You Have Had a Data Breach - Now What?

Moderator – Tim Gavin, Klein Hall CPA
Speakers:
Marc Thorson – GMIS Illinois, Village of Schaumburg
Brian Johanpeter – GMIS Illinois, City of Mattoon

FINANCING FOR THE FUTURE

ILLINOIS GFOA 2015 CONFERENCE
SEPTEMBER 13-15 IN SPRINGFIELD

Agenda

- Introduction
- Tabletop Exercise
- Questions

Quotes

"Failing to plan is planning to fail"

– Alan Lakein

Author – "How to Get Control of Your Time and Your Life"

http://www.brainyquote.com/quotes/quotes/a/alanlakein154654.html#QuIMC21GyCFPzgWM.99

Quotes

"Everyone has a plan 'till they get punched in the mouth."

–Mike Tyson

http://www.brainyquote.com/quotes/authors/m/mike_tyson.html#x1ORyvbXEzYzfgSI.99

Definitions

- **Exfiltrate** – This means data has left the private network by means of a malicious act or breach
- **Phishing** – A scam, typically by mass Email to gather information from an unsuspecting victim
- **Spearphishing** – Using Phishing tactics targeting a specific business or industry

Definitions (cont.)

- **IP Address** – Internet Protocol Address, an address given to each device on the network
- **Credentials** – login information such as username and password
- ERP – Enterprise Resource Planning, business management software that collects, stores, and manages business activities

Definitions (cont.)

- MS-ISAC – Multi-State Information Sharing & Analysis Center

  The mission of the MS-ISAC is to improve the overall cyber security posture of state, local, tribal and territorial governments.

Scenario

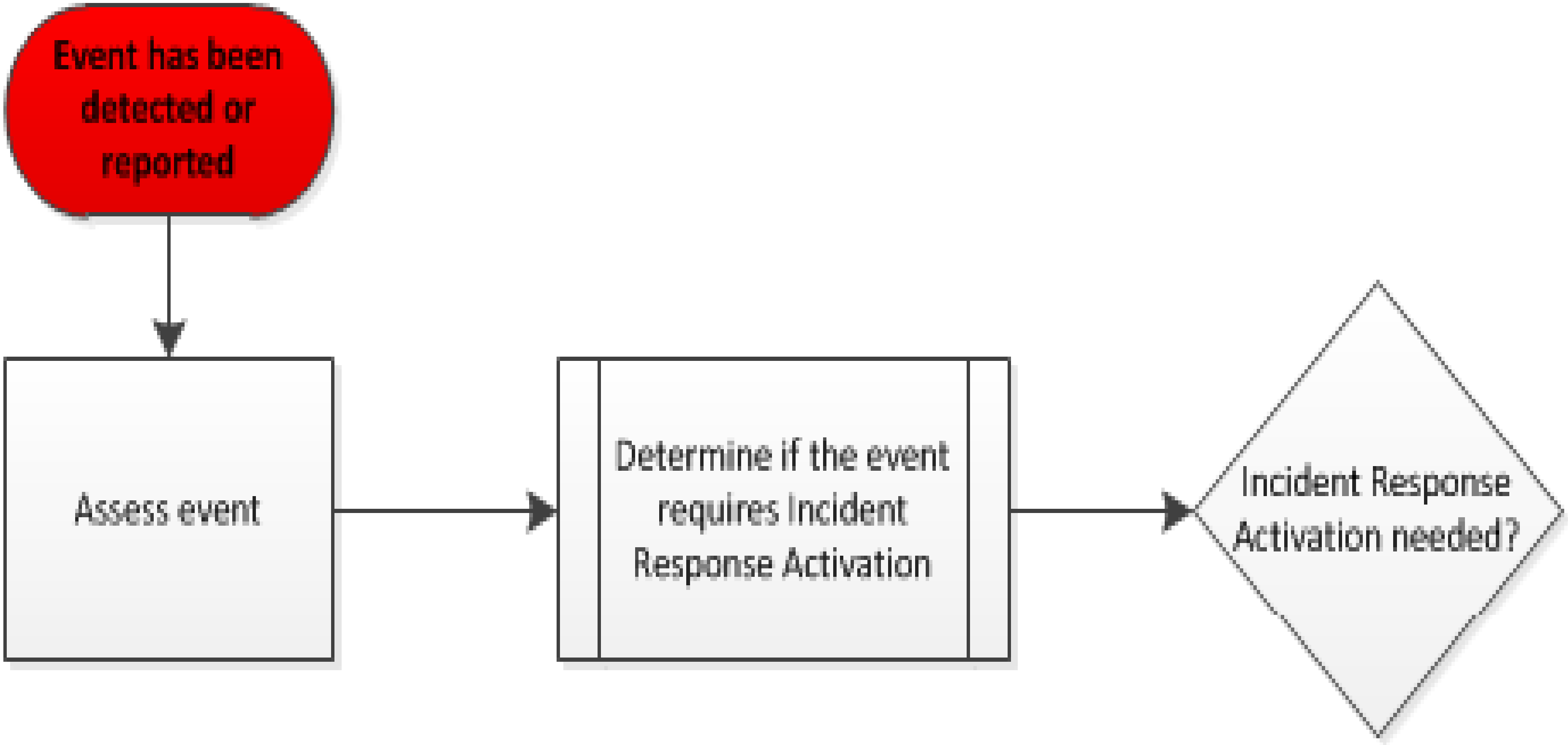
On Friday, September 11, 2015, Hill Valley employees are scheduled to be paid. Check stubs are received by the employees, but later in the morning Jennifer Parker, the payroll specialist, receives a call that an employee has no deposit in his account. Then another call, and another call…

