Case Study: 10 Tips for a Successful Incident Response Team

Darrell Elven
CISSP
Senior Information Security Specialist
Caterpillar Inc.

Where we're going

- What is an IRT
- How does an IRT start
- Characteristics of a successful IRT
- Top Tips

What is an IRT
(Best Case Scenario)

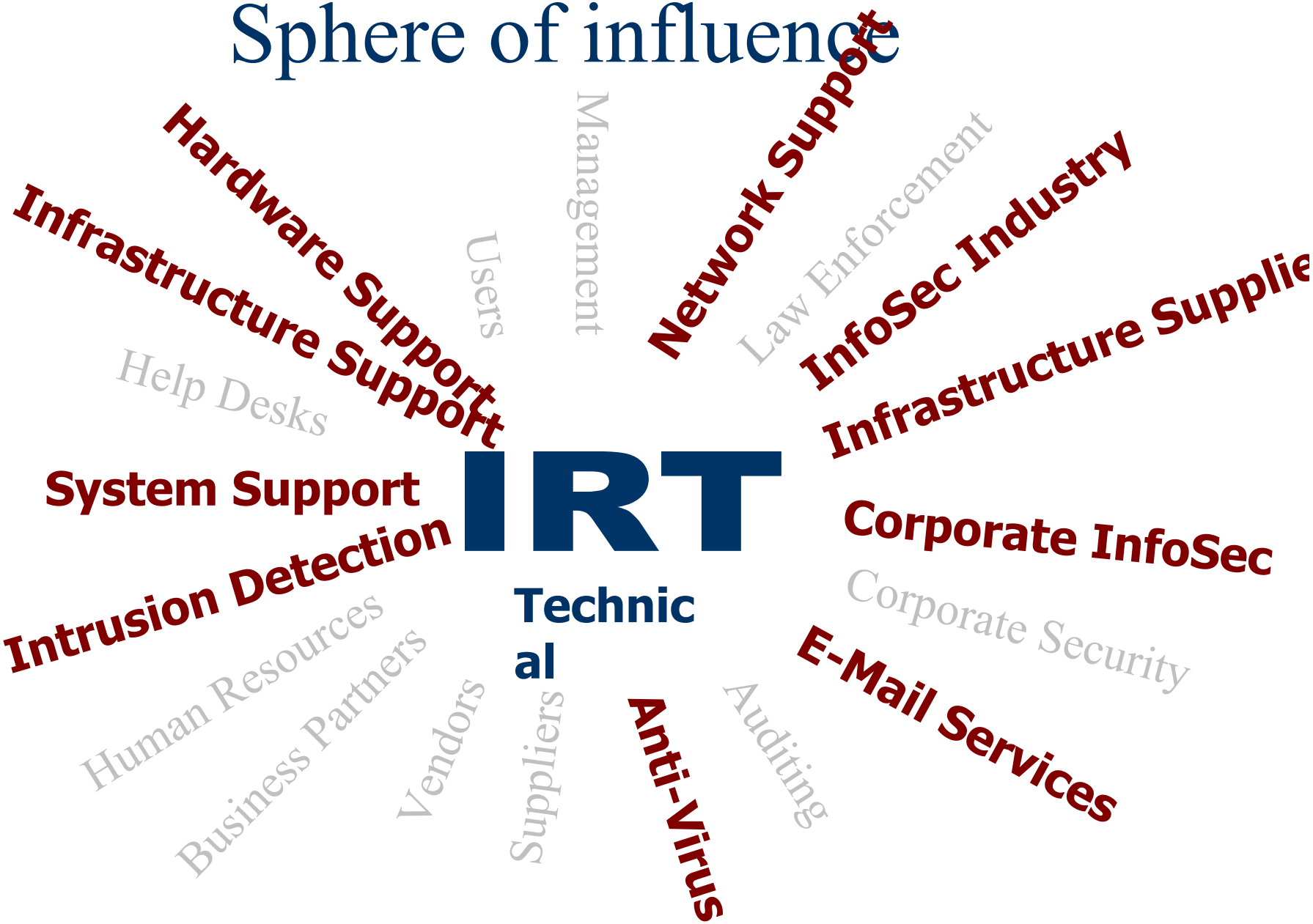
- A group assigned to limit the adverse effects of misuse or abuse of computer or network resources and/or prevent loss of or damage to electronic information, resources, and systems.
- Reactive **and** Proactive
- Responsibility to Investigate/Evaluate/Communicate

