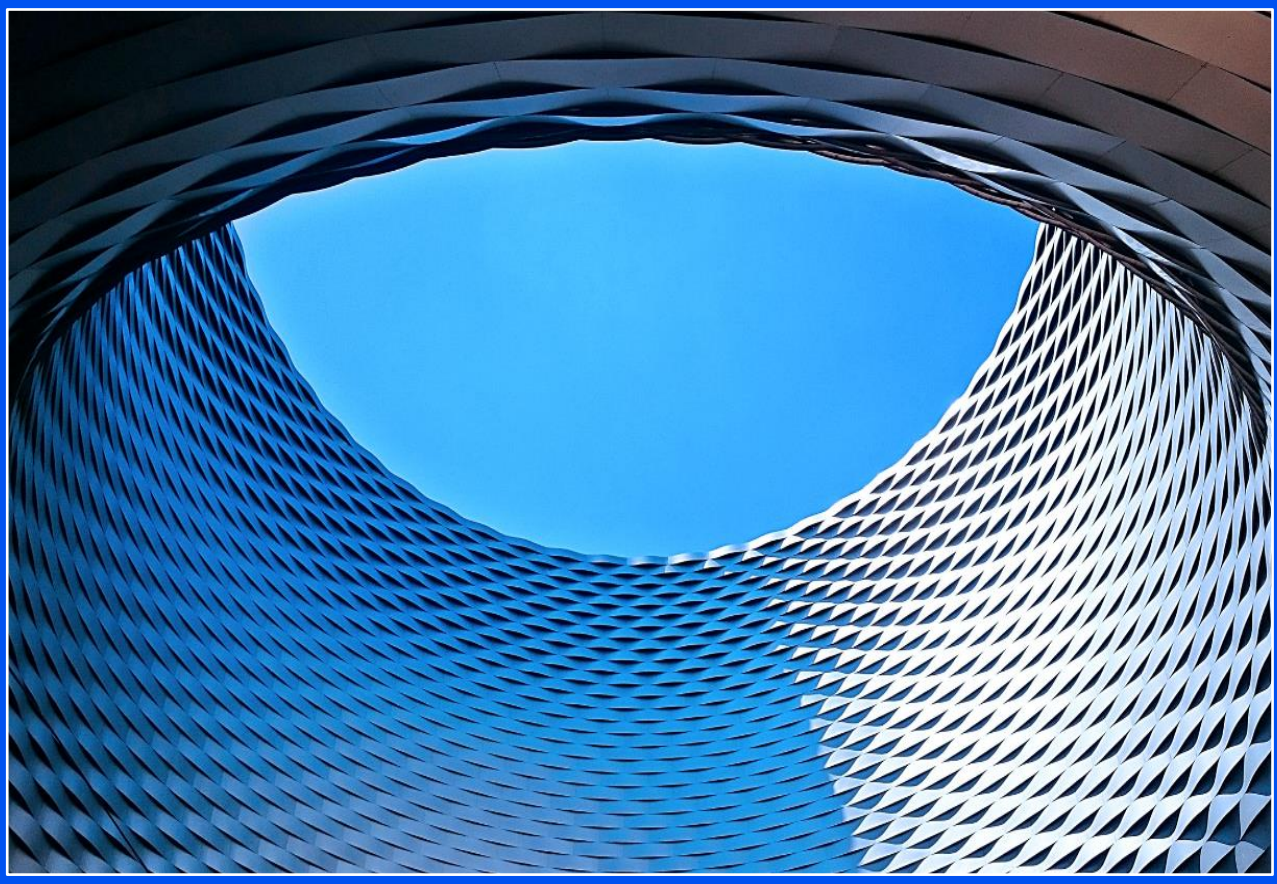
European Risk Management Council

Risk Landscape Review

March 2021



- Operational Resilience and Cyber Integrity
- UK Risk Sentiment Index: Q1 2021 Update
- APAC Risk Sentiment Index: Q1 2021 Update

DEAR READER,

I am delighted to present Q1 2021 edition of the Risk Landscape Review.

According to the recent surveys conducted by European Risk Management Council, cyber risk remains the prime concern of chief risk officers. To address this concern, we publish an article "**Operational Resilience, for Cyber Integrity**" written by Kevin Duffey, CEO at Cyber Rescue Alliance. Kevin provides an analysis of fast-evolving cyber threats. He specifically focuses on the cyber integrity which will be an important element of the forthcoming Cyber Stress Test announced by the Bank of England.

We also continue our publications of the **Risk Sentiment Index (RSI)**, an expert driven forward-looking index that reflects expectations of experts about the risk landscape of the financial sector in the next 12 months. The results of surveys that we recently conducted in the UK and APAC reflect the dynamic of the COVID-19 crisis. After the doom and gloom of 2020, the first quarter of 2021 is characterised by a change of the mood in the UK and APAC. The successful rollout of the vaccination programme created more optimistic expectations about the timing of the economic recovery.

