

STOic TTX (Tabletop Exercise) Framework

A STANDARDISED APPROACH TO
CYBERSECURITY RESILIENCE EXERCISING



A HEFESTIS project funded by the Scottish Government.

Authors

David Robertson, Regional CISO, HEFESTIS, Ltd.

Steve McIntosh, Regional CISO, HEFESTIS, Ltd.

Norice Bain, Project Lead, HEFESTIS, Ltd.

© HEFESTIS, Ltd., 2021

This information is licensed under the Open Government Licence v3.0. To view this licence, visit <http://www.nationalarchives.gov.uk/doc/open-government-licence/>.



Contents

- Introduction..... 3
- The STOic TTX Framework..... 4
 - Strategic, Tactical, and Operational Tabletop Exercises 4
- The STOic TTX Process 5
 - A few questions about your Organisation 5
 - Identifying Objectives 6
 - Identifying Attendees 7
 - Scheduling 8
 - Building Scenarios 9
 - Delivering STOic TTX Scenarios 10
 - Scenario Sequence 11
 - TTX Output and Actions 12
- Certification..... 13
 - Certification Levels 13
- Additional Resources..... 14
 - Facilitator Training..... 14

Introduction

Cybersecurity Incident Response is a focus of the Scottish Public Sector Action Plan but assessing an organisation's readiness and response maturity is extremely difficult without a real or imagined incident to use as a catalyst. An organisation that merely has policies, procedures and plans is not ready for an incident. Rather, it is the organisation that has tested and exercised its policies procedures and plans against the unknown that is better prepared.

In order to deliver a consistent approach to cybersecurity resilience exercising, there needs to be a standardised approach to use as a point of comparison. A standard framework with trained facilitators helps to ensure consistency of results and help to assure that the results are actionable and comparable from one exercise to another.

The STOic TTX framework provides an approach for organisations to:

- exercise management and operational teams' cybersecurity incident response
- identify gaps in people (skill and knowledge), process (policies and procedures) and technology in order to efficiently respond to cybersecurity events
- assess the organisation's cybersecurity incident response maturity (HEFESTIS members only)
- produce standardised output so that results can be compared from exercise to exercise
- encourage frequent exercising through engaging and streamlined incident scenario design
- provide remote and in-person delivery methods

While there are multiple sources of cybersecurity tabletop exercise (TTX) scenarios, the challenges that most organisations experience in carrying out exercises are found in the complexity and uncertainty of the facilitation process. The success or failure of a tabletop exercise and the organisation's desire to repeat the exercises process is largely determined by the quality of the facilitation.

Facilitation, like auditing, requires asking the right questions and asking the questions that participants may not be prepared for. Training and experience can help facilitators do this well. STOic TTX seeks to grow and train facilitators from within the organisation itself, so that effective and frequent exercising can be performed.

This Framework consists of the elements required to deliver successful tabletop exercises with actionable outcomes to test and improve an organisation's ability to respond to cybersecurity incidents.

The STOic TTX Framework

Strategic, Tactical, and Operational Tabletop Exercises

Every level of an organisation needs to be ready to respond to cyber threats at any time. The STOic TTX Framework is designed to adapt and be presented to the three incident response layers in a typical organisation:

1. **Strategic:** senior management, C-suite, Boards, business leaders, etc.
2. **Tactical:** department management, IR coordination teams, crisis teams, communications teams, legal teams, etc.
3. **Operational:** IR teams, IT specialists, Help Desks, Security Operation Centres, etc.

STOic TTX is designed from the start to encourage frequent exercising. To achieve this, the Framework trains facilitators to deliver fast and flexible scenarios that provide the optimal level of challenge for the participants, provides a Scenario Builder to ensure that an organisation always has relevant scenarios to exercise, and makes exercising inclusive and approachable.

