Discuss why Cyber Security is now a global issue and why it is important for companies to invest in Cyber Security.

COVID-19 , globalisation and digital transformation caused a paradigm shift with regards to the type of cyber threats reported. Industrialisation and globalisation is at its peak and inversely had an incremental effect on loss of production. The industries that experienced an increase in attacks was technology, telecommunications, transport ,manufacturing and distribution sector. It has become critical to preserve confidential information and data integrity. Geo-political tensions have increased supply chain disruptions, which negatively affect economies due to costs involved in avoidance, mitigating and corrective actions.

Despite the physical Russian-Ukraine invasion occurring in 2022, the cyber invasion had long been brewing behind the scenes as early as 2016. Russian covert cyber operations have been targeting Ukraine's infrastructure, financial and energy sector. As a result businesses have suffered greatly due to import/export operations and enforced economic sanctions which trickle over to global economies.

Russian forces are still conducting global cyber influencing operations to garner support. To offset and counteract these operations, cyber agencies have started using AI to track and forecast cyber threats. These countermeasures come at a significant cost and have increased cyber insurance rates.

Reports estimate that close to $600 billion, nearly 1% of the global GDP, is lost to cyber-crime annually. This makes cybercrime a very lucrative business. Unlike other forms of crime, it has the ability to impact a higher population than any other type of

crime and the risk profile to payoff ratio is lower. The increase in availability of digital currency has also made it easier for criminals to be untraceable.

International cyber law enforcement cooperation between countries and the robust adoption of pragmatic orientated approaches will see the cost of cyber-crime reducing. The question is will we be able to stay abreast of the criminals?

Nomusa you made good point. Following Russia's attack on Ukraine, the National Cyber Security Centre continues to call on organisations in the UK to bolster their online defences. (Gov.uk, 2022)

The invasion occurs when the pandemic is at its lowest point and people are tired and looking for normalcy. Since so much work is now done online, any disruption to communication networks puts employee productivity in jeopardy. Supply chains are having trouble recovering and will have much greater trouble as a result of restrictions and regional limitations. (Ministry of Defence, 2013)

The production of microchips, which has had trouble keeping up with demand, will suffer from a drop in the supply of raw materials like neon gas and palladium, both of which are largely obtained from Russia. Inflationary pressures will increase across the board, from grocery stores to server rooms, as gas prices climb amid an increasing likelihood of stagflation. Of course, the threat of cyberattacks is still quite real on a global scale.

While the NCSC is not aware of any specific threats that are now posed to UK organisations as a result of events in and around Ukraine, there has been a pattern of cyberattacks against Ukraine in the past that have had an impact on other countries. The wiper software known as HermeticWiper, which is employed against Ukrainian organisations, may also have an effect on organisations abroad. A PC with wiper malware can delete data from the hard disc.

As mention Nomusa 'The question is will we be able to stay abreast of the criminals?'

UK nuclear power and the NHS are being warned of a Russian cyberattack. In response to the economic crisis, the Russian government's hackers are allegedly attempting to engage in "malicious cyber activities." (the Guardian, 2022)

The Russia-Ukraine conflict has triggered turmoil in the financial markets, and drastically increased uncertainty about the recovery of the global economy. Since our last publication, the world has shifted, so have the risks.

- Higher commodity prices intensify the threat of long-lasting high inflation which increases the risks of stagflation and social unrest.
- Certain sectors such as automotive, transport or chemicals are more likely to suffer.

- Coface forecasts a deep recession of 7.5% for the Russian economy in 2022 and downgraded Russia's risk assessment to D (very high).
- European economies are most at risk: at the time of writing, Coface estimates at least 1.5 percentage point of additional inflation in 2022, while GDP growth could be lowered by 1 percentage point. Together with a complete cut of Russian natural gas supply, this could cost at least 4 points of GDP, thereby leading EU GDP growth close to zero – more probably in negative territory – in 2022.

Russia is the world's 3rd oil producer, the 2nd natural gas producer and among the top 5 producers of steel, nickel and aluminum. It is also the largest wheat exporter in the world (almost 20% of global trade). On its side, Ukraine is a key producer of corn (6th largest), wheat (7th), sunflowers (1st), and is amongst the top ten producers for sugar beet, barley, soya and rapeseed.

On the day the invasion began, financial markets around the world fell sharply, and the prices of oil, natural gas, metals and food commodities surged. Following the latest developments, Brent oil prices breached USD 100 per barrel for the first time since 2014 (125$/b at the time of writing), while Europe's TTF gas prices surged at a record EUR 192 on 4 March.

While high commodity prices were one of the risks already identified as potentially disruptive to the recovery, the escalation of the conflict increases the likelihood that commodity prices will remain higher for much longer. In turn, it intensifies the threat of long-lasting high inflation, thereby increasing the risks of stagflation & social unrest in both advanced & emerging countries.

