Cyber security resources and guidance

A toolkit for those who completed Immersive Labs training

As a newly trained cyber security expert for your organization, you will need to stay alert and informed to safeguard your business's data, systems, and people from cyberattacks.

Having completed the Immersive Labs Cyber Million cyber security training, you are familiar with the key principles and potential threats. This toolkit provides resources to assist you in implementing your knowledge and guide you through ensuring your entire system, assets, and users are secure. It may seem daunting at first. However, by following the advice in this toolkit and recommendations from the UK National Cyber Security Centre (NCSC), U.S. Cybersecurity and Infrastructure Security Agency (CISA), Rolls-Royce or others, you can make a significant difference.

Who is this toolkit for?

This toolkit is for those who have gained some knowledge of cyber security and want to improve the security posture of their business. It does not replace advice from cyber security experts.

By working through the steps below, you can feel more confident in your role, and ensure your organization is not an easy target for those seeking to cause harm, steal data, or use your systems to exploit trusted business relationships with customers or suppliers.

How to use the resources provided

Managing your cyber security program requires a structured approach to ensure that you effectively identify and mitigate security risks to your organization. Here is a step-by-step guide to help you get started.

1 Define the objectives and scope

Identify key areas of your organization and assets that need protection, and set goals. Define clear and measurable objectives for your cyber security program. Be realistic. Rome wasn't built in a day.

If you work in a small business (up to 250 employees), by answering a few simple questions at this NCSC resource site, you can create a free, personalized action plan to help you get started. Or you might decide to use the CISA's Cybersecurity Performance Goals (CPG) checklist to determine the current status of security within your organization and identify areas for improvement.

2 Assess security risks to your organization and assets

Performing risk assessments is often a daunting task, even for cyber security professionals. Understanding the risks will assist you to prioritize and plan the treatment of risks.

Start by documenting your organizational assets, including data, technology (hardware and software), facilities, and people.

Ask:

- What data does your business rely on to function?
- What would cause the most damage or disruption if it were lost, stolen or compromised?
- What types of personal or confidential information do you collect and store?
- What software, systems or tools are essential to your daily operations? (Remember they may also be operational technology that manage processes.)
- Do you have any proprietary processes, designs or intellectual property that competitors might want?
- Which departments or functions hold the most sensitive or high-value data?
- Who has access to your most important systems and data, and how is that access controlled?
- What external parties or third parties have access to your data or systems?
- How would a cyber attack, data breach or system failure impact your reputation or ability to serve customers? Is it possible for an attack to cause harm?
- What are your regulatory, legal and customer obligations regarding data protection and privacy?

The answer to these questions will help you focus on identifying key assets, and consider both tangible and intangible resources that require protection within your business.

NCSC provides a basic risk assessment and management method with clear guidance to assist you with this step. CISA also offers resources and guides to help you. Or if you prefer a formal approach, you may decide to follow the U.S. National Institute of Standards and Technology (NIST) Guide for Conducting Risk Assessments (NIST Special Publication 800-30).

Special note on operational technology:
Considering the safety risks of cyber attacks on your organization's systems, particularly operational technology (OT) systems, is critical because these systems control physical processes such as manufacturing, transportation, and critical services. A successful attack on OT systems can lead to severe consequences, such as equipment malfunctions, environmental hazards, or even physical harm to individuals. Unlike IT systems, where the focus is on protecting data, OT systems require safeguards against threats that can disrupt operations and harm human safety. Securing these systems is essential to prevent catastrophic outcomes. In response to this, the NCSC, CISA, and international partners collaborated with the Australian Signals Directorate's Australian Cyber Security Centre (ASD ACSC) to develop the Principles of Operational Technology Cyber Security.

3 Develop security policies

Create comprehensive security policies and procedures to guide employees' behavior, and establish standards for safeguarding data, access control, incident management, and more. The policies should focus on key areas such as password management, data encryption, remote access, and acceptable use of company resources.

It may be your responsibility to write and communicate the security policies. However, it is your executive leaders or directors who ultimately are responsible for prioritizing cyber security within your organization. NCSC created the Board Toolkit and Toolbox to assist you in communicating more effectively and assist your executive leaders in understanding their duties to govern cyber risk more effectively.

