

Your campaign in a box

Resources and guidance to help
you talk about **cyber cover**

Let's go



How to use these resources

You can use the marketing content in this document as it is,
or you can use it as inspiration to create your own.

From email templates, to social posts, to comprehensive guides,
to claims scenarios, you'll also find links to extra content that can
help you start communicating with your clients today.

Ultimately, we all want to help clients understand the risks posed by
cyber attacks, so the sooner we get the message out the better.

This guide is intended for brokers selling commercial lines insurance. It is important to make sure that your prospecting and pipeline management strategy complies with all applicable law. This guide should not be relied on as legal advice. For information about your obligations under data protection law, see the UK Information Commissioner's Office website at <https://ico.org.uk>. The ICO produces guidance and resources for organisations, including about direct marketing. See [here](#) for an example. Note that different rules can apply to direct marketing to sole traders, some types of partnerships and unincorporated bodies.

Contents

Your toolkit



**Changing your clients'
view of cyber cover**



**Your ready-made
five-stage campaign**



**Cyber resources
for you to use**

Best practice for best results

**Campaign top tips –
best practice for best results**

**Email marketing –
in a nutshell**

**Social media marketing –
made simple**

**Writing website content –
the right way**



03



Your campaign in a box – Resources and
guidance to help you talk about cyber cover



Changing your clients' view of cyber cover

If you want to change the way your clients view cyber insurance, it helps to understand what they are thinking and feeling, and what they are doing at different points of their decision journey.

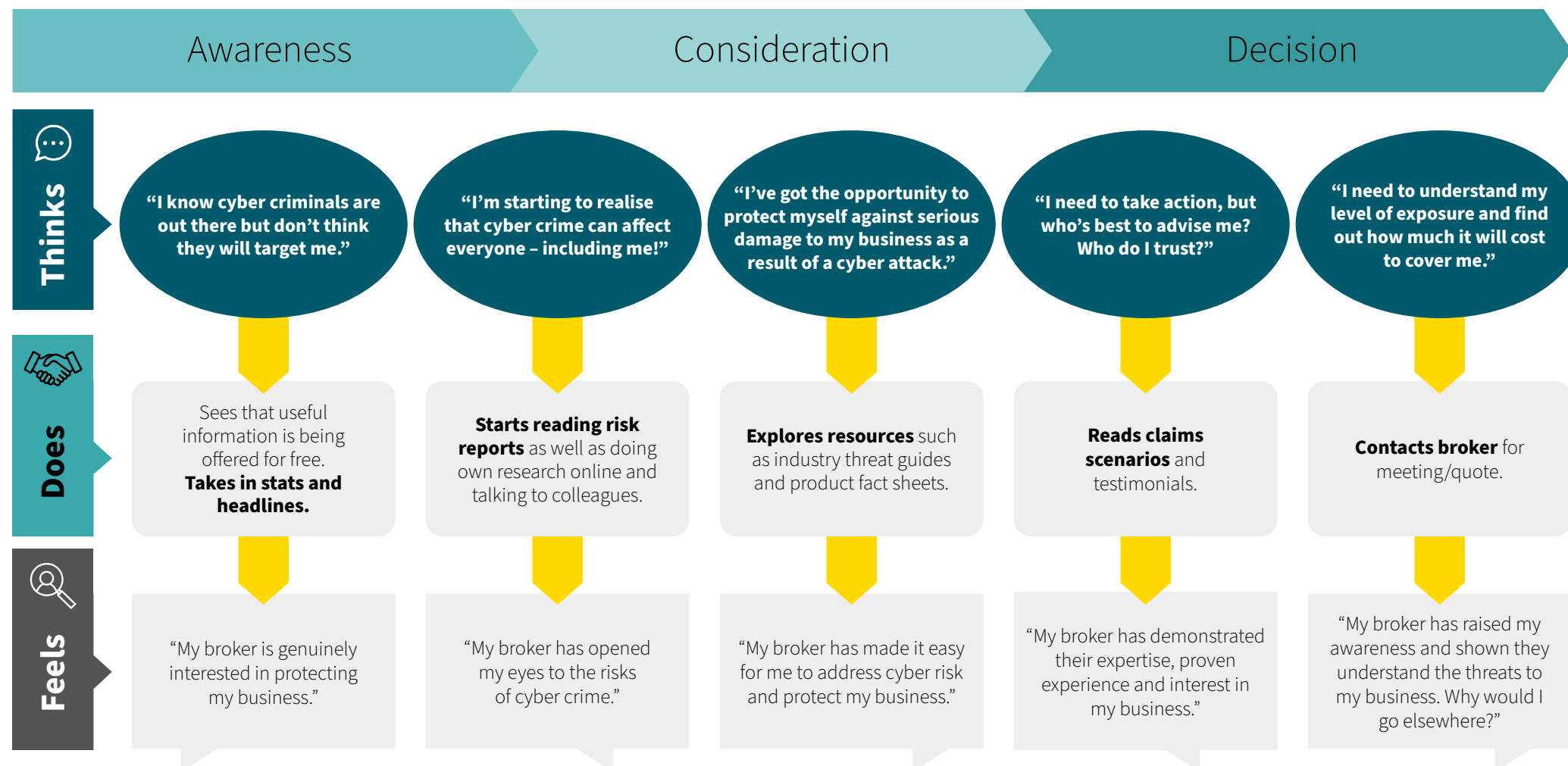
The aim is to help take them from thinking they won't be impacted by cyber crime, to wanting to take steps to ensure they're protected if it happens to them.

Your clients' view ▶



Protection against the impact of cyber crime

The potential decision-making journey of your clients





Your ready-made five-stage campaign

Use our ready-made campaign to quickly and easily share helpful information with your clients.

The five-stage model ▶



Running a campaign in five stages

Ready to start your cyber cover campaign? **Click on each stage to see example comms for each.**

Want to know more about best practice? Keep reading!

