CYBER SECURITY AND THE WORLD CUP

Manish Gohil *focuses on the cyber security issues that this celebration of football faced*

Picture credit: Getty

The FIFA World Cup in Qatar was always likely to be a key focus for a range of hostile cyber actors, including nation states, hacktivists and cybercriminal groups. While large events like the World Cup provide opportunities for organisations to reap commercial and reputational benefits, these throw up a range of risks, and their exposure to cyber threats was rather different to usual. The World Cup presented a unique risk landscape for organisations involved in the event, and required them to proactively plan for potential cyber threats to help protect their people, brand and assets.

As with previous World Cup tournaments, it has proven challenging to separate politics from sport. There have been repeated allegations of corruption against the Qatari authorities and FIFA since Qatar was awarded the 2022 tournament in 2010. The Gulf state has been in the spotlight since then due to a range of human rights issues, particularly over the alleged systematic abuse of migrant workers and discrimination against the LGBTQ+ community. Furthermore, this was the first major international football event since FIFA excluded Russia's national team following the country's invasion of Ukraine in February 2022.

These issues forced some organisations involved in the tournament, including sponsors, to adopt a political stance over the event. The sports brand Hummel in September revealed a 'monochrome World Cup kit' for the Danish national team in protest of alleged human rights violations in Qatar; the brand said that it does: "not wish to be visible during a tournament that has cost thousands of people their lives". Several European cities announced that they would not be hosting major 'fan zones' for the public to watch the World Cup games on large screens. Further symbolic actions by brands and authorities in the West grew increasingly likely as the tournament got closer.

An understanding of these political developments is vital in comprehending how nation states perceive the World Cup, particularly those that are established cyber actors. Russian state-sponsored cyber groups have a proven intent and capability to interfere with past international sporting events. They almost certainly conducted reconnaissance and espionage activities against firms involved in or sponsoring such events, as they have previously done around major sporting events. They will have also tried to directly target the event itself through disruptive cyber operations, given Russia's exclusion from the tournament.

Russian state-sponsored cyber groups have a proven intent and capability to interfere with international sporting events

In 2020, the UK authorities accused Russian intelligence of conducting cyber reconnaissance against officials and organisations linked to the Olympic and Paralympic Games in Tokyo (which was postponed to one year later due to Covid-19). They said that targets included organisers, logistics services and sponsors. The US in 2020 also charged several Russian military intelligence officers for developing malicious email attachments and sending spear phishing emails to people working for the 2018 South Korea Winter Olympics 'official timekeeping partners and their subsidiaries'. This campaign began in November 2017, a month before the IOC suspended Russia from the competition.

Russia is a proven disruptive actor to international sporting events. Russian state cyber actors deployed the so-called 'Olympic Destroyer' malware targeting an IT vendor, which allowed them to disrupt the Olympics website, display monitors and wi-fi during the Winter Olympics opening ceremony in South Korea in 2018. A US indictment suggests that planning for this attack occurred shortly before the IOC suspended Russia in 2017 due to a doping scandal. The World Cup in Qatar was highly symbolic as it is one of the first major international sporting events since Russia invaded Ukraine. Russian actors trying to disrupt the event were always most likely to affect coverage or cause logistical problems to organisers.

Other established nation-state cyber actors were probably not as motivated to disrupt the World Cup in Qatar or target sponsors; there appeared little reason for them to do so. Qatar has cordial relations with China and Iran for example. While North Korean state-sponsored cyber groups already frequently steal and extort money from businesses globally, mainly through ransomware and brazen thefts of crypto and fiat currencies, their attempts to do so do not appear to have increased around previous global sporting events.

Attempts by nation states to disrupt the World Cup through cyber operations was most likely to target companies involved in the logistical success of the event, and a surge of online scams and cyber criminality targeting wider businesses was widely expected ahead of the tournament. The tournament's global popularity almost certainly incentivised cybercriminals to pursue pervasive scams, social engineering and phishing campaigns using event-related content as it approached. This is because cybercriminals perceive these as being a good opportunity to extract money from football fans and businesses globally, and travellers to Qatar for the event. This has been a consistent feature around past international sporting events, including the World Cup.

