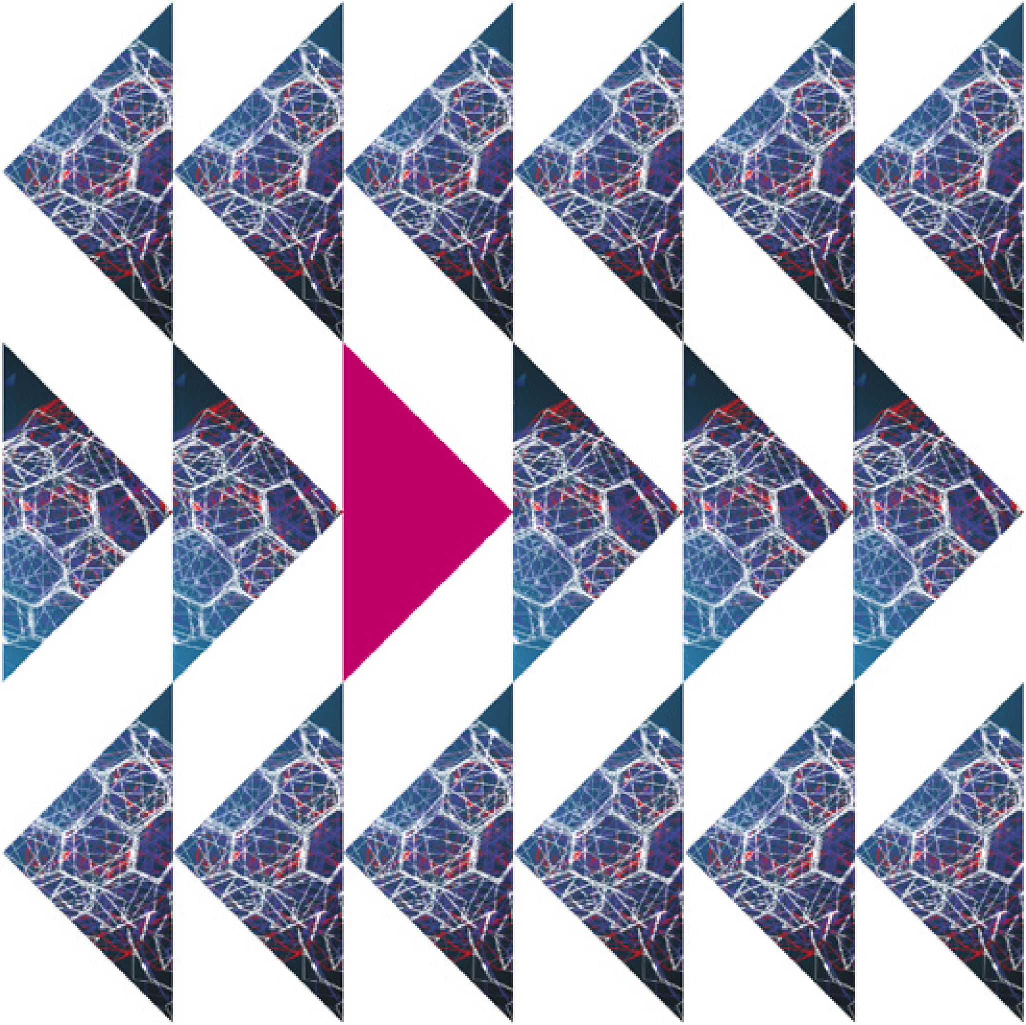
MDR CYBER

Cyber Threats to the FIFA 2018 World Cup



The information in this document is given without financial or other liability on the part of the writer or Mishcon de Reya LLP. This firm cannot be held responsible for any errors contained in this document. This document sets out findings following an analysis of open source, publicly available material. No reliance should be placed on this document in whole or in part by other parties.

Contents

A Developing Threat

Modern global sporting events are not only a world stage for competing national teams: they are increasingly an arena for a wide range of online attackers. The 2018 FIFA World Cup in Russia presents opportunities for cyber threat actors looking to exploit the unique conditions such an event creates.