What is going on?

Do we have an incident?

Code	Impact	Description
Vuln 3	1	Intruder must apply substantial effort to compromise asset and exfiltrate sensitive data
Cat 6	4	Intruder is conducting reconnaissance against asset with access to sensitive data
Cat 2	6	Intruder has compromised asset with access to sensitive data but requires privilege escalation
Breach 1	10	Intruder has exfiltrated sensitive data or is suspected of exfiltrating sensitive data based on volume, etc.

Village of Hill Valley
Incident Response Protocol

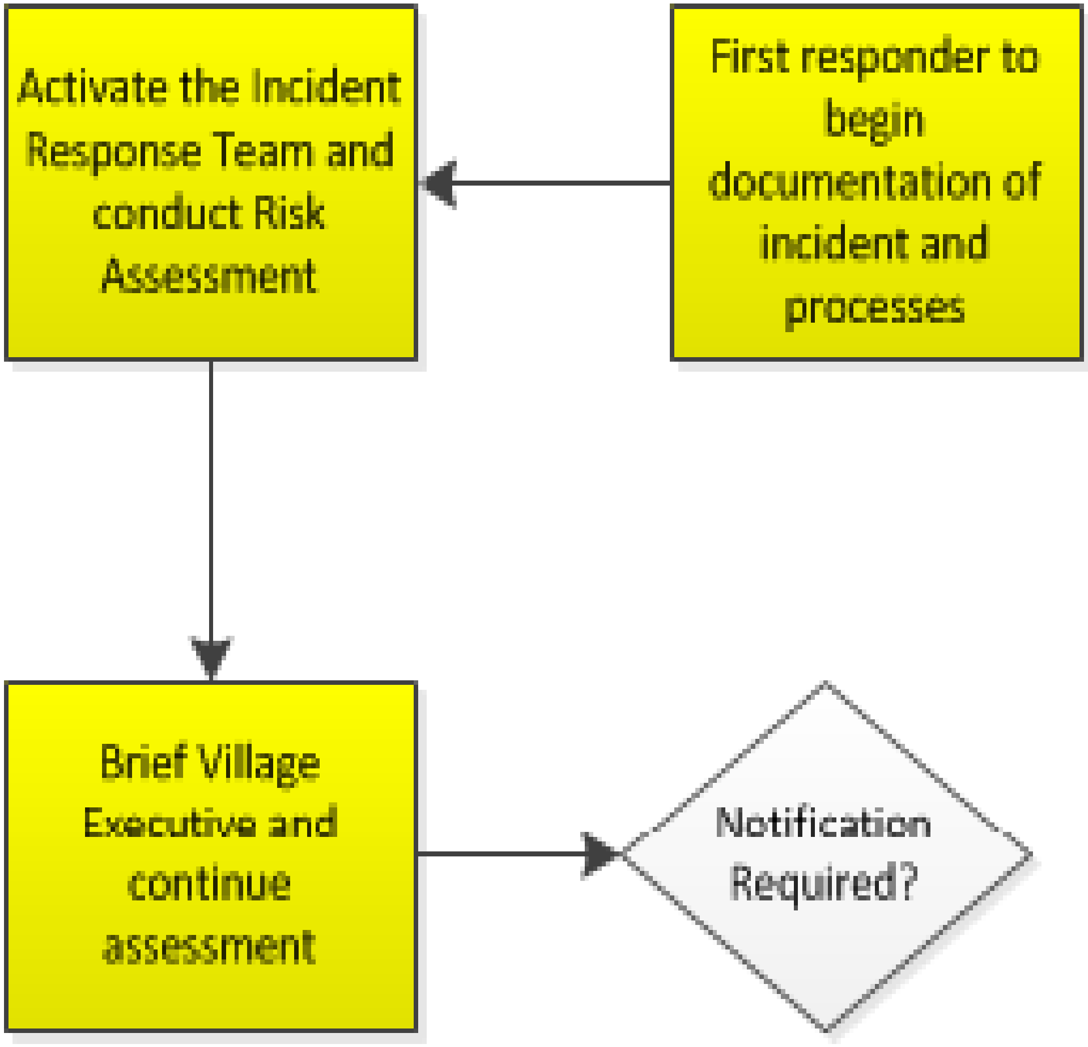


Event has been detected or reported

Assess event

Determine if the event requires Incident Response Activation

Incident Response Activation needed?

