HEFESTIS
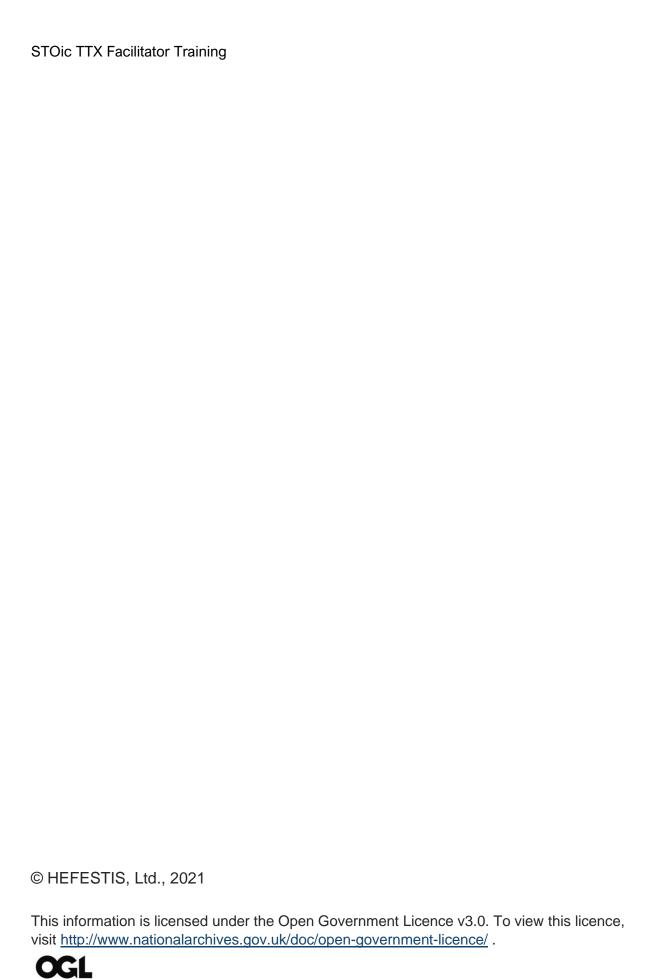
STOic TTX (Tabletop Exercise)
Facilitator Training

A STANDARDISED APPROACH TO CYBERSECURITY RESILIENCE
EXERCISING

Contents

List of Tables

Introduction

Cybersecurity Tabletop Exercises (TTX) are an important and efficient method for organisations of every size to prepare, practice, and improve their cybersecurity incident response capabilities. They are also an efficient and safe way to identify gaps, inefficiencies, and deficiencies in an organisation's security posture when nothing is under active threat.

So, why are TTXs overlooked?

Most often, the reason that TTX is not done is because TTX requires a facilitator willing and trained to put a team, department, or organisation through an exercise. There are very few professional facilitators that organisations can hire, and there are few, if any, guides or training materials for organisations to raise their own facilitators from within. The second most common reason that TTX is not done is that those who might want to be facilitators are intimidated by thinking that they need to have all the answers to every possible question that might arise in an exercise.

This guide seeks to address these issues. One of the original goals of the STOic TTX project was to make facilitation more approachable, more flexible, and more inclusive for non-technical facilitators and cybersecurity novices. The more facilitators there are, the more organisations there can be that can do more exercising and gain the benefits of the process and protect themselves and the public at large.

This guide provides training on the STOic TTX facilitation process and the core skills required to be a good facilitator.

The Author

Jordan M. Schroeder has been involved in tabletop exercises in one form or another for over 20 years. From province-wide Canadian Public Health global pandemic exercises to city-wide earthquake preparedness exercises, to corporate Business Continuity exercises, and countless cybersecurity TTXs for organisations across the US, Canada, and the UK.

In addition to the public sector and corporate TTXs throughout his career, Jordan has run a variety of regular, weekly recreational tabletop exercises for 10 years. In other words, Jordan is a long-time "Dungeons & Dragons" Dungeon Master. The skills learned while sending waves of fantasy creatures at imaginary heroes played by people of all walks of life are the same core skills required to make a cybersecurity TTX engaging, flexible, fun, and ultimately effective at achieving the goals of the TTX. This STOic TTX training guide includes the discussion of many of these shared skills.

> **Roleplaying Game Analogy**
> Throughout this guide, notes like this will appear that will explain STOic TTX concepts in terms of roleplaying games like Dungeons & Dragons. The connection between STOic TTX and roleplaying games is intentional. By breaking the facilitator out of the mindset that a TTX has to be formal, official or serious puts the facilitator in a more creative mindset and will hopefully result in TTXs that are more engaging, flexible, and fun.
>
> If you are not familiar with roleplaying games, that is OK. Think about being a facilitator like creating a safe experience for participants to explore ideas and to encourage innovative solutions to novel problems.

Video Training

A video course accompanies this guide and is found at:

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

STOic TTX Concepts

For organisations with well-established cybersecurity incident response processes (IR), TTXs are like a fire drill; they exercise the established processes to make those processes second-nature for the participants, for long-time and new staff alike. However, unlike fire drills, the cybersecurity landscape and the organisation's digital landscape changes all the time. It would be as if fire regularly changed how it burned and the layout of the building changed every month. If those things happened, the organisation would need to run fire drills far more often than once a year. And so it is with cybersecurity.

For organisations without well-established IR processes, TTXs might be the best, or arguably, the only way to identify gaps in their IR processes before those gaps are experienced in an incident.

Therefore, TTXs need to be run as often as possible and at all levels of the organisation. Those levels are:

- **Strategic**: senior management, a.k.a. Gold level
- **Tactical**: team management, a.k.a. Silver level
- **Operational**: responders, technicians, analysts, etc. a.k.a. Bronze level

This is where STOic gets its name.

Only exercising the Operational level, which is what most organisations do, hampers the organisation from identifying the gaps in the interactions with the Operational teams, and misses an important opportunity to train senior management and make them aware of the true nature of the existential digital threats the organisation faces.

However, to be able to run TTXs more often and throughout the organisation requires that the TTXs to be designed and run in such a way so that the organisation would want to run TTXs more often and gain a tangible benefit after every exercise.

Fast, Flexible and Fun

To accomplish that goal, STOic TTX framework was designed to be "fast, flexible, and fun". The aim was to make it feasible for an organisation to run TTXs weekly, whether every organisation does that or not, and to ensure that the organisation received defined value from each exercise.

Fast

Some other TTX frameworks are multi-day events that involve the whole organisation at once. STOic is designed so that small groups of participants (up to 10) who are familiar with the TTX process could run a TTX in as little as 20 minutes. For those new to the TTX process, a TTX should not take more than 90 minutes.