Threats surrounding sporting events are nothing new, but in recent years cyber threats in particular have intensified. For example, the 2012 Summer Olympics in London reportedly suffered six major cyber attacks with little public impact, whereas the 2018 PyeongChang Winter Olympics was impacted publicly downing broadcaster drones and taking offline the official website.

Russia finds itself hosting the World Cup at a time of intense international scrutiny. Russia's unique geopolitical standing, and the growing threat to large international events are signs that the World Cup may be more than just a spectacle of football.

Just as technology is a huge part of a fan's enjoyment and engagement in an event, it is also part of a player's life both on and off the pitch. Social media and Internet access is a necessity for most travellers and journalists, making the World Cup more connected than ever before.

Cyber risks can affect every organisation and individual associated with the World Cup, from potential attacks against the host nation to financial scams targeting friends and family of fans who are staying behind at home.

‘Major sporting events now attract deliberate cyber attacks, and in the case of the 2018 World Cup, attacks may be fuelled by the current diplomatic standing of the host nation. Avoiding the public embarrassment of a breach will be a key priority of the Russian government.’

Fans
Visiting fans are at risk of cyber crime from point of sale malware, credit card skimming and phishing scams at home.

Sponsors
Sponsors are at risk of being targeted by hacktivist groups looking to tarnish brand reputation and operations.

Sports Professionals
Sports Professionals are at risk of being targeted by cyber criminals and hacktivists for sensitive information.

Broadcasters
Broadcaster networks have previously been attacked by suspected nation states in attempts to stop their operations.

Host nation
Government websites, state officials and other state-related entities are at risk of being targeted from activists, espionage and potential disruption from other nation-states.

Local businesses
Hotels and retailers are at risk of being targeted by cybercriminals wishing to steal credit card data and misuse Wi-Fi networks.

> Fans are as likely to be targeted at home with World Cup-related scams as they are when travelling to Russia.

> Fans are likely to be targets of payment fraud, with cybercriminals targeting point of sale systems in hotels, bars and restaurants and ATMs near World Cup venues.

Fans, Home and Away

Financially motivated cybercrime has been a consistent threat looming over sporting events, not only to individual fans, but also to businesses operating in support of the games, such as retail, hospitality and travel companies.

The process of buying a ticket for the World Cup and its popularity provides criminals with opportunity. Before and during previous large sporting events, criminals have used several online and digital techniques to directly target fans for financial gain. An example is phishing emails that manipulate victims into thinking they have won a lottery ticket draw, which stipulate that a processing fee must be paid in order to claim the prize. Another example is criminals creating a fake contest related to one of the World Cup's partners, and asking individuals to provide personal information, including credit card data, to receive a prize.

Some individuals may also lure spectators into making illegitimate ticket purchases. FIFA is attempting to restrict the potential for unauthorised ticket sales via third parties, and tickets can only be legally resold via the official FIFA website. However, profit-seeking individuals may offer tickets at extremely inflated prices on secondary ticket-selling websites, and request payments in advance.

The most obvious threats to fans when in Russia and to local Russian businesses lie in two other popular criminal tactics. Malware can steal credit-card data from users of point of sale (POS) terminals, and small 'skimming' devices attached to cash machines can steal data from cards' magnetic strips, which can then be used to create counterfeit cards.

Russian authorities expect to see up to a million fans from around the world, with the event taking place in 12 stadiums across 11 cities. This huge influx of people will spawn a temporary boom in tourism and hospitality, generating significant returns for local retailers, hotels, and travel companies. With this concentration of tourism, cybercriminals are highly likely to see the event as a viable target to make some easy money using a range of tactics.

Sporting events now drive huge online traffic from social media to fan websites and news. Every visitor will want to connect. When travelling Wi-Fi from hotels, shops and sporting venues provides an alternative to data roaming charges.