My huge thanks to all contributors and survey respondents.
Enjoy the reading.

Yours sincerely,

Dr Evgueni Ivantsov

Chairman of European Risk Management Council

Table of Contents

Operational Resilience, for Cyber Integrity

By Kevin Duffey, CEO, Cyber Rescue Alliance

The Bank of England has announced its next Cyber Stress Test, and it's all about Integrity!

On 26th March, the Bank of England announced plans to test how firms respond to a cyber-attack on the *integrity* of payments data. Chief Risk Officers should start thinking about such integrity attacks, because they represent a far more profound challenge to operational resilience than typical cyber-attacks.

Of course, CROs already know that a major cyber-attack is a serious threat to their firm. And regulators know that an extreme attack is a systemic risk to the financial system. But forward-looking leaders focus on how such threats are evolving. And super-profits made by cyber criminals are funding a great acceleration in cyber innovation. Some ransomware gangs have increased R&D a hundred-fold over the last four years, as ransom demands have increased from $50,000 to $50,000,000 at the upper end.

Consider how fast cyber criminals adapt, by reflecting on these comments made by the Bank of England on 26th March: "it would be against the public interest… to publish the text relating to the discussion… given the heightened level of cyber risk." This phrase was published by the Bank in March 2021 to explain why it redacted its own records in May 2020, because of "the possibility of inadvertently increasing risk" as cyber criminals exploited security gaps created during the transition to work-from-home.

COVID-19 created specific opportunities for cyber criminals, and the vast majority of banks responded very well. (It was the health sector that suffered most, with successful ransomware attacks on highly-stressed hospitals quadrupling over the previous year.) Banks should reflect on the "cyber security deficit" that their exhausted IT teams might still be suffering, but in general the lessons of the last year are about how quickly the unthinkable can become the new-normal.

Four years ago, it seemed unthinkable that over 100,000 firms could be breached by one attacker. But in May 2017, the North Koreans released WannaCry, and stopped computers at firms as diverse as Boeing, Honda, PetroChina and Sberbank. For several days, the UK's National Health Service had over 50,000 computers out of action. Later, the Russians launched the (Not)Petya attack on Ukraine, with collateral damage stopping work at firms like DLA Piper, Maersk and TNT. Cyber professionals describe these kinds of attack as "availability breaches," because data and systems are rendered unavailable by the hackers.

Two years ago, hackers started to combine "availability breaches" with "confidentiality breaches," by issuing ransomware demands that stopped computers working *after* data had been copied and stolen. This innovation has dramatically increased the profitability of ransomware attacks, as firms are willing to pay more to protect themselves from the reputational harm and intellectual property loss that comes from combined attacks. For example, on 29th March 2021, Acer Computing (the world's 6th largest PC maker) has offered to pay $10 million to end to such an attack, but the REvil cyber gang are demanding $50 million.

The speed at which ransom demands are increasing is worrying, but that trend is "merely" a quantitative issue. The qualitative change that Regulators are worried about is the risk of a third type of attack: the integrity breach. Integrity is the central pillar in what cyber experts call the "CIA triad," as Confidentiality, Integrity and Availability are the three foundations of cyber resilience. And the greatest of these is Integrity.

An integrity breach is where hackers actually manipulate sensitive data. And that's the kind of breach that the Bank of England is planning to simulate during its 2022 cyber test for regulated entities. The simulation will focus on:

- data integrity (financial records are manipulated)
- retail payments (risk of direct harm to individuals)
- impact tolerances (unacceptable scale and scope of disruption)
- recovery options (looking in particular at dependencies on third parties)