Most other TTX frameworks require a pre-written incident scenario that contains all the relevant details of the event. While these make it possible for the TTX facilitator to not require expert knowledge of the type of event being exercised, it can take quite a lot of preparation. STOic TTX is designed so that a facilitator could possibly choose a scenario minutes before an exercise, or even change scenarios in the middle of an exercise.

Flexible

Because most other TTX frameworks require a pre-written scenario, the exercise becomes focused on the details of the attack or incident. While there is a place for those types of exercises, and in the Gold level of the STOic certification path, a detailed attack scenario run by an expert is required, this makes the scenario constrained to the scenario details.

STOic takes the approach of being **participant-focused**, not scenario-focused. This design choice provides several benefits to a facilitator:

- The focus is placed on the participants, not the facilitator
- Any type of scenario can be run
- The facilitator does not need to be an expert in the scenario details
- The scenario is not a puzzle to be solved but a springboard for discussion
- Scenarios do not need to be detailed
- The scenario can be adjusted on the fly to fit the skill levels and limits of the participants

The consequence of a participant-focused approach means that a facilitator requires resources to support this open flexibility, and this training is designed to help with that.

Roleplaying Game Analogy

In games, the world is created by the game designers and the Players explore it and solve its finely crafted challenges. Most other TTX frameworks take the same approach by using detailed scenarios that the participants try to 'solve'.

STOic TTX takes the inverse approach. The people, processes, and technologies have already been brought together by the organisation. The facilitator explores this world created by the organisation by presenting threats and seeing how the participants respond.

Put another way, STOic TTX is a "Tower Defence" game and the facilitator releases "creeps" towards the participants. Note, however, that the facilitator is not trying to "win" but to facilitate discussion between the defenders.

Fun

In order to have the possibility for weekly TTXs in most other frameworks, there would have to be a massive library of scenarios available so that participants did not get bored with running the same scenarios again and again. By not having a scenario-focus, STOic TTX avoids this problem and allows for creativity of the facilitator and to have the participants suggest and even lead in the scenario selection.

Roleplaying Game Analogy

In game terms, STOic TTX has a very high "replay value".

The other quality to make a TTX "fun" is to borrow the concept of "The Flow State" from game design. This guide goes through an explanation of Flow in a later section, but briefly, a Flow State is when challenges increase within the range of the participant's skill range. If challenges are far below the participant's skill range, the exercise is boring, and no one learns anything. If challenges are much higher than the participant's skill range, then the exercise gets frustrating, and no one learns anything either.

As a facilitator, having a flexible scenario approach means that you can adjust the complexity and difficulty during the exercise to be challenging enough so that the participants need to rise to the challenge and learn something from the exercise, but not so challenging that the participants give up.

By being "fast, flexible and fun" STOic TTX can meet the goal of enabling the whole of an organisation to exercise frequently while learning from each exercise and enjoy doing so.

Facilitators can learn the three skills required to deliver this goal consistently for their organisation.

TTX Element	STOic TTX
Participants	Up to about 10
Exercise time	20-90 minutes
Design approach	Participant-focused
Scenarios	Springboard for discussion, participant-led
Replay value	High
Facilitator goal	Maintain a good challenge level during the exercise

Table 1: STOic TTX Design Cheatsheet

Core Facilitator Skills

To be a facilitator, there are three core skills that anyone can learn but that even experienced facilitators work to improve upon:

1. Managing exercise logistics
2. Maintaining participant engagement
3. Crafting the participant experience

Exercise logistics are the practical elements of preparation, execution, and resolution of an exercise.

Participant engagement is the skill during the exercise to keep discussions flowing and making sure that everyone feels like a valued participant. This is the set of "soft skills" for facilitating a group that many people might already have or might need to enhance to fit the unique environment of a TTX.

Participant experience is the skill to craft a unique experience for the participants and maintaining the right challenge level (i.e., a "Flow State"). This skill is, arguably, the most difficult to learn of the three and is the one that experienced facilitators work on every time they facilitate an exercise.

Exercise Logistics

Framework Steps

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

These steps are laid out and explained in the STOic TTX Framework core document for your review. However, the last three steps are expanded below.

Building the Scenario

Once the objectives are determined, the scenario can be chosen and built. The scenario is the heart of the exercise, and it becomes the situation that the participants respond to.

External Scenario Sources

Because STOic TTX is not scenario-focused, the facilitator is free to use scenarios from any source. There are commercially available sources of TTX scenarios as well as free sources. The following is a list of some free sources.

Source	Provider	Link
Exercise in a Box	NCSC	https://www.ncsc.gov.uk/information/exercise-in-a-box
@BadThingsDaily	Twitter	https://twitter.com/badthingsdaily?lang=en
NIST SP 800-61r2	NIST	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
Six Table Top Exercises	CIS	https://www.cisecurity.org/white-papers/six-tabletop-exercises-prepare-cybersecurity-team/

Table 2: Free Scenario Sources

The thing to remember is that for a STOic exercise, the facilitator should use pre-made scenarios as a flexible catalyst for discussion and exploration and not a rigid narrative that must be told the way it is written.

Roleplaying Game Analogy

Some roleplaying games are criticised for being too much of a "railroad" and not enough of an "open world". As a facilitator, try to make the scenario more of an open world, although the specific threat in the scenario should have focus to ensure that the participants are prepared for that threat. Also, chasing tangents in an exercise does not often result in a satisfying experience without the main scenario coming to some form of resolution.

Building Your Own Scenarios

Whether the facilitator borrows scenarios from somewhere else or builds their own STOic TTX provides a framework to help build relevant and interesting, scenarios based on four building blocks.

- Threat
- Level
- Initial Impact
- Injects

The **Threat** is the main issue that has occurred that the participants will explore. This is often determined when the objective is determined, but not always. This could be ransomware, phishing, DDoS, etc. The threat may be a single instance of an issue or a complex, multi-staged issue with different threats. The depth of the threat is covered by injects later in this guide.

STOic TTX includes eight core scenario descriptions that represent the most common and the most impactful threats organisations face. Every organisation must be prepared and practice their response to each of these scenarios and these are a good set for facilitators to start from.