How an IRT is Started

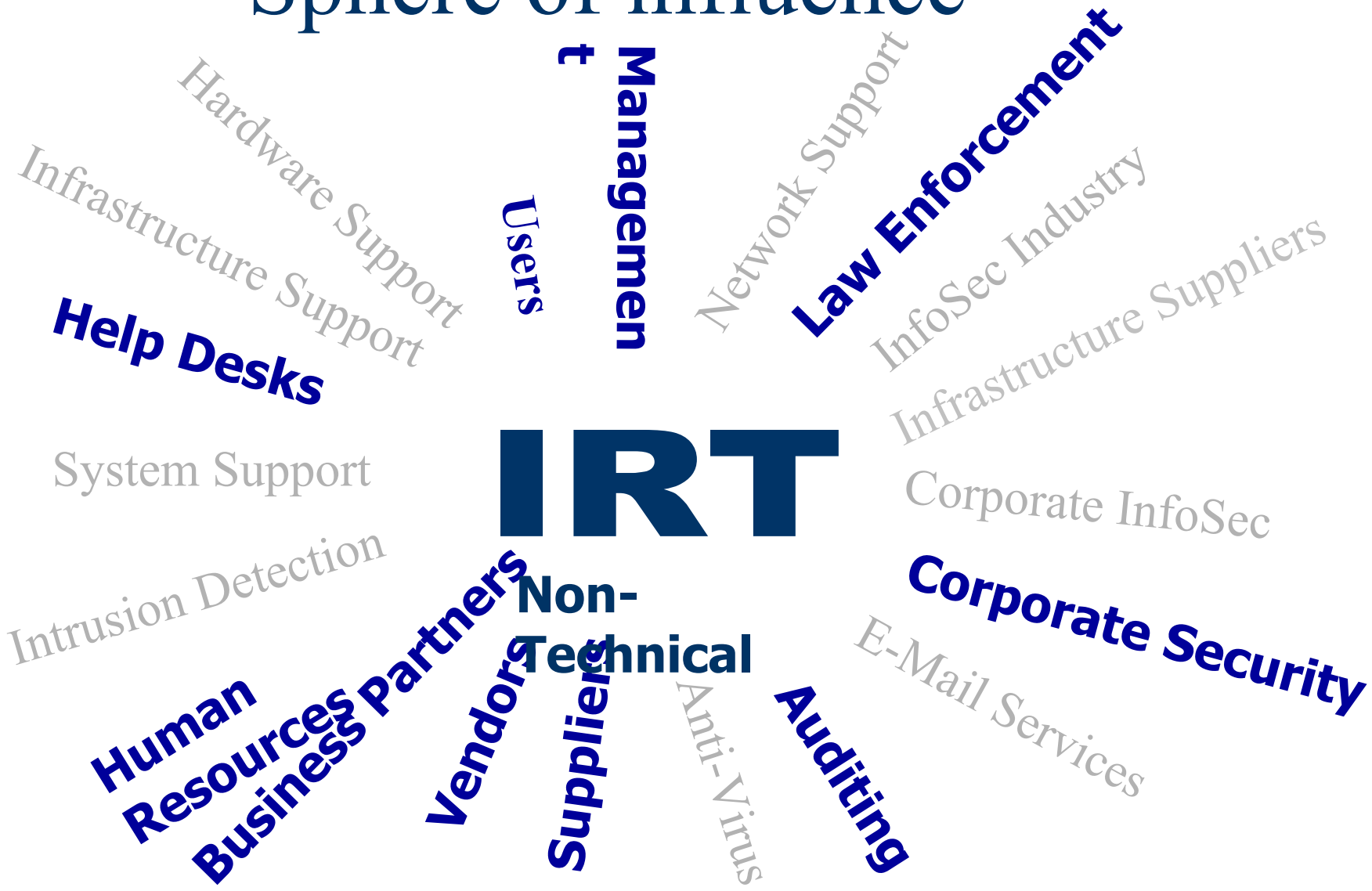
- Management attends a seminar
- Management reads a magazine article
- Management friend tells a story
- Crisis response