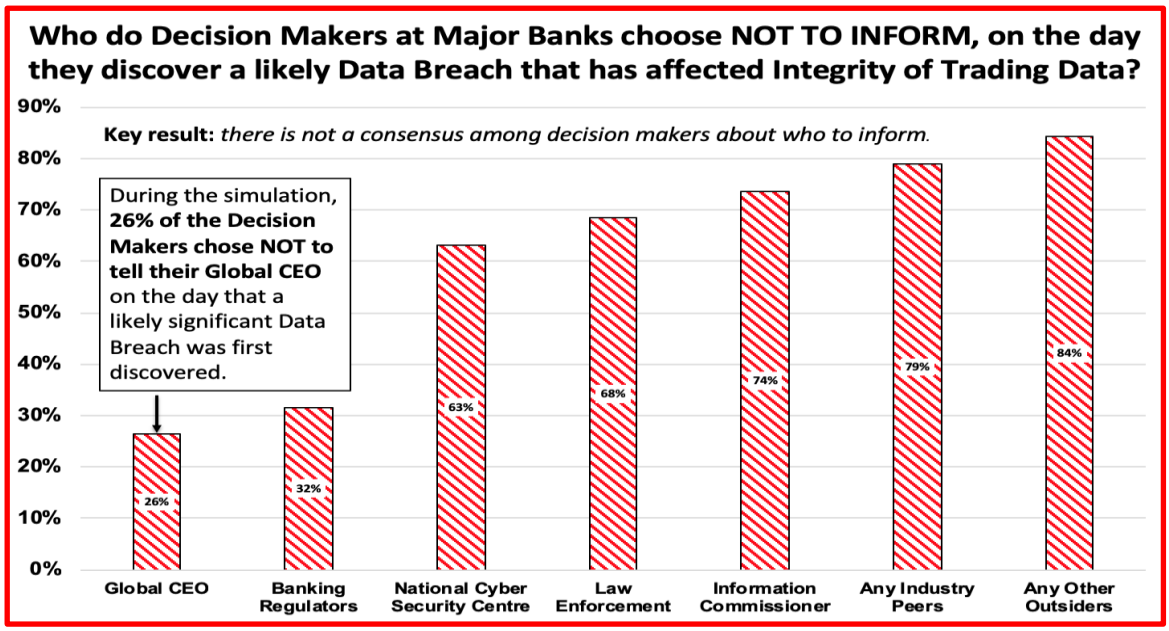
The Bank of England has wisely decided that this test will be "exploratory," ie not a simple pass-fail assessment. My colleagues and I at Cyber Rescue think this is appropriate, because we led an integrity breach simulation for senior executives from eighteen of the world's largest banks in 2019. We learnt that banking executives find a breach of integrity *much* more challenging than a breach of availability or confidentiality. Observations from the simulation included:

a) Command and Control are stressed by the ambiguity of an integrity breach, because commercial decisions must be executed in an environment of enormous uncertainty.

b) Fear of reputational and commercial harm causes executives to have different opinions about what and when to tell regulators. Most choose not to inform corresponding banks.

c) The National Competent Authority and National Cyber Security Centre are both expected to provide critical guidance, support and instruction as an integrity breach escalates.

For example, during the simulated integrity breach, the large majority of executives made a conscious decision not to inform important third parties, corresponding banks, the police or their national cyber security centre. Almost a third said they would not have told their regulator on the first day.



But this simulation was in 2019, and most executives will take a more mature approach to cyber resilience now. Mature reflection is being driven by the new Operational Resilience expectations that are being rolled out in several jurisdictions. Mature reflection is also happening at firms that are paying attention to the escalating threat landscape.

For example, regulators have been warning loudly since 2018 about "cyber supply-chain attacks." Such attacks can be much worse than most *physical* supply-chain risks. A physical problem can take out an individual supplier through a fire, or a region through an earthquake, or a vital trade-route like the Suez Canal, but most physical supply-chain breaches are not contagious. Of course, COVID-19 has shown us that some threats to our suppliers are infectious. So we should be prepared for the fact that a "cyber supply-chain attack" can propagate worldwide within days.

Indeed, several such attacks have happened in just the last three months, with hundreds of thousands of firms put at risk. Fortunately, the attackers were not prepared or motivated to do much damage, so we should use the recent SolarWinds and Microsoft Exchange breaches as opportunities for reflection.

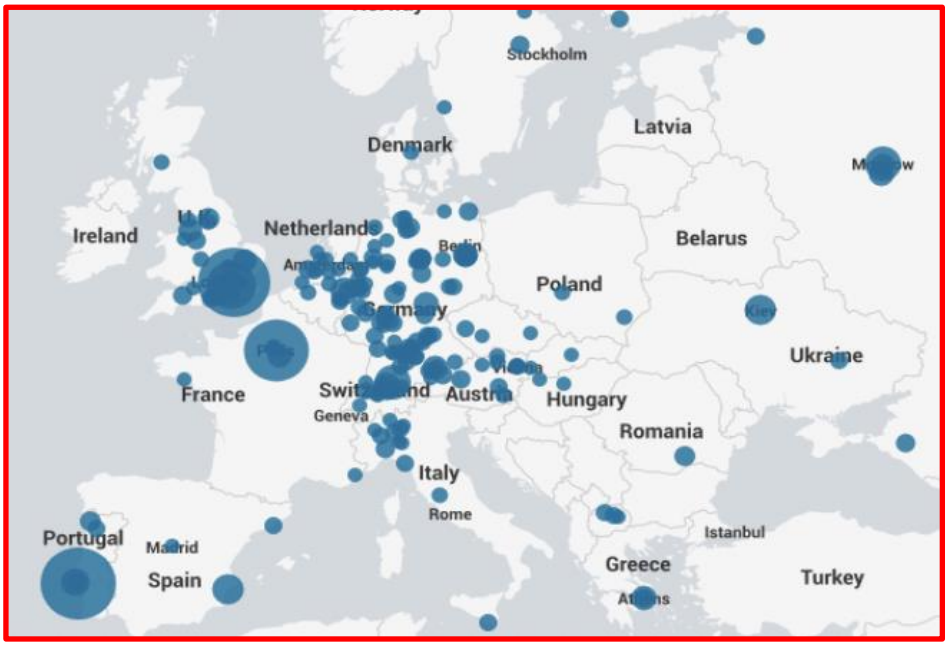
The SolarWinds attack that became public in December 2020 gave hackers the ability to take control of software at over 10,000 firms that buy network-control software from SolarWinds. The hackers appear to have only had the resources to exploit this supply-chain breach at less than 300 of those 10,000 organisations, and even then, only for espionage purposes. The US Government quickly attributed this attack to Russia, and most of the 300 organisations that were spied on were US Government agencies.