Scenario	Description
Virus	A user has clicked a link in a spear phishing email, This has installed malicious software on the device.
Distributed Denial of Service (DDoS)	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.
Unauthorized computer on network	An attempt is made to connect an unauthorized laptop to the organisation's network.
Malicious external scanning	An in-depth, long-running external scan of the organisations network is being performed.
Malicious internal scanning	A device on the network is performing scans on the internal network.
Computer compromise	Unattended computers with no password screensaver lock have notes in the on-screen text editor that the computer has been compromised.
Phishing via email	A phishing email is sent to multiple employees attempting to capture credentials.
Ransomware	Core servers and many end points have been infected with ransomware and are non-functional.

Table 3: STOic TTX Core Scenarios

The **Level** is determined by the exercise objective and sets the exercise to be either Strategic, Tactical, or Operational. The level of the exercise has a significant impact on how the scenario is built because the level, along with the threat, determines the specific impact the exercise will present. For instance, the scenario does not need to describe specific technical details in a Strategic exercise, and legal issues do not need to be raised in an Operational exercise.

The **Initial Impact** is what is presented to the participants to start off the scenario. An exercise that starts off where nothing has gone wrong falls flat. Start off with an impact. That impact might be the main thrust of the exercise, or it might be the "tip of the iceberg" of a much larger and more complex issue that the participants will uncover.

For participant groups that are new to TTXs, always start off with a simple and straightforward initial impact. For example:

- "A user reports their machine is infected with a virus"

- "The webserver is unresponsive"
- "The IT Manager says that there is a ransomware outbreak, and they need to shut down the entire network"
- "The CEO is contacted by the media asking for comment on the fact that large amounts of company data have just been leaked."

As the participants get more comfortable with TTXs and their own ability to respond to incidents, the facilitator can bring in more complexity using injects.

Injects are how a facilitator can dynamically adjust the complexity and difficulty of an exercise. Injects are changes or new stages to the scenario. The facilitator should prepare several injects for the exercise, but also be prepared to not use any or all of them, depending on how the participants respond. The facilitator should also have a way to add ad hoc injects into an exercise so that every exercise can adapt to the participants.

The topic of injects are discussed in greater detail below.

Scenario Levels

The level of the scenario changes how the scenario is presented to the participants. The facilitator needs to keep the level in mind when choosing the initial impacts and the injects to ensure that they are relevant to the level and the participants.

Level	Typically deals with
Operational	Containing the incident, restoring service, and recovery
Tactical	Local team coordination, resource management, people management
Strategic	Organisation-wide resource management, people management, and communications, legal, third-party stakeholders

Table 4: STOic Level Concerns

Presenting, for example, the details of how ransomware is spreading to different servers is likely uninteresting to Strategic participants since there is nothing for them to decide or do about that specific problem. The same details might be very interesting to Tactical and Operational participants since they are required to respond to that problem.

Therefore, the facilitator needs to choose the initial impacts and injects that are relevant to the level of the exercise. The qualifying question is: do the participants have a responsibility to act on this information?

The facilitator might find that it is easier to run multiple different versions of the same scenario for Operational teams than it is for Tactical teams, and even less so for Strategic teams. Since the Tactical and Strategic teams deal with more generalised problems, it is difficult to make the same threats interesting and relevant to those groups more than a few times. This is expected, and the facilitator could choose to scale back the number of TTXs for these groups over time once those groups are confident that they have covered the unknown unknown gaps in their response.

Simple Injects

Choosing the threat, level, and initial impact is straightforward and aided by the exercise objective. Injects are what makes the exercise fun for both the participants and the facilitator. Injects change the scenario by advancing the event to the next stage or by changing the scenario.

Injects give the facilitator power to meet the needs of the participants. Some injects should be prepared ahead of time based on the threat and level of the scenario but having a toolset to introduce ad hoc injects as the need arises means that participants can remain engaged, the scenario can be highly relevant, and the facilitator can adapt to whatever comes up during the exercise.

The following is a list of simple, escalating injects that can be added to most scenarios. The facilitator should keep a list like this on hand during an exercise for quick inspiration, if needed.

Inject Type	Example	Level
Volumetric	1, 5, 50, all computers/servers/devices/users affected	O/T
User Criticality	Compromised system or account of: - average user - C-Suite - Developer - system administrator	O/T
System Criticality	Compromised: - end user device - server - web server - database server - virtual hypervisor - backup server	O/T
External forces	- Media contacts main office about breach - Media contacts IT staff personally about breach - Staff use social media to discuss incident - Law enforcement informs of compromise/breach - Anonymous contact informs of compromise/breach - Contractual partner complains about incident	T/S
Resource unavailable	- Email - Phones - DNS - Cloud system access - Network infrastructure - Key worker (admin, manager, developer, etc.) - Data centre	O/T/S
Time	- Friday afternoon - 2am Sunday morning - During a shift change - Christmas day - The organisation's busiest, most critical day - During a critical point in IT operations (during backups, while patching, etc.)	O/T/S

Table 5: Simple Inject Cheatsheet

Hopefully this list will inspire the facilitator to come up with their personal collection of simple injects based on their own experience.

Using these simple injects, it is possible to deliver an engaging, challenging, and custom-fit exercise to many different groups.

For example, consider the following setup:

- **Threat**: ransomware
- **Level**: operational
- **Initial impact**: a single user reports infection

A facilitator could advance this simple scenario by:

- Adding more affected users over time
- Specify specific users that have been affected
  - ○ CFO
  - ○ lead developer
  - ○ IT manager who has domain admin access
- Specify that the scenario is happening on Christmas Day

If the scenario was changed to the Strategic level, the facilitator could add:

- The loss of email
- All the participant's computers are non-functional
- The media calling for comment

For many organisations, the above-mentioned scenarios might be more than challenging enough. For some organisations, the base scenario is enough of a challenge without the need for injects. With the use of flexible injects, the facilitator can adjust to most participant groups.

Advanced Injects

The more mature the organisation is at incident response, the more detailed and specific the injects need to be, especially at the Operational level. A mature incident response process may see little difference between 5 computers and 5000 or an average user and the CFO.

To challenge an organisation that is mature in incident response, the scenario needs to be more complex and to replicate the process of an advanced attack.

Using detailed reports of actual attacks can be very useful in this case. News and vendor reports can be a facilitator's gold mine for complex scenarios, timelines, and injects.

Name	Link
Dragon News Bytes (Team Cymru)	https://team-cymru.com/community-services/dnb/
The Register	https://www.theregister.com/security/
Sophos Labs Uncut	https://news.sophos.com/en-us/category/sophoslabs/sophoslabs-uncut/

Table 6: Sources of Detailed Attack Reports

Another useful source for real incidents is the organisation's own history. Replaying incidents that have happened in the past, using the same or modified details, can be very effective.

