Incident Response

Security

Otago Polytechnic
Dunedin, New Zealand

Problem scenario

Suppose that a significant and apparently fast spreading malware outbreak has affected the Polytech campus. You are an IT staffer who has been called in to respond to the problem. What do you do?

Organise into 2 - 3 person groups to discuss the actions you will take to deal with this problem.

Here's the thing...

- You're going to face security incidents during your careers.
- When you do, you're going to have to act quickly and decisively.
- At the same time you're going to be under stress, and most people don't perform that well under stress.
- You need to make a plan *before* these things happen.

Form a team

To deal with security incidents, organisations need to form a Computer Security Incident Response Team (CSIRT). These teams generally include the following roles:

- Team Leader
- Incident Lead
- IT Staff Contact
- Legal Representative
- Public Relations Officer
- Management Representative

Team Priorities

To form a response plan we have to identify a list of priorities. Different organisations and different incident types have different priorities, but here's a starting point:

1. Protect the safety of people.
2. Protect sensitive data.
3. Protect other data.
4. Protect systems from damage.
5. Minimise disruption to business.

Response process

1. Relevant staff throughout the organisation need to know how to identify and report possible security incidents.

Response process

2. The CSIRT team performs an initial assessment of the problem and communicates its findings. Assessment criteria need to be defined as part of the plan.

Response process

3. Contain damage and manage further risk.

Response process

4. Gather information and protect evidence.

Response process

5. Notify external parties as necessary.

Response process

6. Recover systems.

Response process

7. Perform a postmortem analysis.

Response process

After operations are restored, use what was learned to update and improve

- systems;
- policies and procedures;
- security response plans.

CSIRT Resources

The CSIRT team will need resources for recovery, analysis, and communication. Since the organisation's primary ICT resources may be compromised, you need to prepare seperate resources.

More information

- http://www.ncsc.govt.nz/assets/NCSC-Documents/New-Zealand-Security-Incident-Management-Guide-for-Computer-Security-Incident-Response-Teams-CSIRTs.pdf
- https://technet.microsoft.com/en-us/library/cc700825.aspx