Attackers have also compromised hotel and public Wi-Fi networks to spy on guests, gather intelligence and to collect financial data. In 2014, cyber-security researchers reported that hotel guests in countries including Russia, South Korea and Japan had been targeted by the Darkhotel malware campaign. The malware infected computers and searched for sensitive corporate data, passwords and login credentials. In 2017, a variant of the same campaign also targeted political figures.

Harvesting credentials from insecure Wi-Fi often supports other financially motivated frauds. With access to legitimate accounts attackers target friends and family in a travellers home country or can use access to online accounts to carry out frauds.

Family and friends are also likely targets. There are examples of the 'stranded traveller' e-mail scam where an individual's account is hijacked and used to lure concerned relatives and friends into sending funds.

Dark Web Match-Fixing

Football match-fixing has also moved to the Dark Web in keeping with many other forms of crime. MDR Cyber's intelligence team has uncovered sites offering privileged sport information, and the ability to purchase fixed matches.

We identified multiple sites each offering match-fixing information and services. The sites were directly aimed at bettors indicating the odds of matches and charging more for those that were more favourable or had a higher chance of success for a gambler. According to the individuals running the sites, they could fix matches in several sports, including European football in all major leagues.

The sites claimed to be based on insider information rather than directly altering the outcome of games, which may indicate links to other match-fixing groups not operating online. Spot-fixing, where parts of a match such as timings of throw-ins or substitutions are deliberately manipulated, is reported to be a prevalent technique in various sports, with claims that it directly affects football matches.

In 2013 Europol and police from 13 countries uncovered an extensive criminal football match-fixing network. According to Europol, the investigation extended to 425 match officials, club officials, players and criminals from more than 15 countries, who were suspected of involvement in fixing more than 380 football matches.

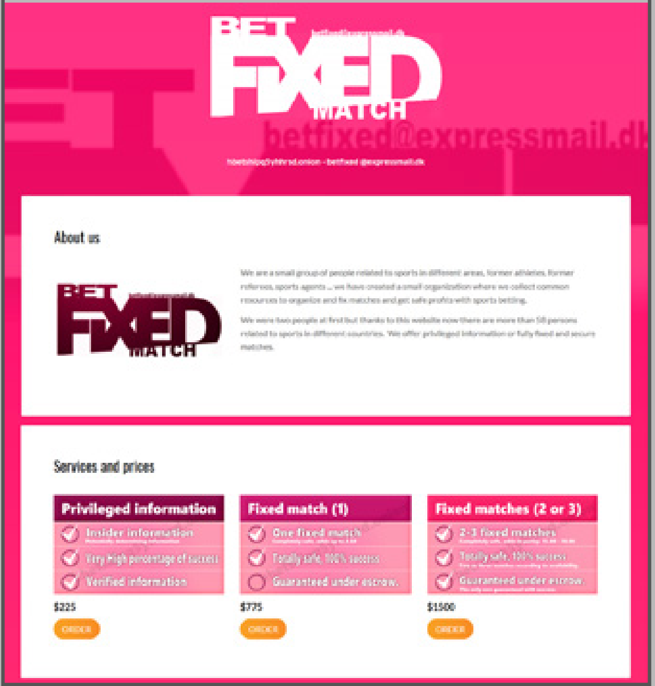
Prices ranged from $99 for 3/1 odds to $400 for a 19/1 match in European minor leagues. Other sites provided more premium services at $1500 for 2-3 matches at between 15/1 to 70/1 odds with a claimed 100% success rate. Payments are accepted in a variety of cryptocurrencies, including bitcoin. There is always a chance that these sites are simply scams, with no genuine information. The sites were unable to provide any proof of their access or validity.

Although there has been no indication that matches in the World Cup will be targeted, this is a threat organisers and betting companies will want to consider during local and international sporting events.

> Match-fixing is now online. Although the World Cup shows no evidence of corruption, the billions in gambling revenue it produces make it a target, both now and in the future.

> Sites identified charged from $99 for a European National minor League match, up to $1500 for 2-3 matches.

Figure 1 – Match-fixing Dark Web site



About us

We are a small group of people related to sports in different areas, former athletes, former referees, sports agents ... we have created a small organization where we collect common resources to organize and fix matches and get safe profits with sports betting.