	What do you want them to know?	What do you want them to do?	What can they learn from?	What channels should you use?
Stage 1	How cyber threats pose a risk to their business	'Find out more about the cyber threat landscape'	Business Attitudes to Cyber Security and Cyber six reasons	  
Stage 2	Why your clients should listen to you about cyber risks	'Find out more about us'	Industry threats guide	  
Stage 3	What solutions are available to help them	'Ask us about the cover available'	Cyber Respond and Cyber Complete product sheets	  
Stage 4	How breaches can happen and how they can be avoided	'Read our claims scenarios'	Cyber claims scenarios	  
Stage 5	Why they should consider acting now	'Make an appointment/call us today'	Cyber cover checklist	  
Cross-sell	How cyber insurance can be added to their policy at renewal	'Make an appointment/call us today'	An indicative quote and cover details from Aviva	  



Top tip:

monitor email opens to capture warm leads



Top tip:

get employees to share social content



Top tip:

follow up on warm leads over the phone if possible

Campaign stage 1: How cyber threats pose a risk to their business



Email example:

Subject line: **It's never been more important to protect your business against cyber attacks**

When everything's digital, everyone's vulnerable

Dear <Name Surname>

The increased digitalisation of our world is just a fact of life. Whatever line of business you're in, there's no escaping the internet and computerised systems. But alongside the many benefits the digital age brings, it can present criminals with more opportunities than ever before. As such, there's a growing need for all businesses to be aware of the cyber threats they face.

Here are **six reasons from Aviva** why all businesses should consider cyber cover.

<<Download a dual-branded version of Cyber six reasons from Broker Create and either insert a link to the report held on your website, or add a copy of the report to your email as an attachment>>

How common are cyber attacks?

Government research shows that:

- **32%** of UK businesses have experienced a breach or cyber attack in the last 12 months*
- the average annual cost of cyber crime for UK businesses is estimated at **£15,300** per victim*

And it's not a problem limited to bigger businesses. The majority of cyber attacks aren't specifically targeted, meaning any business, large or small, can be the victim. And as cyber criminals employ increasingly sophisticated strategies, it's never been more important to ensure your business is protected.

You can find out more about the cyber risk landscape in this useful report from Aviva:

[Business Attitudes to Cyber Security Report](#) **<<Download a dual-branded version of the report from Broker Create and either insert a link to the report held on your website, or add a copy of the report to your email as an attachment>>**

We're here to help you get suitable cyber insurance that enables you to continue to trade with confidence and allows you to build resilience in a landscape that is ever-changing and increasingly complex.

To help you understand what level of cyber insurance is right for your business and your budget, please get in touch either by calling us on <tel no> or emailing us at <email address>.

*Source: Cyber Security Breaches Survey, 2023, DCMS. Government sources contain public sector information licensed under the Open Government Licence v3.0.
<<include telephone call charge/recording information as applicable>>

Social post example:

Almost every business holds valuable information – from payment details and employee data to intellectual property and supplier agreements. Cyber criminals could use this information to disrupt, extort or steal from your business.

Find out more about the risks cyber criminals pose to your business by taking a look at Aviva's latest Business Attitudes to Cyber Security Report.

<<Download a dual-branded version of the report from Broker Create and either insert a link to the report hosted on your website, or add it to the social platform as an attachment>>

32% of businesses experienced a cyber attack or breach in the last 12 months.

What would your response be?

Source: Cyber Security Breaches Survey, 2023, DCMS
Government sources contain public sector information licensed under the Open Government Licence v3.0

In association with
AVIVA

<Broker logo here>



Like



Comment



Repost



Send

Discover resources created for your cyber insurance campaign **here**.

Download assets to feature in your campaign at **Broker Create**.

Campaign stage 2: Why your clients should listen to you about cyber risks



Email example:

Subject line: **Cyber threats are putting UK businesses at risk**

The fallout of a cyber breach can't be ignored

Dear <Name Surname>

Most SMEs assume cyber attacks are an issue only big organisations need to worry about. But the truth is, cyber crime is a numbers game – criminals cast a wide net, using malware, ransomware and social engineering to attack indiscriminately, then quickly take advantage of any weaknesses they find.

If you don't have a plan for how you'd respond to finding yourself locked out of your system and facing a ransom demand, the consequences could be extremely damaging.

Potential outcomes of a cyber attack

- **Reputational damage** – rebuilding customer trust after a data breach can be challenging, and reputational impact can be significant and long-lasting.
- **Financial impact** – the costs associated with addressing and recovering from an attack could have a negative impact on how the business is able to trade moving forward.
- **Operational disruption** – if an attack leaves you unable to carry out business for a prolonged period, it may be challenging to fully recover.
- **Legal and regulatory implications** – failure to adequately protect customer data can lead to legal consequences, including fines and lawsuits.
- **Intellectual property theft** – the competitiveness of your business could be affected if valuable IP such as proprietary processes, patents or trade secrets are revealed.

How can we help protect your business?

You can find out more about the specific threats to your sector and the impact they might have in this [Industry threats guide](#) from Aviva. <<Download a dual-branded version of the guide from Broker Create and either insert a link to the guide hosted on your website, or add a copy to the email as an attachment>>

And if you'd like our help with understanding how a cyber event or attack could impact your business, you can reach us on <tel no> or email at <email address>

*Source: [Cyber Security Breaches Survey, 2023, DCMS](#)
Government sources contain public sector information licensed under the Open Government Licence v3.0
<<include telephone call charge/recording information as applicable>>

Social post example:

More and more businesses are recognising that their own in-house IT capabilities may not be sufficient should a cyber attack or breach take place. Yet despite this, there's a big gap between awareness and action.

To understand more about the specific threats to your sector and the impact such an event might have, take a look at this [Industry threats guide](#) from Aviva.

<<Download a dual-branded version of the guide from Broker Create and either insert a link to the guide hosted on your website, or add it to the social platform as an attachment>>

63% of UK businesses
do not have adequate
cyber cover in place.
Is yours one of them?

