

Executive Summary

Popular Indonesian tourist destination Bali will be hosting the 17th Annual Group of 20 (G20) summit from November 15–16, 2022. Residents and visitors will begin to experience physical security preparations as early as November 11, when drivers will be restricted by their license plates on certain roadways until November 18. The conference is especially notable because it will be the first gathering of global leaders since Russia's war in Ukraine. However, Russian President Vladimir Putin will not be attending given the criticism over the war's humanitarian and cost-of-living impacts, which are expected to feature prominently. Leaders from the other 18 largest economies will be in attendance, plus a seat for the European Union (EU). This includes a planned meeting between U.S. President Joe Biden and Chinese President Xi Jinping, who recently secured a third term in leadership that will likely see him remain leader of China for the rest of his life. The relationship between the two countries is tense over Taiwan and recent U.S. export rules that prohibit Chinese access to advanced technology.

Efforts to solve the global cost-of-living and energy crises will also continue during the summit; many of the leaders will have recently attended the COP27 environmental summit in Egypt as well as the ASEAN summit in Phnom Penh, where both Biden and Xi were expected. Lastly, the G20 precedes the Asian-Pacific Economic Conference in Bangkok, which will be headlined by U.S. Vice President Kamala Harris. The presence of three major international summits in the same geographic region occurring in the same week with important political leaders at all three increases the risk of nation-state and hacktivist activity. The G20 also has added physical security and cyber risks, as it is taking place at a popular tourist destination. Bali and Indonesia experienced a series of damaging al-Qaeda attacks in the early 2000s. However, coordinated counter-terrorism efforts over the last 10 years have significantly weakened jihadist groups in the region, making a terror attack unlikely. Similarly, protest groups are not predicated to gather en masse the way they have for previous summits.

Indonesia has a relatively poor recent cybersecurity record with several notable cyber breaches related to government-held data. This includes a late 2021 data breach on its COVID-19 tracking app, which delegates are still required to download. Threat actors may attempt to obtain sensitive personal information from delegates or visitors by impersonating apps and websites, such as those of hotels, G20-related events, and tourism services on the island. Given that G20 is occurring between two other major international summits, cyber threat actors have a larger window than normal to threaten world leaders. Heightened geopolitical rhetoric on account of Russia's war in Ukraine and tensions between the United States and China, coupled with financial motivations, could give cyber threat actors added incentive to target any of the three major summits.

Key Risks and Threats



Hacktivism may target the event over the war in Russia



Security will be tight around venue locations.



Internet-based activism is a likely occurrence to demonstrate concerns over Russian participation.



The threat of terrorism during the summit is low.



Concerns persist over the security of the event's required COVID-19 tracing app.



Russian-backed groups are the most likely source of a nation-state cyberattack.



Road and aviation travel will be greatly restricted during the event.



Effective security is a main focus for Indonesian officials.

Key Findings

- Indonesia is requiring delegates to download a COVID-19 tracing app that was compromised in 2021.
- Indonesia has a weak record protecting government-held data; it has experienced a series of cyberattacks and data breaches since 2020.
- Security will be tight around the series of venue locations and the over 20 sponsoring hotels providing accommodations.
- Travel through the local airport and along major roadways will be restricted by license plates.
- Russian President Vladimir Putin will not attend but Ukrainian President Volodymyr Zelinsky will.
- U.S. President Joe Biden is planning to meet with Chinese President Xi Jinping.
- Important global summit ASEAN will be held before G20 and APEC falls afterward, where more consequential trade and political agreements could be reached.



Physical Security

A heavy security presence is expected across the island of Bali, particularly at the meeting venues and the airport where world leaders will arrive. Indonesia expects to commit 18,000 security personnel, including police and members of the military, to maintain order in the area.^[1]

The main meeting will take place at the Apurva Kempinski hotel, which is also in proximity to other popular hotel chains in Bali, including the Hilton and Ritz Carlton. There will be a gathering at the Garuda Wisnu Kencana cultural park, about 11 kilometers inland. There will also be gatherings at the Ngurah Rai Mangrove Forest and the nearby Sofitel Hotel, which are in proximity to the Ngurah Rai International Airport; the airport is about 30 minutes away from the Apurva Kempinski Hotel.