STOic TTX is unique in that it is organisation-focused, not attack-focused. That means that the focus is not on the specific technical details of the attack in a scenario, but rather on the organisation's people, processes, and technology poised to respond to attacks. This also means that the facilitator does not need to be a cyber-attack expert in order to be successful, and that means that people from non-technical backgrounds can facilitate STOic tabletop exercises.

The steps of the STOic TTX Framework are:

1. Pre-Assessment
2. Identifying objectives
3. Identifying attendees
4. Scheduling
5. Building the scenario
6. Delivering the scenario
7. Capturing outputs and actions

The STOic TTX model also includes:

- A certification path to provide assurance to management and to guide the organisation towards maturing in their ability to exercise their incident response capabilities
- Facilitator training to ensure that the organisation can experience high-quality exercises as often as it needs in order to develop a mature incident response capability

The STOic TTX Process

A few questions about your Organisation

To ensure that appropriate scenarios are created for a tabletop exercise, the facilitator should identify how familiar the organisation is with tabletop exercises and what Incident Response (IR) documentation is available.

The Framework includes a set of questions that will provide the facilitator with some background information for the organisation. Ideally this should be done before the initial planning meeting.

STOic TTX Pre-assessment Questions

- Do you have a Cyber Incident Response Plan?
- Have you tested your Cyber Incident Response Plan?
- Do you have a Cyber Incident Response Team?
- Do you have a process to action the outcomes of testing your Cyber Incident Response Plan?
- Have your staff received Cyber Security Awareness Training?

Answers to these questions allow the facilitator to gauge the organisation's level of experience with tabletop exercises.

Once the organisation's readiness for tabletop exercises is established, the next step is to identify what is desired from conducting an exercise in the organisation by setting some objectives for the exercise.

Identifying Objectives

In order to measure the success of the TTX programme, it is essential for clear objectives to be identified before each event. This also allows for appropriate scenarios to be created that are aligned to the objectives. There is no point in having a scenario test an organisation's response to a stolen laptop containing confidential data if the main objective is to test the organisation's ability to detect and properly react to hostile activity.

The typical objectives of a tabletop exercise are listed in the table below. The levels associated with each objective relate to the expected STOic TTX certification path levels. However, an organisation can set their own objectives no matter what certification level the organisation might hold.

	Objectives of TTX	Level
1	Determine the effectiveness of cyber training provided to staff	Basic
2	Determine what enhancements or capabilities are needed to protect an information system and provide for operations in a hostile environment	Basic
3	Test effectiveness of the organisation's incident response plans	Basic
4	Test the effectiveness of communications processes during an attack	Basic
5	Test the organisation's capability to determine operational impacts of cyber-attacks and implement proper recovery procedures	Target
6	Enhance cyber awareness, readiness, and coordination	Target
7	Expose and correct weaknesses in cyber security systems, policies and procedures	Target
8	Test ability to detect and properly react to hostile activity	Target
9	Understand the implications of losing access to IT systems and test the workarounds for such losses	Advanced
10	Develop contingency plans for surviving the loss of some or all IT systems	Advanced
11	Test the organisation's capability to respond to uncertain and complex incidents and attacks	Advanced

Once the objectives are understood, it will be clearer who from the organisation should attend the exercise. For example, if the main objective is to test the effectiveness of communications processes during an attack, then participation from the communications team, and probably representation from HR and Legal will be required, not just participants from IT.

The scenarios are designed to escalate from basic to target than advanced in all instances. This is to reflect the escalation of an incident from the identification stage which is an operational scenario, through the propagation/limited compromise stage as the effects of an incident are experienced in increasing areas of the digital estate, requiring wider notification and engagement to the advanced stage where significant compromise has developed and strategic level decisions must be made, and business continuity plans triggered.

Identifying Attendees

The attendees of a tabletop exercise are related to the identified objectives and the level of the exercise (Strategic, Tactical, or Operational). Who attends also depends on the roles and responsibilities those people hold within the organisation.

