




Hacked, or Human Error, (in Fifteen Minutes or Less).

**Jon Allen, Francoise Begin, Shelley Giesbrech and Phillip
Bosco, John Dittmer, Balaji Balakrishnan**

Introduction

-  The SANS Technology Institute has an exercise for the grad students where they work as teams to solve a problem and give an oral and written report
-  Surely you have heard the old IT configuration management joke: What does United Airlines have in common with the New York Stock Exchange and the Wall Street Journal? *They will get back to us on that.*
-  In the course I authored and will be teaching online starting Nov. 3, we talk about the importance of good configuration management.

What did you think when you first heard about the crashes?

- 🌐 It's the Chinese
- 🌐 It's Anonymous
- 🌐 It's ISIS
- 🌐 United, really, again?
- 🌐 My point is really simple, we didn't know what it was. They didn't either. With apologies to the Oracle from the Matrix, "I thought you'd have figured that out by now. "

Can you type when someone is looking over your shoulder?

- 🌐 My fingers turn to putty, and then when I realize they are looking at my terrible typing, it gets worse.
- 🌐 Imagine you are doing incident response or trouble shooting on a global stage?
- 🌐 At some point we have to find root cause.
- 🌐 Have we been hacked, or is our hardware/software design and management simply badly broken?

From the scenario assigned to the students: Senior Engineer Chris replied, "I am not sure anyone knows, and if they do, they aren't talking, at least not yet."

"Hmmm", CIO Karen remarked, "we ought to review our incident response procedures so that when we make the call whether is it malicious or just a mistake, we have a good chance of being right. I think I will put a team together and I will sleep better if I have a first cut tomorrow about this time."

The three glitch scenarios (United Airlines, NYSE, WSJ) should be considered guidance for “use cases” that have a significant impact; i.e., network/router glitch, computer glitch, web site glitch.

For each scenario, create a checklist to help the incident response leader determine if the cause of the glitch is human error or malicious intent. The checklist should be technical in nature and based on a technology that you understand. **Make sure to explain the “why” for each step.** For each check, give examples of what you would expect to find if it was user error or what you would expect to find if it was malicious intent.

CONCLUSION

- 🌐 When you are under fire, it is a lot easier if you have a checklist
- 🌐 The files are posted for your reading enjoyment, they were done in 24 hours, you may want to check them before using
- 🌐 Please either take or send someone to my class
- 🌐 We will open this to questions q@sans.org