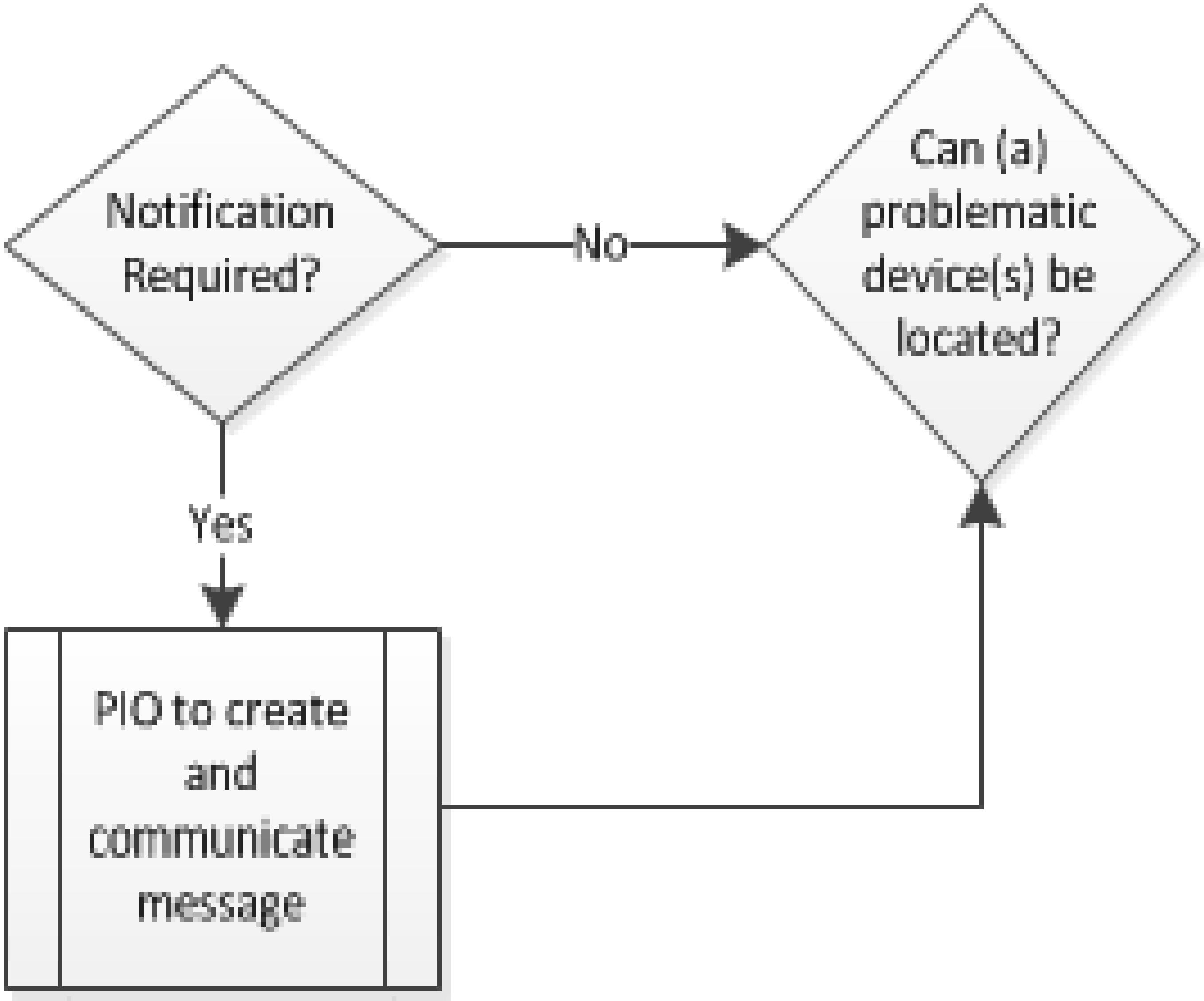


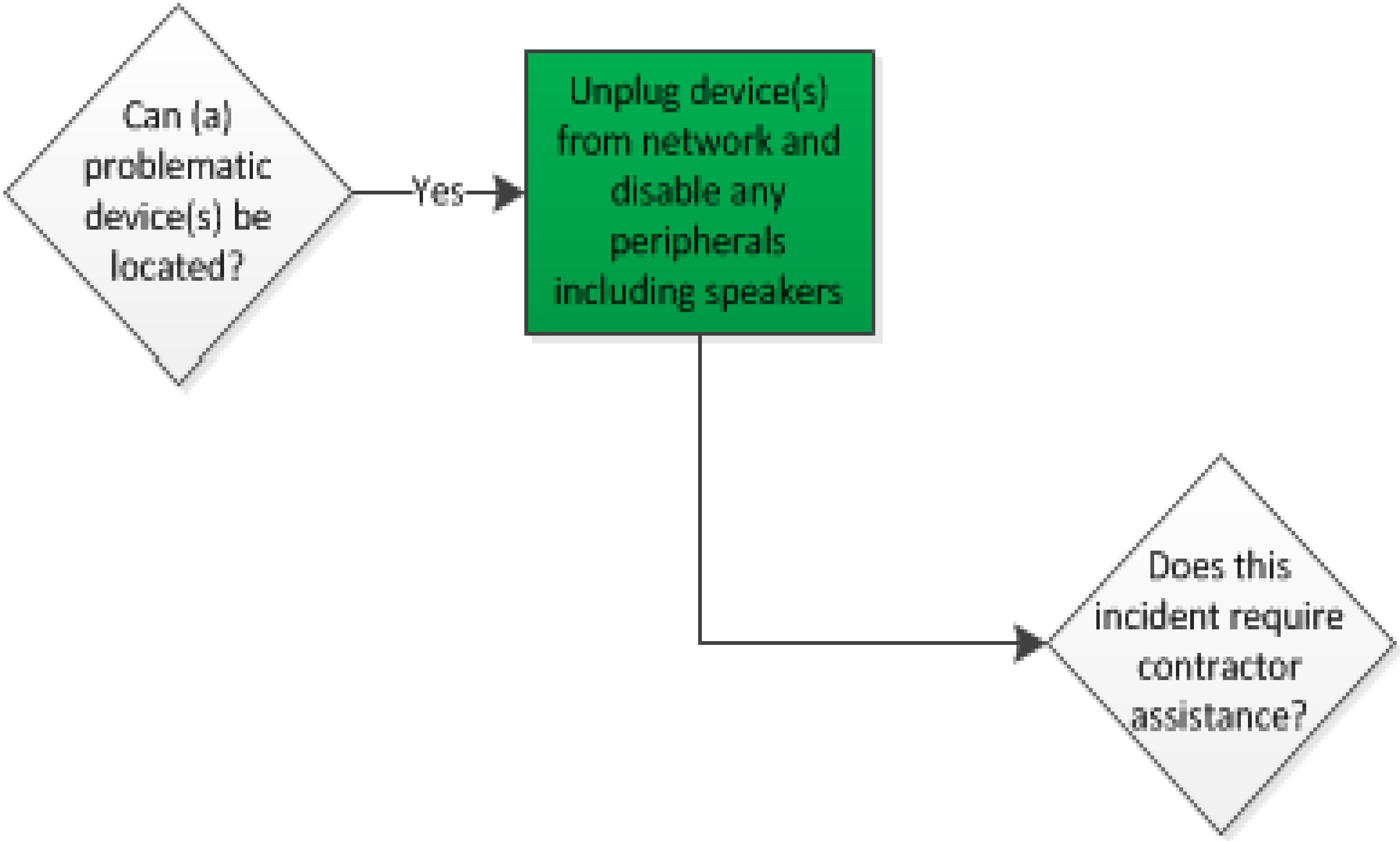
First responder to begin documentation of incident and processes