The Microsoft Exchange attack that became public in March 2021 gave hackers the ability to take control of software at over 100,000 firms that buy "on-premises" email software from Microsoft. Hackers used automated processes to implement "back-doors" at thousands of the small businesses that use the Microsoft Exchange "on-premises." This gives hackers the ability to access those computers again even after the Exchange software has been patched. Microsoft quickly attributed the main attack to "a group assessed to be state-sponsored and operating out of China." The motivation of the hackers appears – again – to be "only" a breach of confidentiality, to conduct espionage, not to make systems unavailable or to manipulate sensitive data.

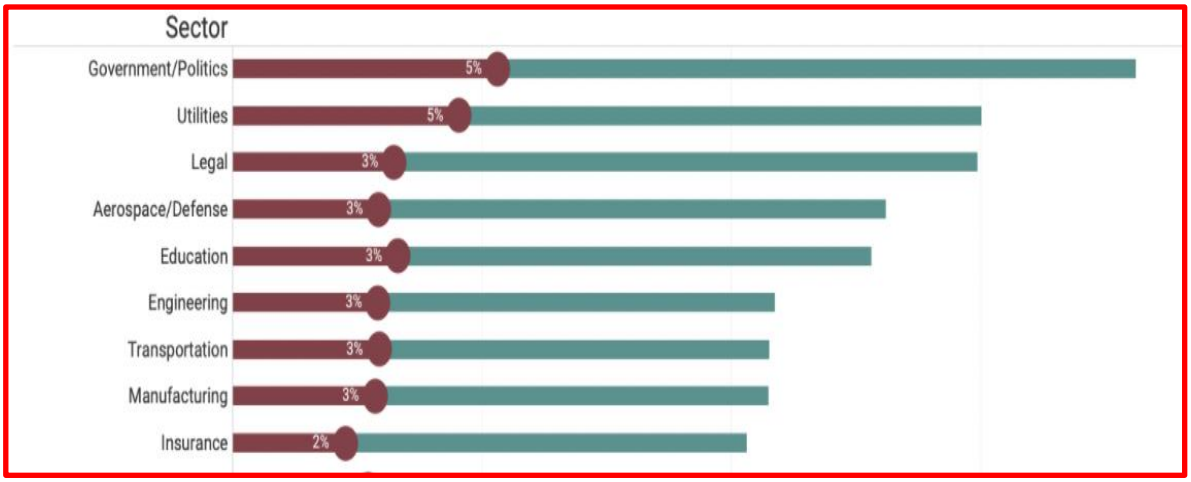
The graphs below show how many firms in various countries and industries were vulnerable to the Microsoft Exchange attack, weeks after Microsoft had issued a patch.

Countries with most Unpatched Servers

European Cities with most Unpatched Servers



Percentage of firms by Sector that use MS Exchange (Green) including those still Vulnerable (Red)



The European Banking Authority (EBA) and the Chilean Banking Regulator (CMF) were among the organisations impacted by the Microsoft Exchange attack graphed above, so it is clear that the Financial Sector is not immune to cyber supply-chain attacks.

So the right thing for Chief Risk Officers to do is reflect on the threat to integrity that their firms face from future cyber-attacks, including those that might propagate via a supplier.

Risk Sentiment Index: Q1 2021 Update

Finally, the mood has changed but concerns remain…

The European Risk Management Council has updated its UK and APAC Risk Sentiment Indices (RSI). Fresh data have been collected for Q1 2021. Chief Risk Officers and other senior risk executives from banks provided their views on the future trends of seven types of risk (credit, market, liquidity, operational, cyber & IT, conduct and regulatory risks). Using the survey results, the Council aggregated the data into forward-looking indices that reflect expectations about a change of the risk landscape for the financial services sector in the next 12 months. Numerically, the RSI reflects the adjusted percentage of respondents who consider that risk will increase in the next 12 months. While the trends in UK and APAC are broadly similar, the substantial differences are observed on how risk experts perceive changes of different risk types.