Source: Cyber Security Breaches Survey, 2023, DCMS
Government sources contain public sector information licensed under the Open Government Licence v3.0

In association with
AVIVA

<Broker logo here>



Like



Comment



Repost



Send

Discover resources created for your cyber insurance campaign [here](#).

Download assets to feature in your campaign at [Broker Create](#).

Campaign stage 3: What solutions are available to help them?



Email example:

Subject line: **Give your business stronger protection from the impact of cyber threats with Aviva's new cover**

The right protection for a fast-evolving threat landscape

Dear <Name Surname>

Are you prepared to deal with a cyber attack, or aware of what you'd do in the event of a breach?

This is where cyber insurance can provide real value. Without continuity plans in place or access to specialist IT support, an attack could have a huge impact on your business, compromising your reputation and livelihood.

The rapid breach response your business would expect

A rapid response to an incident or breach is vital. Recovery requires co-ordinated expert support to reduce the impact. That's what the new Aviva Cyber cover is designed to deliver – quick and effective restorative action, tailored to the needs of your business.

For small and micro businesses, there's **Cyber Respond**, available from as little as £50 a year.*

At the heart of Cyber Respond is a 24/7 incident response service giving you the immediate support you need to minimise any damage. This includes:

- a dedicated incident manager
- specialist IT forensics and consultants
- PR reputational experts
- support throughout your recovery activities
- no excess for any expert guidance or initial advice, applicable as standard

Aviva's **Cyber Complete** cover offers all the features above, alongside cover designed for the needs of larger businesses and mid-market organisations, including resilience improvement, cyber extortion and business interruption.

You can find out more about the benefits of Aviva's cyber offering by taking a look at the [product factsheets for Cyber Respond and Cyber Complete](#). **<<Download dual-branded versions of the Cyber Respond and/or Cyber Complete product factsheets from Broker Create and either insert a link to them hosted on your website, or add to your email as attachments>>**

And of course, you can always discuss your cyber protection needs by calling us on <tel no> or via email at <email address>

*Plus Insurance Premium Tax and subject to individual circumstances and cover level.
<<include telephone call charge/recording information as applicable>>

Social post example:

A rapid response to a cyber incident is vital. Your recovery rests on co-ordinated expert support that can act with immediate effect to reduce the impact.

Aviva's Cyber Respond and Cyber Complete offerings both provide 24/7 rapid incident response alongside protection suited to businesses of all shapes and sizes.

CTA 1: For information on Aviva's cyber products, take a look at our factsheets.

<<Download dual-branded versions of the Cyber Respond and/or Cyber Complete product factsheets from Broker Create and either insert a link to them hosted on your website, or add to your social platform as attachments>>

or CTA 2: Get in touch with us today about arranging cyber cover tailored to the needs of your business.



Like



Comment



Repost



Send

Discover resources created for your cyber insurance campaign **here**.

Download assets to feature in your campaign at **Broker Create**.

Campaign stage 4: How cyber breaches can happen and how they can be avoided



Email example:

Subject line: **What impact would a cyber incident have on your day-to-day business?**

How the right cover can bolster your business continuity

Dear <Name Surname>

It's easy to underestimate the impact a cyber event could have on your business. But the fact is, a breach has the potential to be just as damaging to your livelihood as a fire or flood – if not more so.

What impact can a cyber breach have?

From ransomware to social engineering scams, there's a whole host of attacks criminals can hit you with to take control of your systems, funds or data. Attacks occur indiscriminately and can result in devastating setbacks such as:

- severe disruption to your ability to do business, leading to loss of revenue
- blackmail and significant financial loss
- contractual penalties due to delays in work
- reputational damage and loss of customer trust
- loss of intellectual property or confidential commercial information
- theft and use of stolen customer banking details
- regulator involvement and legal action.

If you'd like to know more, [these short claims scenarios](#) from Aviva will give you a good idea of the consequences having insufficient cyber cover can have. <<Download dual-branded versions of the **Cyber Claims scenarios from Broker Create** and either insert a link to them hosted on your website, or add to your email as attachments>>

To speak with us about how a cyber attack could affect your business, get in touch on <tel no> or via email at <email address>

<<include telephone call charge/recording information as applicable>>

Social post example:

What happens to a business when it needs to make a cyber claim?

These short claims scenarios from Aviva can help you see the impact – and the importance of making sure you're properly protected from digital disruption. <<Download dual-branded versions of the **cyber claims scenarios from Broker Create** and either insert a link to them hosted on your website, or add to your social media platform as attachments>>



Like



Comment



Repost



Send

Discover resources created for your cyber insurance campaign [here](#).

Download assets to feature in your campaign at [Broker Create](#).

Campaign stage 5: Why they should consider acting now



Email example:

Subject line: **Is this the rapid cyber breach response your business requires?**

24/7 cyber incident response service to get your business back on track

Dear <Name Surname>

Research shows that businesses are far more likely to put in place sufficient cyber cover *after* having experienced a cyber attack, rather than before – showing that those who have been through the distress of an attack are determined not to go through it again.

A rounded response to the threats businesses face

As well as 24/7 access to experts in the immediate wake of an incident, Aviva's cyber solutions – Cyber Respond, designed for small businesses and micro enterprises, or Cyber Complete for larger SMEs and mid-market organisations – offer:

- data security breach cover for the costs of managing a breach including IT forensic experts, legal advice, notifying affected individuals and identity fraud monitoring services
- data recovery cover for the cost of restoring lost data and damaged computer equipment
- increased cost of working cover for expenses incurred as a result of an incident
- cover for the costs of improving your system's resilience to prevent further incidents.¹

With premiums for Cyber Respond starting from as little as £50 per year,* Aviva's choice of cyber products can give you instant peace of mind and cover against the ever-evolving cyber threats of today and tomorrow. Why not arrange to get a cyber insurance quote for your business today and help make sure you've got the protection your business needs?

