Notice to Suppliers

Cyber Threat

Originator: Neil Cassidy
Job Title: Global Chief Information Security Officer
Business Unit: All

NTS Number: 549
Issue: 1
Date: 12th February 2022

Scope/Applicability:

All Rolls-Royce suppliers.

Dear Supplier,

Introduction

Rolls-Royce has received several reports from security agencies sharing their advice on how to improve our cyber security resilience in response to heightened cyber threats. Although, no specific threats have been identified, by following their advice, Rolls-Royce and its suppliers and partners can build resilience and stay ahead of potential threats to our business.

Rolls-Royce has undertaken a review and carried out activities in preparedness for an escalation in cyber threats. We encourage our supply chain and partners to also take this opportunity to review their cyber security and address any gaps.

What action to take

Using advice and guidance provided in the links below, assess how cyber security resilient your organisation is, and create plans to remediate the gaps.

1. The UK National Cyber Security Centre (NCSC) has prepared guidance on steps to take to improve your organisation's security: https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened
2. US Cybersecurity and Infrastructure Security Agency (CISA) issued a Joint Advisory (on behalf of Australia, Canada, New Zealand, the UK and the US): Technical Approaches to Uncovering and Remediating Malicious Activity: https://www.cisa.gov/uscert/ncas/alerts/aa20-245a
3. The Federal Office for Information Security (BSI) offers an overview and information on how to manage sophisticated threats: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/empfehlungen-nach-gefaehrdungen_node.html

Share this guidance with your IT managed service providers and supply chain. Ask them - how resilient are they to current cyber threats?

Reporting cyber incidents

Please inform your Rolls-Royce point of contact and Security Operations Centre (SOC) (UKSOC@Rolls-Royce.com) as soon as you know or believe a cyber security incident has or may have taken place on your IT systems used to support Rolls-Royce.

Provide full details of the circumstances of the incident and any mitigation measures already taken or intended to be taken.

NTS Category:

General Information / Communication

Authorised by:

Dave Deakin
Chief Procurement Officer, Group