Q1 2021 UK Risk Sentiment Index

- The aggregated RSI for seven risk types decreased from 0.63 in Q4 2020 to 0.45 in Q1 2021. It shows a change of expectations from very pessimistic to more optimistic (Figure 1). The quarter-to-quarter drop of 0.18 points is the largest improvement of the index since its launch in October 2018. In Q4 2020, when the second COVID wave surged, the index hit its highest level. Three months later, the mood of respondents improved. The successful rollout of the vaccination programme in the last several weeks created more optimistic expectations about the timing of the exit from the lockdown and the path to the economic recovery.

- The change of the mood is demonstrated by a shift in the vote distribution among main categories. While a percentage of respondents who expected that risk will increase slightly in the next 12 months was broadly unchanged (49% in Q1 2021 vs 50% three months ago), almost a quarter of respondents now expect no change in risk (in Q4 2020, only 9%). It is a clear indication of the expected migration from a turmoil stage to a stable risk environment (Figure 2).

- Among individual risk types, RSIs for all seven types of risk improved this quarter which is another indication how massively the mood has changed since Q4 2020. RSI for credit risk, liquidity risk and conduct risk had the largest improvements: 0.20, 0.38 and 0.29 (Figure 3). RSI for liquidity risk not only had the largest quarter-to-quarter reduction but also hit the all-time low.

- Credit risk and cyber& IT risk remain the prime concern for UK respondents. Despite some improvement from the previous quarter, RSIs for these risks remained on the very high level (Figure 4). A large majority of respondents expect that credit and cyber risks will continue to grow in the next 12 months (86% and 93% of respondents respectively). Operational risk is another area for a potential future deterioration.