The main cyber implications for travellers and match-goers around the World Cup centred on credential and financial theft. Such activities are rich in follow-on financial rewards for criminals, particularly if they obtain bank details or personal information of victims that facilitate fraud. These would most likely have included malware-embedded phishing campaigns offering deals for accommodation and travel related to the event. However, it was fairly easy for those travelling to Qatar to mitigate these risks, by carrying out simple actions such as not clicking on suspicious-looking emails. Ahead of the 2018 World Cup in Russia, the UK authorities had also warned travellers to avoid connecting to public and hotel wi-fi.

For businesses operating in Qatar and firms sponsoring the event, there was an increase in the risk of ransomware and data-compromising attempts as the World Cup drew closer. Hotel, aviation and technology firms were also susceptible to such efforts by cybercriminals, given their critical importance to the logistical success and broadcasting of the event, and because they possess a large amount of customer data. As a result, cybercriminal groups will have perceived such businesses as financially lucrative targets. Tactics that have been particularly effective by ransomware groups over the past year have included the encryption of victim's systems and threats to publish sensitive company information that they have obtained (called double-extortion). These attacks have already impacted hotels, logistics and aviation firms this year.

RUSSIA WAS ACCUSED OF CYBER RECONNAISSANCE AGAINST ORGANISERS OF THE TOKYO OLYMPICS

Hacktivism has developed into a key source of cyber risk since Russia invaded Ukraine, and this was expected to form a key part of the cyber threat against the World Cup. We have routinely been monitoring discussions online, and on deep and dark web channels, to provide early warning of any emerging hacktivist threats. Hacktivists were widely expected to start directly threatening the event of companies involved in the World Cup in November – especially given the media coverage that any such attacks would create with global attention focused so much on the event.

Hacktivist groups were motivated by their own perceived injustices, such as Russia's exclusion from the tournament by FIFA. We have observed pro-Russia hacker groups online criticise football bodies such as UEFA for expelling Russian teams from European competitions after the country invaded Ukraine and for 'mixing sports with politics'. Groups such as Killnet – which has mainly conducted DDoS attack campaigns on public and commercial interests in Ukraine, NATO and EU countries this year – have a proven intent to disrupt major entertainment events. It unsuccessfully tried to disrupt voting for the Eurovision contest in Italy in May through DDoS attacks as part of its 'war' on the country at the time.

Qatar's human rights record was an additional motivation for data-compromising activity and website defacements from hacktivists on the other side of the political spectrum, like the international hacker collective Anonymous. The group has been mainly focused on issues such as the Ukraine war, elections in Brazil and anti-regime protests in Iran. But given its stance on human rights issues, it was

▶

widely expected to call for data breaches and leaks of international football agencies, government and public agencies in Qatar as well as potential sponsors in the lead up to the event.

But it's not just outside forces that posed a threat during the month of football. With an influx of travellers and workforces to Qatar for the event itself, personal cyber risks posed by the Qatari state were also a serious consideration – most notably data or device compromise and surveillance. As part of data that Dragonfly has compiled, Qatar is one of the most hostile countries globally in regards to state behaviours such as online surveillance, particularly against sensitive sectors such as the NGO and media sectors. The country has relatively high levels of social media surveillance, government filtering of the internet and arrests of online users, which are all key indicators of the high level of exposure to personal cyber risks there. That said, the Qatari authorities were always unlikely to conduct arrests against travellers that criticised the state during the World Cup – due to the negative press which would almost certainly result in global media coverage. Qatar has tried to downplay and assuage criticism it has received from foreign states and human rights organisations in recent years over issues such as human rights. High-profile controversies such as the arrests of match-goers, journalists or human rights workers would deeply harm any efforts to portray the tournament as a success.

HACKTIVIST GROUPS WERE MOTIVATED BY THEIR OWN INJUSTICES SUCH AS RUSSIA'S EXCLUSION

It is clear the World Cup in Qatar posed a bespoke cyber threat landscape for organisations involved in the tournament and travellers there during the event. Such events are prime opportunities for hostile cyber threat actors for a wide range of reasons. Therefore, it is crucial for organisations to understand their risk profile at such events, how the threat landscape that they may encounter is evolving, what geographical or sectoral sensitivities can mitigate or amplify threats to their business, and what longer-term impacts and legacies of the World Cup can leave for their reputations and risk profile. Politics will always be mixed with sport, and understanding this context can be crucial to mitigating risks ahead of time ●

Manish Gohil is the lead analyst on cyber risks at Dragonfly, a geopolitical and security intelligence service for professionals who guide decision-making in world leading organisations.

The main cyber implications for travellers and match-goers around the World Cup centred on credential and financial theft