Sphere of influence

Sphere of influence



Sphere of influence



Characteristics of a Successful IRT

- Authorization and Budget
- Processes defined, written, used
- Contact lists
- No Newspaper articles about your company
- Get “dumb” questions
- People ask to work in security
- Continued employment

The Tips 1-10

1. Act like you know what you're doing and as if you have the authorization to do it.

1. Act like you know what you're doing and as if you have the authorization to do it.

- Take Charge
- Ask questions
- Listen
- Evaluate
- Humor
- Decide
- Direct
- BE CONFIDENT

ACT!

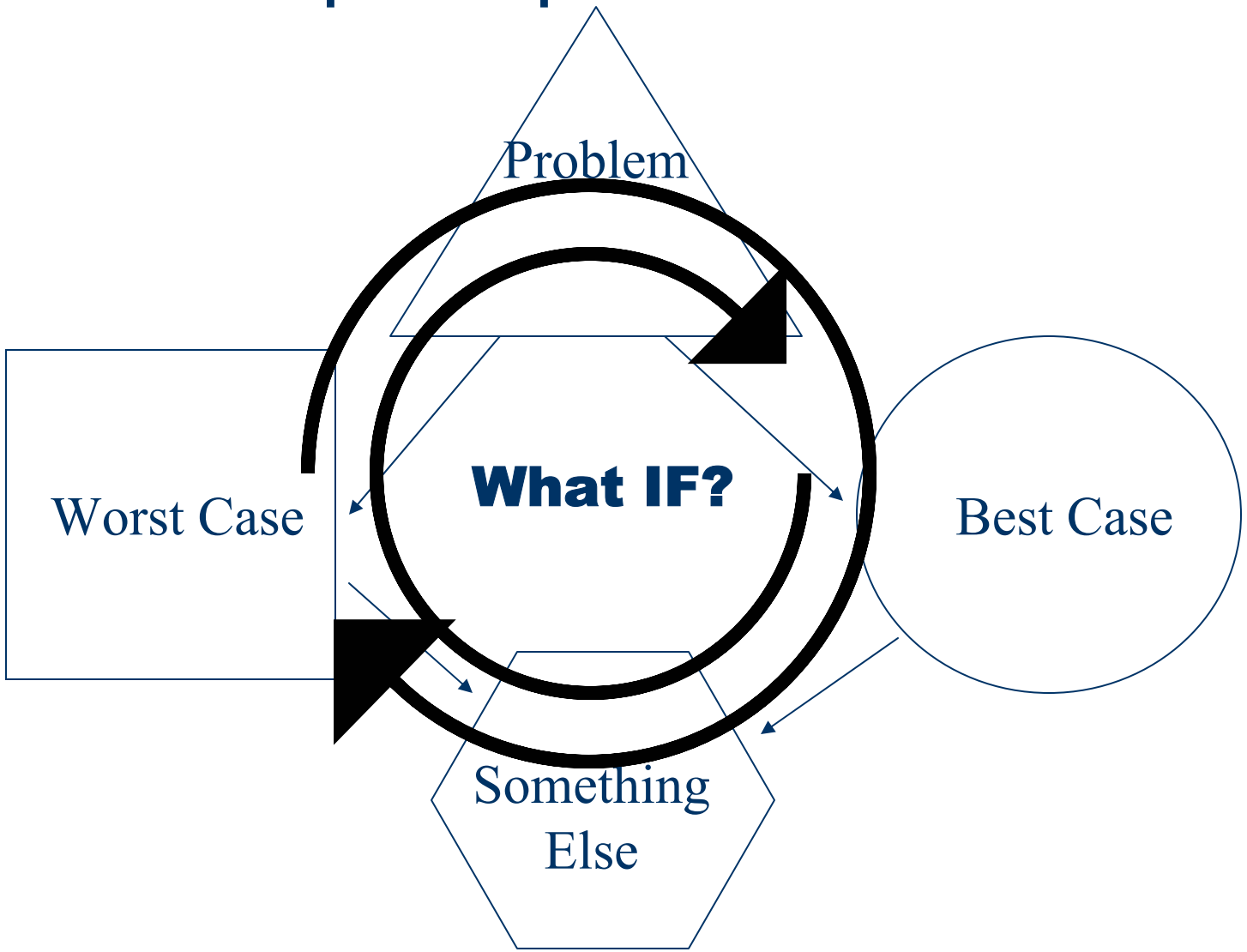
2. You do not have to know how to do everything; you just have to know who does.