By using the analysis of real attacks as a basis for an exercise, a facilitator can challenge even the most mature organisation and bring stark realism to an exercise.

Delivering the Scenario

The following is an excerpt from the STOic TTX Framework.

Most participants, if not all, will not be informed of the scenario until they are actually participating in the exercise. This helps to make the scenario as realistic as possible. There is no advanced warning given in real life attacks.

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 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 happened to make that possible?"

The facilitator will make it clear to attendees that the exercise is not a test nor an audit. There is no score. This is an opportunity to practice decision-making and rehearse processes 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 skills, tools, knowledge and procedures.

A typical sequence within an exercise:

Step	Notes
Introductions	• Introductions from participants and their role in the exercise

Explanation to Participants:
 	
Don't Fight the Scenario
	• Explain the exercise
	• No time pressure
	• Safe environment
	   • not recorded, only actions/outcomes logged
	• No right or wrong answer
	• Not a test or exam
	• Exercise designed to stimulate discussion
	   • the more you engage, the better the outcome
	• Treat it as a real scenario

Begin Exercise	• 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 this in this situation?" • Facilitator will provide injections as needed
Document the Exercise	• Take notes during the discussions • Forms a basis for after-exercise review • Note areas that need more research • Summarize action items • Document issues identified

After Exercise Review	• 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

Of course, the above is simply the logistics of holding an exercise. The details and the nuances of how to do it well are covered in later sections.

Notetaking

A facilitator takes notes during the exercise for two reasons:

- To remember details that are helpful to adjust the scenario
- To use as material for the O&A Report

It can sometimes help if there is a scribe to take the notes for the O&A report, but a facilitator will be aided by taking their own notes, as well.

The framework includes a notetaking template designed to help a facilitator keep track of useful information. No matter what notetaking process you choose, you need to be able to capture the relevant parts of the exercise as a resource for the report.

It is not necessary to "take minutes" of the exercise, and because of the freely interactive nature of the interactions, a minuting approach is not likely to work. Nor is it necessary to record who said what. The focus is on what was said, not who said it.

You need to capture:

- Key controls that the participants rely on in the scenario
- Concerns and open questions
- Action items specifically mentioned

Listen as people talk to identify the technologies, tools, processes, etc. that they mention as part of their response. Each of those things are in some way important to the participants. Seeing a list of those crucial things in a report can be an eye-opener for some teams and it can become obvious when there are dependencies between them. In addition, the list of items becomes a list of things to protect, enhance, or replace to maintain or improve the participant's ability to respond to incidents.

For example, WhatsApp was used so heavily in one scenario, that because of the exercise, the organisation halted their plans to forbid the use of the app until a more suitable alternative was found, implemented, and tested by the IR teams.

Concerns, open questions, and action items are the things that the participants will follow up on after the exercise. Those are the gaps, both large and small, that either need to be confirmed as gaps or plans made to close.

Nothing in the report needs to be confirmed as an actual problem. The report is a structured record of the identified gaps. Even if the gaps are not real, knowing that there was confusion about them is informative for identifying where greater awareness and training can be applied.

Participants often describe their actions in a sequence of steps. Recording these steps can be useful if the facilitator or the scribe has the ability to do so. These recorded steps can be compared against the official incident response playbooks as a means of identifying gaps. They are also very useful if the team does not have a playbook for the scenario being exercised as the start of a new playbook. In other words, a "proto-playbook".

Do not attempt to create a fully formed playbook in an exercise because that process requires a different thought process that accounts for different things. Instead, record the steps and sequences and use that as material for a project to create a playbook.

In practice, facilitators and scribes do not always have time to record the proto-playbook, so it is considered secondary to the core items to record; the key controls, open questions, and action items.

Capture	Description
Key controls	Things the participants relied on in the scenario
Open questions	Things the participants were not sure about but should be
Action items	Things the participants stated needed to be done
Proto-playbooks	(Optional) the sequence of steps taken by the participants to respond to the scenario

Table 7: STOic TTX Notetaking Cheatsheet

Samples of the notetaking form can be found in the Appendix.

Report

The report brings together all the information created by the exercise and recorded by the scribes and/or facilitators notes. STOic TTX provides a report template that includes the relevant items to include that form the expected outcome of a TTX.

The report template is intentionally formatted to encourage conciseness and to be completed efficiently. Almost everything in the template is designed to be list-based.

Header

The top of the report holds the information about the exercise and the participants. Record the date, location, and the names of the participants.

Scenario/Injects

Record the base scenario and any injects that were used. Do not record the injects that were planned but were not presented. The facilitator could mention the unused injects in the Proposed Future Scenarios section, if desired.

The more detail about the scenario and injects, the better, so that reviewers of the report can get a more complete context of the findings.

Key Controls

List the things that the participants relied on to respond to the incident. These things form the tools that are important for the organisation to respond to an incident. The items can be reviewed for fitness and for improvement.

Typical things that might be mentioned:

- 3rd party email or chat apps
- Personal phones
- Antivirus
- Logs
- SIEM
- Endpoint agents
- Backups
- Etc.

Key Findings

List the concerns and open questions raised by the participants. Number them ("Cid", or "Concern ID") for reference in the Action Items section. Determine if the concern or question represents a suspected gap or is merely a desire for more information or something to check on.

Categorise the item as an issue with skills, knowledge, technology, process, or some combination.

Recommendations/Action Items

List the recommendations for action by the facilitator, action items raised by the participants, and actions arising from the Key Findings and concerns. If relevant, reference the pertinent "Cid" for the action.

Proposed Future Scenarios

Often during the heat of an exercise, participants propose follow-up exercises they want to do. These are important to record and follow up on as they can be considered highly relevant to that collection of participants. If the facilitator has asked participants specifically for scenario recommendations, then those can be recorded here as well.

If the facilitator feels that the participants could benefit from a particular follow-up exercise, then those may be included.

Project Planner

The end of the template includes a helpful table to track action items. This is merely for the convenience of the participants and is not meant for the facilitator.

Capture	Description
Header	Details of the exercise event
Scenario/Injects	Record the scenario and the injects that were presented
Key Controls	List the things the participants used to respond to the incident and what it was used for, specifically
Key Findings	Concerns and open questions, categorised as Skill/Knowledge/Technology/Process and identified as a gap to close or informational
Recommendations/ Action Items	Specific actions mentioned by participants, actions arising from concerns, or recommendations from the facilitator, tied to the concerns, if possible.
Proposed Future Scenarios	Scenarios mentioned by the participants or scenarios recommended by the facilitator.
Project Planner	This section is a convenience provided by STOic to help manage the completion of the action items.