Research has shown that exercises with more than ten participants present a challenge in terms of allowing all attendees to provide their individual perspectives. To get the most from the exercise, and to ensure everyone is able to provide input, attendance should be limited to around ten people. Although, if there is a point where a staff member would be required for a small amount of time, the facilitator can arrange a window of time in the exercise, so the staff member does not have to sit through the entire exercise.

Examples of who should attend which scenario:

Level	Who	Why
Strategic	Executive Leadership Team	There can be a tendency for executive leaders to underestimate the importance of cyber security. STOIc TTX gives executive leaders hands-on practice in a scenario where they have to: <ul style="list-style-type: none"> - make critical decisions (e.g., whether or not to pay a ransom) - create and approve communications statements regarding a breach - make decisions on sharing breach information (e.g., with Police) Exercising these scenarios will provide the skills to enable executive leaders to respond effectively during the stress of a live scenario.
Tactical	Senior Management	Participation will exercise skills in: <ul style="list-style-type: none"> - understanding the impact to the organisation - making critical business decisions regarding services shutdown/runtime - giving authorisation to departmental resources - enforcing policies
Operational	IT – Department	For IT staff, participation will exercise the focus on creating smooth handovers, escalation protocols, crisis management and communication channels. As well as testing their capabilities to: <ul style="list-style-type: none"> - uphold and enforce security policies - ensure response processes are in place
Operational	IT – Front Line Helpdesk	To test front line teams' ability to monitor and triage alerts efficiently and effectively and give staff the confidence and knowledge to escalate events when necessary
Operational	IT – 2 nd /3 rd Level	Improving teamwork and knowledge in procedures, keeping skills sharp, knowing your responsibilities in crisis.

Scheduling

Once objectives and attendees have been identified, a date and duration for the event should be arranged.

Tabletop exercises that are being delivered remotely should, ideally, be no longer than 90 minutes. With the actual exercise lasting around 60 minutes and time before for introductions and time after the exercise for the “hotwash” session to document actions, and general review. This timescale is for tabletop exercises for bronze maturity level organisations. Those with silver or gold maturity levels should consider a minimum of 2 hours with comfort break(s) at convenient points in the exercise.

Something worth considering is “hijacking” an existing regular meeting where all/most optimal attendees will be present. In real life, there is no prior warning to organisations that they are about to be attacked. Hijacking brings with it the element of surprise which can make the tabletop exercises more true-to-life as participants will not expect or be prepared for the event.

Once the date for the tabletop exercise has been scheduled, with confirmed availability of those required to be in attendance, the next step is to build the scenario.

Building Scenarios

The facilitator will build the scenario using the STOic TTX Scenario Builder or a pre-made scenario, in line with the defined objectives of the tabletop exercise and the level of the exercise (Strategic, Tactical, or Operational). The scenario will consist of an initial outline brief of the cyber incident including any assumptions, artificialities, and simulations. There will also be a series of injects to drive the objectives of the exercise, these will be designed to not overwhelm the training audience.

The table below lists some STOic TTX Core Scenarios and the objectives that are tested within each.