2. You do not have to know how to do everything; you just have to know who does.

- Satellite Resources
- Reserves
- Local Security Agents
- Management
- Subject Matter Experts
- Help Desks

3. Plan for the worst, hope for the best, and expect surprises.

3. Plan for the worst, hope for the best, and expect surprises.



4. At the beginning of an incident find out everything you know and this will show you what you don't know or need to know.

4. At the beginning of an incident find out everything you know and this will show you what you don't know or need to know.

- ✓Establish a pattern of activity
- ✓Names – Lead Investigator, Affected, Managers, Contacts
- ✓Descriptions – Incident, Physical, Discovery, Effect
- ✓Logs
  - •System
  - •Proxy
  - •Phone
  - •Gates
  - •??
  - •IDS
  - •Firewall
  - •Anti-Virus
  - •Access
- ✓Confirm Everything

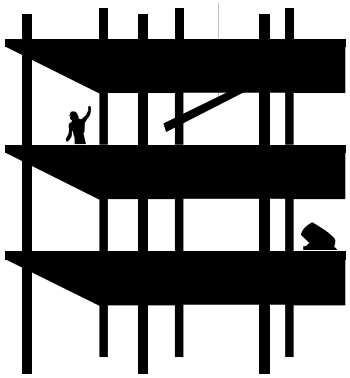
5. When you hear hoof beats, don’t think zebras.

5. When you hear hoof beats, don't think zebras

6. It is reckless to act too quickly, but it's stupid to act too slow.

6. It is reckless to act too quickly, but it's stupid to act too slow.

- Survey the land
- Take core samples



- Get the financing
- Find the contractors

- Lay the foundation

Somewhere in here the detailed blueprints are developed

6. It is reckless to act too quickly, but it's stupid to act too slow.

Somewhere in here the incident takes place

- Survey the land and know your network
- Take core samples to reveal your system vulnerabilities
- Get the financing established through management support
- Find the contractors on the staff who can build the solutions
- Lay the foundation for further action by having the proper resources on hand

