https://www.eiopa.europa.eu/document-library/report/joint-committee-report-risks-and-vulnerabilities-eu-financial-system-1_en

Number 7

BIS Working Paper No 1039

Cyber risk in central banking

by Sebastian Doerr, Leonardo Gambacorta, Thomas Leach, Bertrand Legros and David Whyte - Monetary and Economic Department

BIS

The rising number of cyber attacks in the financial sector poses a threat to financial stability and makes cyber risk a key concern for policy makers.

This paper presents the results of a survey among members of the Global Cyber Resilience Group on cyber risk and its challenges for central banks.

The survey reveals that central banks have notably increased their cyber security-related investments since 2020, giving technical security control and resiliency priority.

Central banks see phishing and social engineering as the most common methods of attack, and the potential losses from a systemically relevant cyber attack are deemed to be large, especially if the target is a big tech providing critical cloud infrastructures.

Generally, respondents judge the preparedness of the financial sector for cyber attacks to be inadequate. While central banks in most emerging market economies provide a framework for the collection of information on cyber attacks on financial institutions, less than half of those in advanced economies do.

Cooperation among public authorities, especially in the international context, could improve central banks' ability to respond to cyber attacks.

The survey reveals four main insights.

First, central banks from AEs and EMEs differ in their assessment of the frequency and cost of different cyber attacks. All central banks deem phishing and other forms of social engineering as the most likely type of attack vectors. AE central banks are significantly more worried about supply chain attacks than their EME counterparts.

When it comes to the costs resulting from an attack, advanced persistent malware and ransomware attacks rank highest. Turning to the who of these attacks, AE central banks deem organised crime and state-sponsored entities to be the main perpetrators. Among EME central banks, it is organised crime and individuals or activists.

Second, central banks actively discuss and develop policy responses to cyber attacks and have increased their cyber security-related investments notably since 2020.

Technical security control and resiliency feature high on the priority list in terms of areas for investment in cyber security.

Training existing staff on cyber security or hiring new staff with the relevant skills are also considered important, especially among EME central banks. Beyond investments, central banks focus on developing concrete policy responses.

All central banks put a high focus on developing an incident response plan in case their own institution is attacked, and several central banks are also developing a formal strategy for responding to an attack on the financial system at large.

All central banks run internal exercises to simulate cyber attacks, and the most frequently modelled scenarios are an attack on the system of the central bank itself, as well as an outage of the payments system or other critical FMI.

While supervisory authorities in most EMEs provide a framework for the collection of information on cyber attacks on financial institutions, less than half of those in AEs do.

Similarly, while supervised firms are mandated to report losses related to cyber attacks to the central bank in almost all EMEs, only two-thirds of AE respondents report that such disclosure is required.

No jurisdiction requires firms to disclose such losses publicly, however.

Third, central banks deem the potential losses from a systemically relevant cyber attack to be large, and think that losses from cyber attacks in the financial sector have increased over the past year.

Only a few central banks fully agree that the financial sector is adequately prepared for cyber attacks, and over half of the respondents think that investment in cyber security has been inadequate over the past year.

Beyond traditional financial institutions, respondents reported that they see fintechs to be more at risk from a cyber attack than big techs, even though most respondents agree that a successful attack on a big tech would lead to materially higher aggregate costs than an attack on a fintech.

And **fourth,** central banks in AEs and EMEs already cooperate widely on a range of topics. Bilateral cooperation among central banks, as well as cooperation in bodies at the regional and global levels, is the norm.

When it comes to specific topics related to cooperation, information sharing, simulations and policy formulations to improve cyber resilience stand out in AEs. Among EMEs, central banks frequently cooperate in the realms of information sharing and policy formations.

In addition, over two-thirds of respondents develop common standards and protocols for the financial sector.

The BIS supports central banks' cyber security work, as well as global cooperation in this domain, in several ways – for example, through its Cyber Resilience Coordination Centre or projects of the BIS Innovation Hub.

To read more: https://www.bis.org/publ/work1039.pdf

Number 8

Consultation outcome

Proposals for new telecoms security regulations and code of practice - government response to public consultation

GOV.UK

"This government has been clear in its ambition to make the United Kingdom a world leader in digital connectivity. Over 69% of the country has access to gigabit-capable broadband, and the government's ambition for the majority of the population to have access to a 5G signal by 2027 has been delivered five years early.

