CUBICLES
AND
COMPROMISES

BLACK HILLS
Information Security
CELEBRATING 10 YEARS
•2008-2018•

THE RULES

For every action your IR team takes, roll the 20-sided dice.

An 11-20 is successful. 10 or less, it fails.

+5 if your organization has documented procedures for the action.

+2 if your organization has someone trained to do that action.

Randoms will be injected by a pre-designated person. (Examples on the back)

Afterward, address gaps in policies, etc.

RANDOMS

- The attacker posts the incident data on Pastebin.
- Bobby the intern kills the system you are reviewing.
- It was a blackbox pen-test hired by the CEO… You can sleep well.
- Legal takes your only skilled handler into a meeting to explain the incident.
- Lead handler's wife has a baby.
- Someone pulls the memory, while the system is running!!! From the infected system!
- An unrelated DDoS attack breaks out.

BLACK HILLS INFORMATION SECURITY

www.blackhillsinfosec.com

@BHinfoSecurity