The Russian economy will be in great difficulty in 2022, falling into deep recession. Coface's updated GDP forecast for 2022 stands at -7.5% after the recovery experienced last year. **This has lead us to downgrade the country's risk assessment** from B (fairly high) to D (very high).

Sanctions notably targets major Russian banks, the Russian central bank's, the Russian sovereign debt, selected Russian public officials & oligarchs, and the export control of high-tech components to Russia. These measures put considerable downward pressure on the Russian ruble, which has already plummeted, and will drive a surge in consumer price inflation.

Russia has built up relatively strong financials: a low level of public external debt, a recurrent current account surplus, as well as substantial foreign reserves (app. USD 640 bn). However, the freeze imposed by western depositary countries on the latter prevents the Russian central bank from deploying them and reduces the effectiveness of the Russian response.

The Russian economy could benefit from higher prices for commodities, especially for its energy exports. However, EU countries announced their intention to limit their imports from Russia. In the industrial sector, restricted access to Western-produced semiconductors, computers, telecommunications, automation, and information security equipment will be harmful, given the importance of these inputs in the Russian mining and manufacturing sectors.

EUROPEAN ECONOMIES ARE THE MOST AT RISK

Because of its dependence on Russian oil & natural gas, Europe appears to be the region most exposed to the consequences of this conflict. Replacing all Russian natural gas supply to Europe is impossible in the short to medium run and current price levels will have a significant effect on inflation. At the time of writing, with the barrel of Brent trading above 125$ and natural gas futures suggesting prices durably above 150€/Mwh, **Coface estimates at least 1.5 percentage point of additional inflation in 2022 which would erode household consumption and, together with the expected fall in business investment and exports, lower GDP growth by approximately one percentage point.**

While Germany, Italy or some countries in the Central and Eastern European region are more dependent on Russian natural gas, the trade interdependence of Eurozone countries suggests a general slowdown.

On top of that, we estimate that a complete cut of Russian natural gas flows to Europe would raise the cost to 4 percentage points in 2022, which would be bring annual GDP growth close to zero, more probably in negative territory – depending on demand destruction management.

For oil: • An adjustable import tax (or tariff) designed to transfer funds away from Russian or Belarus exporters; • A special escrow account to hold net proceeds due to exporters; • Sanctions against material-service providers enabling seaborne exports to non-EU consumers. For gas: • Require that the sales of Russian gas to Europe be channelled through the Ukrainiantransmission system (see here); • Impose a levy on Gazprom for sales into the EU and retain the payments in an escrow account; • Cease purchases of Russian gas from the least dependent countries; and • Support Ukrainian reconstruction through a levy imposed on Gazprom (see further down this briefing on financing Ukraine).

Russia- Crude Oil

Ukraine -steel

https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Andrew, James, and Kenneth Geers. "'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine." *Cyber war in perspective: Russian aggression against Ukraine*. NATO CCDCOE, 2015. 39-48.

Lange-Ionatamishvili, E., Svetoka, S. and Geers, K., 2015. Strategic communications and social media in the Russia Ukraine conflict. *Cyber war in perspective: Russian aggression against Ukraine*, pp.103-111.

Cisco. (2017). *Annual cybersecurity report.* San Jose, CA. Retrieved from http://www.cisco.com/c/en/us/products/security/security-reports.html

P.S, Seemma & Sundaresan, Nandhini & M, Sowmiya. (2018). Overview of Cyber

Security. IJARCCE. 7. 125-128. 10.17148/IJARCCE.2018.71127.

Mathew Schwartz, “How Do We Catch Cybercrime Kingpins,” Data Breach Today, 2015

Europol, “Internet Organised Crime Threat Assessment 2017,” 2017

(Jacob Dadzie, 4 July 2022)

Reference List Dadzie, J. (2022) Peer response by Jacob Dadzie, 4 July.

List Walters, F. (2018) Conversation with John Stephens, 13 August.

GOV.UK. 2022. Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion. [online] Available at: [Accessed 6 July 2022].

The Guardian. 2022. UK firms warned over possible Russian cyber-attacks amid Ukraine crisis. [online] Available at: [Accessed 3 July 2022]

Davis, K. (May 23, 2018) Economic Consequences Of The Russia-Ukraine Conflict: Stagflation Ahead. Forbes. Available from: https://www.coface.com/News-Publications/News/Economic-consequences-of-the-Russia-Ukraine-conflict-Stagflation-ahead [Accessed 06 July 2022].

D. Winkler & L. Wuester: Implications of Russia’s invasion of Ukraine for its value chains (11 May 2022)