But we know that today the security and resilience of our communications networks and services is more important than ever. From heightened geopolitical threats through to malicious cyber criminals exploiting network vulnerabilities, global events have shown the importance of providing world-leading security for our networks and services.

That's why the creation of a new telecoms security framework via the Telecommunications (Security) Act 2021 was so important. With the help of the telecoms industry, we've now been able to move that framework forwards.

In March 2022 we launched a ten-week public consultation on drafts of the Electronic Communications (Security Measures) Regulations and Telecommunications Security Code of Practice that will form the central part of the new security framework.

The consultation enabled individuals and organisations to share their views on the drafts with us. It has also enabled the government to finalise the drafts, taking into account those views, to create a security framework to identify and address risks to the UK's public telecoms networks and services both today and in the future.

This government response sets out the changes we have made to the draft regulations and code of practice to ensure they are appropriate and proportionate ahead of the planned commencement of the new framework in October 2022.

I want to thank all of those who responded to the consultation for sharing their views and insights, drawing upon their extensive knowledge and experience. We have taken into account the range of views provided by respondents, which have been vital in developing the documents. Now is

the right time to put those final parts of the security framework in place, and defend the public networks and services that we all rely on."

Matt Warman MP
Minister of State for Digital, Culture, Media and Sport

Executive summary

The UK is becoming ever more dependent on public telecoms networks and services. The increased reliance of the economy, society and critical national infrastructure (CNI) on such networks and services means it is important to have confidence in their security.

As the value of our connectivity increases, it becomes a more attractive target for attackers. It is important to make sure that our networks and services are secure in this evolving threat landscape.

To protect the UK's public telecoms networks and services against security compromises, the government introduced the Telecommunications (Security) Act 2021. It provides the government with new powers to make regulations that place specific security obligations on the providers of public telecoms networks and services. The Act also enables the government to issue codes of practice containing guidance on how to meet those obligations.

The government held a public consultation on the draft Electronic Communications (Security Measures) Regulations and a draft code of practice between 1 March and 10 May 2022. We sought views on the security requirements set out in the draft regulations and the guidance measures within the draft code of practice.

We also asked for views on a proposed system of 'tiering' and implementation timeframes, which are intended to help ensure the measures are implemented appropriately and proportionately depending on the nature of the provider. Finally, we sought views on the security measures that should be applied to legacy equipment within telecoms networks.

There were 38 responses to the consultation, from public telecoms providers, industry trade bodies, telecoms suppliers, and interested stakeholders from the wider telecoms and technology industry. The responses have all been recorded and analysed by the government. A significant number of the responses focussed on the approach to phasing-in new measures in the draft code of practice, with many suggesting that implementation timeframes should be pushed back for larger ('Tier 1')

providers to align with smaller ('Tier 2') providers. Other responses focussed on specific measures in the draft regulations and draft code of practice, including those related to privileged access workstations, national resilience, legacy networks and relationships with suppliers.

This document sets out the government's response to the views raised in the consultation. It explains how we have considered those views, and where appropriate, taken them into account to revise the draft regulations and draft code of practice. For example, in light of the feedback we received, we have altered the implementation timeframes for Tier 1 providers. We have also made changes to those security measures relating to national resilience, legacy networks and the supply chain.

The government will shortly lay the Electronic Communications (Security Measures) Regulations 2022 and accompanying draft Telecommunications Security Code of Practice in Parliament. These versions will reflect changes made by the government in light of the consultation responses it received.

Introduction

Context

The UK's future prosperity rests on the security and resilience of the public electronic communications networks and services that connect us. Yet as technologies evolve, new threats to those networks and services are emerging. Cyber hackers are now capable of threatening communications worldwide, as the cost barriers to mass-scale disruption continue to fall.

Countering state threats is a high priority, with greater competition and aggression in cyberspace by countries such as Russia, China, Iran and North Korea. Actors may seek to exploit weaknesses in telecoms equipment, network architecture and/or operational practices, in order to compromise security.

We are becoming ever more dependent on telecoms as the speed and scale of networks and services develop. The increased reliance of our economy, society and critical national infrastructure (CNI) on telecoms means we need to have confidence in its security.

Without effective telecoms security, disruption due to cyber attacks will continue to grow, including the potential for connectivity compromises and outages that could be catastrophic.

