Lessons Learned from Objective and Subjective Data

Table of Contents

Objective and Subjective Data ................................................................. 2
Objective and Subjective Data ................................................................. 3
Objective Data ....................................................................................... 4
Subjective Data ..................................................................................... 7
Notices ................................................................................................. 9
Okay. So when you talk about lessons learned and how to approach things, there’s something we’re calling objective and subjective data.
**Objective and Subjective Data**

Objective data are facts related to an incident.

Subjective data are based on perception, assumption, and feelings.

---

**007 Right. Objective, subjective.**

We’re calling objective data facts and/or maybe statistics related to an incident. And subjective data are based on perception, assumptions and feelings. Kind of a way to gauge things. Some things are just straight up, right, how many hosts were compromised, that sort of thing. And then subjectively you might have a scale of some sort to deal with.
Objective Data

Metrics on the incident response and forensic processes provide valuable insight.

Capability and performance

• What was the total cost of the incident response?
• How many hours were worked on each process?
• What was the timeline of the incident response, forensic analysis?

Incident Data

• How many systems were affected?
• What indicators were identified or missed?
• What could have prevented the incident?

**008 Right. Objective data. We’re talking metrics on the incident response. Forensics processes. And a lot of this can help you improve capability and performance. What was the total cost of the incident response? This is where that well organized documentation will come into play at the end of it. You don’t want to get to the end of it and you’re trying to figure out how much cost in man hours, how much new equipment had to be purchased and you’re running around trying to find maybe receipts or something like that. You don’t want that to happen at the end of this. So organization at the beginning will help you and
maintaining that organization throughout is key.

How many hours were worked on each process? What was the timeline of the incident response and forensic analysis? That's relatively simple. Should be, you know, the start date and stop time.

So for incident data, how many systems were affected? What indicators were identified or missed? Right. You want to talk about your misses as much as you want to talk about your successes on this. That's what's going to get you better. You learn more from your mistakes, as many of you may have heard. So this is a great time to point them out. Like I say, it's a non-attribution environment. You're not trying to get people in trouble or saying, "So-and-so from so-and-so's team didn't do this right. They missed it. It's their fault." It's not that. Why is it that that group or that team or that person, did they miss it because of the process or the procedure or the checklist didn't ask him or her to do so? Or if they did, is it a training issue? They just skipped around the checklist and they weren't very thorough? So this is where you want to identify that.

And then what could have been prevented--I'm sorry--what could have prevented the incident? Sometimes you want to look at it from that. We talked about that attack chain, right? You start out with your numeration and you do
your exploitation. And there's phases within that attack chain and part of the defense side of things is you want to try to break that attack chain if at all possible. If you can prevent something from continuing past a certain point in that attack chain, the defense can consider that a success, a win.

So in looking back at the incident, if you can figure out, "Oh, well, if we never did give the insider access to these folders that he or she should never have seen to begin with, they would never have stolen what they stole." That sort of information is key too during your lessons learned. If you can find out where certain parts could've stopped the incident, this is a great time to talk about it and maybe implement remediation.
Subjective Data

Assessing performance subjectively can help identify performance issues or potential efficiency increases.

Team Performance

• Was the team adequately prepared and trained?
• Is the team structure effective?
• Was communication and reporting sufficient for stakeholders?

Incident Response

• Is the IR plan sufficient?
• Are there better/different tools that would increase efficiencies?
• Where could processes/procedures be improved?

**009 So subjective data. Right. Assessing performance objectively can help you identify performance issues or potential efficiency increases that you can get. Although these are "yes/no" type questions. Generally when you're talking about, "Was the team adequately prepared and trained?" you can say, "Yes," and/or "No. However--" and you could talk about how much better they could've been had this been the case. Is the team structure effective? Or maybe a more, a better question, might be, "How effective was the team structure?" And you talk about amongst the team and other people, the relevant
stakeholders, was communication and reporting sufficient for stakeholders? Right. You talk to the stakeholders and you find out. "Hey. We gave you this much stuff. We tried to give you this much lead time on information. Was this enough? Would you appreciate more, or was it more than enough?" And can we chip that down a little bit so we can do other things in the meantime?

During the incident response, right, is the IR plan sufficient? Was things that were missed, is it a gap in your process and your procedures in the IR plan, or was it missed because of a person missing it?

Are there better/different tools that would increase efficiencies? Right. You find out that a tool you’ve been using for quite a while is now semi-obsolete because of the new operating system or our new patch that happens to make your tool ineffective. This is the time to bring that up and talk about that.

Where could processes and procedures be improved? Same thing, right? Part of the IR plan. Part of the digital forensics checklist that you have. This is a great time to bring them out and say, "Yep. This was good. This one worked fine. This one did not." And you start talking about how you can fix them.
Notices

© 2016 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.