Figure 1. UK RSI trend: Q4 2018 – Q1 2021

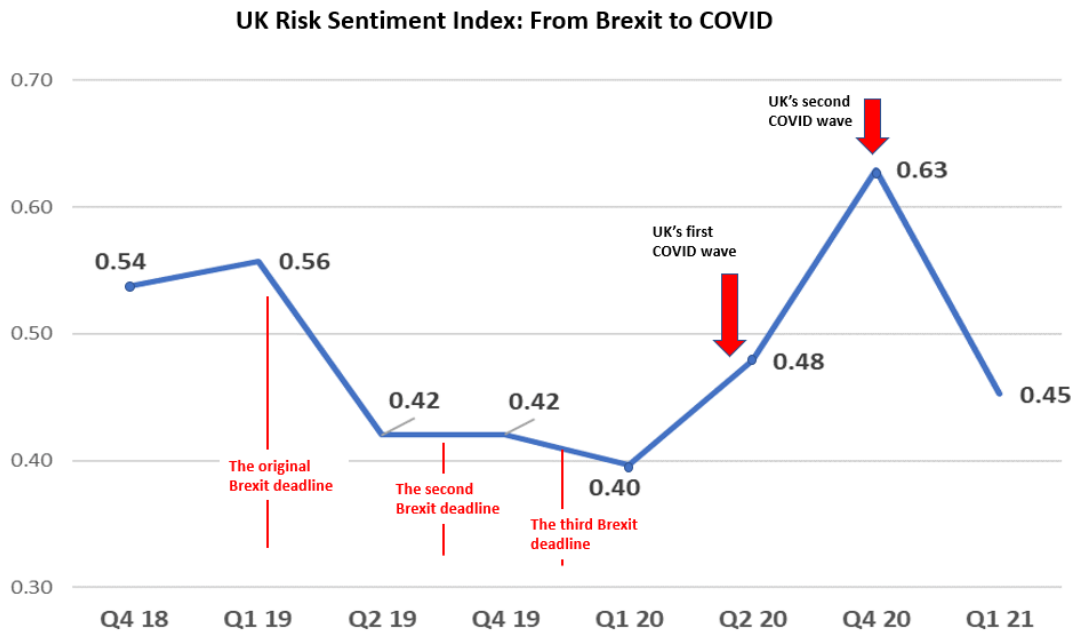


Figure 2. UK RSI: Distribution of respondents' votes

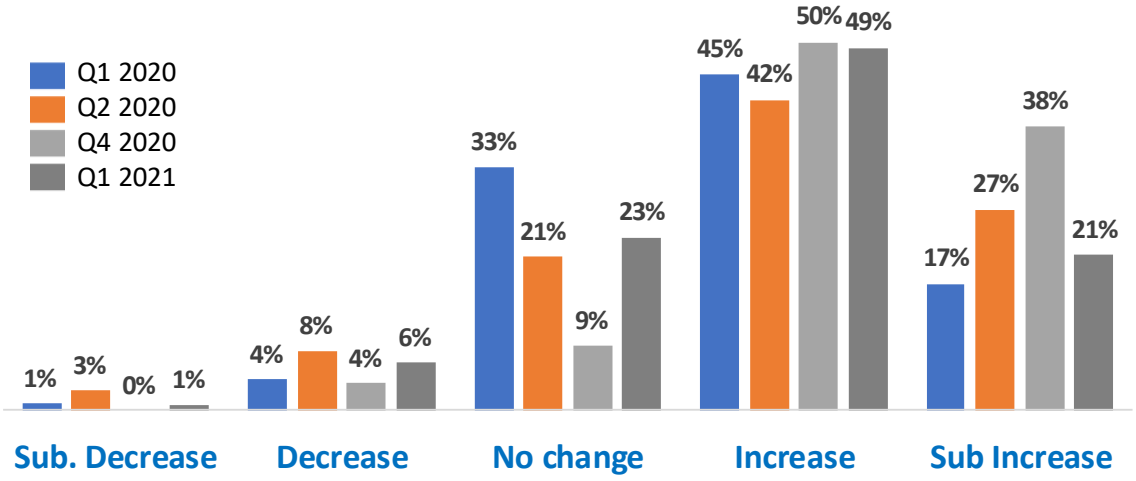


Figure 3. UK RSI: 1-year RSI trends for individual risk types

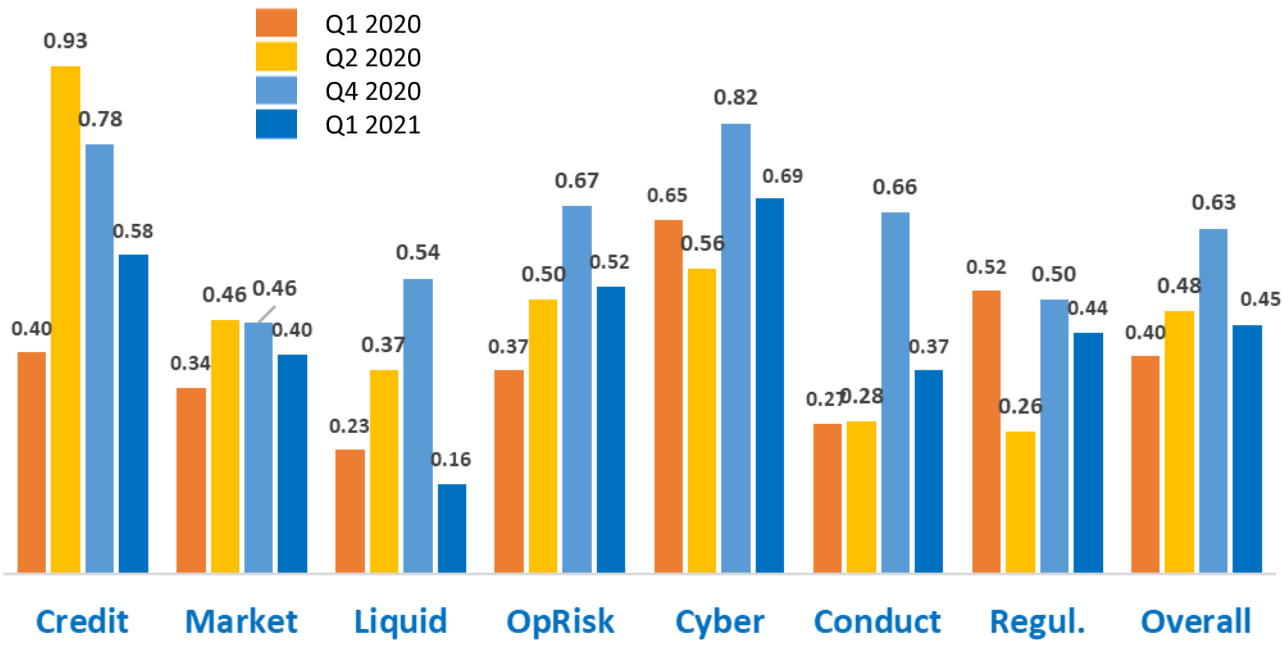
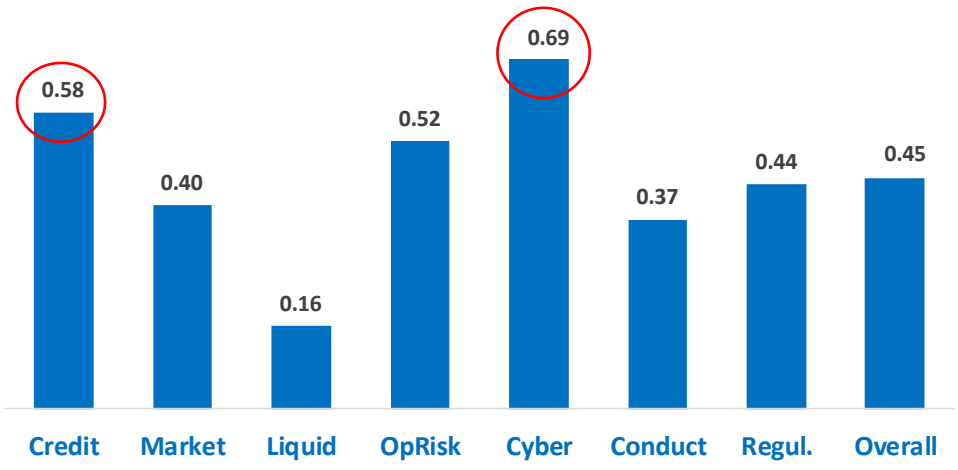