Call us on <Tel no.> or email <email address> to find out how we can help.

¹Available with Aviva Cyber Complete cover.

*Plus Insurance Premium Tax and subject to individual circumstances and cover level.
<<include telephone call charge/recording information as applicable>>

Social post example:

We're committed to helping you trade, adapt and evolve in an ever-changing cyber risk landscape. Talk to us about what cyber insurance solution would be right for your business and your budget. Call your <brokerage name> broker today on <<Tel number>>.



Like



Comment



Repost



Send

Discover resources created for your cyber insurance campaign **here**.

Download assets to feature in your campaign at **Broker Create**.

Cross-sell: How cyber insurance can be added to their policy at renewal – option 1



Email example:

Subject line: **Add cyber cover to your policy renewal – here's your indicative quote**

Heading: **Here's your indicative quote for cyber cover**

Dear <Name Surname>

With digital acceleration gathering pace, and the increasing risks posed by cyber crime, we're encouraging all our clients to consider the benefits of cyber insurance.

Research has shown that 71% of businesses see cyber risk as a high priority – yet 63% still don't have adequate cover in place.*

As you're approaching your insurance renewal time and protecting your business is front of mind, we thought now would be a good time to let you know your options when it comes to cyber insurance.

How can we help you get covered?

As an existing Aviva policyholder, adding cyber insurance to your policy renewal could cost from **£XX** **<insert the indicative quote price from the client's profile on Aviva Broker eDocs, accessed via the automated cross-sell docs for Speciality Lines, including Cyber>** as an addition to your quoted business renewal price.

Together with Aviva, we can provide suitable cyber insurance that helps you continue to trade with confidence and allows you to build resilience in a landscape that is ever-changing and increasingly complex.

To discuss adding cyber to your insurance renewal, please contact us today on <tel no> or <email address>

Read all that Aviva's Cyber Complete product has to offer here. **<<Download a dual-branded version of the Cyber Complete product fact-sheet from Broker Create and either insert a link to it held on your website, or add as an attachment to your email>>**

*Source: Cyber Security Breaches Survey, 2023, NCMS

This source contains public sector information licensed under the Open Government Licence v3.0

<<include telephone call charge/recording information as applicable>>

Social post example:

With cyber threats evolving and attackers employing increasingly sophisticated strategies, does your business have effective cyber insurance in place?

If you're approaching your insurance renewal time and protecting your business is front of mind, now could be a good time to understand your options.

Call us for a cyber quote today on <tel no>.

Could your business survive the financial and reputational damage of a cyber attack?

Talk to us about adding cyber cover to your business insurance at renewal.



<Broker logo here>



Like



Comment



Repost



Send

Discover resources created for your cyber insurance campaign **here**.

Download assets to feature in your campaign at **Broker Create**.

Cross-sell: How cyber insurance can be added to their policy at renewal – option 2



Email example:

Subject line: **Add cyber cover to your policy renewal – get a quote from us today**

Heading: **Get a quote for cyber cover today**

Dear <Name Surname>

With digital acceleration gathering pace, and the increasing risks posed by cyber crime, we're encouraging all our clients to consider the benefits of cyber insurance.

Research has shown that 71% of businesses see cyber risk as a high priority – yet 63% still don't have adequate cover in place.*

As you're approaching your insurance renewal time and protecting your business is front of mind, we thought now would be a good time to let you know your options when it comes to cyber insurance.

How can we help you get covered?

We're here to help you get suitable cyber insurance that enables you to continue to trade with confidence and allows you to build resilience in a landscape that is ever-changing and increasingly complex.

If you're interested in knowing how much adding cyber insurance to your policy renewal could cost, please contact us today on <tel no> or <email address>

*Source: [Cyber Security Breaches Survey, 2023, NCMS](#)

This source contains public sector information licensed under the Open Government Licence v3.0

<<include telephone call charge/recording information as applicable>>

Social post example:

With cyber threats evolving and attackers employing increasingly sophisticated strategies, does your business have effective cyber insurance in place?

If you're approaching your insurance renewal time and protecting your business is front of mind, now could be a good time to understand your options.

Call us for a cyber quote today on <tel no>.

Could your business survive the financial and reputational damage of a cyber attack?

Talk to us about adding cyber cover to your business insurance at renewal.



<Broker logo here>



Like



Comment



Repost



Send

Discover resources created for your cyber insurance campaign **here**.

Download assets to feature in your campaign at **Broker Create**.



Cyber resources for you to use

Sharing expertise

We've put together a range of useful videos, documents and tools you can use to help your clients understand the threat of cyber crime.

Feel free to share these in your conversations – or you can use them as inspiration, feature them or point to them when creating your own communications. We've provided a link to each one opposite.

If you'd prefer to dual-brand content with Aviva, head to [Broker Create](#) where you'll also find a full suite of social media graphics ready for you to use.

Your resources

**Specialist Partner
support and accredited
broker training**

Marketing support

**Useful facts and figures
on cyber crime**





Cyber resources for you to use

Sharing expertise

We've put together a range of useful videos, documents and tools you can use to help your clients understand the threat of cyber crime.

Feel free to share these in your conversations – or you can use them as inspiration, feature them or point to them when creating your own communications. We've provided a link to each one opposite.

If you'd prefer to dual-brand content with Aviva, head to [Broker Create](#) where you'll also find a full suite of social media graphics ready for you to use.

Your resources



Business Attitudes to Cyber Security Report

A summary of what the Aviva Risk Insights Report 2024 reveals about UK business attitudes to cyber security.



Cyber six reasons

A handy overview of the top six reasons why a business should start thinking about cyber cover.

Claims scenarios (on Broker Create)

Short case-study scenarios outlining what could happen when a business is subject to a cyber attack.



Cyber industry threats (on Broker Create)

An overview of the most common cyber threats specific to different business sectors, and their potential impacts.