Indonesia's National Police has identified five areas of particular concentration and arranged forces in "rings" to cover them. These areas include the hotels where the leaders and their entourages will stay, the meeting spaces where the formal summit proceedings will occur, and the locations where gala dinners and keynotes will be held. In the words of an Indonesian security official, the areas were chosen because "all delegates, including presidential activities, will be centralized there."^[2]

Security preparations are not limited to the venues themselves. Traffic flow has been adjusted on 10 roads, and 4,600 CCTV cameras have been set up to link to the central command. In accordance with a government emphasis on sustainability, electric vehicles will be used to provide police response.

The Indonesian security forces are under heavy pressure to perform well during the summit, as they have been subjected to more than a month of strong criticism over a crowd crush at a soccer match in October. More than 130 people were killed after a soccer match in East Java when police fired tear gas into a crowd, provoking a stampede. Since then, Indonesian authorities have been quick to halt or cancel events.^[3]

Assessment:

- Indonesia's government is aware of the importance of this summit and has consistently put out statements describing its progress in the lead up.
- Effective security is a particularly high priority in the aftermath of a deadly crowd crush at a soccer game in October that killed at least 130 people.
- From November 11-18, 2022, increased security on roadways is likely that could include spontaneous vehicle inspections. Key roadways will only permit civilian vehicles with odd or even license plates on rotating days during this time.

Recommendations:

- Carry identification around event sites and avoid unnecessary travel.

Broader Geopolitical Context

This year's G20 summit occurs against a worldwide backdrop of rising inflation and supply chain issues, spurred in part by the Russian invasion of Ukraine and by China's continued struggles to maintain its economy and its zero-COVID-19 policy in the face of increasingly virulent strains of COVID-19.

Russia's invasion of Ukraine in February caused substantial disruption to the worldwide energy market, particularly in Europe. Though it appears the European G20 nations have managed to head off the predicted winter heating catastrophe for this year, one focus of the summit will likely be adjustment to a "new normal" wherein Russian gas is less abundant and accessible. Europe has historically been largely dependent on cheap and abundant supplies of Russian natural gas, but in the aftermath of EU sanctions Moscow reduced the supply, in particular by sabotaging its own Nord Stream undersea pipeline in September. If and how Russia will participate in these discussions remains to be seen. President Putin has stated that he will not attend after 16 of the 20 attendees voted in October to condemn Russia's annexation of Ukrainian territory.^[4]

Three years after the outbreak of COVID-19, the world continues to grapple with the economic shockwaves created by the pandemic. Perhaps no country is as affected as China, where the "zero-COVID" policy that looked like an international model in earlier years is increasingly a handbrake on the country's economy. Snap lockdowns are imposed whenever and wherever a single positive case is detected, a practice that creates huge uncertainty for businesses. The ripple effects are felt throughout the world—especially when these lockdowns strike a port, which has happened in Guangzhou and Shanghai. The worldwide rise in consumer goods prices can be partially attributed to this domestic Chinese situation; with the annual Chinese Communist Party (CCP) Congress just last month opting for no changes.

Forward Look:

- Ukraine is not a G20 member but has been invited to attend, while Russia is weighing what representation it will send. Shows of support for Ukraine or opposition to Russia are nearly certain outside the meeting zone and are possible between delegates. Any form of protest or expressed dissent could lead to elevated geopolitical tensions. Russian-backed cyber groups may conduct propaganda activities in an attempt to change the prevailing narrative surrounding the summit or to delegitimize it.

Recommendations:

- Configure ZeroFox geopolitical team monitoring and alerting for geographic areas of interest.

