NIG Cyber Cover

Our Cyber policy is available alongside a range of complex products, including Commercial Combined, Protect, Essential Property Owners, Premier Property Owners and Motor Trade.

Our Cyber Cover product is designed to cover cyber risks which could be damaging to businesses that use technology and are involved in the storage or use of data.

Features

- Costs up to £50,000 for locating and removing a computer virus from your computer system (even if damage or disruption has not been caused) and hiring professionals if your computer system has been affected by a virus or attack to recommend how to prevent your computer system from being infected by a computer virus or being hacked.
- Investigation costs for possible repair, replacement or restoration where a claim has been accepted up to £50,000.
- Loss prevention measures to prevent or minimise further expected damage or future losses up to £50,000.
- Temporary and fast-tracked repair, replacement or restoration where a claim for damage has been accepted up to £100,000 (but no more than 50% of the cost of damage or other loss covered by the policy).
- Contractual fines and penalties up to £25,000 as a result of not keeping to your data privacy obligations (not fines and penalties which you cannot insure against by law).

All sums insured, limits of liability and extra cover limits operate on a per occurrence basis rather than a total for the period of insurance, other than the Cyber Attack Limit.

Key selling points

- Minimum cyber premiums from £92 + IPT.
- Statement of Fact for risks with limits under £500,000.
- Variable excesses and Indemnity periods available.

Standard covers

Cover	Minimum	Maximum
Cyber crime	£25,000	£100,000
Cyber liability	£25,000	£1,000,000
Data-breach expense	£25,000	£1,000,000

Optional covers

Cover	Minimum	Maximum
Hardware	£25,000	£5,000,000
Data corruption and extra cost	£25,000	£1,000,000
Cyber event - loss of business income	£25,000	£1,000,000

Policy level

Cover	Maximum
'Cyber attack limit'	£250,000*

The amount in brackets denotes the standard limit provided. *The most we will pay in total for the period of insurance for all claims that are the result of events which is not just targeted at the insured and your computer system will be the lower of the total of the sums insured, limits of liability and extra cover limits or the Cyber attack limit. The Cyber attack limit will be reduced by amounts previously paid. This is a summary of the cover available. Please refer to the Policy Booklet for full terms and conditions.

To find out more about NIG Cyber Cover, talk to your local team today.

If you would like more copies of this guide to share please visit www.nig.com for a digital version.

UK BUSINESS, COVERED

Is your business cyber safe?

UK BUSINESS, COVERED

Are you at risk of a cyber attack?

Every organisation is a potential victim, depending on the opportunities you offer your attacker, their technical capabilities and their motivation.

46% of all UK businesses identified at least one cyber security breach or attack in the last 12 months. This rises to 66% among medium firms and 68% for large firms.*

Who might attack you?

- Cyber criminals to make money through fraud or by selling your information.
- Industrial competitors to gain economic advantage.
- Hackers who enjoy the challenge of breaching security.
- Hacktivists with political or ideological motives.
- Employees or those with legitimate access either accidentally or deliberately.

Common types of breaches*

72% were caused when staff received fraudulent emails

33% resulted from viruses, spyware or malware

27% by people impersonating the organisation by email or online

17% caused by ransomware

This shows that vigilant staff are just as important as good technical systems in ensuring your cyber security.

What advice can you give your staff to help avoid security breaches?

Systems security

Restrict personal use of systems and prevent software downloads. Keep computers locked when not in use.

Acceptable email use

Email is a major cause of security breaches so THINK before sending and receiving emails, especially those with attachments.

