Common Tabletop Exercise Failures

Michael Murray
Robert Lelewski
Over 15 years of experience in cyber security.

Focused on delivering proactive incident response services that prepare our clients to act when an incident strikes by ensuring that they have defined, implemented, and exercised the necessary plans and processes, and by augmenting client incident management capabilities during an incident response event.

Previously Technical Manager for the CSIRT Operations Team at the CERT Coordination Center, Carnegie Mellon University.

Provided on-site support to U.S. national-level cyber centers to include US-CERT, the Department of Defense Cyber Crime Center (DC3), and Joint Task Force Global Network Operations (JTF-GNO).

About

Passion for Security

Coordinated collaboration amongst global network of CSIRTs with National Responsibility.

Served on the Forum of Incident Response and Security Teams (FIRST) Board of Directors.

North America FIRST membership committee representative.

Has played a number of roles, starting as junior analyst triaging tickets and answering the CERT/CC hotline.

“Team sport” focus – community, collaboration, information sharing.

Previous Focus Areas

Public / Private sector information sharing

International cooperation, National-level CSIRT capability development

Analysis infrastructure development and deployment

Operational process and tooling improvements
About

• 15+ years in Information Security in a variety of client facing and management roles.
• Developed several incident response practices from the ground up.
• Expert witness testimony in state and federal courts on computer forensic issues.
• International consulting experience, enabling a wide view of unique cultural and legal issues.
• In-depth experience in applying the Incident Response Lifecycle to preparing for incidents via the development and review of incident response plans, facilitation of tabletop exercises, and the facilitation of lessons learned events.

Previous Focus Areas

• Managed a flyaway incident response team, participating in high-profile breaches around the world.
• Primary investigator for the Colorado Public Defenders specializing in computer crimes and electronic evidence.
• Adjunct professor teaching courses on network security, computer forensics, and other topics.

Passion for Security

• Possesses several security-related certifications including: SANS GCIH, CIPM, CISA, CISM, CRISC, CISSP-ISSMP, EnCE, CCE, CASP.
• MBA – University of Northern Iowa, MS – University of Denver, BS – Syracuse University.
• Speaker for major industry events including the IBM Security Summit in Mexico City, ISACA’s CSX in Ghana, FIRST Annual Conference in Edinburgh.
• Regular featured contributor to ISACA’s The Nexus journal on cyber security and risk management topics.
• Presented to boards and leadership circles on cybersecurity risks and the changing threat landscape.
Background

Proactive IR consulting:
What we do,
why we do this,
why we care...

Why tabletops?

Where do they go wrong?

https://www.zapiro.com/110120mg
We strive to prepare our clients to act when an incident strikes by ensuring that they have defined, implemented, and exercised the necessary plans and processes to respond to such events, and by supplementing their incident management capability during an incident response activity.
Why Tabletops?

- Whether a plan and program is old or new, there is a need to regularly review and validate.
- Looking for unknown unknowns.
- Increasingly, clients/customers, insurers, and regulators requesting or requiring evidence of preparedness, or weighing repercussions on proof thereof.
- Building cross-organizational relationships and raising awareness / gaining support.
- Low-impact / high-ROI
Where Exercises Go Wrong

If you fail to plan, you are planning to fail...

If you don’t capture and action items to improve upon, you are limiting the benefit...

Planning

Execution

Follow-through

Level of Effort

80%

20%
Let’s get into some specifics...
Failure 1: The Need to Find the “Right” Answer
Take Off Those Blinders!

The value of a tabletop is not getting to a final answer. It is:

• getting everyone in the same room,
• discussing individual interests,
• taking time to explore unforeseen issues, and
• fostering communication paths.

When your sight is set on the “right” answer, you may lose the real value to be gained from a tabletop.
Failure 2: Not Performing Cross-Functional Tabletops

It’s not a party unless somebody invites Legal.

Typically the most valuable tabletop exercise.

Do prior-relationships exist between cross-functional roles?

Resistance to performing cross-functional tabletops.

Each function should be defined within the incident response plan.

Cross-functional tabletops ≠ technical scenarios.
Failure 2: Not Performing Cross-Functional Tabletops

It’s not a party unless somebody invites Legal.
Failure 3: Not Defining Tabletop Goals

What are you *really* trying to accomplish?

Tabletops may experience diminished value due to a lack of defined goals.

Before getting started, consider what are your goals for the tabletop?