FOOTNOTES

[1] <https://www.aljazeera.com/economy/2022/11/8/strong-impression-putin-will-skip-g20-indonesias-widodo-says>

[2] <https://en.antaranews.com/news/251005/police-set-five-priority-security-areas-for-bali-g20-summit>

[3] <https://www.aljazeera.com/news/2022/11/5/k-pop-bands-concert-in-indonesia-halted-after-30-faint-in-crush#:~:text=K%2Dpop%20band%20NCT%20127,deadliest%20disasters%20in%20football%20history>

[4] <https://www.nytimes.com/2022/11/10/world/europe/putin-russia-g20-summit.html>



Boycott and Protest Activity

The G20 summit will be held under tight security in an out-of-the-way location, so the chances of external protests disrupting the activities will be minimal. However, an ongoing movement to remove the Russian Federation from the meetings and the organization as a whole could have some impact, depending on the attitudes of the attending states.

Russia's invasion of Ukraine in February 2022 resulted in multiple rounds of economic sanctions as well as widespread symbolic actions; for instance, Russian athletes in international competition are not allowed to compete under the Russian flag and instead use neutral symbols. Though these actions have served to isolate Moscow, Russia still retains its seat on the UN Security Council, its membership in the G20, and other positions in the international diplomatic sphere.

The Ukrainian government has issued statements calling for Russia to be excluded from the upcoming G20 summit and/or expelled from the organization entirely as a response to the invasion—specifically in light of Russian missiles targeting the Ukrainian power grid and civilian infrastructure, which is a war crime. Despite these requests, Indonesia has steadfastly refused to countenance the expulsion of Russia and indicating that the G20 is a neutral economic forum. Given the presence within the G20 of multiple countries that have not condemned the Russian invasion, Russia will almost certainly not be expelled. Ukraine's statements should be viewed more as a means of maintaining public pressure given the current circumstances.

Internet-based activism surrounding Russian participation is a near certainty but is unlikely to achieve any tangible results. The key question is what actions will be taken by the Western nations that make up a large proportion of the G20 and are particularly opposed to Russia's recent foreign policy. While it seems certain that whatever Russian representation attends will receive an unfriendly reception, protest activity could be a minor and quickly-forgotten storyline of the summit, or it could be the dominant feature of this year's conference, depending on how the West chooses to express its displeasure.

> Assessment:

- Large-scale physical protests are unlikely at this event.
- Internet-based activism is a more likely occurrence to demonstrate concerns over Russian participation.

> Recommendations:

- Avoid the vicinity of event locations and any possible protests, as security is likely to be tightly controlled with security forces sensitive to possible threats.

Key Topics of Discussion

Indonesia set three priority topics for its year-long presidential administration: Global Health Architecture, Digital Economy Transformation, and Energy Transition. As often happens, world events have upended this planning, and the upcoming G20 summit is likely to be dominated by other issues that have arisen throughout the year.

Chief among these is the worldwide increase in inflation and the cost of living. A survey of business executives by the World Economic Forum ahead of the summit identified inflation as the primary concern among business executives[5]. The impact of rising consumer goods prices has also been felt strongly by the public at large; the massive anti-government protests in Sri Lanka earlier this year are perhaps the best example of the worldwide current of discontent with the generalized economic climate.

Recent tensions between the United States and China will also be discussed. President Biden and President Xi Jinping have already announced they will meet face-to-face and that the main topic will be Taiwan. The Biden Administration has made it clear they will support Taiwan militarily in the event mainland China attempts reunification by force. The U.S. Department of Congress has also announced a series of trade rules that greatly prohibit China's ability to access advanced technology.[6] While this may not be discussed at the conference, it factors greatly into the relationship between the world's two largest economies.

