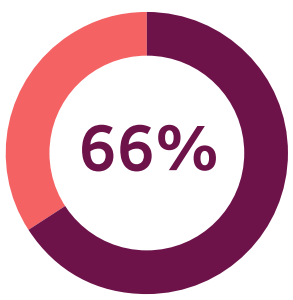
FINANCIAL CONDUCT AUTHORITY

Good cyber security – the foundations

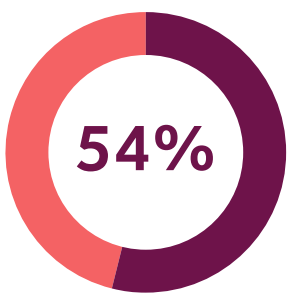
Cyber attacks are increasing in number, scale and sophistication, and pose a threat to all financial services firms. We expect you to be able to protect the sensitive information you hold.

Is your firm capable of defending itself against cyber attacks?

Cyber threats in the financial sector

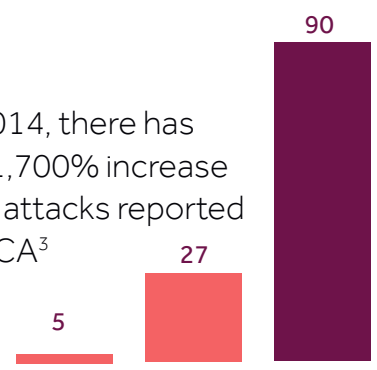


of medium/large UK businesses were subjected to cyber attacks in 2016[1]



of UK businesses have been hit with ransomware attacks[2]

Since 2014, there has been a 1,700% increase in cyber attacks reported to the FCA[3]



1. Cyber Security Breaches Survey 2017
2. Malwarebytes: 'State of Ransomware 2016'
3. FCA data

Effective cyber security practice

Manage the risk:
You need to know what information you hold and why you hold it. **Is it classified? Do you review who has access to your most sensitive data? Do you understand your vulnerabilities?**

Encryption:
Protect your sensitive data. **Do you use encryption software to protect your critical information from unauthorised access?**

Disaster recovery:
Backup your critical systems and data, and test backup recovery processes regularly. **Do you know if you are able to restore services in the event of an attack?**

Network and computer security:
Keep systems, software and apps up-to-date and fully patched. **Do you make sure your computer network is configured to prevent unauthorised access?**

User and device credentials:
Ensure your staff use strong passwords when logging on to hardware and software. Change the default Administrator credentials for all devices. **Do you use two-factor authentication where the confidentiality of the data is most crucial?**

Awareness:
People are an integral part of the cyber security chain. **Do you educate your staff on cyber security risks?**

Accreditation:
Gaining a recognised accreditation, such as ***Cyber Essentials***, could improve the security of your firm. **Do you align your firm to a recognised cyber scheme?**

Information sharing:
Sharing threat information with your peers, through networks such as the ***Cyber Security Information Sharing Partnership (CiSP)***, is a vital tool in strengthening your cyber defences. **Are you a member of any information-sharing arrangements?**

Cyber incident response – what should you do?

Reporting a cyber incident

Under Principle 11 of the FCA Handbook, you must report material cyber incidents. An incident may be material if it:

- results in significant loss of data, or the availability or control of your IT systems
- affects a large number of customers
- results in unauthorised access to, or malicious software present on, your information and communication systems

We will update these requirements in line with any future regulations.

How to report a cyber incident

1. If you judge a cyber incident to be material, report it as follows:
   - **Fixed firms** should contact their named FCA supervisors, and **flexible firms** should call **0300 500 0597** or email ***firm.queries@fca.org.uk***
   - If your firm is **dual-regulated**, you should also contact the ***Prudential Regulation Authority***
   - If the incident is **criminal**, you should contact Action Fraud by calling **0300 123 2040** or through ***their website***
   - If the incident is a **data breach**, you may need to report it to the ***Information Commissioner's Office***
2. Refer to the ***NCSC guidance*** on reporting incidents
3. Share on the ***CiSP*** platform

Find out more

Cyber Security Information Sharing Partnership (CiSP)
www.ncsc.gov.uk/cisp

CiSP is a secure joint industry and Government initiative for exchanging cyber-threat information. Membership gives you full access to the UK Financial Services Cyber Incident Response Framework and provides you with vital threat information.

10 steps to cyber security
www.ncsc.gov.uk/guidance/10-steps-cyber-security

The National Cyber Security Centre's website gives further advice on how to protect your firm from a range of cyber and information security threats.

FCA Cyber resilience webpage
www.fca.org.uk/firms/cyber-resilience

Our website has further guidance on cyber security and we will keep this up to date.

In partnership with BANK OF ENGLAND PRUDENTIAL REGULATION AUTHORITY, HM Treasury, National Cyber Security Centre a part of GCHQ