Cyber product sheets (on Broker Create)

Cover details and key benefits of the Aviva Cyber Respond and Cyber Complete offerings.

Cyber cover checklist

A handy checklist allowing you and your client to compare Aviva cover options with another provider's cyber policy.

Broker Create assets

On Broker Create you'll also find a range of help guides, social assets and downloadable videos to help your clients understand the signs and impacts of cyber attacks.



Cyber resources for you to use

Sharing expertise

We've put together a range of useful videos, documents and tools you can use to help your clients understand the threat of cyber crime.

Feel free to share these in your conversations – or you can use them as inspiration, feature them or point to them when creating your own communications. We've provided a link to each one opposite.

If you'd prefer to dual-brand content with Aviva, head to [Broker Create](#) where you'll also find a full suite of social media graphics ready for you to use.

Your resources



**Specialist Partner
support and accredited
broker training**



Marketing support



**Useful facts and figures
on cyber crime**





Cyber resources for you to use

Sharing expertise

We've put together a range of useful videos, documents and tools you can use to help your clients understand the threat of cyber crime.

Feel free to share these in your conversations – or you can use them as inspiration, feature them or point to them when creating your own communications. We've provided a link to each one opposite.

If you'd prefer to dual-brand content with Aviva, head to [Broker Create](#) where you'll also find a full suite of social media graphics ready for you to use.



Specialist Partner support

Aviva policyholders have access to our network of Specialist Partners at preferential rates, one of which is [Bob's Business](#).

Bob's Business offers cyber security and awareness training to teach businesses how to spot and stop cyber attacks before they become breaches.



Aviva Certified Cyber Insurance and Risk Professional (ACCIRP) training

Improve your cyber knowledge so you can confidently discuss cyber risks with your clients. From understanding cyber terminology to why customers need cyber insurance, this eight-hour online Continuous Professional Development (CPD) course takes you through seven learning modules, with a final assessment for the qualification. Hosted on the Aviva Development Zone. [Aviva Development Zone](#).



National Cyber Resilience Centre Group (NCRCG)

The NCRCG is a collaboration between the police, government, academic institutions and private-sector organisations (this includes Aviva). The aim is to help strengthen cyber resilience across the UK's small and medium-sized business community.

You and your broker clients can join your nearest regional Cyber Resilience Centre (CRC) for free, to help guard against cyber risks your business faces. You'll get access to a range of valuable resources, guidance, training and support for all things cyber. [Read more here](#).



Cyber resources for you to use

Sharing expertise

We've put together a range of useful videos, documents and tools you can use to help your clients understand the threat of cyber crime.

Feel free to share these in your conversations – or you can use them as inspiration, feature them or point to them when creating your own communications. We've provided a link to each one opposite.

If you'd prefer to dual-brand content with Aviva, head to [Broker Create](#) where you'll also find a full suite of social media graphics ready for you to use.



Your resources



**Specialist Partner
support and accredited
broker training**



Marketing support



**Useful facts and figures
on cyber crime**





Cyber resources for you to use

Sharing expertise

We've put together a range of useful videos, documents and tools you can use to help your clients understand the threat of cyber crime.

Feel free to share these in your conversations – or you can use them as inspiration, feature them or point to them when creating your own communications. We've provided a link to each one opposite.

If you'd prefer to dual-brand content with Aviva, head to [Broker Create](#) where you'll also find a full suite of social media graphics ready for you to use.

Marketing support



You can find a wealth of additional marketing support and guidance on www.brokermentor.co.uk – including our [Marketing Elevator](#) tool, which can help you track and improve your skills.

We're here to help, always!

You can also reach out to the Aviva Marketing team for more support by emailing marketingsupport@aviva.com





Cyber resources for you to use

Sharing expertise

We've put together a range of useful videos, documents and tools you can use to help your clients understand the threat of cyber crime.

Feel free to share these in your conversations – or you can use them as inspiration, feature them or point to them when creating your own communications. We've provided a link to each one opposite.

If you'd prefer to dual-brand content with Aviva, head to [Broker Create](#) where you'll also find a full suite of social media graphics ready for you to use.

Your resources



**Specialist Partner
support and accredited
broker training**



Marketing support



**Useful facts and figures
on cyber crime**



Cyber crime – key facts and figures

Sometimes hard facts can help people get to grips with the true scope of cyber crime – or change their existing perceptions of the topic. Try sprinkling a few of these at relevant points throughout your communications to help people understand the scale of the problem.

What are the Government stats on cyber risk?



What are Aviva's insights into cyber risk?



Cyber crime – key facts and figures

Sometimes hard facts can help people get to grips with the true scope of cyber crime – or change their existing perceptions of the topic. Try sprinkling a few of these at relevant points throughout your communications to help people understand the scale of the problem.

What are the Government stats on cyber risk?



What are Aviva's insights into cyber risk?



UK Government research says:

32%

of businesses experienced a cyber attack or breach in the last 12 months

34%

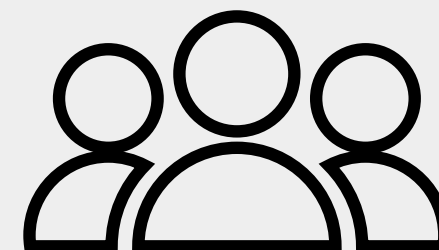
of the businesses who experienced a cyber attack or breach in the last 12 months ended up being victims of cyber crime

£15,300

is the approximate average annual cost of cyber crime per victim for UK businesses

49%

of businesses sought outside cyber security guidance or information in the past year



Sources:

Source: All statistics sourced from the [Cyber Security Breaches Survey, 2023, DCMS](#)

All government sources throughout this document contain public sector information licensed under the Open Government Licence v3.0.

Cyber crime – key facts and figures

Sometimes hard facts can help people get to grips with the true scope of cyber crime – or change their existing perceptions of the topic. Try sprinkling a few of these at relevant points throughout your communications to help people understand the scale of the problem.

