Notice to Suppliers

Cyber Incident Reporting

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

NTS Number: 561
Issue: 1
Date: 26/11/2022

Scope/Applicability:

All Rolls-Royce suppliers.

Dear Supplier,

Introduction

Cyber incidents may be opportunistic or targeted and threats can originate from outside or within your organisations. A good cyber incident plan ensures you can build resiliency and prepare your response, to minimise damage to your business and reputation and harm to your customers, including Rolls-Royce.

In response to evolving cyber threats, Rolls-Royce regularly reviews and tests its incident response plans. Incidents can and will happen, so it is important to be prepared.

The purpose of this notice is to share with you the changes we introduced for reporting cyber incidents to Rolls-Royce Security Operations Centre (SOC). If you do not have an incident response plan, we encourage you to get started with the weblinks below offering useful advice and guidance.

Process for reporting your cyber incidents

Rolls-Royce has made changes for reporting your cyber incidents. In the event of an incident, please send your notification to your business point of contact and Rolls-Royce Security Operations Centre (SOC):

sec.reporting@rolls-royce.com and/or
sec.reporting.us@rolls-royce.com (for US based organisations)

Your initial report should include a brief description of the incident and contact details for your incident manager or other points of contact.

After submitting your report, the SOC will contact your incident manager/points of contact by email from UKSOC@Rolls-Royce.com or US-SOC@rolls-royce.com, or by phone using the details you provide us.

We request your full cooperation and assistance. The SOC will ask you to share details of the incident and any mitigation measures already taken or you intend to take. Your support and corporation ensures Rolls-Royce fully understands the impact on its data, systems, services, and operations, and to comply with its obligations to customers and regulatory authorities.

What action to take

1. Update your Incident Response Plans:
    a. To include email address(es) for reporting incidents to Rolls-Royce SOC:
        sec.reporting@rolls-royce.com and/or
        sec.reporting.us@rolls-royce.com (for US based organisations)
    This initial report should be brief, and contain contact details for your incident manager/points of contact.

    b. Add a step for sharing further incident details with the SOC when contacted from UKSOC@Rolls-Royce.com or US-SOC@rolls-royce.com, or by phone using the details you provide us.

    c. Add a step to share your remediation plans with Rolls-Royce SOC and business point of contact. Provide regular reports on progress, through to completion.

2. If you do not have Incident Response Plan(s), the following advice and guidance can help you:
    - The UK National Cyber Security Centre (NCSC) provides guidance on the benefits and steps for creating and testing your Incident Response Plans (Incident management - NCSC.GOV.UK), with specific advice for your Board Members (Planning your response to cyber incidents - NCSC.GOV.UK)
    - US Cybersecurity and Infrastructure Security Agency (CISA) offers guidance and assistance for US businesses to plan and recover from cyber incidents (Cyber Incident Response | CISA), and useful playbooks to help you get started (Federal Government Cybersecurity Incident and Vulnerability Response Playbooks (cisa.gov)

NTS Category:	**Authorised by:**
General Information / Communication	Dave Deakin Chief Procurement Officer, Group