4 Establish a cyber security governance structure

Your organization's leaders should be aware of the risks of cyber security to your business and how to manage them. When done right, cyber security concerns are considered when making strategic decisions.

Cyber security governance encompasses policies, procedures, roles, responsibilities, organizational structure, and controls to protect your organization from cyber threats. As the champion for cyber security in your organization, you need to elevate the conversation and connect with all employees. Cyber security is a team sport. This means you must engage people to ensure the cyber security risks are understood, managed, and mitigated. You must work with the audience, and not assume everyone has the same level of understanding as you. The key is to develop ways to communicate regularly with everyone about the need for vigilance.

Establish a security steering or working group. Through structured processes, communication and monitoring, this group can maintain oversight of risks and issues, and ensure continuous monitoring or support for delivery of mitigation plans and activities. Security working groups often include representatives from various departments (e.g., IT, HR, legal, compliance) to ensure that the discussion and decisions consider different perspectives. Regular communication with executives ensures transparency and alignment on progress and priorities. This also helps to secure their support, and makes it easier to request resources for delivering improvements, reducing risks, and maintaining alignment with the overall risk management strategy.

5 Implement security controls

You identified your critical assets and evaluated the cyber security risks. Now you need to consider the security controls necessary to protect them.

There is a wide range of controls, standards, and frameworks, so you need to determine the best approach for your organization. If you are unsure how to approach this step, use the "Your Systems" section of the U.S. CISA **Cyber Essentials Starter Kit** to help get started.

6 Train your employees

Conduct regular cyber security awareness training to educate your employees and contractors on common cyber threats (e.g., phishing, social engineering) and the importance of following best practices and processes (e.g., applying security patches and updates as soon as possible, creating good passwords).

Ensure they understand the security policies and their role in protecting the organizational assets.

The "Your Surroundings" section of the U.S. CISA **Cyber Essentials Starter Kit** contains many useful resources to help you create and implement a training and awareness program, including links to **Cyber Readiness Program — Cybersecurity Awareness Workforce Training** and NCSC's training course, **Cyber Security for Small Organisations — Overview**.

That takes care of your employees, but have you thought about you and your development? **Cybersecurity Workforce Training Guide** offers you an opportunity to chart your career pathway and identify areas for upskilling and growth.

7 Create a cyber incident response plan

You must develop a plan to respond quickly to security incidents, highlighting the steps to detect, contain, investigate, and recover from an attack.

Establish roles, responsibilities, and a communication framework for handling incidents. Everything you need to get started is contained in the Cyber Security Incident Response Guidance on the Rolls-Royce website.

8 Monitor and audit systems

Some organizations do not have the tools, services, or expertise available to continuously monitor and detect suspicious activities or breaches in real time (i.e., using Security and Information Event Management (SIEM) tools). For those who have limited resources but technical knowledge, CISA's Logging Made Easy (LME) offers a no-cost management solution for small and medium-sized organisations.

9 Ensure compliance

Verify that your cyber security program aligns with industry regulations and standards, including security requirements in contracts with Rolls-Royce.

Implement a regular review process to ensure that policies, processes, technology, and best practices remain consistent with the evolving laws and regulations applicable to your organization.

Conduct internal security assessments and audits. Assess the effectiveness of controls and processes to manage cyber security risks to your organization and identify gaps in your security policies and cyber security standards. If you require an objective independent examination, engage an external auditor who can verify controls are implemented and operated according to the standards.

Prioritize compliance activities based on your organization's risk profile and available resources.

10 Continuously improve

Cyber threats evolve, so review and update your security program regularly. Conduct post-incident reviews to learn from breaches or security events.

Stay informed on new threats and technologies and adapt your security program as needed. Sign up for newsletters and subscribe to alerts and advisories:

- Subscribe to updates from CISA
- Subscribe to alerts and advisories from NCSC
- Sign up for the MxD newsletter

By following these steps, you can establish a solid foundation for your cyber security program that evolves alongside the ever changing regulatory and threat landscape. **Trust in your abilities, and remember: This is your opportunity to develop new skills and enhance your cyber security knowledge.**

For more information, contact **Clare McBrearty**, Rolls-Royce Supplier Cyber Security Lead: ***clare.mcbrearty@Rolls-Royce.com***