Cybersecurity Breach Incident Notification

What our suppliers need to know

Despite best efforts at prevention, cyberattacks can hit their mark and disrupt operations. If such a breach affects the goods and services our suppliers provide to Rolls-Royce, or to the information systems storing Rolls-Royce data, suppliers are required to take certain steps. These steps keep Rolls-Royce informed and keep you compliant with the Rolls-Royce Supplier Minimum Cyber Security Standard v1.2, released in December 2023.

Notification and documentation

Suppliers must notify the Rolls-Royce Security Operations Center (SOC) **within 48 hours** of learning of or suspecting a cybersecurity incident. Notification is made to your buyer, business point of contact, or via the SOC mailbox address contained in the Rolls-Royce Supplier Minimum Cyber Security Standard. Also, when affected by a cyber incident, suppliers must begin documenting actions, decisions, and other information related to the incident.

Reports and responses

As soon as possible, suppliers must provide the Rolls-Royce SOC with reports and findings of the incident investigation, including any Indicators of Compromise (IOCs)[1]. The SOC will contact you with a list of questions about the incident. You must reply promptly to these requests, although Rolls-Royce recognizes that detailed responses may be delayed while a cyber incident is ongoing. Rolls-Royce must meet its own reporting notification obligations, especially involving data loss or compromise or if a threat actor can use a trusted IT connection you may have with Rolls-Royce.

Containment and mitigation

Suppliers must promptly take all steps necessary to **contain** the incident, **mitigate** any impact, and **prevent** reoccurrence. Suppliers must inform Rolls-Royce of corrective actions taken and provide plans of further remedial action if warranted, including joint actions to be agreed upon between the supplier and Rolls-Royce.

[1] Indicators of Compromise (IOCs) refer to data or evidence that indicates malicious activity has occurred within the supplier's system(s).

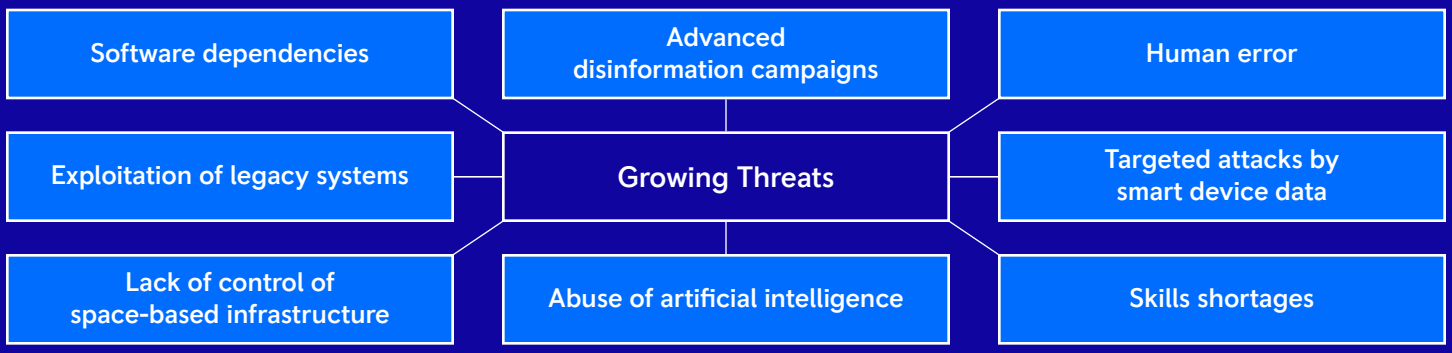
Additional incident response resources

Planning today for challenges tomorrow

Rolls-Royce wants suppliers to **be prepared to respond** to any cybersecurity breach and return to normal operations as quickly as possible. We have resources available to help suppliers develop and refine their cyber incident response plan. Some current information and best practices can be found here.

Emerging security threats

Cyber threats are growing in sophistication and frequency. Experts say that over the next several years, security threats will grow even further from these areas:



Assistance with response plan implementation

Rolls-Royce recognizes that our suppliers may have multiple customers, complicating responses to a cybersecurity incident. Reporting may be generic at first, before it becomes more targeted for affected customers. Our suppliers often enlist a third-party incident response team to address the incident while suppliers focus on communications and ensuring that all business relationships — including with Rolls-Royce — are kept apprised.

Communication is critical

▶ Before an incident: All firms must develop a culture so that cybersecurity is viewed as a business enabler and not a blocker. Rolls-Royce is committed to sharing best practices and guidance, and making our cyber knowledge available.

▶ During an incident: Transparent and inclusive lines of communication among all areas involved are essential for a good outcome, both within the supplier organization and between the supplier and Rolls-Royce.

SUPPLIER COMMUNICATION
Rolls-Royce's Global Supplier Portal is your first stop for information and documents, such as Notices to Suppliers (NTS).