We were two people at first but thanks to this website now there are more than 50 persons related to sports in different countries. We offer privileged information or fully fixed and secure matches.

Services and prices

Privileged information
- ☑ Insider information
- ☑ Very High percentage of success
- ☑ Verified information

$225

ORDER

Fixed match (1)
- ☑ One fixed match
- ☑ Totally safe, 100% success
- ○ Guaranteed under escrow.

$775

ORDER

Fixed matches (2 or 3)
- ☑ 2-3 fixed matches
- ☑ Totally safe, 100% success
- ☑ Guaranteed under escrow.

$1500

ORDER

A Platform for Protest

Worldwide sporting spectacles, such as previous World Cups and Olympic Games, have also attracted protests, both on- and offline, by individuals and groups wishing to draw attention to their causes and gain support.

In 2014 the World Cup in Rio de Janeiro was targeted by ideological hacktivists wishing to highlight perceived corruption and inequality in the country. Multiple hacktivist groups from around the globe attacked Brazilian targets, including government websites and those of sponsors affiliated with the competition. Although not specifically aimed at the World Cup, such tactics are expected by many throughout the 2018 event—with hacktivists targeting state infrastructure, governmental bodies and private individuals.

Often motivated by political or social ideologies, online activism has traditionally been carried out by small networks of individuals. They operate with little to no overarching, established command structure or long-standing group hierarchy. Their division of power and lack of outwardly defined hierarchical structures place the majority of online hacktivist collectives within the 'semi-organised' crime bracket. There are multiple geographically defined splinter groups, as well as those focused on a single issue.

Tracing their origins to the Anonymous movement, hacktivist groups have targeted financial institutions, central banks, governments, stock exchanges and law enforcement agencies, among others. They have combined grassroots demonstrations with targeted—but often un-complex— cyber attacks to punish entities they see as opposing their relative "cause", and draw widespread attention to it. Attacks have included distributed denial of service (DDoS), website defacements and doxing, which is the unauthorised online publication of targets' private data.

Broadly speaking, the overall threat from established hacktivist groups has subsided. Well-known and well-supported collectives, such as Anonymous, have become less galvanised by specific causes, and the capability and intent of supporters has remained weak. Although a latent threat from various groups still exists, typical tactics represent a low threat to the World Cup and associated organisations beyond reputational damage.

> Protest groups create noise and attention, but their impact on the event's biggest investors is generally limited.

> A high-profile sporting event creates an opportunity for online protesters to gain coverage and boost their own profiles.

Two ongoing hacktivist operations, #OpKremlin and #OpRussia, have focused primarily on remonstrating Russian state-sponsored actions abroad and human rights violations. The global attention on the World Cup will likely reinvigorate activity around these operations and provoke an increase in attacks.

Although most hacktivism is unsophisticated, there are recent examples of more complex, apparently politically motivated, vigilantism: targeted messages sent in response to specific policies or actions.

In 2018, for example, a hacking group known as JHT targeted and defaced a substantial number of Cisco brand devices belonging to Russian and Iranian-related firms, displaying an image of the American flag and the caption *'Do not mess with our elections.'* This demonstrates how politically motivated groups can respond on an international stage to perceived wrongdoings against their own nation-state or identity-based grouping.

> "Protest groups are already targeting Russia to express opposition to state actions abroad and to draw attention to human rights issues."

> "Politically motivated attackers have already targeted Russia, but their impact was minimal outside the security community."

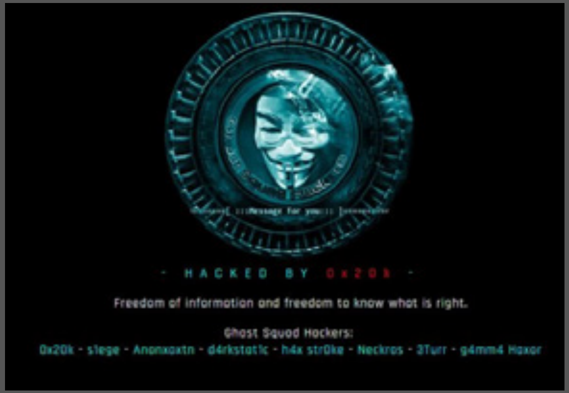
#OpRussia

#OpRussia is a hacktivist operation that has been running for several years and has been adopted by ideologically motivated groups opposed to the Russian regime. In the past two months, attackers have made several claims of attacks against Russian websites, asserting they have stolen databases and suspended the operation of a Russian telecoms company.

