nccgroup
freedom from doubt

An NCC Group Publication

# Cyber Red-Teaming Business-Critical Systems while Managing Operational Risk

**Prepared by:**

**Ollie Whitehouse**





# Contents



# 1 Introduction

Cyber red-teaming allows mature organisations to gauge their true resilience to sophisticated, planned, and somewhat sustained cyber-attack. These organisations use red team engagements to assess multiple facets of their cyber security strategy, maturity, and implementation, including:

- Open source intelligence footprint.
- Staff awareness and susceptibility to social engineering.
- System and software design and implementation.
- Technical countermeasures and defence-in-depth level.
- Detection, response, and remediation capabilities.
- Crisis management processes and procedures.

With the advent of programmes such as the Bank of England's CBEST[1] (Central Bank Ethical Security Test) and CREST's[2] STAR, and the general increase in demand from customers for sophisticated threat simulation by red-teaming, more and more assessments are being conducted in live environments, involving live users and real exploits. Most importantly, these assessments are being carried out against business-critical systems and functions.

The desire for these kinds of assessment is often driven by senior leadership's need to understand their organisations' real-world susceptibility. Assessments of this nature help measure the likelihood that that a threat actor could -- via the Internet, partner connection, supply chain, or other means -- gain remote access to their most sensitive systems and data, bypassing existing preventative or remedial controls.

This kind of assessment also necessitates minimising the risk of unexpected operational impact on or exposure to a business during any such an activity.

NCC Group's first experience dates to 2000, when we worked with the very early IP-based mobile telecommunication networks. We performed live red-team assessments against 2G, 2.5G, 3G and 4G networks from a subscriber handset perspective against the network core. When dealing with live Critical National Infrastructure (CNI) with lawful intercept, billing, and service delivery functions present, clients were rightly anxious as to the potential impact of a no-holds-barred approach.

In response to these concerns, we have developed and refined a strategy and supporting methodologies which, when adopted, minimise the risks posed to these systems and functions during red-team engagements no matter which vertical the organisation operates in. With the advent of CBEST/STAR and the red-teaming of critical economic functions in the United Kingdom these strategies have been further augmented; the Bank of England require the experience and capability of the individuals leading the assessments to be demonstrated and documented in a way which complements our existing strategy.

The key to managing the risks associated with red-teaming is a process of stakeholder engagement and communication, education, operational planning, ongoing visibility, and optional oversight. Due to the nature of such assessments, detailed technical plans are often not shared broadly within the target organisation, nor in some cases can they always be produced in the first instance due to the fluidity of engagement or level of detailed knowledge available upfront. However, even given these constraints, operational risk can be managed to acceptable levels for most organisations to allow such engagements to occur.

In this short paper, we outline how we support our clients in ensuring they can conduct red team engagements while managing their operational risk levels to within acceptable levels when working with business-critical functions and their underlying systems.

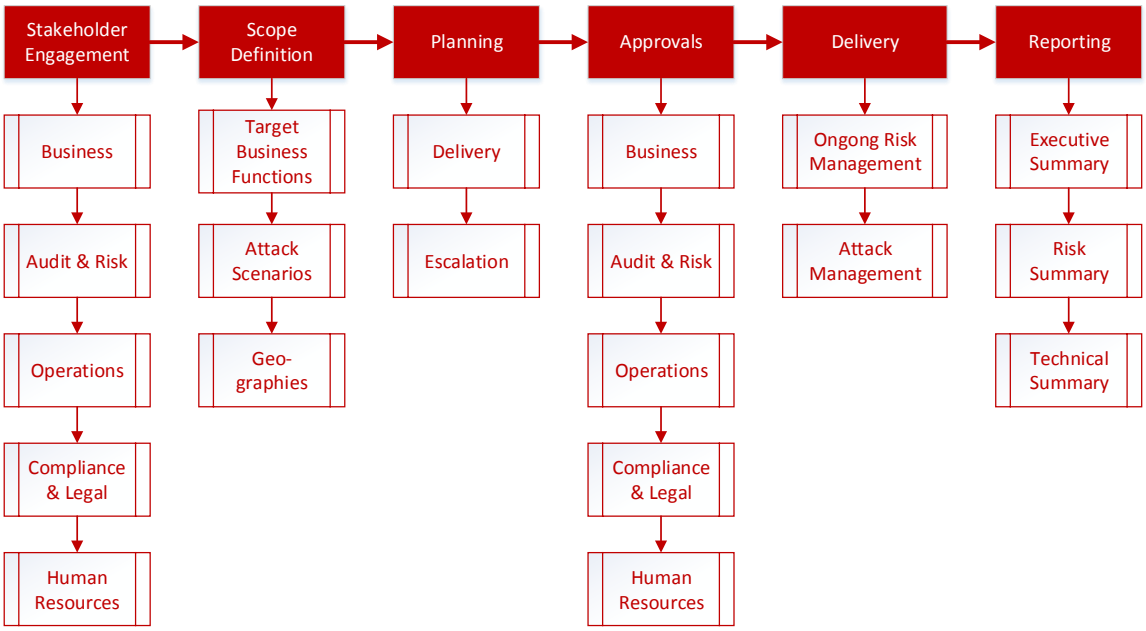
[1] http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx
[2] http://www.crest-approved.org/

# 2 Cyber Red-Teaming Business-Critical Systems

## 2.1 Red Team Engagement Process

The typical red team engagement process for clients who are undertaking their exercises against business-critical functions is shown below. Adopting this process ensures an informed and risk-managed delivery.




## 2.2 Risk Management Stakeholders and their Function

Within the stakeholder engagement and approvals processes there are a number of business functions and roles represented. Each of these functions has a part to play in ensuring that operational risk is kept to acceptable levels.