What are the Government stats on cyber risk?



What are Aviva's insights into cyber risk?



Aviva research says:

38%

of SMEs without cyber cover didn't believe they would be a target for a cyber attack

18%

of SMEs said cyber insurance was too expensive

16%

didn't know cyber insurance even existed

15%

of businesses said they'd turn to their broker for help in the event of a cyber attack

Sources:

SME Pulse survey conducted by YouGov, on behalf of Aviva, in which 512 British SMEs were questioned. Fieldwork took place between 5-12 October 2022. All percentages are rounded to the nearest whole number.



Campaign top tips – best practice for best results

Posting



Sharing



Responding



Social platform checklist





Campaign top tips – best practice for best results

Posting**Sharing****Responding****Social platform checklist****1****Know your audience**

All campaigns work best if you understand when and where to reach your audience. You know them best! But a little extra research could make all the difference. Use the channels and content you know will get most engagement.

2**Think about when to post – and when not to**

When you're thinking of sharing any of the content in this document, make sure you do so when it will have the most impact. Clients are busy in the run-up to Christmas, for example. Will they want to think about insurance too? Or might you have a renewals period you want to align with?

3**Link your campaign together**

Putting together an email and social posts on the same topic? Post these close together (either on the same day or within the same week) so there's consistency and a clear narrative for your audience to follow.

4**Remember momentum**

Space different topics out across your campaign, so you share new and engaging stuff at each stage of the campaign – with every piece being a natural progression from the last.



Campaign top tips – best practice for best results

Posting



Sharing



Responding



Social platform checklist



Encourage interaction

Always make it easy for people to respond – with clear language, prominent calls to action (CTAs) and links that take them where you want them to go.



Start the sharing

Get a few of your team, or some key contacts, to share your content. This not only gets the word out – it also positions you as a relevant and valuable voice of authority that people are already listening to.



Campaign top tips – best practice for best results

Posting ▶

Sharing ▶

Responding ▶

Social platform checklist ▶

Keep the conversation going

Make sure you monitor your emails and social posts (including the comments) to identify any potential queries, conversations or leads.

Be responsive

Be ready to respond ASAP, ideally within a matter of hours, but certainly no longer than a day. Setting aside a small amount of time could help.

Consistency is key

Try to respond in the same tone you're using for the campaign itself, and always remember to be clear what steps you want them to take next.

Capture that data

If you already have lead capture on a contact page, newsletter sign-up or similar, is it possible to link to it, so you can collect and keep all your data in one place? You can find guidance on your regulatory responsibilities when collecting client data here: <https://ico.org.uk/>



Campaign top tips – best practice for best results

Posting ▶

Sharing ▶

Responding ▶

Social platform checklist ▶



LinkedIn

Text viewable before 'Read more' cut-off:	150 characters
Paid post headline recommendation:	70 characters
Image dimensions:	1200 x 627 pixels
Profile picture dimensions:	400 x 400 pixels
Cover/header image dimensions:	1128 x 191 pixels



Facebook

Text viewable before 'Read more' cut-off:	125 characters
Paid post headline recommendation:	27 characters
Image dimensions:	1200 x 630 pixels
Profile picture dimensions:	170 x 170 pixels
Cover/header image dimensions:	851 x 315 pixels



X

X character limit:	280 characters
Character limit on paid posts:	257 (with 23 characters used for CTA link)
Image dimensions:	1024 x 512 pixels
Profile picture dimensions:	400 x 400 pixels
Cover/header image dimensions:	1500 x 500 pixels



Instagram

Text viewable before 'Read more' cut-off:	125 characters
Paid post headline recommendation:	27 characters
Image dimensions:	1080 x 1350 pixels
Profile picture dimensions:	320 x 320 pixels
Cover/header image dimensions:	N/A

Specifications correct as of summer 2023.



Email marketing – in a nutshell


This example email shows just one way of starting a conversation about cyber risk. We've included some tips to think about when writing your own emails. But remember to give it your own spin – and test and learn what works for your clients.

Just click here  to show the tips.

To help get you started, you can also find a range of templates you can dual-brand with Aviva, and other campaign collateral, on [Broker Create](#).


New message

To:

Subject: Cyber threats are putting UK businesses at risk 



The fallout of a cyber breach can't be ignored

Dear <Name Surname>


Most SMEs assume cyber attacks are an issue only big organisations need to worry about. But the truth is, cyber crime is a numbers game – criminals cast a wide net, using malware, ransomware and social engineering to attack indiscriminately, then quickly take advantage of any weaknesses they find. 


If you don't have a plan for how you'd respond to finding yourself locked out of your system and facing a ransom demand, the consequences could be extremely damaging.

Potential outcomes of a cyber attack

-  • **Reputational damage** – rebuilding customer trust after a data breach can be challenging, and reputational impact can be significant and long-lasting. 
- **Financial impact** – the costs associated with addressing and recovering from an attack could have a negative impact on how the business is able to trade moving forward.
- **Operational disruption** – if an attack leaves you unable to carry out business for a prolonged period, it may be challenging to fully recover.
- **Legal and regulatory implications** – failure to adequately protect customer data can lead to legal consequences, including fines and lawsuits.
- **Intellectual property theft** – the competitiveness of your business could be affected if valuable IP such as proprietary processes, patents or trade secrets are revealed.

How can we help protect your business?

You can find out more about the specific threats to your sector and the impact they might have in this [Industry threats guide](#) from Aviva. **<<Download a dual-branded version of the guide from Broker Create and either insert a link to the guide hosted on your website, or add a copy to the email as an attachment>>** 

And if you'd like our help with understanding how a cyber event or attack could impact your business, you can reach us on <tel no> or email at <email address> 



Email marketing – in a nutshell


This example email shows just one way of starting a conversation about cyber risk. We've included some tips to think about when writing your own emails. But remember to give it your own spin – and test and learn what works for your clients.