As with many hacktivist operations, typical tactics involve website denial of service and subsequent publicising of these attacks on social media.

Hacktivist attacks such as these are highly likely to continue and intensify into the World Cup, since it provides a world stage for political messages, but impact is expected to be minimal.

Figure 2
Hacktivist website defacement message from #OpRussia



[:::Message for you:::]

- HACKED BY 0x20k -

Freedom of information and freedom to know what is right.

Ghost Squad Hackers:
0x20k - s1ege - Anonxoxtn - d4rkstat1c - h4x str0ke - Neckros - 3Turr - g4mm4 Haxor

The Developing Threat

2012

London Summer Olympics

- Head of the UK's GCHQ confirmed that systems supporting the games were hit by daily attacks during the Olympics.
- DDoS attack brought down internet access for Olympic press agencies (potential disruption from other nation-states).

2014

Brazil FIFA World Cup

- More than 2000 daily cyber attacks against Brazilian government infrastructure.
- Over 90,000 attempts to launch malicious programs in Brazil – the majority of which were phishing emails containing malware.
- #OpWorldCup targets Brazilian websites.

Sochi Winter Olympics

- A DDoS attack launched on Olympic relates sites, bringing down the website of the Russian National Games Committee.
- Botnets emerged targeting 4G networks and popular hotel websites.

2016

Rio Summer Olympics

- Volume of 'malicious and phishing artifacts' grew by 83% within Brazil alone.
- World anti-doping agency suffered a widespread breach of their online systems.

2018

PyeongChang Winter Olympics

- Attack disrupted PyeongChang organising committee's internet connected systems – downing broadcaster drones and knocking down their official website.

Russia FIFA World Cup

- Ongoing concerns regarding the security of the online and Wi-Fi systems employed by the games.
- The English Football Association has requested that players, coaches and technical staff refrain from connecting to any public Wi-Fi networks.

Political Football

An event such as the World Cup is an opportunity for countries to make powerful political statements. Host nations often wish to present strong messages of leadership, capability, resources, and economic prosperity to their own citizens and to other nations. As such, any threatened or actual interruption to event operations also threatens this projected image, and can negatively affect perceptions of the event's success.

The most pressing cyber concern for Russia in 2018 is being targeted by other nation-states. Previous games and sporting events have been subjected to more severe and sophisticated cyber attacks each year, not just by financially motivated criminals and hacktivists, but increasingly by sophisticated state-backed threat actors with political objectives.

Recognising this, nation-states have increasingly targeted events to apparently discredit and embarrass host nations. Most recently, the opening ceremony of the 2018 Winter Olympics in PyeongChang was disrupted by operationally and technically sophisticated attackers, which suggested it could have been a state-sponsored perpetrator. The multiple targets included Internet access, television broadcasts, broadcasters' drones, the official website and ticketing systems. The purpose of this attack is open to speculation, and has been variously attributed to the governments of North Korea and Russia, among others.

The huge and temporary infrastructure required to run an event of this nature creates risks. Internet access will be required by journalists, media outlets, sponsors and a host of other organisations all of whom will have varying levels of security. During the PyeongChang Winter Olympics, Wi-Fi provided in the event venue stopped working.

> The main concern for Russia as host nation will be attacks from other nations or affiliated groups seeking to capitalise on geopolitical tensions to mar the event's success.