Terrorism

October 2022 was the 20th anniversary of the dual al-Qaeda terror attacks in Bali, which targeted locations frequented by foreigners. The attacks took place in Denpasar just north of the airport and killed over 200 people. The attacks were carried out by the Indonesian al-Qaeda affiliate Jemaah Islamiyah (JI), which had cells across the region at the time.[7] In the years following, JI continued to carry out attacks, including in Bali again in 2005 and in Jakarta through 2009. The leader of JI, Abu al-Bashir, has been imprisoned since 2010. Since then, the group's activities have been limited, although al-Bashir did publicly claim allegiance to the Islamic State in 2014. The primary jihadist threat in the region comes from the Philippines. Counter-terrorism cooperation with neighboring Australia and domestic counter-terror operations have been largely successful despite repeated criticism from human rights groups. Threats continue to exist in Indonesia, with a major cell in Jakarta disrupted as recently as 2021.[8] However, the terror threat has considerably diminished since the 2002 attacks.

> Assessment:

- The risk of a terror attack on the G20 is low.
- Locations in Bali outside of the immediate vicinity of G20 events are the most likely site for an attack.

> Recommendations:

- Avoid attending non-G20 sanctioned events, as security risks are higher.

FOOTNOTES

[5] <https://www.reuters.com/markets/rates-bonds/inflation-top-worry-g20-countries-survey-2022-11-07/>

[6] <https://www.ft.com/research/corporate-finance/new-us-export-controls-to-challenge-semiconductor-companies-20-10-2022>

[7] <https://www.aspiestrategist.org/au/indonesias-response-to-terrorist-threats-has-grown-much-stronger-since-bali-bombings/>

[8] <https://nasional.kompas.com/read/2021/11/25/2137382/densus-88-tangkap-24-orang-terduga-teroris-kelompok-ji-14-dari-bm-aba-dan-10>



Cybersecurity Threats

In 2011, the G20 meeting in Paris was targeted by cyber threat actors. The attack originated from an email with a malware attachment. The attack occurred during one of the preliminary meetings of finance ministers, which take place in the weeks ahead of the main meetings. Hackers were likely targeting the event early, hoping to find incident responders understaffed. The malware went on to infect 150 computers belonging to the French Ministry of Finance, including those working on the event.[9]

As one of the most anticipated political gatherings in the world, coming on the heels of and before other important events, the G20 could be a target for both financially- and politically-motivated actors. As such, threat actors could leverage the event to target attendees, organizations, and host city entities; cyber risks will significantly increase for brands associated with the G20 as well as governing bodies. Threat actors could aim to compromise networks by exploiting vulnerabilities within interconnected systems, including operational technology and Internet of Things (IoT) devices.

Mobile App

Indonesia is requiring attendees to download and register their vaccination status through the PeduliLindungi mobile app, which is available on iOS and Android devices. It also serves as a digital contact tracing app, which is controversial because it requires access to some of the phone's files and GPS at all times, unlike other similar apps that only require a Bluetooth connection. While the app is not strictly mandatory, it is required to access bus stops, train stations, airports, markets, hospitals, and office buildings. It is also interconnected with 15 other consumer-oriented apps, which means user information could be obtained through a cyberattack on these apps as well. [10]

In September 2021, at least 1.3 million residents' personal data was leaked online, including President Joko Widodo's vaccine certificate.[11] The data leak was also reported on eHAC, a mandatory app used for air passengers. This likely led to cybercriminals trading patient data from COVID-19 tracking apps, which could be used to target affected users.

This has led to fears that user data will not be adequately protected, especially considering the important information that may be stored on delegates' mobile devices. Indonesia has a recent history of notable cyberattacks and data leaks, many of which have affected government-held data. The 2021 eHac breach was the sixth major cyber incident in a year—including the Tokopedia data leak, which compromised the personal information of 15 million Indonesians.[12] Another incident involving Indonesia's General Election Commission also resulted in the electoral data of 2.3 million Indonesian citizens being put up for sale on dark web marketplace RaidForums. Threat actors could use the stolen data to trade on dark web markets or for impersonation, phishing, social engineering, or extortion attempts in the future.

Social Engineering

Social engineering poses one of the greatest threats to organizations and participants of the G20. There is likely to be a spike in event-related lures both in the lead-up to and during the event, as threat actors will aim to capitalize on heightened global interest to harvest credentials, deploy follow-on payloads, and conduct financial fraud. Indonesia's weak record of protecting government-held data coupled with high-profile attendees from the world's 20 largest economies could further inspire cyber criminals.

