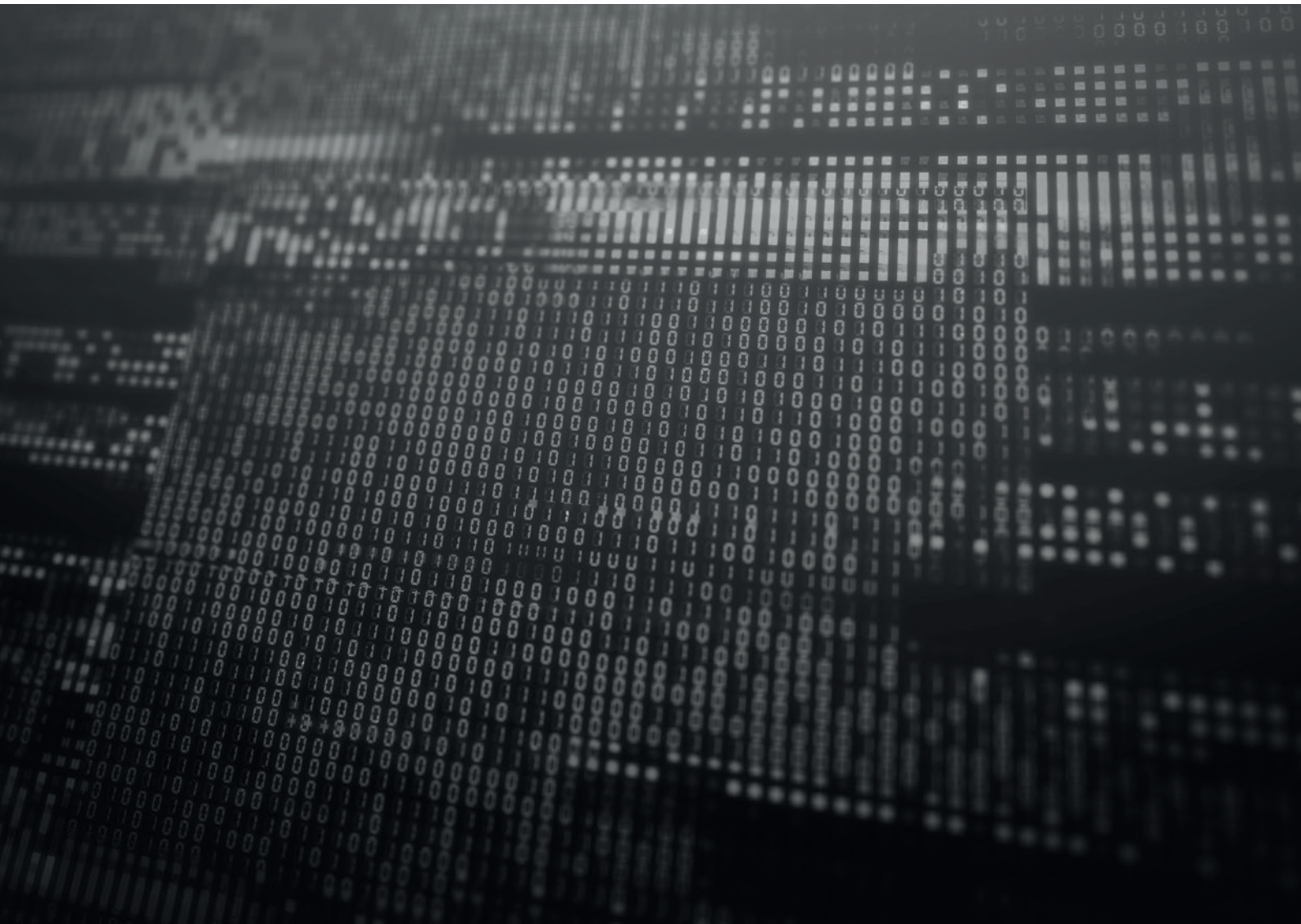
CAPCO

COVID-19 & CYBERCRIME:

HOW TO MITIGATE THE RISKS



INTRO

The financial services industry has long been a target for cybercriminals seeking financial gain, however the threat landscape is changing as criminals seek to exploit the COVID-19 pandemic.

Reports show an increase in coronavirus-themed scams, fraudulent activity, and remote working network vulnerabilities. Back in April, Europol, The European Union Agency for Law Enforcement Cooperation, reported that 'the impact of the COVID-19 pandemic on cybercrime has been the most visible and striking compared to other criminal activities'.