Operation Olympic Destroyer

During the opening ceremony of the 2018 Winter Olympics in PyeongChang, a cyber attacker targeted key IT infrastructure with denial of service. The attack took systems offline, shutting down display monitors and Wi-Fi connections, as well as the official Olympic Games website. Malware essentially turned off all services and stopped them from rebooting. Security researchers assessed that the attack was highly sophisticated and likely orchestrated by a nation-state or a state-sponsored group. Of particular interest is the web of confusion researchers believe the attackers sowed to complicate attribution to a particular country.

This attack highlights that sophisticated attackers have both the intent and capability to disrupt large-scale events, irrespective of leaving a definitive political message. The threat actors behind this attack seemingly wanted to disrupt the event to embarrass South Korea on the international stage.

Attacks targeting the PyeongChang 2018 Winter Olympics aimed to disrupt the games' infrastructure to create headlines. This is a possible method of attack against Russia as the World Cup host nation.

Host nations are only too aware of such threats. Recent media reports suggested that Russian officials have recognised the cyber threat and are taking steps to strengthen cyber security around the World Cup in response.

The 2018 World Cup is likely to provide opportunities for state-sponsored threat actors to target visiting foreign officials, executives, journalists, and other influential figures who may hold information valuable to intelligence agencies. This kind of targeting is common and is, to some extent, expected at major sporting events.

Foreign and domestic visitors may also be targeted with spyware, as was the case prior to the 2018 Winter Olympics. Leading up to the opening ceremony, some Olympics-affiliated individuals, such as athletes and sponsors, received phishing emails with information-gathering malicious software malware attached.

Any nation playing in the tournament represents an opportunity for embarrassment whilst their profile is raised. Disclosing damaging information on players, management or home clubs will attract more attention during the World Cup.

During the 2016 Summer Olympics in Rio de Janeiro, the World Anti-Doping Agency (WADA) network was compromised, and multiple athletes' sensitive medical information made public online. Attackers, the Fancy Bears, are suspected of being the perpetrators.

There are similarities between the geopolitical issues in South Korea, which may have led to targeted cyber attacks against the PyeongChang Winter Olympics and the current diplomatic standing of Russia.

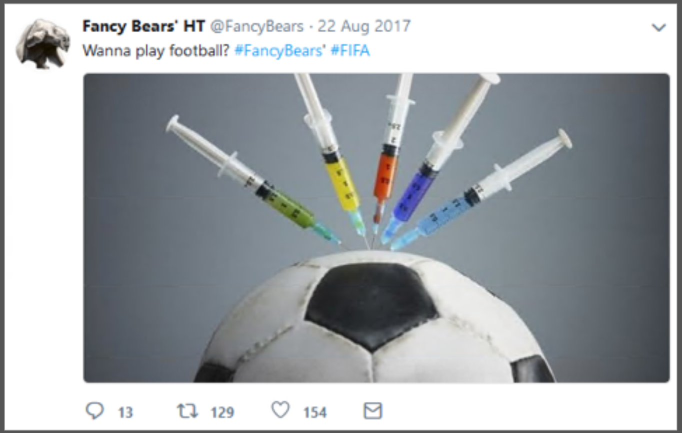
There is a possibility that threat actors hostile to the Russian regime may launch politically motivated cyber attacks against the host nation and World Cup infrastructure to enact retribution or embarrass the hosts.

High-profile fans and delegations present a target for cyber espionage and crime. The increased level of travel to Russia will likely precipitate a rise in attacks.

WADA hack

In September 2016 a suspected Russian state-sponsored espionage group hacked into the World Anti-Doping Agency network. Subsequently, confidential medical data of athletes was released on a website and publicised via social media by a group calling themselves the Fancy Bears. The hack coincided with the Olympic Games in Rio de Janeiro and the data was related to athletes' permissioned use of controlled substances.

The incident followed WADA's recommended blanket ban of all Russian athletes from the 2016 Summer Olympics, for suspected state-run doping programmes. The Fancy Bears have implied doping in football in the past, but whether they will target 2018 World Cup players remains to be seen.