Just click here  to show the tips.


To help get you started, you can also find a range of templates you can dual-brand with Aviva, and other campaign collateral, on [Broker Create](#).



New message

To:








Subject: Cyber threats are putting UK businesses at risk 

Hard-hitting, succinct subject line grabs attention and answers the question “why should I open and read this email?” 
Top tip: keep it below 60 characters and make sure it reflects the content of the email.

The fallout of a cyber breach can't be ignored 

A bold statement or question-based headline starts the conversation and gets them thinking. 
Introductory paragraph is succinct and relatable but also intriguing. The rhetorical question encourages them to read on. 

Potential outcomes of a cyber attack

- **Reputational damage** – rebuilding customer trust after a data breach can be significant.
- **Information is chunked into short paragraphs. Question-based headlines make the subject of each section clear.** 
Top tip: two-sentence paragraphs are best – using clear, informative subheadings. You can even use bullet points for key points if appropriate.
- **Jargon-free, succinct explanation (in plain English) focusing on what it means for the reader.** 
- **Intellectual property theft** – the competitiveness of your business is affected if valuable IP such as proprietary processes, patents or trade secrets are revealed.
- **How can we help protect your business?** 
Sign-off focuses on the benefit to the reader and pushes them towards what you want them to do next. 
Clear, succinct CTA. Don't forget, you can offer multiple ways to keep the conversation going if you have them. 
- **Add value for the reader by pointing them towards any relevant resources. This also helps demonstrate your credentials and expertise in this area.** 
Top tip: stats are another great way to demonstrate expertise. Just make sure they're relevant and properly referenced. 



Social media marketing – made simple

A good social post is short and punchy, so don't try to do everything in every post. Think about what you want people to do at each stage of your campaign. Notice you? Engage with you? Click on some content? Take action? The table on the next page gives you some quick guidance on what to think about when writing each post type.

[Quick guidance](#)[Examples](#)

Quick guide to social media marketing



Content style

Easily digestible.
Stand-alone.
Highly shareable.
Bitesize data
and insights.

Interactive.
Community-focused.
Audience-led.

Content-focused.
Intriguing.

Clear.
Succinct.
Conversion-focused.

Top tips

Add relevant hashtags
with a substantial
following (max. 3
per post).

Use eye-catching
copy with a
stand-alone leading
sentence that outlines
your theme.

Ask questions that
are open, on-topic
and easy to answer.

Focus on
client needs.

Adopt a helpful,
supportive tone.

Be clear and specific
about what they
will get if they click
(e.g. 'Discover our
six top tips').

Focus on the insights
most interesting to
your audience.

Focus on the 5 Ws:
who you are, what
problems you can help
with, and when, why
and where people can
reach you.


Make sure your CTA
is clear about what
people need to do next.

The examples below show how you could get a conversation about cyber insurance started... and keep it going. You can also find ready-made resources and assets on [Broker Create](#) that you can share or use as inspiration.

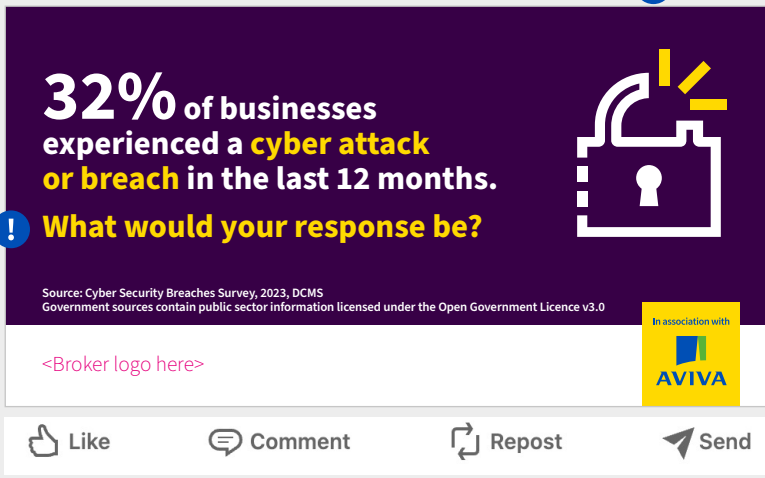
Just click here to show the tips.

Example 1:

Almost every business holds valuable information – from payment details and employee data to intellectual property and supplier agreements. Cyber criminals could use this information to disrupt, extort or steal from your business.

 Find out more about the risks cyber criminals pose to your business by taking a look at Aviva's latest Business Attitudes to Cyber Security Report.

<<Download a dual-branded version of the report from Broker Create and either insert a link to the report hosted on your website, or add it to the social platform as an attachment>>



Source: Cyber Security Breaches Survey, 2023, DCMS
Government sources contain public sector information licensed under the Open Government Licence v3.0

<Broker logo here>

Like Comment Repost Send

Example 2:

More and more businesses are recognising that their own in-house IT capabilities may not be sufficient should a cyber attack or breach take place. Yet despite this, there's a big gap between awareness and action.

 To understand more about the specific threats to your sector and the impact such an event might have, take a look at this [Industry threats guide](#) from Aviva.

<<Download a dual-branded version of the guide from Broker Create and either insert a link to the guide hosted on your website, or add it to the social platform as an attachment>>



Source: Cyber Security Breaches Survey, 2023, DCMS
Government sources contain public sector information licensed under the Open Government Licence v3.0

<Broker logo here>

Like Comment Repost Send

The examples below show how you could get a conversation about cyber insurance started... and keep it going. You can also find ready-made resources and assets on [Broker Create](#) that you can share or use as inspiration.

Just click here to show the tips.

Example 1:

Almost every business holds valuable information – from payment details and employee data to intellectual property and supplier agreements. Cyber criminals could use this information to disrupt, extort or steal from your business.

Find out more about the risks cyber criminals pose to your business by taking a look at Aviva's latest Cyber Security report.

Conversational language makes sure your posts feel like a two-way interaction rather than a sales pitch.

version of the report from Broker Create and either insert a link to the report on your website, or add it to the social platform as an attachment>>


These hashtags are just examples. Remember to research which ones are getting the most people talking on your topic. A quick search on your chosen social media site should tell you.

32% of businesses experienced a cyber attack or breach in the last 12 months.

What would your response be?

Open-ended, intriguing questions grab attention and encourage interaction.

Source: Cyma Cyber Security Survey 2018. Licensed under the Open Government Licence v3.0

In association with 

<Broker logo here>

Like Comment Repost Send

Example 2:

More and more businesses are recognising that their own in-house IT capabilities may not be sufficient should a cyber attack or breach take place. Yet despite this, there's a big gap between awareness and action.

To understand more about the specific threats to your sector and the impact such an event might have, download our new threats guide from Aviva.

The client need or problem is placed upfront and a solution is offered.

download version of the guide from Broker Create and either insert a link to the guide on your website, or add it to the social platform as an attachment>>


A clear CTA makes it obvious how people can get in touch. Remember, you could test different contact methods to find out what works best for your audience.

63% of UK businesses do not have adequate cyber cover in place.

Is yours one of them?

Offering is clearly spelled out in powerful terms.

Source: Cyma Cyber Security Survey 2018. Licensed under the Open Government Licence v3.0

In association with 

<Broker logo here>

Like Comment Repost Send



Writing website content – the right way

Your website is your shop window. You want everything in it to reflect well on you and draw people in. That's why it's so important any content you publish helps position you as authoritative experts. And that means getting the quality, expertise level and presentation right.

Questions to ask yourself before you post ▶

Example of core principles in action ▶



Questions to ask yourself **before you publish**



Is your
content...



High-quality

Trustworthy
(e.g. clearly sourced
and referenced, author
credentials clear)?

Written by an expert?

Free from
factual errors?



Expert

Up-to-date and topical?
Insightful and interesting?

Clearly signposted
(easy to see what
it's about)?



Well-presented

Free from spelling or
style errors?

Focused on insight
rather than sales?


Looking good on
mobile devices?


As accessible as possible?

Example of core principles in action

Just click here  to show the tips.

Cyber threats are evolving – we all need to evolve with them

As businesses and industries embrace digitalisation to drive operational efficiencies and meet customer expectations, new opportunities for cyber attacks open up. Consequently, there's a growing need for businesses to ensure they're protected against such threats. 


 Cyber attacks can happen to businesses of any size, and most attacks are untargeted – meaning all businesses are at risk. But despite this, 38% of SMEs don't think it would happen to them.*

Here are a few key things you need to consider:

1. Everything rests on the response


A rapid response to an incident or breach is vital. Recovery requires co-ordinated expert support to reduce the impact, so it's important to ensure that your protection delivers immediate support to minimise any damage and get your business back on track.

This should include:

-  • A dedicated incident manager to co-ordinate activity and bring in the right experts when necessary
- Specialist IT forensics and consultants to identify the type of attack, the extent of the damage and whether data has been compromised
- Reputational experts to help minimise any negative impact on your brand, customers or suppliers across press and social media
- Support with recovery activities, including access to free counselling services for any staff affected by a cyber event or online incident.

2. All businesses are at risk

Most criminal activity isn't targeted at a particular business

or industry. Instead, sophisticated tools are used to search the internet for system vulnerabilities. This means any business, large or small, can be targeted – with 32% of UK businesses suffering a cyber incident in the last 12 months 

3. People make mistakes

If you and your employees aren't aware of the risks of phishing or social engineering, you're more likely to fall for such attempts and your people could end up being the weakest link in your cyber security. Effective training can help safeguard against this.

4. Operations and reputations need protecting

Many businesses are heavily reliant on technology to carry out day-to-day business operations. Not being able to access vital IT systems due to a cyber attack or data breach could result in significant business interruption and reputational impact.

What can you do to protect your business?

The good news is that we can provide you with the right protection for your business now and in the future. We're all facing a fast-changing, ever-evolving threat landscape – but whatever your size and sector, we can find you cyber insurance that fits your needs and specific exposures in a way that's affordable and easy to understand.

Call us today on <tel> or email us at <email> 

 *Source: SME Pulse survey conducted by YouGov, on behalf of Aviva, in which 512 British SMEs were questioned. Fieldwork took place between 5-12 October 2022. All percentages are rounded to the nearest whole number.

Example of core principles in action

Just click here  to show the tips.

Cyber threats are evolving – we all need to evolve with them

Intriguing statement gets attention while also briefly summarising content.

This content is written by an expert and can be trusted.

Here are a few key things you need to consider:

1. Everything rests on the response

The content is chunked into sections with clear headings, making it digestible and easy for readers to scan.

Bullet points are useful for summarising complex information.

While you don't want your content to be sales-y, it's important to offer some solutions towards the end. Leading them into...

2. All businesses are at risk

Most criminal activity isn't targeted at a particular business

Signpost your references at the bottom of the page.

Short intro outlines content – starting with the client need (why it's relevant to them), then moving onto reasons to read further.

Data is accurate and clearly referenced.

4. Operations and reputations need protecting

Many businesses are heavily reliant on technology to carry out day-to-day business operations. Not being able to access vital IT systems due to a cyber attack or data breach could result in significant business interruption and reputational impact.

What can you do to protect your business?

Good news is that we can provide you with the right

protection for your business now and

all facing a fast-changing, ever-evolving

– but whatever your size and sector

insurance that fits your needs and

way that's affordable and easy to understand.

Call us today on <tel:01234 567890> or email us at info@aviva.co.uk

...a clear CTA signposting where they should go next, offering options where appropriate. Remember, you can also test and learn what works best for your audience across different pieces of content.

Contact **marketingsupport@aviva.com**
for any queries or additional support

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

aviva.co.uk

BMGI116422024. 04/2024.