Activate the Incident Response Team and conduct Risk Assessment

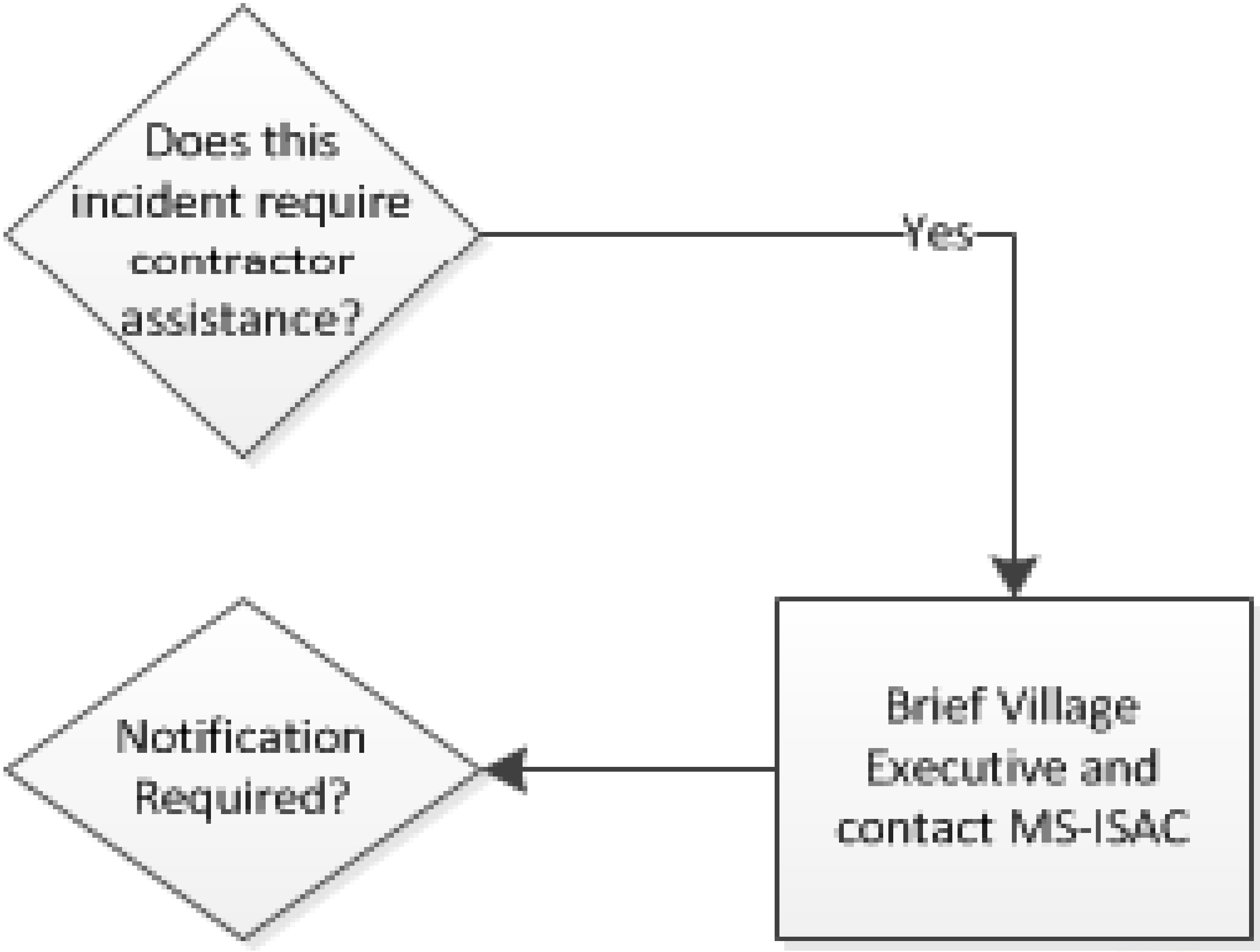
Brief Village Executive and continue assessment