Table 8: STOic TTX Report Cheatsheet

Samples of the report can be found in the Appendix.

Participant Engagement

Participant engagement is the skill to be the best facilitator for the participants around the table, asking the right questions, and keeping the exercise on track.

The Golden Rules of Facilitating

The first rule a facilitator needs to follow is:

The exercise is theirs, not yours

The facilitator must respond to the needs of the participants and not to rigidly stick to the plan the facilitator might have made. Additionally, the participants need to feel like the exercise went well more than the facilitator needs to feel it went well.

The second rule is:

You are not the threat

It can be very tempting to try to force participants into a failing situation. But the facilitator's job is to facilitate discussion and exploration of the scenario, not to "win". The facilitator should use the scenario and clever uses of injects to achieve a state of Flow and uncover areas where the participants are unprepared or have not considered. But, the participants should never feel like they failed. At the end of the exercise, the participants should feel like they know the path to prepare for what they experienced in the exercise. An exercise should be empowering, not defeating.

Roleplaying Game Analogy

Instead of thinking of yourself as a narrator or storyteller, or even the "Big Bad Evil Guy" that the Players are trying to defeat, think of yourself as a Non-Player Character (NPC) who gives out quests. You provide the minimum number of details to start the Players off, a little guidance to keep them on track, and what happens next is up the Players.

Asking the Right Questions

Once the facilitator presents the scenario, it is up to the participants to respond. But the participants often need help to think about what needs to be done and what gaps they might have. It is very difficult to see one's own blind spots. The facilitator can help the participants explore the scenario by asking questions designed to get the participants thinking about the scenario in new ways.

There are four types of questions that might be helpful:

- Confirmation questions (sometimes called "active listening")
- Curiosity questions
- Consequence questions

Confirmation questions ask the participants to confirm that what they said.

"You do x. Is that right?"

This type of question is important to make sure that the facilitator understood what the participants said. It is also very useful for providing an external perspective on what a participant said.

Often, people assume things or fall into habits without thinking about it very much. An exercise can bring all these assumptions and habits out in the open. Hearing someone else, like the facilitator, verbalise these unexamined things, even after the person said it themselves, can be a way for the person to get valuable outside perspectives on their own ideas.

Having the facilitator repeat what someone else said also allows the other participants to challenge the idea more comfortably because it is the facilitator who said it (last) and not a co-worker. This is a simple but surprisingly effective tool to avoid conflict and encourage open discussion.

Be careful not to do this too much, especially if the participants are not engaging with it. If the facilitator only asks confirmation questions, the participants will become frustrated.

Confirmation questions are the easiest and simplest ways to keep conversation flowing, but they will not move the group into more unknown territory.

Curiosity questions are a way to explore the unknown by asking the participants about the things around what they have said (or not said).

The easiest curiosity questions to ask are the "5 Ws" (who, what, where, when, why) around what a participant has said. Forcing the participants to explain engrained behaviours or responses can do what confirmation questions do by providing a chance to examine habits. Doing this at unexpected times can be very impactful. Be careful not to ask "why" too often or else the participants can get frustrated.

The next easiest question to ask is a "what if?" question. Typically, the most relevant what-if question in a cybersecurity incident is:

"What if that didn't work?"

If the facilitator has experience in other organisations, the facilitator could ask why the participants do not respond the way that other organisations have. It is crucial that the facilitator does not ask this question with any tone of comparison. Every organisation is different. Treat what other organisations have done as a set of options for the participants to consider, not what the facilitator expects from the participants.

"At any point, would you consider doing x? Why/why not?"

Sometimes the most important curiosity question to ask in the middle of an exercise is:

"Is this process written down somewhere?"

Participants might be inspired and excited by the exercise and they might be inventing a process in the moment. This is a very good outcome of an exercise (see the Proto-Playbook section) but it can be very important to remind participants to document processes and

decisions so that incident responders to not need to remember all the good ideas that arose in a TTX.

Consequence questions are a more difficult form of curiosity questions and require experience and more imagination from the facilitator. Every action the participants take in response to an incident carries consequences. These consequences might affect the scenario itself or the planned injects. They will have other effects outside of the immediate scenario.

If the facilitator can imagine what consequence an action might have, then those things make great questions to raise. The set of simple injects listed in this training could be used as inspiration for consequence questions.

Some example consequences to consider:

- If something is turned off or unavailable, what else might need that thing?
- If a form of communication is affected, how will communication take place?
- How might different groups within the organisation feel about the proposed course of action?
- What is the chance that someone else will reverse/undo a course of action without your awareness/approval?
- How will the specific information gathered in an incident be used? (Participants love to gather all kinds of information in an imagined scenario.)
- How much will the course of action cost?
- Will the course of action affect the ability for the organisation to process payroll?
- Will the course of action that takes a long time be approved by HR/union/contracts? (A useful question for actions taken after business hours)
- At what point are the participants too tired to be effective? (For an incident that is taking a long time)
- What if a key participant is on holiday/having a baby? (The "baby" question is equally applicable for any gender and age. Brand new parents (or grandparents) are typically unavailable, and if they are available, they are distracted, and sleep deprived.)

By keeping good notes, a facilitator can keep track of various resources and the state they are in and ask good consequence questions when the participants plan to rely on something that they had changed earlier in the exercise.

If the facilitator cannot imagine a consequence, the facilitator can ask the participants directly:

"If you do x, what else might that effect?"

Prompts to Keep Momentum

A far more practical set of questions are the ones to keep the conversations going in useful directions. These types of questions are common to any group discussion or brainstorming session. They need to be completely open-ended and should require a bit of imagination or thinking a little outside of the scenario.

- "Tell me more"
- "What else are you worried about at this point?"
- "If you could have any one thing at this point in the incident, what would it be?"
- "What happened the last time you dealt with something like this?"

- "What's the worst thing that could happen at this point for you?"
- "What does success look like for you the incident the way things stand?"

The facilitator should ask these questions when conversation is flagging and ask these questions of the quieter participants when only a small number of participants are doing most of the talking.

There are also a couple of points that you want to ask more open-ended questions: when people look **shocked**, and when people get **dismissive**.

If someone says something, especially the facilitator, and some or all participants look shocked, the facilitator should dig into that reaction. The reaction could mean several things, but it is likely that the shocked participants and the speaker have mis-matched assumptions or expectations. If the speaker is the facilitator, then the facilitator should take the time to give the participants time to express themselves.

When people are explaining a process or how they might respond, at some point they will often get dismissive about their reliance on the availability or effectiveness of some resource. It is very important for the facilitator to explore why the participant holds such strong assumptions that the resource will work they way they expect.