Figure 4. UK RSI: Comparison of RSIs for different risk types in Q1 2021



Q1 2021 APAC Risk Sentiment Index

- The aggregated RSI for seven risk types decreased from 0.68 in Q4 2020 to 0.46 in Q1 2021. It reflects a change from very pessimistic to more optimistic expectations of APAC respondents (Figure 5). The quarter-to-quarter drop of 0.22 points is the largest improvement of the index since its launch in October 2018. In Q4 2020, the index hit its highest level. Three months later, the mood of respondents improved. The ability to successfully suppress the COVID virus by the lockdown measures in many APAC countries combined with the vaccination programme created more optimistic expectations about the economic recovery and the end of pandemic later this year.

- The change of the mood is demonstrated by a shift in the vote distribution among main categories. While a percentage of respondents who expect that risk will increase slightly in the next 12 months marginally increases (47% in Q1 2021 vs 44% in Q4 2020), less than a quarter of the respondents expect that risks will increase substantially in the next 12 months. This is a big difference compared to the previous quarter when almost a half of respondents expected substantial increase of risks. Also, 26% of respondents now expect no change in risk, while in Q4 2020 only 7% expected no change. It is a clear indication that risk experts believe that a turmoil comes to its end and we are gradually move to a more stable risk environment (Figure 6).

- When we compare survey results for individual risk types in Q4 2020 and Q1 2021, the positive dynamic becomes obvious. RSIs for all seven types of risk improved in the past three months. The most significant improvement is for credit risk where the RSI dropped massively from 0.9 to 0.45. Other big improvements are registered in operational risk, conduct risk and regulation risk (Figure 7).

- As in previous quarter, cyber and IT risk remains the top concern for APAC respondents. Despite some improvement from the previous quarter, the RSI for this risk stands at a very high level of 0.72 (Figure 8). Market and regulatory risk are also considered as pressure points with their RSIs of 0.5. At the same time, respondents believe that liquidity risk will grow less than any other risks in the next 12 months. RSI for liquidity risk is just 0.28. This is the all-time low level for liquidity risk since we began our surveys in 2018.