Notification Required?


Notification Required?
No
Can (a) problematic device(s) be located?
Yes
PIO to create and communicate message



Can (a) problematic device(s) be located?
Yes
Unplug device(s) from network and disable any peripherals including speakers
Does this incident require contractor assistance?

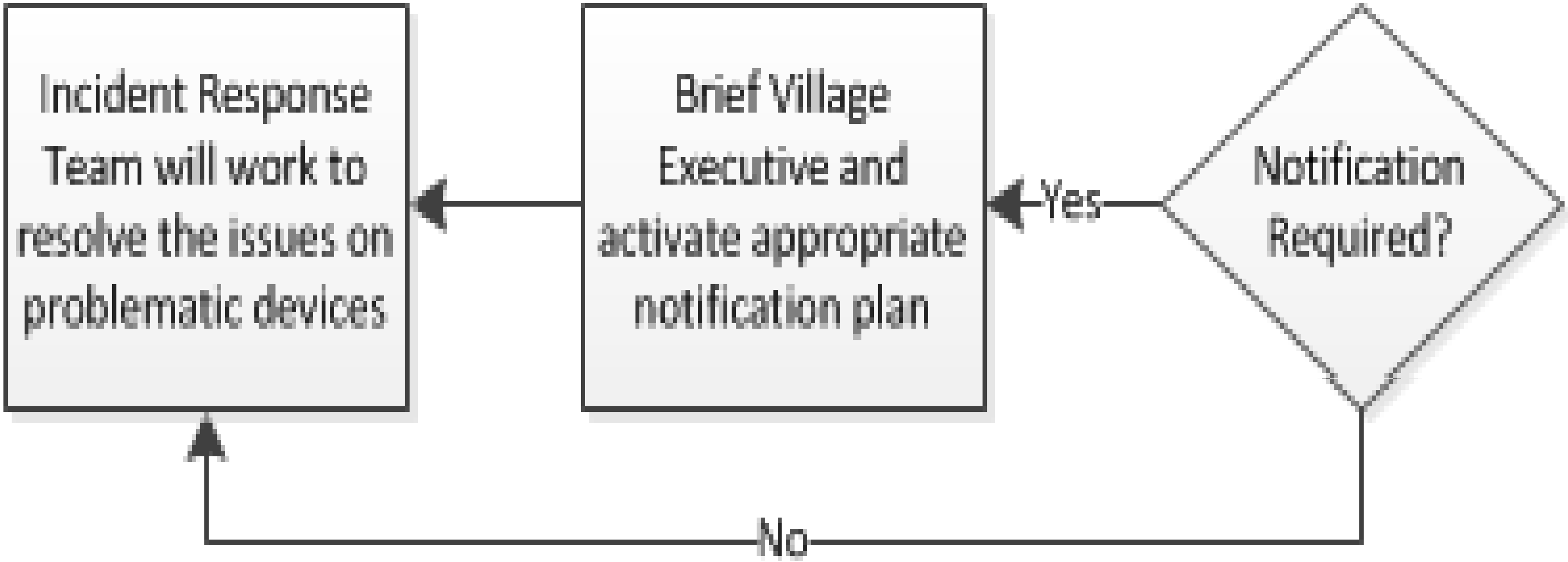


Does this incident require contractor assistance?

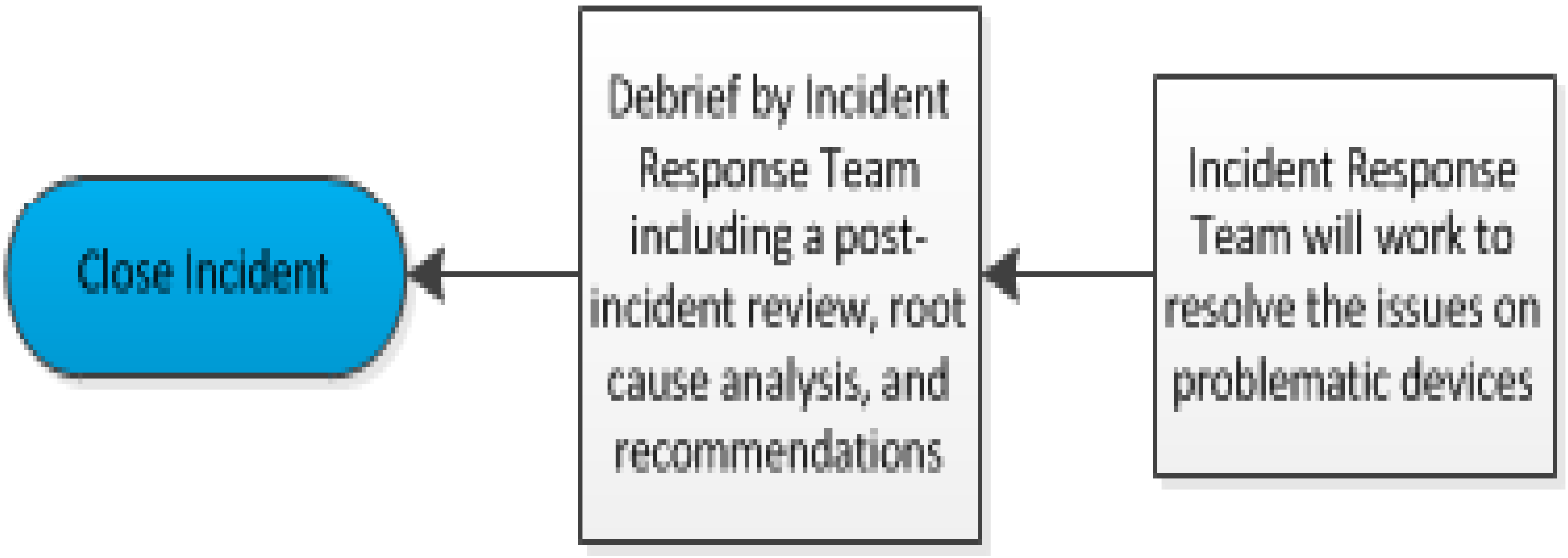
Yes

Brief Village Executive and contact MS-ISAC

Notification Required?



Incident Response Team will work to resolve the issues on problematic devices
Brief Village Executive and activate appropriate notification plan
Yes
Notification Required?
No



Incident Response Team will work to resolve the issues on problematic devices

Debrief by Incident Response Team including a post-incident review, root cause analysis, and recommendations

Close Incident

Conclusion

- Resolution… until the next time.

Contact Information

- Marc Thorson
  mthorson@gmisillinois.org
- Brian Johanpeter
  bjohanpeter@gmisillinois.org
- www.gmisillinois.org