In the extreme, participants will fail to explore the unknown unknowns regarding their responses to incidents, due to this dismissiveness. Often, by asking some open-ended questions, the facilitator can find some important details to then ask some curiosity or consequence questions about.

Basic	Confirmation/Curiosity	Open-Ended Prompts
Who	You do x. Is that right?	Tell me more
Where	What if that didn't work?	What else are you worried about at this point?
What	Would you consider doing x?	If you could have any one thing at this point in the incident, what would it be?
When	Is this process written down somewhere?	What happened the last time you dealt with something like this?
Why	If you do x, what else might that effect?	What's the worst thing that could happen at this point for you?
What if?	What would the CEO want you to do?	What does success look like for you the incident the way things stand?
		(after inject) What do you do?
		(after inject) How does that change things for you?

Table 9: STOic TTX Question Cheatsheet

Participant Experience

Learning how to craft a positive and engaging participant experience takes time and practice. It is a skill that even the most experienced facilitators work on every time they facilitate. This section will cover the core skills and methods that can accelerate a facilitator's process to improve.

Start with the End in Mind

A TTX facilitator knows that they did their job very well when the participants leave the exercise feeling:

1. Mentally exhausted
2. A little scared
3. Very hopeful

They are **exhausted** because they have had to think of things they have not needed to think of before and to devise ways to handle a situation for which they have not prepared. This is accomplished through clever uses of injects during the exercise.

They might feel a little **scared** because the situation they are not prepared for is credible, probable, and relevant to them. This is accomplished through understanding what is relevant to the participants.

They feel **hopeful** because the exercise let them navigate a path to be prepared for the situation next time. This is accomplished through pointed but open-ended questions posed to the participants.

The secret to using injects well, understanding the needs of the participants, and knowing what questions to ask is to manage the participants' Flow State.

The Flow State

There is an entire field of study around Flow and its nuances, but for our purposes, managing the Flow State is defined as:

Increasing the challenges to meet the capacity of the participants.

Why is a Flow State important?

Achieving a sense of Flow results in very high satisfaction with the experience and higher levels of engagement of the participants.

Think of the games you have played as a child that now you can win without even thinking about it or the ones that you realise are entirely up to luck and not skill. You probably consider these games boring. Then think of games you played where the rules were so confusing that you had no idea how to play, let alone how to win. Or games that required a level of linguistic or mathematic skill that you did not possess. You probably consider those games frustrating and too difficult to play.

Alternatively, the games that provided:

- Clear, achievable goals
- Clear and timely feedback about your choices during the game
- Difficult challenges that you felt like you could meet with a mix of your current abilities and new abilities that you felt that you could develop

Those games are engaging, and the types of games people tend to like to play. A TTX can benefit from the same structures. Since STOic TTX allows the facilitator the flexibility to adjust the scenario according to the actions taken by the participants, STOic is structured to encourage Flow.

In a cybersecurity exercise, the **goal** is obvious; to contain and recover from the scenario's incident. There will be a natural desire of the participants to accomplish this goal. The desire might even be so strong that they try to reach that goal as quickly as possible without considering the impacts, alternatives, and parallel issues, but if that happens, it is the facilitator's job to use good use of questions to break the participants' out of their patterns.

When everyone feels like their contributions are valued, participants will often provide **feedback** to each other. But the facilitator should provide timely feedback about participant's choices if the participants do not do it. A facilitator's feedback should not be to evaluate the responses but to engage with the responses by validating a response as a valid open question or action item, asking questions to dig into responses, and, possibly, to provide injects based on those responses.

Providing **challenges** that adjust to every different participant group requires a little skill and practice. Dynamically adjusting challenges to the participants is the focus of the next section.

Dynamically Adjusting Challenges

If the goal of providing dynamic challenges to a participant group is to provide scenarios that are not too easy and not too difficult, then the facilitator needs to focus on injects and to have a wide range of injects to pull from so that every participant group can be properly challenged. The discussion of injects has been covered in an earlier section. Now, the discussion turns to how to apply them in clever ways.

The general strategy is to:

1. provide a simple and generic initial impact from the scenario
2. gauge the participants' ability level based on how they respond
3. provide the next inject that is closer to the participant group's ability level
4. adjust the injects and details to properly challenge the participants

In other words, the key to a successful exercise is not the first thing the facilitator says about the scenario; the key to success is the next thing the facilitator says. The subsequent injects or details are usually small adjustments up or down in challenge level towards where the participant group's ability level really is.

Roleplaying Game Analogy

Consider the initial impact of the scenario like a tutorial level or a "kill 5 rats" beginner quest. The facilitator gets to see how the participants respond and provides the next "quest" at a level that will be most interesting and challenging to the participants.

For experienced and expert participant groups, the first inject might end up being the most advanced inject that the facilitator prepared, or the group's ability level is beyond the challenge that the facilitator prepared.

For unprepared participant groups, the initial impact details might be more than challenging enough and the facilitator might not need to add injects or provide additional details.

In either case, the facilitator should choose the next injects based on the participants. The facilitator should not run through the injects just because they were prepared for the exercise.

How do you know where the group's ability level is?

The biggest clue the facilitator has is the easy confidence of the responses. If the participants sound like they are reciting a well-worn process, then the participants are beyond that level of ability. However, if the participants are over-confident, then that can be a sign that the skills are new, or the responses are being invented on the spot and require some probing.

One of the things the facilitator can keep in mind are the four stages of skill acquisition:

1. unconscious incompetence (failing and you do not know why)
2. conscious incompetence (failing and you know why)
3. conscious competence (succeeding and you know why)
4. unconscious competence (succeeding and you do not know why)

A facilitator can gauge responses against this model. The further along the skill acquisition process a group is, the greater the challenge the TTX scenario needs to be. The different clues to look for:

- explaining the steps of a process quickly, seemingly without thinking about them
- assuming that the facilitator knows something that was not mentioned before
- confidently and deliberately explaining a response
- reaching to recall facts, processes, or resources, but succeeding
- reaching to recall facts, processes, or resources, but failing to recall them all
- lots of hesitation, "deer in headlights" look, telling a joke to fill time before responding

However, a facilitator might be able to simply "tell" whether the participant knows what they are talking about without needing the model above. As a facilitator gains even a little experience, gauging a group's skill level will be very easy.

Nonetheless, keeping this model in mind can be helpful for a facilitator to remember to challenge the "unconsciously competent" to ensure that they have not started to take things for granted or started to make inappropriate assumptions about their skills.