The Telecommunications (Security) Act 2021 amends the Communications Act 2003 ('the Act') to introduce new duties on providers of public

electronic communications networks and services (hereafter referred to as 'providers') to identify and reduce the risk of security compromises, and prepare for the possibility of their occurrence (s.105A). The Act also places duties on providers to prevent, remedy or mitigate any adverse effects of security compromises (s.105C). These overarching security duties are intended to provide an effective and enduring basis for protecting UK public telecoms networks and services.

In addition, the Act provides the government with new powers to make regulations (s.105B and 105D) and issue codes of practice (s.105E). The regulations set out specific security measures in secondary legislation, indicating where providers must focus their efforts to secure their public networks and services. Codes of practice provide detailed technical guidance measures to demonstrate how providers can meet their legal obligations.

The Electronic Communications (Security) Measures Regulations 2022 ('the regulations') and the associated Telecommunications Security Code of Practice will be the first use of these powers. Their development has been informed by advice provided by the National Cyber Security Centre (NCSC), Ofcom and industry.

Draft versions of the regulations and code have been subject to public consultation to ensure that the measures they contain to improve the security of public networks and services are appropriate and proportionate to implement.

Ofcom will take on new responsibilities for monitoring and enforcing compliance with the Act and the regulations. In doing so, it will take into account the guidance measures within the code of practice. How Ofcom intends to meet its new duties and exercise its powers and functions are set out in Ofcom's draft procedural guidance, which has also been subject to consultation.

The government and Ofcom recognise that improving the security of UK networks and services is a shared endeavour, and Ofcom will seek to work closely with public telecoms providers to meet the objectives of the new security framework.

The consultation

The public consultation on the draft Electronic Communications (Security Measures) Regulations and the associated draft code of practice took place from 1 March to 10 May 2022, and sought views on the following four areas in particular:

- the government's proposed approach to securing public electronic communications networks and services as set out in the draft regulations and guidance measures in the draft code of practice

- the tiering system set out in Section 1 of the draft code of practice, which was proposed to ensure the guidance measures are implemented appropriately and proportionately depending on the nature of the provider

- the approach to phasing-in new measures in the draft code of practice, so that the recommended implementation timeframes for individual measures set out in the code account for both security imperatives and proportionate delivery

- the ways in which measures in the draft code of practice and the draft regulations account for legacy equipment due to be phased out, so that investment in security improvements is distributed appropriately

There were 38 responses to the consultation, including from public telecoms providers, industry trade bodies, and telecoms suppliers. A list of the organisations that responded can be found in Annex B. All responses to the consultation we received have been considered by the government.

This document sets out:

- the views expressed in those responses, drawing out common themes and points of particular concern to respondents

- the government's response to those views, including the changes it has subsequently made to the regulations and draft code of practice, as well as its justification for not making some of the changes that were proposed

- next steps that will be taken to finalise the regulations and code of practice

Responses

The consultation on the draft regulations and draft code of practice received responses from public telecoms providers, their suppliers, industry trade bodies, and interested stakeholders from the wider telecoms and technology industry. A greater proportion of responses were received from larger providers, with relatively few from smaller providers.

Most respondents either answered the specific questions contained within the consultation document, or expressed views in relation to the four areas upon which those questions focused. This section is therefore structured in a similar manner:

- Part 1 focuses on responses to proposals in the draft regulations and code of practice for securing networks and services

- Part 2 focuses on responses to the government's proposed approach in the code of practice to determining the tiering of providers

- Part 3 focuses on responses to the government's proposed implementation timeframes for measures set out in the draft code of practice

- Part 4 focuses on responses to the government's proposed approach in the code for securing legacy networks and services in the draft code of practice

In each Part, context is provided on the government's specific proposals in the draft regulations and code of practice, information is provided on the views we received from respondents, and the government's response to those views is set out.

to read more:
https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice/outcome/proposals-for-new-telecoms-security-regulations-and-code-of-practice-government-response-to-public-consultation

Number 9

NIST and Google to Create New Supply of Chips for Researchers and Tech Startups

Cooperative research agreement aims to unleash innovation in the semiconductor and nanotechnology industries.

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

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has signed a cooperative research and development agreement with Google to develop and produce chips that researchers can use to develop new nanotechnology and semiconductor devices.

The chips will be manufactured by SkyWater Technology at its Bloomington, Minnesota, semiconductor foundry.