For financial institutions, cybercrime presents consumer fraud risks, as well as risks to data, networks, and systems. To mitigate these risks, firms should examine their risk management strategy, ensuring the holistic control framework is still effective and a strong security culture – the human firewall – remains intact.

THE RISKS

Consumer fraud risks

For a long time now, cyber tools such as hacking, malware, and phishing have provided opportunities to commit fraudulent activity at arms-length with little chance of prosecution. Today, the ongoing pandemic provides cyber criminals with new and sadly effective 'click bait' to augment these cyber tools. A joint advisory report published by the UK's National Cyber Security Centre (NCSC) and the US Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Agency (CISA) stated that criminals have adjusted social engineering techniques to exploit curiosity and fear of the pandemic, to lure victims into revealing confidential data or downloading malware.

Using COVID-19 as 'click bait' is proving to be effective. The Met Police, the National Crime Agency and Action Fraud have all released warnings about the increase in scams. Examples include criminals sending emails from what appears to be a trustworthy source such as The World Health Organisation or SMS messages from UKGOV. The email or SMS may direct the receiver to a fake login page requesting confidential data or bank details, which criminals can then sell or use for fraudulent activity. The 'human firewall' – the commitment to strong security culture and best practice – seems to be flawed when detecting such messages.

For financial institutions, COVID-19 has provided a platform for increased fraud risks, often targeting the most vulnerable customers.

Data risks

Criminals also use cyber tools to breach network defences and steal sensitive data. Less secure home working arrangements, due to COVID-19, further increase data risks, providing less secure entry points for cyber criminals that would normally be seen when using a managed corporate network. The NCSC and CISA observed an increase in scanning for known vulnerabilities in remote working tools, including video conferencing software. Criminals are also known to be exploiting vulnerabilities in virtual private networks (VPNs) or unsecured remote desktop protocol (RDP) endpoints to gain access to data.

Data breaches usually involve stealing information such as names, date of births, addresses, passwords and bank details, which can be sold on criminal marketplaces. Recent trends have also seen an increase in biometrics and digital fingerprints being stolen to circumvent new machine-learning anti-fraud systems used to secure mobile banking. In 2019, Kaspersky discovered a large, underground marketplace for digital fingerprints, with over 60,000 digital identities up for sale.

The risk of data loss is high and can severely damage the relationship of trust between a bank and its customer. Data breaches must also be reported to the regulator under GDPR and can result in large regulatory fines.

Network and system risks

As COVID-19 western lockdowns loomed, financial institutions came under increasing pressure to achieve remote working quickly whilst maintaining business continuity. Firms are therefore likely to have implemented some form of information technology workaround, such as allowing the use of virtual desktop instances from personally-owned computers. Introducing workarounds may have been essential from an operational perspective, but often leaves networks open to the risk of malicious access. Workarounds go against fundamental principles of securing a 'system by design' and can weaken previously secure network configurations.

MITIGATING THE RISKS

The FCA recommends firms follow practical guidance from the NCSC on securing IT systems. The NCSC's 10 Steps to Cybersecurity framework offers simple guidance on how to effectively protect against cybercrime, breaking down essential components of cyber defence. The NCSC has also published scores of guidance in response to COVID-19 focusing on issues such as remote working, reiterating the fundamentals in the 10 Steps.

It is perhaps more critical than ever that these core controls are implemented effectively and holistically as part of a cyber risk management framework.

1. Risk management regime

An established risk management regime provides the founding control in mitigating cybercrime risk. Effective risk management should be driven from the top-down, with clear governance structures and embedded roles and responsibilities throughout the organisation. Firms must ensure cybercrime risk is a permanent, executive agenda item and articulated as part of enterprise-wide risk management to ensure appropriate understanding and context.

In response to COVID-19, firms should identify and assess any new cyber risks, and ensure proportionate controls are in place to effectively mitigate these risks. The World Economic Forum recently described cyber risk assessments as a critical 'vaccine' against cybercrime, preventing 'costly wastes of time, effort and resources' and enabling 'informed decision-making'.

2. Network security

To protect networks from intrusion, firms should defend network perimeters as well as secure layers of segregated internal networks – deploying a defence-in-depth approach. Controls and system solutions should be put in place to manage access to the network, including firewalls, malware checking solutions, network scanning and intrusion detection software. Such access controls are even more critical in a remote working environment, with new network access points spawning potential vulnerabilities.