Scenario	Description	CRF Area
Virus	A user has clicked a link in a spear phishing email, This has installed malicious software on the device. Contained = Basic Lateral Spread = Target Successful Attack on entire digital estate = Advanced	2, 11, 4, 1, 13, 17, 14, 7, 8, 16, 10, 12
Denial of Service (DoS)	An abnormally high amount of network traffic is being experienced and is visible in system performance statistics and volume of log data. Additional notification from users about reduced network capability or inability to access website has been received. Standalone event = Basic Part of masked/staged activity = Target Launch of subsequent full scale attack = Advanced	2, 11, 4, 1, 13, 17, 14, 7, 8, 16, 10, 12
Unauthorized computer on network	An attempt is made to connect an unauthorized laptop to the organisation's network. Identified and contained = Basic Successful with malicious activity = Target Launch of subsequent full-scale attack = Advanced	2, 11, 4, 1, 13, 17, 14, 7, 8, 16, 10, 12, 3, 15
Malicious external scanning	An in-depth, long-running external scan of the organisations network is being performed. Identified and blocked = Basic Successful with malicious activity = Target Launch of subsequent full-scale attack = Advanced	2, 11, 4, 1, 13, 17, 14, 7, 8, 16, 10, 12
Malicious internal scanning	A device on the network is performing scans on the internal network. Identified and blocked = Basic Successful with malicious activity = Target Launch of subsequent full-scale attack = Advanced	2, 11, 4, 1, 13, 17, 14, 7, 8, 16, 10, 12, 3
Computer compromise	Unattended computers with no password screensaver lock have notes in the on-screen text editor that the computer has been compromised all affected devices have been using the same third-party application. Identified and contained = Basic Successful with malicious activity = Target Launch of subsequent full-scale attack = Advanced	2, 11, 4, 1, 13, 17, 14, 7, 8, 16, 10, 12, 9, 5, 6
Phishing via email	A phishing email is sent to multiple employees attempting (successfully) to capture credentials. Identified and contained = Basic Successful with malicious activity = Target Launch of subsequent full-scale attack = Advanced	2, 11, 4, 1, 13, 17, 14, 7, 8, 16, 10, 12
Ransomware	Core servers and many end points have been infected with ransomware and are non-functional. Identified and contained = Basic Successful with malicious activity = Target Launch of subsequent full-scale attack = Advanced	2, 11, 4, 1, 13, 17, 14, 7, 8, 16, 10, 12

Delivering STOic TTX Scenarios

Agree with the facilitator whether or not the majority of participants, if not all, will not be informed of the scenario until they are actually participating in the exercise.

Although retaining the exercise materials in advance helps to make the scenario as realistic as possible, especially as there is no advanced warning given in real life attacks – pre-release helps facilitate a more informed session, especially when there are time or attendance constraints for the participants. There is also the option to have potential attendees on call for expert or partial contributions. Defining appropriate contribution/attendance levels for participants is a key part of the exercise and should be performed in liaison with the facilitator.

Participants will be asked to suspend reality and to not “fight the scenario.” There are often events in the real world that do not occur as one might expect. The intention of a tabletop exercise is not to argue about whether or not something could happen, but to explore how participants would act/respond if it did happen. If participants are fighting the scenario, one question that can refocus the participants is, “If this did happen as described, what would have had to happen to make that possible?”

It will also be made clear to attendees that this is not a test nor an audit. There is no score. This is an opportunity to practice the organisations decision-making in a safe setting. In a live incident where emotions are high, facts are few and time is not on your side, clear decisions based on preparation will shorten the time to recovery. This is a learning opportunity, not a personal test or exam. It is a training exercise to identify gaps in people, process, and technology.

Scenario Sequence

Example of a typical sequence within an exercise:

Step	Notes
Introductions	<ul style="list-style-type: none"> • Introductions from participants and their role in the exercise
<p>Explanation to Participants:</p> <p>Do not Fight the Scenario</p>	<ul style="list-style-type: none"> • Explain the exercise • No time pressures • Safe environment <ul style="list-style-type: none"> • not recorded, only actions/outcomes logged • No right or wrong answer • Not a test or audit • Exercise designed to stimulate discussion <ul style="list-style-type: none"> • the more you engage, the better the outcome • Treat it as a real scenario
Begin Exercise	<ul style="list-style-type: none"> • Facilitator introduces the scenario • Let discussions evolve naturally • Identify risks and issues, steps to be followed, etc. • Identify internal and external participants in the scenario • Use leading questions to stimulate conversation. For example, “what would you do in this situation?” • Facilitator will provide injections as needed
Document the Exercise	<ul style="list-style-type: none"> • Take notes during the discussions • Forms a basis for after-exercise review • Note <ul style="list-style-type: none"> • Observations - things that are in place that help during the incident • Actions - things we now know that can be done within current resources • Lessons Learnt - things that we know now that will require additional resource/project to address. • Areas that need more research • Summarize action items • Document issues identified
After Exercise Review	<ul style="list-style-type: none"> • Review exercise objectives • One participant will summarise the discussion and recommendations • Feedback from all participants • Facilitator will document concerns and actions to be taken forward by the organisation

TTX Output and Actions

The facilitator will complete the [STOic TTX Exercise O&A Report](#), which details all outputs and action items generated from the exercise.