Google will pay the initial cost of setting up production and will subsidize the first production run. NIST, with university research partners, will design the circuitry for the chips. The circuit designs will be open source, allowing academic and small business researchers to use the chips without restriction or licensing fees.

Large companies that design and manufacture semiconductors often have ready access to these types of chips. But the cost can run into the hundreds of thousands of dollars, presenting a major hurdle to innovation by university and startup researchers. By increasing production to achieve economies of scale and by implementing a legal framework that eliminates licensing fees, the collaboration is expected to bring the cost of these chips down dramatically.

"By creating a new and affordable domestic supply of chips for research and development, this collaboration aims to unleash the innovative potential of researchers and startups across the nation," said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio. This collaboration was planned before the recent passage of the CHIPS Act, but, Locascio said, "This is a great example of how government, industry and academic researchers can work together to enhance U.S. leadership in this critically important industry."

Modern microelectronic devices are made of components that are stacked like layers in a cake, with the bottom layer being a semiconductor chip. The NIST/Google collaboration will make available a bottom-layer chip with specialized structures for measuring and testing the performance of the components placed on top of it, including new kinds of memory devices,

nanosensors, bioelectronics and advanced devices needed for artificial intelligence and quantum computing.

NIST anticipates designing as many as 40 different chips optimized for different applications. Because the chip designs will be open source, researchers will be able to pursue new ideas without restriction and share data and device designs freely.

"Google has a long history of leadership in open-source," said Will Grannis, CEO of Google Public Sector. "Moving to an open-source framework fosters reproducibility, which helps researchers from public and private institutions iterate on each other's work. It also democratizes innovation in nanotechnology and semiconductor research."

The SkyWater foundry will produce the chips in the form of 200-millimeter discs of patterned silicon, called wafers, which universities and other purchasers can dice into thousands of individual chips at their own processing facilities.

The 200mm wafer is an industry standard format compatible with the manufacturing robots at most semiconductor foundries. Giving researchers access to chips in this format will allow them to prototype designs and emerging technologies that, if successful, can be integrated into production more quickly, thus speeding the transfer of technology from lab to market.

Research partners contributing to the chip designs include the University of Michigan, the University of Maryland, George Washington University, Brown University and Carnegie Mellon University.

Number 10

Revolutionizing Infrared Sensing Could Transform Imaging Applications

New DARPA program seeks to enable quantum-level IR detection at room temperature

The infrared (IR) spectrum is a vast information landscape that modern IR detectors tap into for diverse applications such as night vision, biochemical spectroscopy, microelectronics design, and climate science. But modern sensors used in these practical areas lack spectral selectivity and must filter out noise, limiting their performance.

Advanced IR sensors can achieve ultrasensitive, single-photon level detection, but these sensors must be cryogenically cooled to 4 K (-269 C) and require large, bulky power sources making them too expensive and impractical for everyday Department of Defense or commercial use.

DARPA's Optomechanical Thermal Imaging (OpTIm) program aims to develop novel, compact, and room-temperature IR sensors with quantum-level performance – bridging the performance gap between limited capability uncooled thermal detectors and high-performance cryogenically cooled photodetectors.

"If researchers can meet the program's metrics, we will enable IR detection with orders-of-magnitude improvements in sensitivity, spectral control, and response time over current room-temperature IR devices," said Mukund Vengalattore, OpTIm program manager in DARPA's Defense Sciences Office.

"Achieving quantum-level sensitivity in room-temperature, compact IR sensors would transform battlefield surveillance, night vision, and terrestrial and space imaging. It would also enable a host of commercial applications including infrared spectroscopy for non-invasive cancer diagnosis, highly accurate and immediate pathogen detection from a person's breath or in the air, and pre-disease detection of threats to agriculture and foliage health."

The key to potentially realizing this giant technological leap in IR sensing comes from the synergy of combining the best aspects of three sensor paradigms: First, optomechanical resonators – tiny trampoline-like structures – offer a high isolation, ultrasensitive platform; second, all-optical detectors yield low-noise, quantum-level detection; and third,

designer metamaterials with spectrally selective “made-to-order” IR absorption allow for extremely precise detection of desired wavelengths.

“Trying to enhance IR sensing capabilities using any one of those methods by itself would be hard, but not too hard,” Vengalattore said. “What makes OpTIm such an incredibly difficult challenge, with revolutionary impact if we’re successful, is combining all three.