Based on your goals, what is the most appropriate style of tabletop?
Failure 3: Not Defining Tabletop Goals
What are you really trying to accomplish?

Common Goals:
• Increase plan familiarity
• Determine the impact of incident response on a new process
• Regulatory compliance
• Highlight a known deficiency

• Test process against a new threat or involving a new stakeholder
• Rekindle / forge communication paths
• “Stress test”
Failure 4: Not Capturing and Addressing Deficiencies

We’re done. Off to the pub, right?

Capture feedback early – “hot wash” at the end to gather comments, solicit feedback via questionnaires, and provide your own assessment while it’s fresh in everyone’s mind. Remember – people get very busy again upon return to $DAY_JOB.

Reconvene the participants to discuss areas for improvement, assign, and track actions.
Failure 4: Not Capturing and Addressing Deficiencies

We’re done. Off to the pub, right?

Create a report that clearly identifies:

• What was observed
• Potential impact of the observation
• Recommended actions
• Assignee(s) to take action
• Priority / Due Dates
• Follow up on actions, host working sessions to discuss progress

Set check points to track progress.
Re-exercise those areas.
Failure 5: Not Pushing Boundaries
Stop me if you’ve been in this exercise before...

Exercises are a means to expand the scope of your people, process, and technology assets.

For technologists, the prospect of a several hour long meeting may not be all that exciting, so it is important to drive interest in exercises by making them more interesting.
Failure 5: Not Pushing Boundaries
Stop me if you’ve been in this exercise before...

Easy to make it exciting...
• Take the “table” out of tabletop
• Valid domain account logging into many systems in a few seconds
• Introduce a non-trusted device
• Disable $SECURITY_COTROL on a box
• Simulate data exfiltration
• Call someone and report a “found device”
• Leverage Red Teamers
• Exercise known deficiencies to raise awareness and seek support

Utilize disposable infrastructure
• Easier than ever to spin up and tear down infrastructure for exercises, education, etc.

Engage external entities
• Providers (more to come on this one)
• Partners
• Clients / stakeholders
Failure 6: Always Building and Facilitating Internally
Plug for the consultants in the room!

Internally facilitated tabletops are perfectly acceptable but should periodically be combined with leveraging external facilitators.
Failure 6: Always Building and Facilitating Internally
Plug for the consultants in the room!

An external facilitator:
• Brings a wider perspective.
• Provides independent reporting to management.
• May help discover unknown points of failure.
• Is less likely to “sugarcoat” observations.
• Allows the usual event planners to participate.
Failure 7: Not Testing Vendors
Vendors always adhere to their SLAs. Always.

• Vendors are increasingly used to fulfill a variety of roles.
• Security compromises involving vendors are well known.
• Must be integrated into your incident response process.
• Starts with the SLAs.
Failure 7: Not Testing Vendors
Vendors always adhere to their SLAs. Always.

Simple Vendor Exercise:
Pick a non-critical system operated by a vendor. Contact the vendor and state that, due to a security concern, the following data sets are requested:
• OS Event Logs
• RAM
• Disk Image
Failure 8: Lack of Senior Leadership Participation
When the highest ranking person in the room is the intern, something went wrong.

Sometimes you need their help...

• People
• Process
• Technology

You need their perspective on what matters and why to inform how and where you focus your efforts.
Failure 8: Lack of Senior Leadership Participation

When the highest ranking person in the room is the intern, something went wrong.

Also an opportunity to showcase your team’s capabilities...

Make sure that there is an appreciation for where you become reliant on other parts of the organization.

You are going to be “invited” to the board meeting one of these days.
Key Takeaways

When Planning A Tabletop...

1. **Consider who needs to be involved and how you will involve them.** (hint: it’s not just technologists)

2. **Invest in exercising & push your team.** Make it an open and honest dialogue and discuss a realistic and concerning threat to the constituency.

3. **Have some fun doing it.** People are engaged when the subject matter is pertinent and challenging.
Thank you! Questions?

Michael Murray
MMurray@secureworks.com

Robert Lelewski
RLelewski@secureworks.com

The Need to Find the ‘Right’ Answer
Not Performing Cross-Functional Tabletops
Not Defining Tabletop Goals
Not Capturing and Addressing Deficiencies
Not Pushing Boundaries
Always Building and Facilitating Internally
Not Testing Vendors
Lack of Senior Leadership Participation