How to challenge experts

STOic TTX facilitators are not required to be cybersecurity experts. Having expertise in attacks and incident response can be a valuable asset, but the way STOic TTX is designed, expertise is not always required.

How, then, can a facilitator properly challenge expert participant groups when the facilitator is not as expert as the participants?

There are two approaches the facilitator could take:

1. Get them to challenge themselves
2. Use historical attacks

Getting them to challenge themselves means that you directly ask them to propose a course of action or an inject that makes sense to them. Give them the control over the scenario a little bit to find the right level for them. You can prompt them with questions like,

"What would be something you could not handle?"

"What would have to have happened for something that you say cannot happen to happen?"

"If you were going to attack or doing something malicious here, what would you do?"

An alternative is to know what historical attacks are applicable to your scenario. Historical attacks can be very useful in providing details to a scenario that are realistic. There are sources of historical attacks in Table 6.

Either of these approaches can help a non-expert facilitator challenge expert participants and ensure that the discussions are fruitful and a Flow State is maintained no matter who the participants are.

Summary

Being a TTX facilitator can be a lot of fun and very rewarding. There is no other role in cybersecurity that can accomplish what a TTX facilitator can accomplish and the importance of an organisation exercising regularly cannot be understated.

While many people do not become facilitators, the hope of the STOic TTX development team is that this training has inspired you and equipped you to become a facilitator and to develop your skills.

All that's left to ask is: "So? How do you want to do this?"

Appendix A: Additional Resources

Core Scenario Level Examples

To help facilitators construct meaningful exercises at different levels from the core scenarios, the following table can be used as a guide. Some scenarios naturally lend themselves to more complex exercises than others. This highlights the fact that not all scenarios require a long time to exercise.

Each item in each scenario can be used as separate injects or be used to construct a timeline of the scenario.

In some cases, the Tactical and Strategic items are similar. There may be cases where a core scenario does not make sense to exercise at the Strategic level since senior management would have no involvement, but that will be something for the organisation to decide and should be discussed in the planning phase. It is also a good idea to check with the lead contact to get a sense for which injects would make sense for the participants.

Scenario	Operational	Tactical	Strategic
Virus	- Small to large outbreak - Various critical devices affected - Virus allowed remote access/data exfiltration - Undetectable virus - Part of a larger multi-staged attack	- Outbreak evolves quickly requiring close management of resources and people's time - Undetectable virus	- Complex, widespread outbreak that interrupts services for a long period - Participants' devices infected
Distributed Denial of Service (DDoS)	- Individual server/services affected - Time of day/year complications - Network-wide outage	- Major outage requiring 3rd party coordination - Failover to alternate resources - ISP coordination	- Major outage requiring external stakeholder coordination - Extortion: the org is contacted and threated with DDoS if payment is not made
Unauthorized computer on network	- Difficult to detect and locate - Device has been in place for a long time - Device allows remote access - Device intercepts network communication - Device scans and maps network resources	- Several devices found and used for legitimate purposes (a.k.a. "shadow IT") - "Shadow IT" devices used for critical business purposes - "Shadow IT" devices compromised for malicious purposes	- Several devices found and used for legitimate purposes (a.k.a. "shadow IT") - "Shadow IT" devices used for critical business purposes

Malicious external scanning	- Targeted scans - Broad, potentially disruptive scans - Scans from a botnet (thousands of sources) - Slow, long-term scans that are difficult to detect - Brute force login attempts along with all of the above	- Scans from trusted partners - Targeted scans from multiple sources on uniquely critical services that pose a unique risk	- Scans from trusted partners - Targeted scans from multiple sources on uniquely critical services that pose a unique risk
Malicious internal scanning	- From end user device - From server/container - From unknown device - From admin's device - From network device (firewall, switch, etc.) - From multiple devices	- Slow, long-term scans that are difficult to detect indicating long-term compromise and malicious control of the network - Targeted scans on critical servers (backup servers, virtual infrastructure, etc.) - Scans from critical servers that cannot be disrupted for investigation	- Slow, long-term scans that are difficult to detect indicating long-term compromise and malicious control of the network - Scans from critical servers that cannot be disrupted for investigation
Computer compromise	- Local user found files altered - New files found with network and credential information - Mouse moving by itself (Remote Access Trojan, TeamViewer, etc.) - Protections disabled (AV, firewall, agents, etc.) - New users with admin rights created - Computer is end-user device - Computer is a server - Multiple computers/servers compromised	- New users with admin rights created requiring a full investigation of the impact those new user accounts had - Computer is a server - Computer is a server that cannot be disrupted for investigation - Multiple computers/servers compromised requiring careful management of resources	- Computer is a server that cannot be disrupted for investigation - Multiple computers/servers compromised requiring careful management of resources

Phishing via email	- Single user, multiple users, all users - Phishing with attachment or link or "button" - Phish leads people to fake 3rd party website - Phish leads people to fake version of the organisation's website - Users engage with the email (click, open, etc.) - Users do not engage with the email, but account gets compromised anyway	- Widespread phishing resulting in multiple accounts compromised - Compromised accounts sending phishing internally - Compromised accounts sending phishing to partners - Admins and management locked out of accounts	- Widespread phishing resulting in multiple accounts compromised - Compromised accounts sending phishing internally - Compromised accounts sending phishing to partners - Admins and management locked out of accounts
Ransomware	- Small to large outbreak - Various critical devices affected - Part of a larger multi-staged attack	- Servers and services disrupted requiring multi-team coordination	- Complex, widespread outbreak that interrupts services for a long period - Participants' devices infected - An interruption so disruptive that the organisation might consider paying the ransom - Information held for ransom that is so sensitive that the organisation might consider paying the ransom

Complex Attack Timeline Example

The facilitator training mentions gathering stories and timelines of real attacks to use to guide the use of injects. These real examples are also useful to dynamically adjust the difficulty level of the scenario as needed. As a facilitator, these narratives are very useful because you can progress the attack narrative as far as you need to, stopping at any point, and you can challenge expert participants with realistic attack simulations.

Below is a useful, and real, timeline that can be used for ransomware scenarios and includes several other issues that could be tackled in separate scenarios (phishing, internal scanning, etc.):

1. initial infection of user PC (often via phishing or weak passwords)
2. gain access to other computers/servers directly from the infected PC
3. send internal phishing emails to other staff members
4. gather credentials from other users
5. find admin credentials
6. gain access to all computers/servers/network devices using admin credentials
7. quietly turn off security protection (AV, firewalls, logging, etc.)
8. add new admin users
9. quietly infect all devices
10. inventory critical data, the network, and critical IT processes (like backups and the virtual environment)
11. corrupt (over time), infect and/or encrypt backups
    a. or exfiltrate org data to a public server
12. trigger all infected computers/servers to start encrypting themselves
13. show ransom on the user machines

The facilitator can present the initial impact at any point in this timeline. Either at the end, and have the participants discover the events that happened before, or at the start and have the timeline unfold as part of the scenario.