Fancy Bears' HT @FancyBears · 22 Aug 2017

Wanna play football? #FancyBears' #FIFA

13 129 154

Figure 3
Tweet by the Fancy Bears implying doping in football

Managing the risks

Regardless of cyber attackers' motives and targets, it is clear that modern global sporting events present multiple opportunities for attack, from those that are merely inconvenient to others that are highly disruptive and embarrassing.

Cyber-security will be a key concern for the organisers of the World Cup but, despite their enhanced vigilance, the likelihood of attempted and successful cyber attacks will remain high throughout the event. Geopolitical cyber-attacks often spill over into other organisations caught between nations. Cyber risks will be increased for brands and sponsors associated with the World Cup, as well as football clubs and governing bodies.

> What is not clear is whether cyber attacks at this year's event will provoke the level of political reverberation that previous Olympic Games and World Cups have experienced. Whatever the event's outcome, the eyes of the world will be watching Russian leaders along with the football this summer.

Cyber-security tips for travelling fans

Fans and travellers should be aware of cyber risks during their World Cup travels. If travelling with devices from your business know who to contact if they are lost or stolen, as well as having details of your bank or credit card provider.

- Fans should consider scams targetting payments and Wi-Fi networks or Internet cafes.
- Avoid using ATMs or other payment terminals with obvious signs of tampering. Taking a prepaid card or credit card only reduces the impact a fraud may have.
- Restaurant and hotel staff should also be encouraged to keep cards in view of the customers at all times to reduce the risk of credit card skimming.
- Do not rely on hotel safes for strong security. These will always have a PIN or key that can be used to open them, and access may be open to a wide range of current and former hotel staff. Valuable items should be left with reception to hold; make sure you get a receipt.
- Use your own hardware (chargers) for any devices you do bring. Avoid public charging stations wherever you travel; easily accessible public chargers may have been adapted to infect devices with malicious software.
- Be aware of local laws regarding Internet access, and do not attempt to circumvent any web filtering mechanisms that block specific content.
- Be aware that some communication applications may not work, and have alternatives ready. Telegram has recently had its services disrupted in Russia for its non-compliance with Russian law, and other services may become subject to disruption.

Cyber-security tips for businesses

Businesses with operations in Russia or staff travelling to the World Cup should be aware of the potential threats and take appropriate measures. Have in place a proactive crisis management plan to both support staff travelling to the event and to manage any incidents that may occur, especially where there is a sponsorship or business connection to the event.

- Avoid travelling with any IT equipment from work, apart from 'dumb' phones and hardware cleared of any sensitive work data. Work equipment should not be taken outside the countries in which your employer operates. The less data you travel with, the less time needed to protect your equipment.
- Ensure general cyber-security hygiene measures such as the use of up-to-date software, email filtering, anti-virus and intrusion detection systems.
- Phishing emails with a World Cup theme will continue throughout the event. Educate staff on how to recognise phishing emails and not click on suspicious links or provide personal information.
- Local businesses should protect point of sale devices and look out for signs of tampering. Ensure local WiFi networks are well protected using secure encryption and the regular checking of WiFi access points for signs of tampering. Any damaged devices should be removed from the network.
- Local banks should ensure ATMs are checked regularly for signs of cameras, devices or tampering. Any device should be removed and reported to the local police.
- Sponsors should ensure that they have prepared for the possibility of denial of service attacks against websites by having contingency plans during the World Cup.
- Make use of virtual private network (VPN) software when using public or hotel Wi-Fi to protect personal data, but determine prior to travelling whether your VPN provider is permitted in Russia; many of those that do not comply with Russian law are now blocked.

For more information please email
cyber@mishcon.com

MDR CYBER

A Mishcon Group business

Mishcon de Reya LLP
Africa House
70 Kingsway
London WC2B 6AH

T +44 20 3321 7000
F +44 20 7404 5982
E contactus@mishcon.com

mishcon.com/cyber

The information in this document is given without financial or other liability on the part of the writer or Mishcon de Reya LLP. This firm cannot be held responsible for any errors contained in this document. This document sets out findings following an analysis of open source, publicly available material. No reliance should be placed on this document in whole or in part by other parties.