Social engineering campaigns during the G20 could vary in complexity from low-level, rudimentary email and SMS-based scams targeting mass audiences to sophisticated spear phishing attacks directed at specific organizations and individuals associated with the event, such as diplomats, journalists, and high-profile attendees. Most lures are very likely to use trademarks related to the G20 or Bali, including event sponsors such as hotels that are designed to appear legitimate, as well as attempts to impersonate businesses operating in support of the event, such as hospitality, retail, and travel companies. The most prevalent scams and fraudulent activity observed in previous events include:

- Fake COVID-19 notifications
- Illegitimate accommodation and local experience offers
- Malicious streaming and event sites
- Counterfeit ticket and merchandise sites

Tokopedia 91M

Contact XMPP: [REDACTED] Twitter: [REDACTED]

Sold by [REDACTED] ~ 2 sold since May 03, 2020

Vendor Level 1

Trust level 1

Unlimited items available for auto-dispatch

	Features	
Product Class	Digital	Origin Country
Quantity Left	Unlimited	Ships to
Ends In	Never	Payment

Source: ZeroFox Intelligence

Recommendations:

- Utilize caution when accessing sites associated with the G20 and always review for legitimacy prior to clicking on any email links.
- For event sponsors, ensure that legitimate messaging is frequent and clear to get ahead of campaigns leveraging those brands.
- Enable two-factor authentication for all of organizational accounts to help mitigate phishing and credential stuffing attacks.

FOOTNOTES

- [9] <https://www.parismatch.com/Actu-Match/Societe/Actu/Espionnage-a-Bercy-La-France-face-aux-pirates-258669/>
 [10] <https://www.govinfosecurity.com/2-data-leaks-reported-in-indonesias-covid-19-tracking-apps-a-17478>
 [11] <https://en.tempo.co/read/1515052/pedulilindungi-integrated-with-15-apps-health-ministry-data-encrypted>
 [12] <https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html>



Hacktivism

Politically-motivated hacktivists could attempt to disrupt the G20. Hacktivists often target high-profile events, particularly those that garner a global audience, as these present the opportunity for threat actors to gain notoriety while providing maximum exposure. Hacktivism is most likely to occur through disruptive attacks such as distributed denial of service (DDoS) and website defacements; these have become prevalent during global events and are typically launched in an attempt to interrupt services that are essential to the occasion, including broadcasting and event-related websites. The broadcast of the opening and closing ceremonies of the G20 or key speeches, particularly from U.S. President Joe Biden and Chinese President Xi Jinping, could be targeted.

There could be a spike in hacktivism over issues related to Russia's war in Ukraine and Iran. The most likely source will be the Anonymous collective, which has launched a series of campaigns in recent months—including #OpIran, which targeted supporters of the Iranian government over the suppression of protests that began in September 2022.[13] On October 24, 2022, Anonymous announced that it would be launching the #OpWorldCup campaign specifically for the World Cup in Qatar. [14] Anonymous is continuing to demand that Iran be removed from the tournament and replaced with Ukraine due to Russia's reported use of Iranian drones during the ongoing conflict.

Pro-Russian hacktivist collectives, such as Killnet, also pose a threat to G20, as such groups continue to launch persistent disruptive attacks on Western targets in retaliation for opposition towards Russia following its invasion of Ukraine. In May 2022, Killnet attempted to disrupt both the semi-final and final of the Eurovision contest hosted by Italy, from which Russia had been banned from participating.[15] In the run-up to the final, there was a strong show of support towards the participating act from Ukraine that ultimately went on to win the contest. Similar groups could take umbrage at strong shows of support for Ukrainian President Volodymyr Zelinsky, who is not a leader of a G20 nation but will be attending the event.