For each of these functions, we have outlined their typical role in the engagement, the approvals processes and, in the case of audit and risk management, the delivery phase.

### 2.2.1 Business

The business obviously needs to show willingness for a red team engagement to occur. As such engagements affect many areas of the business, they often involve Director, C level, or in some cases board-level approval. Engagement by and of people at this level is often required because, outside of audit and risk departments, they are the owner for the risk and thus the activity.

### 2.2.2 Audit and Risk Management

Organisations undertaking red team assessments often have audit and risk management functions. A close delivery working relationship with these functions ensures that they are comfortable in providing the required approvals, while also ensuring appropriate oversight and governance of the project.

NCC Group has also developed an approach that allows our clients' audit and risk management teams to have varying degrees of insight and oversight during the delivery phase. This insight and oversight ensures that our clients have ongoing visibility as to their exposure, and confidence that the engagement is being conducted within the agreed parameters via the approved means, targeting only targets that are in scope and minimising the risk.

It is important to stress that the number of people involved in any discussions should be kept as small as is practical, so as not to inadvertently impact or bias the results of the assessment due to inadvertent disclosure.

### 2.2.3 Operations

The operations team involvement must not bias or otherwise influence the results of the red team engagement. Instead, their involvement in the process is to provide input and appropriate approvals for the systems that are in scope and advice around any risks. Typically the operations team will not be told when or how systems will be targeted, but their input is often required when breaking down critical business functions to a system level set of agreed targets.

### 2.2.4 Compliance and Legal

During red team engagements there are often compliance considerations for regulated organisations, and legal considerations for almost all organisations, especially when dealing with business-critical processes and systems. As a result, having input from legal is recommended during the planning and approval stages, to ensure appropriate compliance and management of legal / liability risk.

### 2.2.5 Human Resources

Typically red-teaming will involve as one avenue of attack the targeting of specific individuals or departments using an element of social engineering. It is therefore recommended that human resources have at the very least been informed of the activity and the fact that this type of approach will occur. There are potential risks associated with the identification of individuals, gathering of information on them, and union objection.

NCC Group has a standard policy of not identifying specific individuals who, when targeted, result in a successful compromise. We also ask our clients, as further assurance, to undertake that if they independently identify any individuals they will not take any punitive action.

## 2.3 Delivery Risk Management

This activity is by far the most critical part of the operational risk management strategy with regards to red teaming. We find allowing our clients to have ongoing visibility of the delivery of the project, when coupled with our controls, often addresses their concerns. As a result we have devised several means of reducing operational risk through compensating controls and oversight. These mechanisms help facilitate a risk-minimised delivery without impacting the results due to inadvertent disclosure of NCC Group's plans, progress or successes. This is important as, should such information be disclosed to the operations teams or other business functions, it may bias their performance or capability.

### 2.3.1 Delivery Controls

The delivery controls we have implemented with regards to red-teaming are designed to minimise the risk of incident response and escalation issues, and ensure NCC Group's activities do not lead to increased risk of compromise.

It is imperative that before the red team engagement starts the necessary points in the incident response and escalation processes must be identified.

Red team projects are overseen by an attack manager and attack specialist. The attack manager is responsible for client interactions and liaison, while the attack specialist oversees the technical aspects of delivery. NCC Group adopts a similar requirement to the Bank of England, requiring 14,000 hours of experience for all its red team engagements for the attack manager and attack specialist roles. This requirement ensures that such projects are overseen by highly experienced and skilled staff, thus further minimising risk.

### 2.3.2 Technical Controls

We also implement a number of technical controls designed to minimise the exposure to which clients' systems and data are subject, both during the engagement and after its completion. These technical controls include:

- Attacks will only ever be conducted from NCC Group's physical premises, and thus from secure facilities.
- The attack tools used to breach, access, and control the compromise over the Internet have a time-limited life and are restricted to operating only in the client's environment.
- All communication between the breach end-points and NCC Group is encrypted, to ensure that client data is not exposed to risk of eavesdropping.
- All persistent data associated with the engagement, such as exfiltrated information and supporting evidence, is stored in a government-approved encrypted enclave to which only authorised consultants have access.

These controls address a number of risks associated with the particular methods used in red team assessments.

### 2.3.3 Operational Oversight

The final aspect of NCC Group's risk minimisation approach is to provide optional operational oversight of the technical delivery phase. We offer our clients the ability to optionally embed someone from their audit and risk teams within NCC Group during the project, on the understanding that no details will be relayed. This embedding allows our clients to have sight of and to understand the level of risk they are exposed to in near-real-time, and to ensure that business and technical risk appetites are not exceeded. It is expected that this individual be sufficiently senior to be able to operate in an autonomous manner throughout the engagement and thus not require support or input from the target to make risk decisions.

This mechanism provides a safeguard for the target, as the individual is able to call for the cessation of all further infiltration and exfiltration activities should the level of operational risk appear likely to become too great. Upon a cessation being called, the assessment is ended and any active compromise backed out. We then enter the reporting phase.

## 3 Conclusions

Based on our experience performing cyber red-teaming against business-critical systems, the strategies and the approaches outlined here allow both large and small businesses who run complex operations to manage the corresponding risks when undergoing assessment. The value of such engagements, which closely model real-world threat actors and their techniques while not being limited in the way traditional penetration testing often is today, should not be underestimated. The reality is that threat actors do not observe change windows, scopes, and other limiting factors. To gain a real-world understanding of your organisation's resilience to such threats requires a shift in techniques, and with a red team assessment you can gain the required assurance that your existing controls, processes, and countermeasures work as expected.