Figure 5. APAC RSI trend: Q4 2018 – Q1 2021

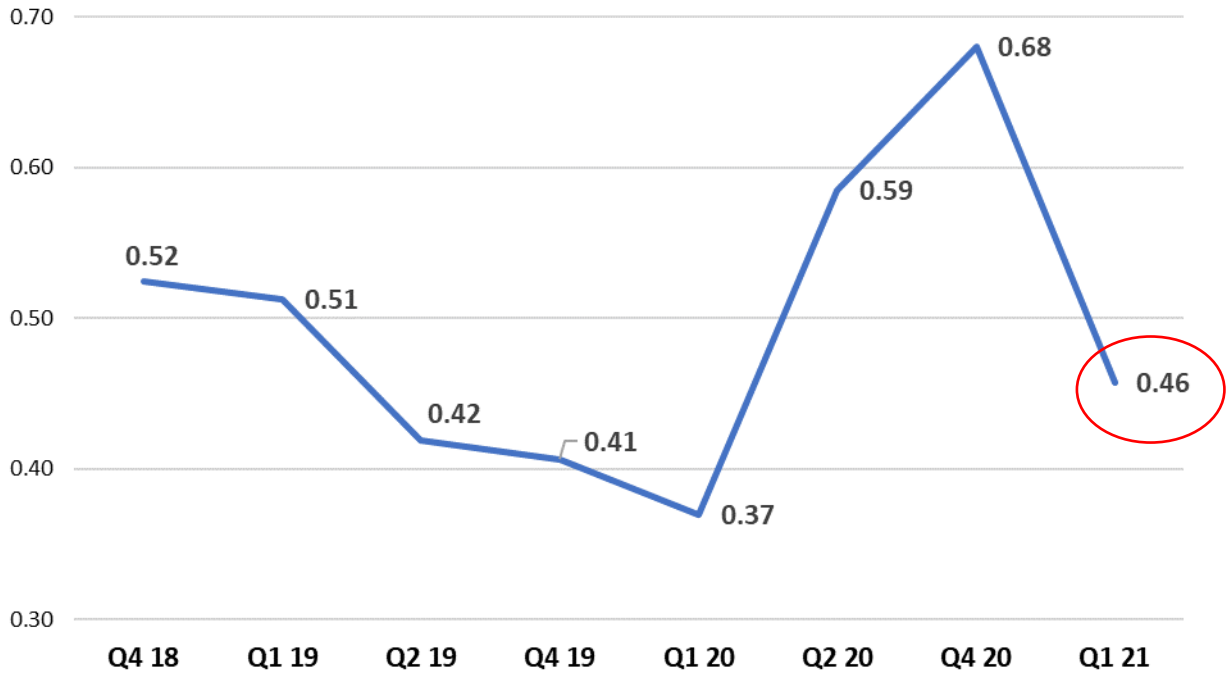


Figure 6. APAC RSI: Distribution of respondents' votes

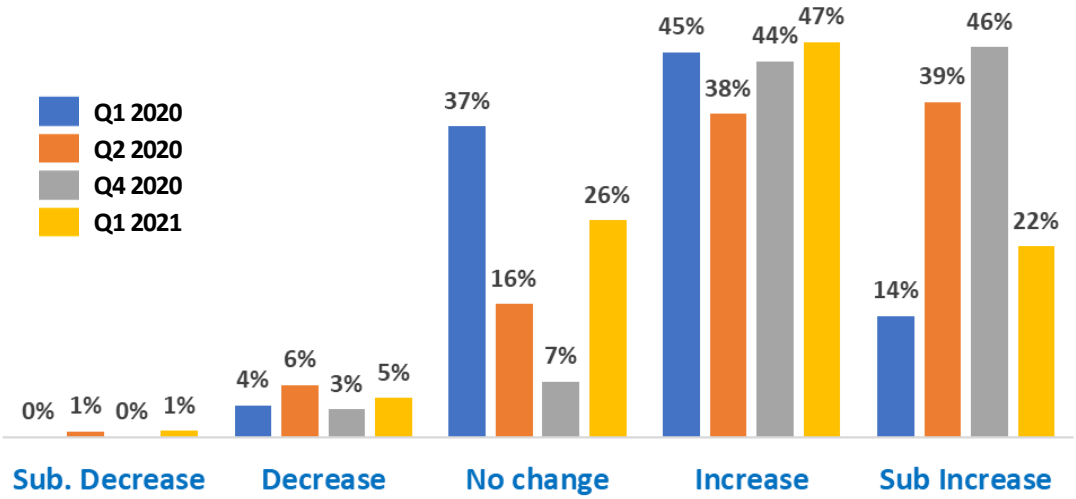


Figure 7. APAC RSI: 1-year RSI trends for individual risk types

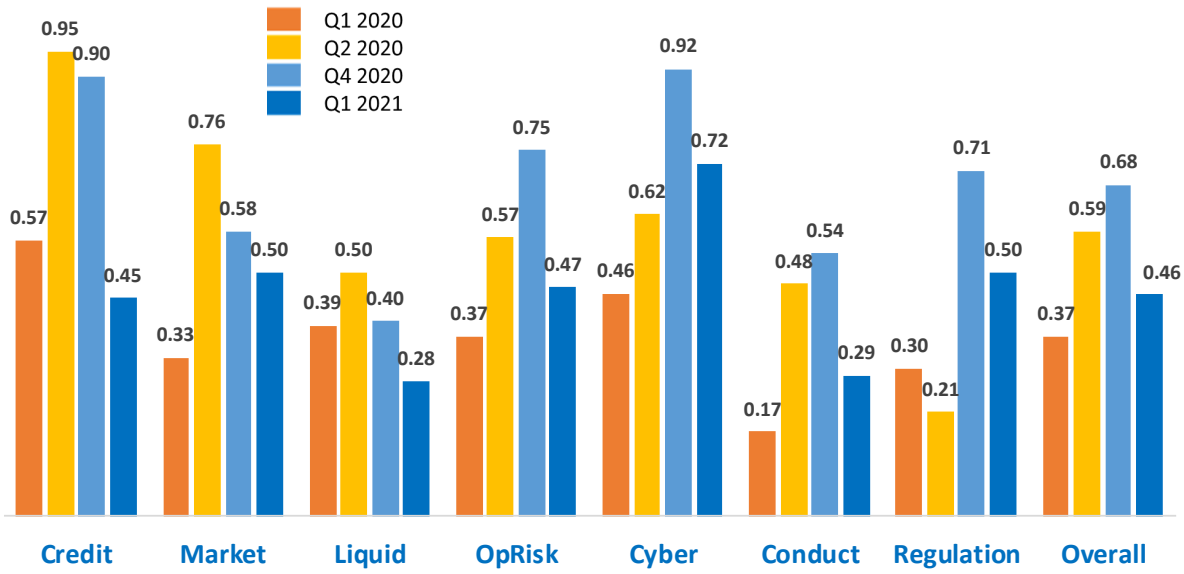


Figure 8. APAC RSI: Comparison of RSIs for different risk types in Q1 2021