3. Managing user privileges

Users should be provided with a reasonable (but minimal) level of system access aligned to their role. Network logs should be deployed to track and review all network access, whilst also acting as an audit log for any post-incident investigations. During COVID-19, it is important that user privileges remain proportionate and particular care is taken to ensure access by any third-party contractor is tracked, logged, and managed.

4. User awareness and education

Training is essential in mitigating cybercrime risk particularly as human error is often the weak link. Users must be aware of expectations set by the Board and their individual roles and responsibilities in terms of cyber risk management, as set out in governance policies and job descriptions.

As recommended by the FCA's Cyber Coordination Groups (CCG) in 2019, firms should ensure 'plain language' is used to articulate cybercrime risks and responsibilities, to ensure staff understand their role. An effective training programme will help instil security conscious habits, which can, over time, help to develop the 'holistic security culture' expected by the FCA.

In response to COVID-19 and the increase in certain types of cybercrime, many firms are rolling-out targeted training and awareness programmes on topics such as email phishing and remote working. This should be followed up with clear communication from management on expectations and escalation routes for any issues.

5. Incident management

Incident management through effective response planning is critical in reducing the impact of cyber incidents. Effective response plans should clearly document immediate actions, roles and responsibilities, investigation protocols, communication channels, and steps to manage business continuity. The FCA CCGs affirm that incident response plans should be embedded before an incident happens through 'scenario-led exercises' and reviewed by external experts as required.

MITIGATING THE RISKS CONTINUED

COVID-19 will likely have triggered elements of an incident response plan. A few months into remote working, firms could start to review this response plan – did it work and how could it be refined? Is the current incident response plan still effective whilst remote working is in place?

6. Malware prevention

Malware can infiltrate a network or system through various exchanges such as email, removable media devices and web browsing, and is therefore very difficult to manage – particularly with an increase in well-engineered phishing attempts relating to COVID-19.

The risk must be mitigated as part of a defence-in-depth approach, with appropriate security controls and an anti-malware policy ensuring consistent implementation across the firm. The NCSC advises that data should be scanned on entry through the network perimeter, content restrictions should be applied to web browsing, and 'end-user device protection' should be applied to protect against host-based malware. Despite difficulties with remote working arrangements, firms should also ensure updates and security patches are still installed regularly to minimise vulnerabilities and malware prevention training is provided to employees. Staff must be empowered to act as the human firewall – the front line of defence.

7. Monitoring

Monitoring is critical in assessing whether a system is being attacked. Inbound and outbound network traffic, log-in flows, and other user activity should be monitored through a monitoring tool and/or intrusion detection system.

Detecting an attack requires an understanding of 'normal' versus 'malicious' system use, however remote working arrangements will have radically changed 'normal' traffic and log activity. Firms should assess and understand the new normal, carefully considering any adjustment or recalibration of monitoring systems. The firm must ensure any adjustments are in line with risk appetite and the established monitoring strategy.

8. Removable media controls

Removable media, such as USB sticks, can be used to transfer malware and sensitive data in and out of secure networks. The NCSC recommends assessing business need for removable media - in most cases, removable media is not needed for daily activities and can be restricted.

If removable media must be used, particularly sharing data in the COVID-19 environment, appropriate controls should be put in place including encrypting data on media, managing any reuse, and destroying media when no longer needed. Employees should also continue to only use company-issued devices.

9. Home and mobile working

Mobile working practices have experienced rapid growth due to COVID-19 lock-down restrictions, increasing risks to data. The NCSC recommends firms have an established mobile working policy, with clear actions and responsibilities for users. Users should be trained on remote working and device maintenance, particularly if they have been issued with new devices such as laptops to facilitate remote working. Data should also be protected through encryption and the amount of data stored on a local device should be minimized.

10. Secure configuration

The NCSC sees proactive configuration management as a 'key security control' against cybercrime. Cybercriminals can exploit software bugs or poorly configured networks to gain access to a secure system. This is particularly the case in COVID-19, with newly (and perhaps hastily) configured network workarounds. These risks can be minimized by adhering to an established configuration strategy, assessing and documenting any unavoidable divergences. This strategy should ensure vulnerabilities are fixed, patches are applied, and systems are configured securely, despite the challenging environment.

AUTHOR

Jessica Cath
Senior consultant
Jessica.Cath@capco.com

CONTACT

Richard Plumb
Partner
Richard.Plumb@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com**, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO