Cyber war language upgrade FAQs

CFC has upgraded its 'war and cyber war' language for all SME policies providing cyber cover. The updated language addresses cyber war and provides customers with greater clarity on the cover provided under their cyber policy.

Why is CFC updating its war language?

Traditional war exclusions were originally intended to address physical acts of war but have not evolved to address the growing threat and impact of cyber warfare. In line with a recent Lloyd's bulletin, many insurers are taking steps to clarify their position and policy language on cyber war.

CFC is using this opportunity to ensure its 'war and cyber war' language is fit-for-purpose and offers our customers certainty about what is covered under their policy and what is not.

What specific changes are you introducing?

Our updated 'war and cyber war' language provides four key enhancements:

- It introduces an explicit definition of 'cyber war', providing greater clarity
- It introduces a high threshold for what is considered to be an act of cyber war
- It provides cover for initial support and advice, even in the event of cyber war
- It provides cover for 'collateral damage' stemming from cyber war

How does this benefit policyholders?

By specifically defining what an act of cyber war looks like and creating a high threshold for it, we're narrowing the scope and removing ambiguity within the policy.

We're also ensuring that our policyholders still have access to initial incident response support even in the event of an act of cyber war, and that we don't unduly penalize victims of cyber war that were not the intended target.

What is the definition of cyber war in CFC's cyber policy?

In our policy, cyber war is considered to be any cyber attack carried out by or on behalf of a state, that directly results in another state becoming an 'impacted state', meaning the state has to suffer a major detrimental impact on its ability to function or to its defence and security capabilities. We believe this sets a high threshold for a cyber event being determined an act of war.

What happens if my client is impacted but they are not located in the target state?

It's possible that an act of cyber war targeting one state could ultimately impact organizations outside of that state. While not the intended victims, these organizations would be considered 'collateral damage' from an act of cyber war. We want to ensure those unintended victims still have access to cover if impacted by an act of cyber war by providing cover for computer systems that are physically located outside of an impacted state.

What incident response cover are you providing?

We have carved back our language to provide cover for initial incident response support from our internal team, CFC Response. We understand that the primary driver in purchasing cyber insurance for most SME clients is access to incident response services. With our language they will still have access to our dedicated in-house incident response team to triage an incident and provide initial technical support and advice.

CFC Response consists of over 120 incident response specialists across our offices in the United States, United Kingdom and Australia.

When does the new war language go live?

The new language will be attached to all quotes and policies that are issued on or after 1 May 2023.

Will CFC be applying this to in-force policies?

We will not apply mid-term adjustments to in-force policies that incepted before 1 May 2023, but we will update the language when accounts are due for renewal.

Can the old language still be used? Can the new language be amended?

No. The new language has been specifically designed with our policyholders in mind and has been approved by both our regulator and external legal review.

We also believe that the new language benefits clients by narrowing its scoping and offering greater clarity to insureds.

Where can I learn more?

If you have any questions about the updated language, you can speak to one of our cyber underwriters or read the latest article from our Head of Cyber Strategy here.

Key war language differences in CFC SME cyber policies

	Clear definition of 'cyber war'	High threshold for 'cyber war'	Cover for initial incident response support	Cover for 'collateral damage'
Old war language	✗	✗	✗	✗
New war and cyber war language	✓	✓	✓	✓