How To Tabletop Like A Boss

Overview

Tabletop exercises can be pretty dry, but we can make them a lot more fun if we sprinkle in some board game elements!

This framework is designed to help build engaging interactive Tabletop exercises. The goal is to make things a bit unpredictable to reduce the number of surprises we encounter for the first time during an actual emergency, provide a way to find improvements. You're also not forbidden from having fun.

Process

1) The first thing we need is a Gamemaster. This is the person who constructs the narrative and helps facilitate the event. (warning, this may be you!)
2) Next, determine the scope of your exercise. Is your whole company impacted, or just a specific app/team/group/vendor, etc.
3) Identify potential stakeholders that should be a part of the exercise. This could be developers, account managers, DBA's, operations, infrastructure, management, whomever might need to be part of an actual response.
4) Next, build out your list of variables (below), then use a die to select a value from each section Google has a free die interface online here
5) Once all variables are rolled, use them to construct an incident narrative. Sometimes variables don't work well together, so you can either re-roll the odd variable, or substitute in a value that makes more sense.
6) Once your narrative is complete, the Gamemaster will present each element of the story to the group and use the responses to each part of the narrative to roll a result.
7) Results are the result of a roll of the die and can be improved by the answering team if they have documentation (+5) or have performed training (+2) on the topic. Any value over 10 points succeeds, which allows the Gamemaster to move onto the next element of the story. A roll below 10 means the response failed, and the answering party will have to come up with an alternative decision, and roll again.

Variables

Build a list of potential problems using the following structure:

- **Origin** - who initially found the problem? (i.e. Headlines, Pen Tester, Feds)
- **Discovery** - how was it found? (i.e. Monitoring, Alert, Social Media)
- **Issue** - what is the nature of the problem? (i.e. Bruteforce, DDoS, Data Loss)
- **Vector** - how did the problem start? (i.e. Vendor Failure, Phishing, Insider Attack)
- **Twists** - unexpected wrinkles in the narrative (i.e. Media coverage, Legal action, Regulatory)
- **Component** - what technology is impacted (i.e. Front end, API, Database)
- Day & Time* - optional
- Project/Client* - optional

See the appendix for a more complete list of variables, adjust to make it work for your environment!

Outcomes

Overall, when I'm running these events, I'm mostly looking to see if people know when and how to escalate to other groups. If all the right people get together but still can't figure it out, then that's probably a finding all by itself ☺
Keep track of rolls and results so we can note improvements and make a plan to address them.

Measure progress by ensuring you work through the 5 steps of an incident response:

1. Identify – still trying to figure out what it is
2. Contain – now we know and need to stop it
3. Eradicate – take steps to prevent future recurrences
4. Recover – ensure all services are restored fully
5. Review – look over what happened to look for improvements

When complete, document any discovered gaps and ensure they are actioned upon

Appendix A

Use a large list of variables to keep things fresh. Get rid of any that aren't needed, add ones that are relevant to your situation.

ORIGIN	Client, Project Team, IT member, headlines, feds, corporate, 3rd party, anonymous report
DISCOVERY	logs, monitoring, unusual behavior report, security tools, email/ransom, social media, mainstream media
ISSUE	Denial of Service, Data exfiltration, Overexposure, Access failure, Service unavailable, Defacement, Account compromise
VECTOR	Phishing, 3rd/4th party failure, Insider attack, Unauthorized device, Unpatched software, overexposed data, Logical access failure, Physical access failure, Malware, Zero-day vuln, Bruteforce attack, Fraudulent access, DDoS, Ransomware, Datadump/Pastebin leak, Undocumented changes, Malicious code, Natural Disaster
TWIST	Press involvement, Legal involvement, Regulatory violation, Nation/State involvement, Political involvement, Federal involvement, After hours, Unsubstantiated Threats, System Tampering, Planned Testing, SME OOO, Unrelated incident occurs, Backups corrupt
COMPONENT	Front end, application, API, data center, cloud provider, database, network, source code

Appendix B

Narrative Worksheet

Date:	
Scope:	
Stakeholders (name/team)	
VARIABLES	