We are not looking to merely augment existing IR detection modalities with evolutionary improvements in signal readout, noise mitigation, or spectral selectivity. What makes this program exciting from a scientific perspective and an application-oriented perspective is that OpTIm seeks to bring together innovative solutions at the confluence of optomechanics, materials physics, photonics, and metrology to take a fresh look at an old problem.

At the end of the day, for all the applications that spring to mind with the projected capabilities of OpTIm-based detectors, there are probably many more applications that we haven’t yet imagined that will be engendered by this new regime of IR detection.”

OpTIm is a 60-month program broken into two 30-month phases where teams will aim to validate, characterize, and benchmark this new class of optomechanical IR detectors.

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,

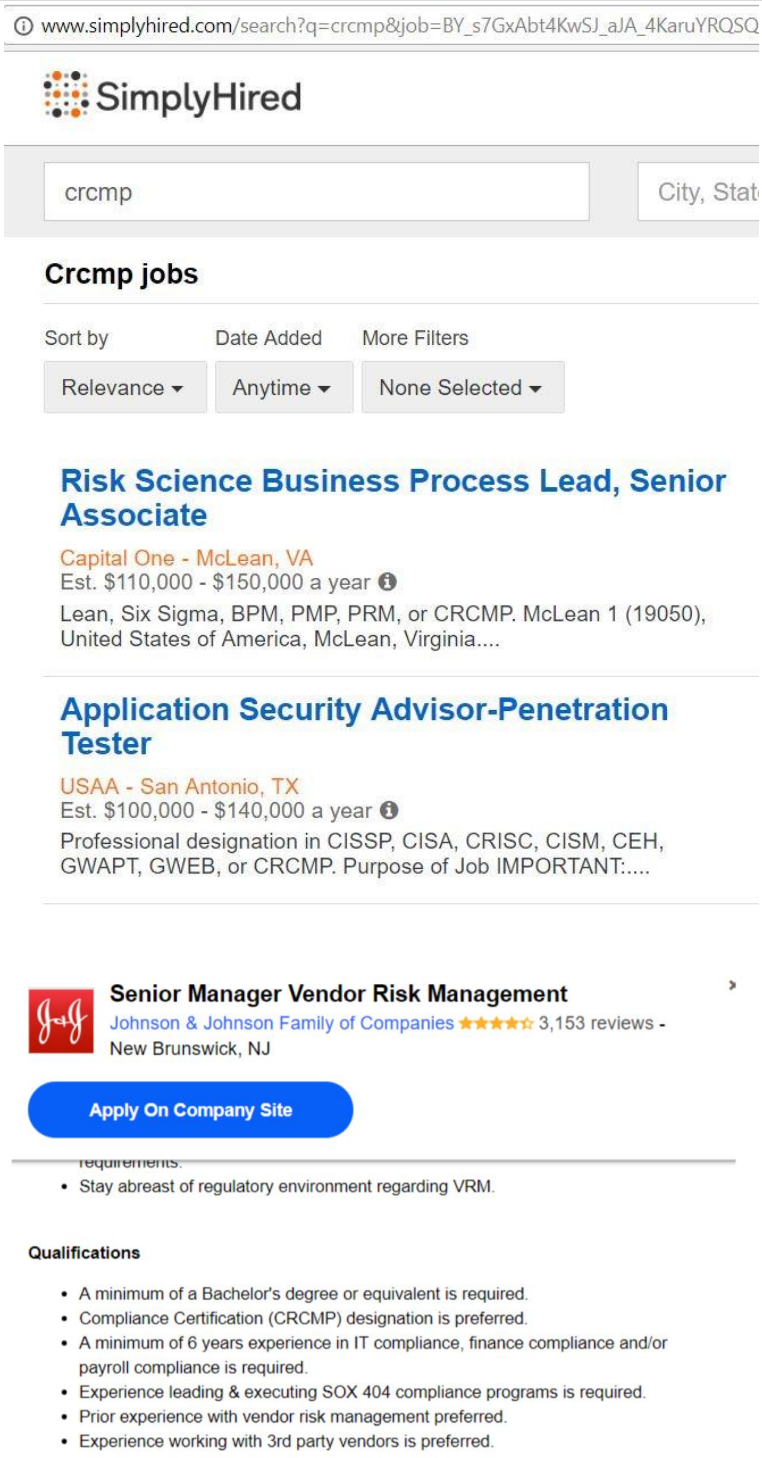
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- 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.