ALERT ▪ London ▪ Government Enforcement / White Collar Criminal Defense

March 17, 2020

UK Financial Conduct Authority Publishes Insights from the Cyber Coordination Groups

The FCA has published a summary of key cyber security issues identified from its Cyber Coordination Groups ("CCGs"). CCG members are drawn from a range of sub-sectors in the financial services industry, including insurance, fund management, investment management, retail banking, retail investments and lending, brokers and principal trading firms, and trading venues and benchmark administrators. The CCGs discussed current industry concerns relating to four themes: cyber risks, identity and access management, third parties and supply chain, and malicious emails. The FCA's summary of those discussions provides a helpful insight into the cyber risks firms in the financial sector are observing and the measures they are implementing to mitigate those risks.

Attorneys
Rosemarie Paul
Rohan Massey
Tom Jackson

Cyber Risks: Key cyber risks identified included supply chain partners (a particular risk for utility and infrastructure providers, which typically have limited choices and thus limited leverage to ensure supply chain resilience), social engineering (use of deceptive tactics to obtain otherwise unauthorised access to information), ransomware, malicious insider threats, and credential stuffing (where credentials obtained from a data breach are used to attempt to log in to other, unrelated services).

Amongst the developing trends in the cyber security space, the CCGs pointed to development and security in operations (known as "DevSecOps"), which involves integrating security into each stage of an organisation's development approach. This contrasts with prior approaches, which tended to be more reactive and remedial in nature. The principal advantage of DevSecOps is that security is "baked into" a firm's security operations, rather than layered on top, meaning security teams can respond to incidents with greater speed and agility. Such an approach also potentially allows earlier identification and correction of vulnerabilities and an ability to respond rapidly to changes in the threat landscape.

CCG members also noted the development of cloud security as an emerging risk area, and that data held in cloud environments should be encrypted and protected by appropriate intrusion detection/prevention controls. In some cases, it may be advisable to include "kill switch" technology, which allows for immediate disconnection to manage the risk of a cyber attack having a more widespread impact.

CCG members also identified payment systems security as a key emerging area of cyber security risk. They noted that attackers are increasingly targeting core banking systems, including those relating to payment messaging and transaction authorisation. CCG members recognised that there needs to be closer industry cooperation to assist financial institutions in identifying threats to payment systems and encourage firms to share best practices to mitigate risks posed by cyber threats to core banking systems.

Identity and Access Management: The CCGs discussed identity and access management ("IDAM") policies, processes and controls. They suggested that financial institutions should proactively review and challenge password policies and procedures governing who is authorised to approve access, and who in fact subsequently gains access, to relevant systems and data. In that regard, automated tools should be used to monitor administrative and important accounts, including those with access to important business services and systems. The CCGs noted that it is best practice to extend such measures to include cloud services, third parties, outsourcing and intra-group arrangements. Administrative or privileged users should utilise a separate, dedicated system for high risk tasks, and personnel employed in such roles should be encouraged to use a separate account for routine tasks such as accessing email and browsing the internet.

With respect to password management, the CCG members agreed that firms should ensure all default passwords should be changed prior to deploying a system. Firms should verify that password changes meet password eligibility criteria and consider password blacklisting or other password hygiene policies. The use of password managers (which store and protect all of a user's password details in one location) and single sign-on solutions was also discussed as a means of mitigating the risks that employees will record passwords in unsecure documents. Finally, CCG members emphasised the importance of implementing appropriate logs and alerts when an account is added, modified, disabled or removed from any groups that contain administrative privilege.

Malicious Emails: The CCGs noted that email-based cyber attacks are constantly evolving and becoming more sophisticated. CCG members stressed the importance of determining what "normal" email traffic looks like by monitoring both emails that are allowed and blocked, which in turn assists a firm in identifying "abnormal" email activity. Email servers should be configured to stop malicious attachments and links at the perimeter, and firms should consider utilising dedicated and freely available resources to identify potentially malicious email sources.

CCG members also emphasised the importance of non-technical controls. Firms should create a mechanism that makes it easier for users to report suspicious emails, which in turn provides data that can be used to help improve controls and awareness training. Firms should also provide basic cyber training, which should be rolled out on a risk basis according to users' roles, access and responsibilities. Finally, CCG members cautioned against making user names something easily guessable, such as user email addresses.

Third Parties and Supply Chain: CCG members agreed on the importance of conducting pre-engagement due diligence to ensure a supplier's approach to managing cyber risk meets standards set by the organisation. Security standards should be clearly defined and communicated to suppliers, and suppliers should be monitored on an ongoing basis to ensure continued compliance with those standards.

CCG members discussed how they screen employees and how they ensure third-party suppliers screen employees and sub-contractors using the same principles. Ideally, the suppliers' employees should be subject to the same vetting standards as employees of the firm using them. Firms noted the risks associated with third-party access control to buildings, systems and data, which should be monitored and managed using good security practices such as virtual private networks, email authentication and secure application programming interface technology. Firms should ensure all contracts with suppliers contain clear guidance on the definition of support security and incident management roles. Critical suppliers should be involved in the firm's business continuity plan and cyber incident exercises.

The CCGs' most recent discussions demonstrate the constantly changing landscape of cyber security threats and the increasingly sophisticated measures firms are taking to combat those threats. Given the FCA's recent strong focus on cyber security and the growing number of costly and reputation-damaging cyber incidents that have taken place in recent years, informational security should clearly be a high priority for firms and their boardrooms moving forward.

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have.