7. It is of no use to provide very precise, clearly written, well thought out answers or solutions if they are wrong.

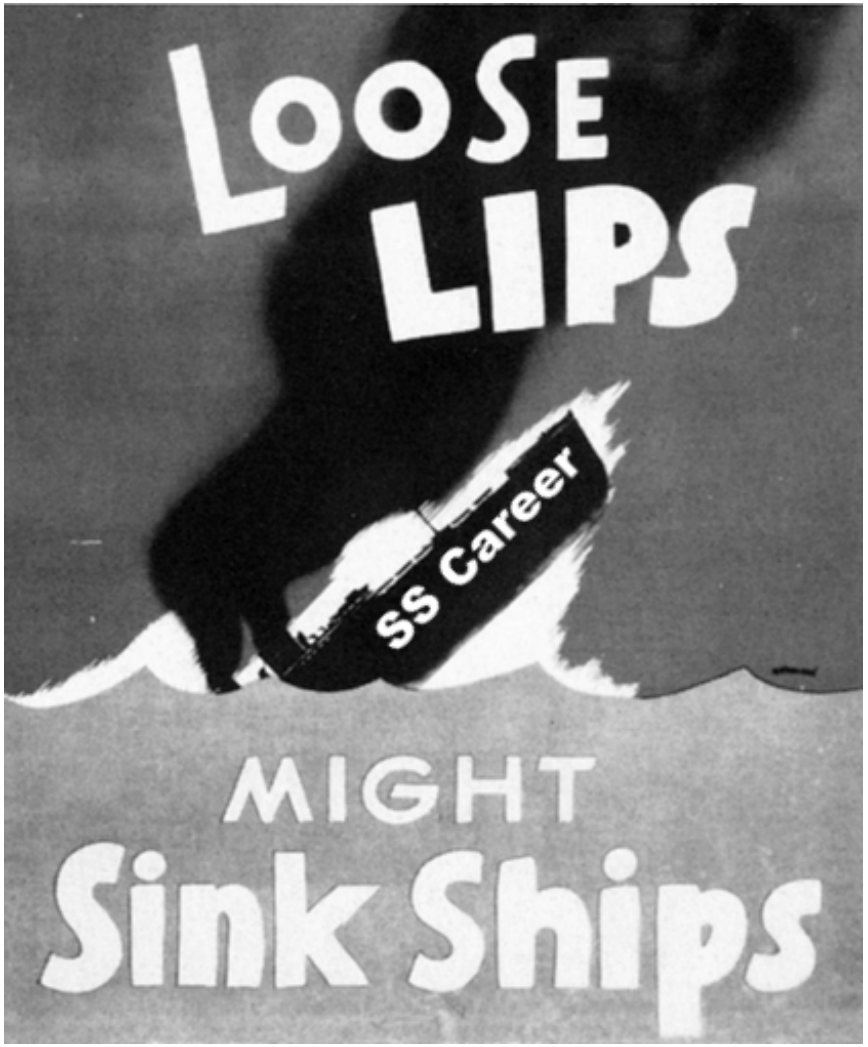
7. It is of no use to provide very precise, clearly written, well thought out answers or solutions if they are wrong.

Directions: To get ***five***, start with an available two, obtain an additional two and combine them in a carefully controlled manner. Any warnings, which may appear after you complete this task, may be disregarded.

2 + 2 = 5 ?