In October 2022, Killnet conducted a series of DDoS attacks on U.S. organizations, temporarily causing the websites of at least 14 airports to go offline and disrupting the websites of several U.S. government entities.[16] It is possible that groups such as Killnet will look to cause disruption by targeting sponsoring organizations, particularly those from Western nations.

Hacktivism at the ASEAN and APEC summits is less likely, as they do not have the high-profile media attention that the G20 does which typically motivates hacktivists.

Nation-State Activity

ZeroFox Intelligence assesses with low confidence that nation-state or state-sponsored actors will leverage the event to target the G20 and sponsoring organizations. In recent years, major events have been subjected to sophisticated attacks by state-backed threat actors conducting cyber espionage, as well as attempts to discredit and embarrass host nations.

State-sponsored attacks during the G20 are most likely to involve sophisticated techniques that will allow threat actors to maintain persistent, undetected, and long-term access in compromised environments.

Given the geopolitical situation, the main threat is likely to originate from Russian-backed groups. Russia has a history of leveraging cyber criminal groups to advance foreign policy goals while maintaining plausible deniability—and could utilize this tactic during the G20, especially since criticism of their war in Ukraine is likely to be one of the key topics at the summit. State-sponsored groups based in China and North Korea are also likely to view the G20 as an opportunity to conduct cyber espionage campaigns due to the global attention the event will bring to the region. These groups may have added incentives to target the other summits as well, where Taiwan and North Korean missile launches will be discussed in more detail.[17]

Because the G20 comes on the heels of and before other major conferences in the region, cybercriminals and nation-state actors have over a week to target some of the most powerful leaders in the world. Indonesia's lack of cyber hygiene has been exposed in recent years, but the level of cyber protections in Phnom Penh, Cambodia, which will be hosting the Association of Southeast Asian Nations (ASEAN) summit, is worse. President Biden is also planning on attending the summit, which is rare, because he is hoping to reach trade agreements with U.S.-ASEAN allies. These potential agreements largely aim to isolate China from its neighbors, many of whom are important manufacturing hubs as well. Similarly, the APEC Summit held in Bangkok after the G20 provides cyber threat actors another opportunity to target political leaders. U.S. Vice President Harris is planning on attending the event, and progress on the same proposed trade agreements is anticipated. Cyber threat actors may choose to target these events instead of the G20, hoping to find incident responders focused elsewhere and with many of the security professionals focused on physical security of the attending political leaders.

Assessment:

- Having three major international conferences back-to-back gives cyber threat actors a larger than normal window to target high-ranking political officials.
- The heightened geopolitical rhetoric coupled with financial motivations of threat actors is likely to lead to more hacking activity.

FOOTNOTES

- [13] <https://www.twitter.com/anonymousoiran>
[14] <https://www.twitter.com/YourAnonTV/status/1586137468696990208>
[15] <https://www.euronews.com/culture/2022/05/16/eurovision-2022-russian-hackers-targeted-contest-say-italian-police>
[16] <https://www.washingtonpost.com/transportation/2022/10/10/hackers-cyber-attack-airport-websites/>
[17] <https://www.reuters.com/world/asia-pacific/myanmar-dominate-asean-agenda-little-progress-expected-2022-11-10/>



Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

About ZeroFox

ZeroFox (Nasdaq: ZFOX), an enterprise software-as-a-service leader in external cybersecurity, has redefined security outside the corporate perimeter on the internet, where businesses operate and threat actors thrive. The ZeroFox platform combines advanced AI analytics, digital risk and privacy protection, full-spectrum threat intelligence, and a robust portfolio of breach, incident, and takedown response capabilities to expose and disrupt phishing and fraud campaigns, botnet exposures, credential theft, impersonations, data breaches, and physical threats that target your brands, domains, people, and assets. Join thousands of customers—including some of the largest public-sector organizations, as well as finance, media, technology, and retail companies—to stay ahead of adversaries and address the entire lifecycle of external cyber risks.

See ZeroFox in action

zerofox.com/demo | zerofox.com

Get in touch with us today

sales@zerofox.com | 855.736.1400

