Backdoor and Breaches Incident Masters Note

General Questions to Ask

- When does an incident turn into a crisis? What does your company need to do when it does become a crisis?
- When the game is over, ask; Was this a plausible incident? Is each of the 4 attack-chain cards possible within our company? Look for “Maybe” responses; you need to know “yes or no.”
- Can you think of any political, financial, technological, or personnel reasons the procedure would fail at this time?

Isolation & Crisis Management Cards

Isolation Card - Home Brew Rule Option #1

Isolation card. If the roll is successful, it gives the team an extra turn. If not, then no extra turn, and they must figure out what to do next.

This card helps an **Incident Master** ask many questions about policies.

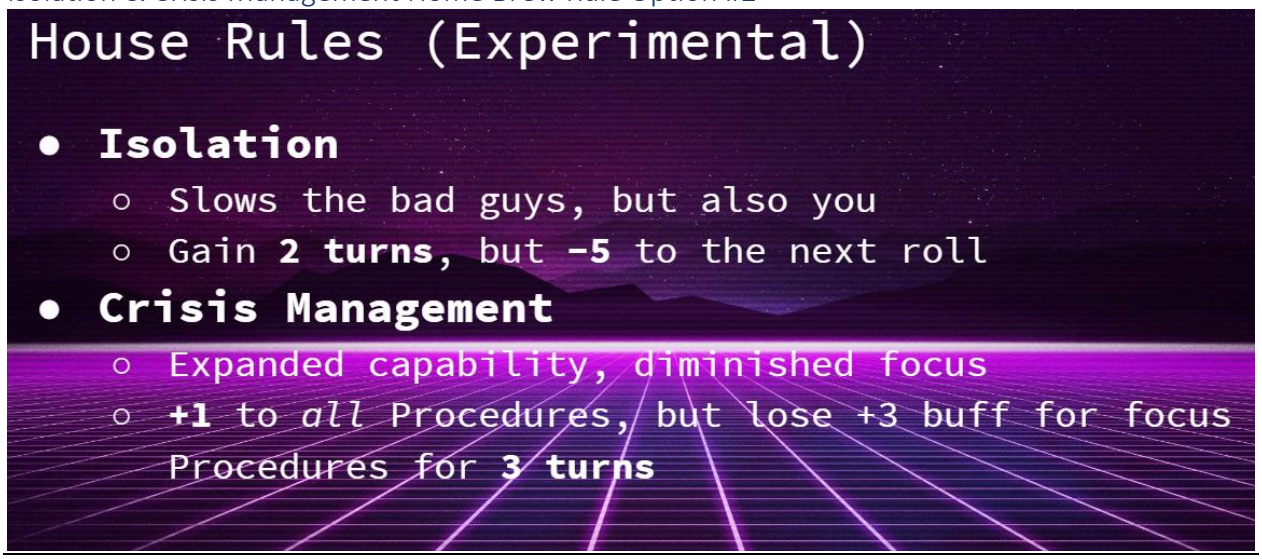
If successful:

1. Who on your team would do the isolation?
2. Who says YES to isolating a system?
3. What type of IR capabilities do you lose if you isolate this system at this time?
4. Who will accept blame if the isolated system causes the business to lose the ability to do business?
5. Is the help desk notified when you isolate a system?

If unsuccessful:

1. Can you give me a reason: this would be unsuccessful at this time due to political, financial, technological, or personnel reasons?

Isolation & Crisis Management Home Brew Rule Option #2



Credit: **Taggart**

Backdoor and Breaches Incident Masters Note

User Awareness Training Detection

The detection method of “User Awareness Training” does not exist but is referenced on cards. Below is a method for Incident Masters to incorporate the “User Awareness Training” detection method.

“”

We didn't create a card for it because it isn't a thing you can "do" to do incident response. BUT... if you did it ahead of time, it might be why your users alert you to issues. ***Essentially, if the team says they want to interview users or talk with people in the department that might know something, then you can reveal the (attack) card to them.*** *Just like on the Insider Threat card, it says, Work with HR, but that isn't a Procedure Card. It would reveal the (attack) card if someone mentions, "**let's talk with HR**."*

”

Call a Consultant Cards Rule

“”

Once you successfully roll the dice for "Call A Consultant," then you can choose the consultant you want to have based on the modifier their card gives you.

If you roll unsuccessfully....all the consultants are "busy" for the next 3 turns, then you can try again.

“”

Unsuccessful Rolls.

As the Incident Master, you need to ask, “*Can you think of any political, financial, technological, or personnel reasons the procedure would fail at this time?*”. There may be nothing wrong with the procedure the team was trying to perform, but due to other factors, it failed.

The goal is to get people thinking about things that could have gone wrong even when they were doing the right thing.

- System Analysis failed this time because your System Log expert was on PTO.
- System Analysis failed this time because logging was disabled on the endpoints you checked.
- System Analysis failed this time because we could not afford more than seven days of logs, and the breach happened eight days ago.

The Roll was successful, but the procedure did not reveal any cards.

If the roll is successful, but no attack-chain cards are revealed, ask the team what new information we can gather. If the team tries a “Server Log Analysis,” but the analysis finds nothing, then maybe the malware is only on the user endpoint.