

Media Factsheet

Cyber Incident Helpline (CIH) Provides Businesses Practical First-Response Support

As businesses continue to digitalise, cyber threats have become an increasingly common operational risk. This can be particularly challenging for SMEs that may not have dedicated cybersecurity resources or established incident response arrangements.

To help businesses navigate cyber incidents, the Singapore Business Federation (SBF) launched the Cyber Incident Helpline (CIH), a dedicated first-response advisory service that provides timely guidance to help businesses assess the situation, take appropriate containment measures, and access further assistance where required.

The CIH was officially launched by Mr Tan Kiat How, Senior Minister of State, Ministry of Digital Development and Information of Singapore, at Singapore International Cyber Week (SICW) 2026. CIH is part of the Cyber Resilience Centre (CRC), jointly established by SBF, SGTech, and the Singapore Chinese Chamber of Commerce and Industry (SCCCI), with the support of the Cyber Security Agency of Singapore (CSA).

Mr Kok Ping Soon, Chief Executive Officer, SBF, said, “When a cyber incident strikes, the first few hours matter. The Cyber Incident Helpline gives businesses, especially SMES, a trusted and confidential first port of call to assess the situation, contain the impact and act quickly. This practical support will help businesses respond with greater confidence and resilience.”

AT A GLANCE

Key Fact	Detail
Who it supports	Businesses of all sizes, including SMEs that may not have dedicated cybersecurity resources.
Role	First-response advisory, incident triage, containment guidance and referrals where specialised assistance is required.
Response	Response from the CIH team within two hours of submitting an incident support request.
Service	No charge; intended to provide a trusted and confidential avenue for advice and assistance.
Access	Submit an incident support request via the Cyber Resilience Centre portal, or contact the Cyber Incident Helpline at 6890 9555 for assistance.

Media Factsheet

KEY INFORMATION

1. What Cyber Incident Helpline (CIH) provides

When a business experiences a cybersecurity incident, CIH provides practical first-response support to help organisations understand what has happened and determine appropriate next steps.

- Immediate first-response advisory: Guidance to help organisations quickly understand the situation and take appropriate actions to reduce potential harm.
- Incident triage: Support in validating suspected cybersecurity incidents, assessing their severity, and prioritising issues requiring urgent attention.
- Containment guidance: Practical recommendations to help limit the spread and impact of a cyber-attack while preserving business operations where possible.
- Referral to specialised assistance: Where specialised support is required, organisations may be provided with a list of pre-approved cybersecurity partners that they may engage for remediation and recovery assistance.

2. What types of incidents can CIH support?

CIH can provide guidance on a wide range of cybersecurity concerns, including:

- Phishing and social engineering attacks
- Business email compromise
- Malware infections
- Ransomware incidents
- Unauthorised access to systems or accounts
- Suspected data breaches
- Other suspicious cyber activities affecting business operations

3. How CIH works

- Step 1: Submit an Incident Support Request
Provide basic information about the incident through the CRC portal
- Step 2: Incident review and triage
A trained CIH operator reviews the information received and assesses the nature and urgency of the reported issue.

Media Factsheet

- Step 3: Call-back consultation
A CIH representative will contact the organisation to gather additional information and provide initial guidance within two hours of request submission.
- Step 4: Guidance and next steps
The organisation receives recommendations on immediate containment measures and incident response considerations.
- Step 5: Referral support (where required)
Where specialist assistance is needed, the organisation may be provided with a list of pre-approved cybersecurity partners that it may engage for remediation and recovery assistance.

4. What CIH does not do

While the Cyber Incident Helpline (CIH) provide first-response advisory and guidance, it does not perform operational or technical remediation services such as:

- Conduct forensic investigations
- Collect digital evidence
- Perform remote technical troubleshooting
- Carry out incident remediation activities
- Restore systems or recover data
- Monitor organisational networks or IT systems
- Act as the organisation's incident responder or breach coach
- Select vendors on behalf of organisations
- Report incidents to regulators or authorities on behalf of organisations

CIH focuses on providing initial incident triage, containment guidance, and practical advice on the appropriate next steps, and may refer businesses to suitable service providers if deeper technical support is required.

###

For media queries, please contact:

Zeno Group on behalf of Singapore Business Federation

E: SBF@zenogroup.com

About Cyber Resilience Centre (CRC) and Cyber Incident Helpline (CIH)

The Cyber Resilience Centre (CRC) is a broader initiative that helps businesses strengthen cybersecurity preparedness and resilience through resources, workshops, exercises, and incident support services. CIH is the dedicated incident support component within CRC, providing timely first-response support when cybersecurity incidents occur.



Media Factsheet

Cyber Resilience Centre portal

Businesses seeking assistance can submit an incident support request through:

Website: <https://www.cyberresilience.sg>

Tel: 6890 9555

About Singapore Business Federation (新加坡工商联合总会)

Singapore Business Federation (SBF) is the apex business chamber with over 34,000 members across diverse industries. With a vision to advance Singapore towards a globally competitive and sustainable economy, SBF mobilises the business community to be future-ready and magnify transformation opportunities through policy advocacy, partnership platforms and capability programmes.

For more information, please visit: www.sbf.org.sg