Notetaking Form Example

Date	18/03/21	Organisation	AnOrganisation		
Scope	Operational				
Scenario	Ransomware			Level	Bronze
Who's Attending					

First Name	Role
Jack Burrow	Head of IT
Janice Sprat	IT Manager
Mina Ahluwalia	Senior ICT Systems Specialist
Jackie Brown	ICT Systems Specialist
Michael Innes	Helpdesk Operator

Objectives of the Exercise – taken from the Form – A few questions about your organisation.
1. Enhance cyber awareness readiness and coordination 2. Test the ability to detect and properly respond to hostile activity 3. Test the effectiveness of communications process during an attack 4. Test the organisations capability to determine operational impacts of cyber attacks and implement proper recovery procedures 5. Expose and correct weaknesses in cyber security systems policies and procedures

Hints and Tips during the TTX.
Preparation: Fill out the information above prior to the start of the TTX. Keep the sheet visible so you can see names and roles. This will help you pose questions to staff who have areas of responsibility to prompt discussion. **Keeping the flow:** Questions to prompt discussion: "What do you do?" "Are you sure? – how do you know that you are sure?" "So [person] are you comfortable with this? Is there anything making you feel uncomfortable at the moment?" Watch for "Big Eyes" indicating disagreement or concern and also quiet participants. Give them opportunities to express any concerns. **Note taking:** Use the blank spaces on following pages to take notes during the TTX. Numbering your pages will help you to keep track if you are completing these manually. You do not need to record who said what – only note relevant information if you're not sure if it is relevant make a note of it and you can decide later once the TTX has played out. Ideally you will have Actions & Open Questions/ Concerns from each inject it is good practice if these are blank to confirm there are no actions or concerns for the inject before moving to the next inject.

Inject Description:	On a drizzly Friday afternoon the Head of Finance calls up to say he has a red box on his screen with something about encryption and bitcoin	Inject No:	1

Instruct the user to disconnect the device from wifi Ask what files, websites were recently accessed Take a screenshot with mobile phone

Open Questions/Concerns How do you disconnect the device ?

Actions Develop initial response process with checklists for helpdesk staff – process on how to isolate the device and its associated accounts & communicate it.

Inject Description:	This is an advanced form of ransomware	Inject No:	2

Check what access infected users have to other systems/ servers Check servers for malicious activity

Open Questions/Concerns Is all access to other systems controlled through security groups? What do you not know about? How do you see server activity, can you detect malicious events ?

Actions Create reports/dashboards for I/O metrics Identify Third party systems which could be compromised and record contact information in the IR plan

Inject Description:	At 4:45 pm 4 more members of C-Suite call in with a red box notification.	Inject No:	3

Look to disable all C-Suite accounts
Shut everything down
Issue communications
Plan the restore

Open Questions/Concerns
How do you make the decision to shut everything down – who approves this?
What and how do you communicate?
Could backups become infected?

Actions
Create one page process with checklists to increase the speed of decision making
Create procedure with criteria for full network shutdown and have it approved by the CEO.
Engage with comms dept to create communications templates for use during an incident and have these pre approved.
Review backup process to ensure they cannot be infected easily or overwritten in a short time frame by infected data.

Tip: Reprint this page a few times so you have spares on hand during the TTX if you are taking notes manually

STOic TTX Recommendations Report Example

Ransomware			
Date	18/03/21	Organisation	AnOrganisation
Location	Remote	Lead Contact	Jack Burrow
Attendees	Jack Burrow, Janice Sprat, Mina Ahluwalia, Jackie Brown, Michael Innes, Jordan Schroeder, Norice Bain		

Scenario

On a drizzly Friday afternoon the Head of Finance calls up to say he has a red box on his screen with something about encryption and bitcoin

Inject	The amount of computers infected are disrupting your organisations ability to perform day to day tasks.
Inject	Webserver has ransomware

Key Controls

List of controls used - what they were used for and how the scenario relied on the control.

Control Used	Used to\Relied on in the scenario for
Configuration Manager	Remote administration of endpoints

Key Findings

List of concerns expressed, identified weakness and gaps in Skills, Knowledge, Tools or Processes (S/K/T/P)

(CID – Concern ID)

Cid	Concern	Gap?	S/K/T/P
1.	How do you disconnect the device ?	G	SKP
2.	Is all access to other systems controlled through security groups? What do you not know about?	G	SKP
3.	How do you monitor server activity, can you detect malicious events ?	G	KT
4.	How do you make the decision to shut everything down – who approves this?	G	P
5.	What and how do you communicate?	G	KP
6.	Could backups become infected?	G	K

Action Items

List of agreed actions from concerns expressed in key findings to address gaps in Skills, Knowledge, Tools or Processes (S/K/T/P)
(AID – Action ID)

Aid	Cid	Action	Gap in S/K/T/P
1.	1	Develop initial response process with checklists for helpdesk staff – process on how to isolate the device and its associated accounts.	KP
2.	1	Communicate & test the response process to all helpdesk staff	SP
3.	2	Identify Third party systems which could be compromised and record contact information in the IR plan	K
4.	2	Check security groups and all system access methods.	
5.	3	Create reports/dashboards for I/O metrics	ST
6.	4	Create one page process with checklists to increase the speed of decision making during an incident	P
7.	4	Create procedure with criteria for full network shutdown and have it approved by the CEO.	P
8.	5	Engage with comms dept to create communications templates for use during an incident and have these pre approved.	STP
9.	6	Review backup process to ensure they cannot be infected easily or overwritten in a short time frame by infected data.	TKP

Proposed Future Scenarios (gathered from the exercise)	
Proposed Scenarios	Exercise at tactical level – invite comms department.

Date of next TTX	
Date (mm/yy)	

Action Items to have resources and dates assigned by lead contact for the organisation.

These actions detailed should be progressed before the date of next STOic - TTX exercise. Updates on actions are essential to drive the scenario for the next STOic TTX. Updates should be sent to the facilitator at least 2 weeks before the next planned STOic TTX

Aid	Cid	Action • Update	Gap in (S/K/T/P)	Assigned to	By (MM/YY)
		Example action listed • Update from organisation			
1.					
2.					
3.					