fladgate

Aon
Empower Results®

COVID-19's Impact on the Insights from the FCA's Cyber Coordination Groups

The following article was a joint collaboration between Aon's Cyber Solutions and Fladgate LLP, an international law firm. This alert explores the FCA's "Cyber Coordination Groups (CCG) Insights" published on the 11th of March, 2020 and the impact that COVID-19 has already had on the threat landscape since its release. Aon explores how the previously outlined cyber risks have evolved and key considerations to help FCA regulated firms stay secure, while Fladgate discusses the Legal and Privacy Implications.

Latest Insights from the FCA's Cyber Coordination Groups

The UK's financial services regulator, the FCA, recently published its further insights[1] emerging from discussions held across the seven Cyber Coordination Groups (CCGs) spanning the financial services sector: Insurance, Fund Management, Investment Management, Retail Banking, Retail Investments and Lending, Brokers and Principal Trading firms, and Trading Venues and Benchmark Administrators. Set up in 2017, the CCGs meet each quarter and allow firms to share knowledge of their common experiences and discuss best practices in their approach to cyber security in order to reduce potential harm to consumers and markets. The conversations held at the CCGs, which often include potential ways to solve common problems, will be of interest to the wider financial industry sector and to other sectors as well.

As might be expected, much of the discussion related to the current threat landscape (primarily risks arising from supply chain, social engineering, ransomware, malicious insider, and credential stuffing (where credentials obtained from breaches of other services are used to access accounts)), and to emerging and futures trends, in particular new technology, developing solutions and user requirements, and other factors which may influence and challenge the security response, including development and security in operations (*DevSecOps*), cloud security and payment systems security.

COVID-19 has already changed the threat landscape for FCA-regulated firms
(Contributed by Aon's Cyber Solutions)

The FCA reports that the CCGs maintain a "Cyber Risk Radar" to highlight numerous cyber risks that the sectors face while tracking and categorising the severity of the threat posed to firms. Since the CCG insights were reported on the 11th March, 2020, COVID-19 has already changed the threat landscape dramatically[2]. Threat actors are using the COVID-19 pandemic to cause greater business disruption by targeting front-line organizations across industries with cyber-attacks, phishing scams, fraudulent schemes, and misinformation[3]. Also, the way in which people are conducting day-to-day business has undergone major changes – including both large-scale transformations and shorter-term workarounds imposed by critical business continuity plans, such as rolling out remote working on a scale previously unseen. Those changes, and the attendant uncertainties around the crisis, mean that elements of the threat landscape previously described by CCG attendees pose even greater risks than previously anticipated.

Social engineering and ransomware appear to be more prevalent

- *How have things changed?* Social engineering risks has increased exponentially since the outbreak of COVID-19[4]. Social engineering and related tactics such as phishing are also the attack vector for many ransomware attacks – which can cripple a firm that is already undergoing tremendous stress in light of the ongoing crisis. While the tactics may appear novel, the exploitation of public fear, growing remote workforce, and rapidly changing global circumstances are resulting in a sharp increase in new and malicious activities by

[1] https://www.fca.org.uk/publications/research/insights-cyber-coordination-groups#lf-chapter-id-ccg-insights-cyber-risk
[2] https://www.ncsc.gov.uk/news/security-agencies-issue-covid-19-cyber-threat-update
[3] https://www.ncsc.gov.uk/news/security-agencies-issue-covid-19-cyber-threat-update
[4] https://www.ncsc.gov.uk/news/security-agencies-issue-covid-19-cyber-threat-update

financially motivated actors and extremist groups. In the first few months of 2020, there have been over 300,000 unique threats identified that take advantage of the coronavirus crisis.[5] The UK's National Cyber Security Centre (NCSC) has issued an advisory to the public, citing the proliferation of phony emails with links and attachments purporting to contain important safety information, which when clicked cause devices to be infected with malware, and malicious websites that lure users to click on links. They also stated that criminals were tailoring these attacks to specific sectors to increase the likelihood of success.[6]

- *Things to consider:* CCG members reported that educating employees is crucial to better identifying and reporting possible social engineering attacks and this is now even more important. Employees should be kept informed and made aware of the changing threat landscape. Firms should cultivate a safe communication channel for its employees about COVID-19 and include a list of trusted resources for information to help ensure employees do not need to rely on external, potentially malicious, sources.[7] Furthermore, to lessen the chance of employees sending funds to cybercriminals, firms should revisit their protocols for funds transfers and ensure all employees are fully aware of applicable policies and any changes thereto.

Supply chain and third-party risks have increased

- *How have things changed?* The outbreak of COVID-19 has increased supply chain risk from existing suppliers, but also added new risks where firms have been forced to use new, potentially unvetted, third-party applications for business continuity. For example, self-isolation on a large scale has led to the adoption of new video-conferencing applications, which saw a record 62 million downloads during the third week of March 2020.[8] As a consequence, malicious actors may be able take advantage of any insecurities in these platforms and may impact huge numbers of people. Prominent applications are also attractive targets for credential stuffing attacks.

- *Things to consider:* As previously stated by CCG members, companies should be aware of the cyber risk posed by third parties and align this to their risk appetite, particularly during the pandemic. Organisations should mandate strict security screening procedures for third-party services and if deployed, staff should be educated on how to use these services such as videoconferencing – which is the site of incredibly sensitive conversations – in an appropriate and safe manner.