Create a password policy

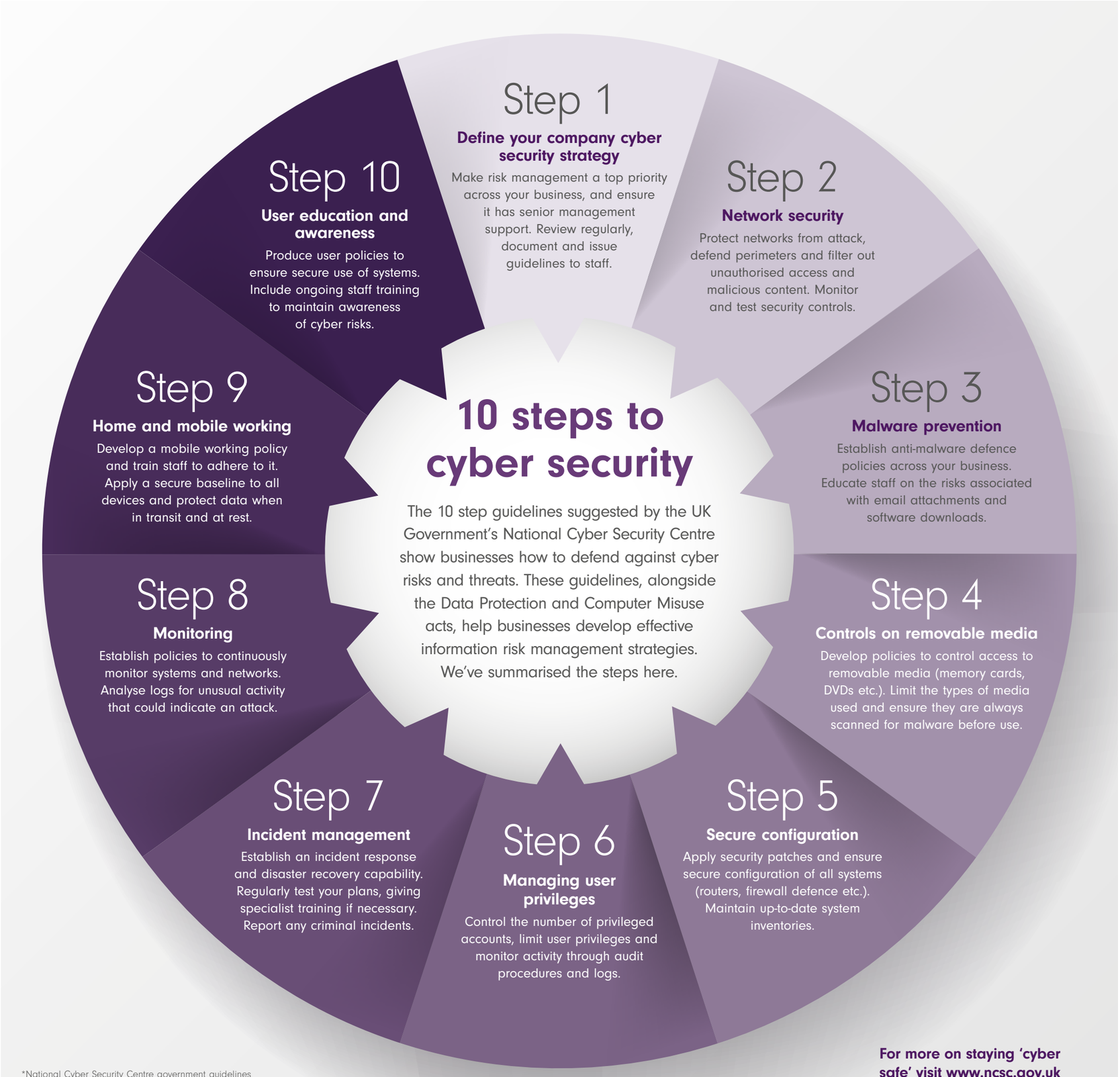
Ensure passwords comply with minimum criteria and are frequently changed.

Internet and social media use

Issue guidelines minimising personal use of the internet and clarifying your social media policy. Don't allow staff to use social media on work systems, or to refer to work related matters on personal social media accounts.

For more details on our Cyber Cover product, please contact your Senior Business Development Manager at www.nig.com/Contact-Us

*2017 Ipsos MORI Cyber Security Breaches Survey



*National Cyber Security Centre government guidelines

For more on staying 'cyber safe' visit www.ncsc.gov.uk