8. Keep your mouth shut when it does not have to be open.

8. Keep your mouth shut when it does not have to be open.

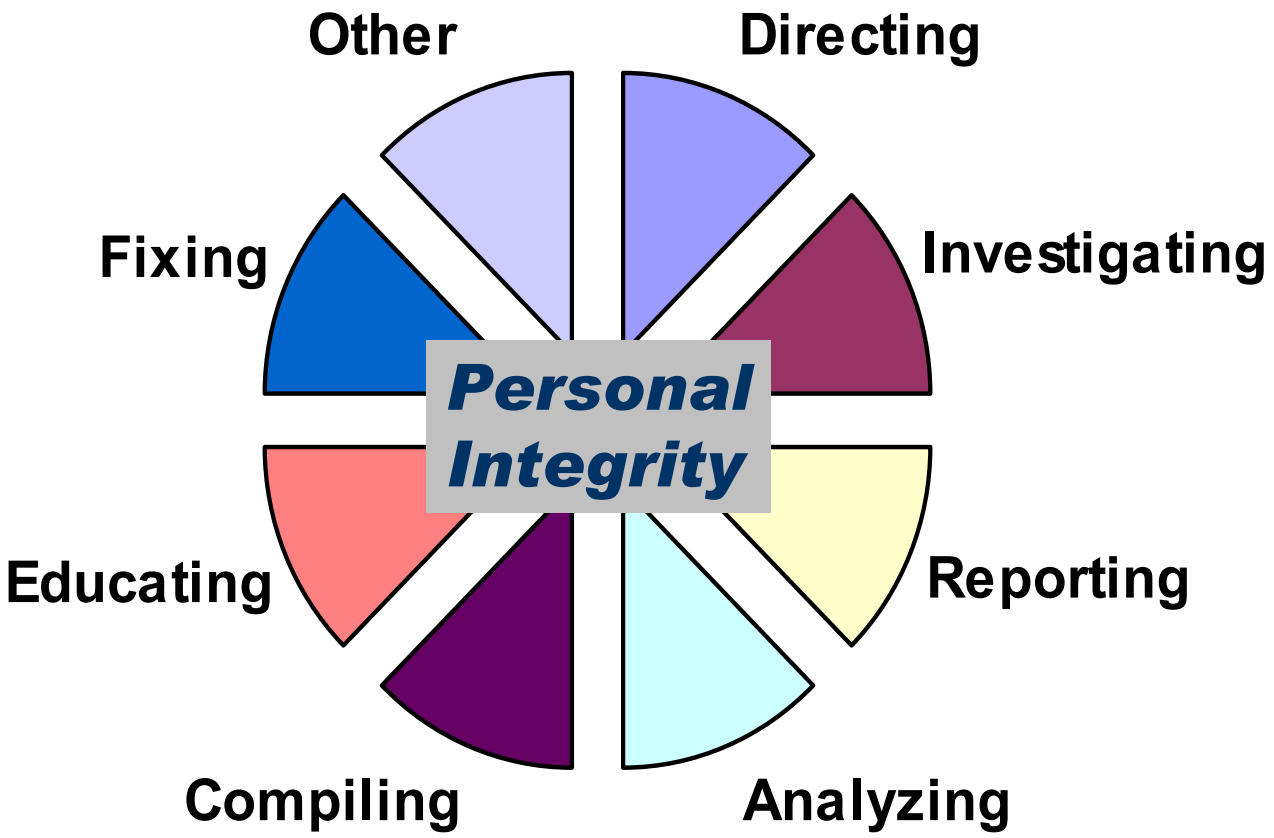


8. Keep your mouth shut when it does not have to be open.

- Incident Reports
- Monthly Incident Summaries (Sanitized)
- News
- Advisories
- Alerts

9. Personal integrity is a non-renewable resource.

9. Personal integrity is a non-renewable resource.



9. Personal integrity is a non-renewable resource.

- What may appear to be ok to you, may not be ok to others.
- Temptation is not a bad thing; giving in is a bad thing.

10. Who watches the watchers? Quis custodiet ipsos custodes?

10. Who watches the watchers?
Quis custodiet ipsos custodes?

- Oversight should be part of formal authorization.
- Oversight protects your customers from you.
- Oversight protects you from your customers.

IRT Authorization

- **Business Purpose**

  Due diligence to protect and secure Corporate Resources

- **Summary**

  Provide authorization to look, go, and do whatever it takes. Budget**.**

- **Organization**

  Define membership, oversight group and reporting structure.

- **Response Objectives**

  Preserve and protect Company Resources.

- **Anticipated Types of Security Incidents**

  Broad terms for everyone's understanding

- **Authorizing Sponsors**

  Bigger the better. CIO, Executive board, others

The tips

1. Act as if you know what you're doing and as if you have the authority to do it.
2. You do not have to know how to do everything; you just have to know who does.
3. Plan for the worst, hope for the best, and expect surprises.
4. At the beginning of an incident find out everything you know and this will show you what you don't know or need to know.
5. "When you hear hoof beats, don't think zebras."

The tips

6. It is reckless to act too quickly, but it's stupid to act too slow.
7. It is of no use to provide very precise, clearly written, well thought out answers or solutions if they are wrong.
8. Keep your mouth shut when it does not have to be open.
9. Personal integrity is a non-renewable resource.
10. Who watches the watchers?
    Quis custodiet ipsos custodes?

References

- Steven Fink, *Crisis management: planning for the inevitable*
- Sun Tzu – *The Art of War*
- Eugene Schultz - *Incident Response: A Strategic Guide to Handling System and Network Security Breaches*

Sun Tzu Says . . .

"The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable."

Sun Tzu VIII-11