"Security by design" in crisis mode

- *How have things changed?* Since the outbreak, the focus of SecDevOps teams has suddenly shifted towards either developing remote working systems or increasing remote working capacities as quickly as possible[9]. This may inadvertently result in less attention being paid to the security of these systems. Furthermore, SecDevOps teams are more likely to look towards cloud storage while there is limited access to physical storage drives[10].

[5] https://www.statista.com/chart/21286/known-coronavirus-related-malicious-online-threats/

[6] https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus

[7] For example - https://www.businessinsider.com/hackers-are-using-fake-coronavirus-maps-to-give-people-malware-2020-3

[8] https://techcrunch.com/2020/03/30/video-conferencing-apps-saw-a-record-62m-downloads-during-one-week-in-march/

[9] https://www.computerweekly.com/news/252480177/Covid-19-NCSC-issues-secure-remote-working-guidance

[10] https://www.forbes.com/sites/emilsayegh/2020/03/26/as-covid-19-pushes-businesses-to-their-limit-the-cloud-rises-above/#1bc9fce47851

- *Things to consider:* CCG attendees previously stressed the importance of effectively integrating security into the design process, which is now even more important. While companies focus on keeping business disruption to an absolute minimum, it is crucial to ensure robust security practices remain embedded in the development process; rushed, vulnerable systems should not be released for use. CCG members also highlighted the importance of security in cloud-based environments; this becomes even more relevant as the uptake of cloud services increases.

IT workarounds flourish with widespread remote working

- *How have things changed?* As large-scale remote working has become the new norm, businesses need to understand the associated risks. For instance, individuals can be tempted to dial into confidential calls using their personal mobile phones with potentially faster connection speeds instead of their more secure, corporate devices. While certain employees may unintentionally put their organisations at risk, malicious insiders can also take advantage of the situation as resources are made more accessible while enhanced remote access systems are in use. Indeed, CCG members previously flagged insider threats as a key part of the current threat landscape.

- *Things to consider:* So-called "shadow IT" has been an ever-looming threat to IT management, but as colleagues are forced to work at home and servers are under heavy loads, they should be reminded of the potential consequences of using insecure services and devices. Furthermore, it would be prudent to expand IT help desk capacities while employees adapt to new systems. Companies should also make sure adequate access controls are in place and information is strictly shared on a need-to-know basis.

Legal and privacy implications
(Contributed by Fladgate LLP)

The FCA stresses that the CCGs' insights are not to be treated as FCA Guidance - they do not, for instance, set out the FCA's expectations for systems and controls that firms should have in place to comply with applicable regulatory requirements. However, the examples discussed were all shared by one or more firms within the CCGs and many support existing guidance from the National Cyber Security Centre.

The other legal aspect for firms to consider is their obligations under GDPR. Many of the compliance steps that are discussed above are underpinned by organisations' need to comply with Art 32 GDPR which requires that an "appropriate" level of security is maintained over personal data that an organisation uses in its business, as well as the "privacy by design" obligation set out in Art 25 GDPR. Breaches do not therefore simply expose organisations to financial or reputational loss, but also potentially to regulatory sanction.

One key aspect of compliance is training of staff. With the sudden change in work methods and technologies in use, every business needs to show that it has explained the risk areas and provided adequate training to staff on the "dos and don'ts" while working remotely or in an environment where physical verification and supervision is impossible. Showing that a data breach incident occurred due to individual error or misdemeanour, where the individual had been properly trained in the risk and how to deal with it, will go a long way towards mitigation and therefore reducing any sanction imposed.

If there is a breach involving personal data, it is important that these are logged and where necessary notified to privacy regulators and/or the individuals concerned within the timetable set by Art 33 and 34 GDPR.

It is worth noting that information about a business' staff is itself personal data, and this may affect the extent to which staff members' information can be used for business communication, whether internal or external. Human Resources teams should check with the rest of the organisation to ensure that staff are properly made aware that their personal/home contact details will be used for business continuity purposes, and appropriate consents obtained where necessary.

Another key aspect of GDPR that should not be overlooked is the need to ensure that new cloud service providers handling personal data are engaged on appropriate contract terms as required under Art 28 GDPR, and that such personal data is not exported outside the EEA, unless the requirements for export of personal data set out in Chapter V GDPR are met (which may include use of standard form contracts, or US suppliers signing up to the US Department of Commerce's Privacy Shield scheme).

The UK data protection regulator, the Information Commissioner's Office (ICO) has published guidance on its enforcement approach during the COVID-19 crisis. It has stated:

> "*In deciding whether to take formal regulatory action, including issuing fines, we will take into account whether the organisation's difficulties result from the crisis, and if it has plans to put things right at the end of the crisis. We may give organisations longer than usual to rectify any breaches that predate the crisis, where the crisis impacts the organisation's ability to take steps to put things right*."

The ICO's pragmatic approach is welcome, but organisations should not believe that this gives them a 'free pass' to ignore GDPR during the crisis.

This material has been prepared for informational purposes only and should not be relied on for any other purpose. You should consult with your own legal and information security advisors or IT Department before implementing any recommendation or guidance provided herein.