It will be of great benefit to complete all actions before a similar exercise is performed, otherwise a subsequent exercise is likely to uncover similar key findings to those already identified.

Indicators of a successful tabletop exercise are:

- Objectives of the tabletop exercise have been met
- Participants are exhausted but hopeful
- Attendees should feel like they have been through an ordeal and emerged triumphantly on the other side.
- Senior management have confidence their IT department have a plan to handle security incidents.
- All departments have a better understanding of what is required from them during an incident.

A timescale and date for the next tabletop exercise should be agreed. It is not imperative that the specific date is arranged at this time, as the objectives and attendees will need to be agreed, but the approximate timescales when the next exercise should occur should be recorded.

Certification

Organisations need to be able to provide assurance that their TTX programme is progressing, is meeting objectives, and that the organisation is better able to respond to cyber incidents. STOic TTX includes a high-level, self-certification path that can provide this assurance.

Having a certification path and goals help the organisation decide what to exercise/tackle next.

The scope of this certification is determined by the organisation. Having layers of certification allows the organisation to decide on the scope which best suits them. This may be across the entire organisation or limited to one department.

Organisation's having decentralised IT may choose to gain certification for certain business units only, or for organisations with a central IT dept, they may choose to only certify the Incident Response Team.

The scope can be defined in the way which makes most sense for the organisation in line with their goals and objectives. It has to be made clear, however that should an organisation choose to limit the scope of certification, to certain areas/departments, they will be potentially missing the opportunity to improve their ability to respond to an incident as an organisation.

The scope could cover the entire organisation or certain departments.

Certification Levels

Each exercise performed provides certification points

- 10 points for each Basic exercise
- 20 points for each Target exercise
- 30 points for each Advanced exercise

Level	Description
Bronze	Achieved at 20 points Participated in at least one Operational Core Scenario
Silver	Achieved at 40 points Plus: Completed bronze certification. Participated in at least one Tactical Core Scenario, which included two additional injects.
Gold	Achieved at 70 points. Plus: Completed silver certification. Participated in at least one Strategic Core Scenario with an expert Cyber Professional in attendance to present adaptive injects.

In order to achieve STOic TTX Gold certification the organisation would therefore need to perform around 4 TTX in total, 1 advanced, 1 target and 2 basic or a mix of exercises at each STO level to reach the 70 - point completion scoring.

As the framework provides all the information required for a facilitator to arrange and deliver these exercises, it is not envisaged that this will be overly onerous for an organisation. In fact, it is hoped that participating in a STOic TTX event will be an enjoyable way to learn and address the more serious topic of a cyber-attack.

There is a tracking document for each level, Bronze, Silver and Gold. Tracking documents should also be completed by organisations for each scope exercised.

Additional Resources

Facilitator Training

Facilitator training is delivered via the STOic TTX Facilitators Training Programme. This is achieved through a series of online training videos, a training guide, and participation in STOic TTX events.

There is a list of requirements a facilitator needs in order to feel properly equipped, supported and resourced to confidently deliver a successful STOic TTX. Some of these requirements the facilitator may already be in possession of. The STOic TTX Facilitators Training Programme is designed to address the gaps in these requirements and prepare facilitators to run engaging scenarios and achieve the goals of the framework.

Training Videos:

<https://www.youtube.com/playlist?list=PLMPfYFGpMbH4rYomEC6xLBrMZ9mcOUdIX>

Training Guide:

[STOic TTX Training Guide](#)