Computer Emergency Response Team

(CERT)

Computer Emergency Response Teams (CERT) were unheard of 10 years ago. This new form of work group was created to identify attacks on the Internet and to provide solutions to these attacks. An attack represents an illegal attempt to steal information (e.g., financial) from transactions on the Internet.

The first CERT team was launched at the Software Engineering Institute at Carnegie Mellon University, the location of this video. Today, this work is conducted in the following way: (1) Individuals monitor for attacks. (2) When the evidence indicates that an attack is becoming severe, a CERT team is convened to discuss whether there should be action. (3) Action comes in the form of an advisory, which is a document sent to a user's community, warning about the attack and identifying immediate and longer term remedies. The advisories must be carefully worded to provide enough information to users while not giving information that might lead to more attacks.

New CERT teams are constituted for each advisory. When people are not working on teams, they may be working with vendors to improve systems in order to prevent future attacks.

This video contains four parts:

Part I	Making a Team Decision
Part II	Describing the CERT Team
Part III	Factors Leading to Team Effectiveness
Part IV	Assessing Group Effectiveness

For Hour Long Classes

Use Part I alone to demonstrate effective group process.

For Longer Classes

Group Process and Results: Show Part I and discuss effective group process (discussion questions below). Part I can be coupled with Part IV to provide examples of how internal group processes can affect external group outcomes (e.g., client satisfaction, quality of service).

New Forms of Work Groups: Coupling Parts I, II (Describing the CERT Team), and IV (Assessing Group Effectiveness), the video can be used to illustrate the features of cross-functional groups whose decisions have serious impact on external constituencies. CERT Teams are different from traditional work groups because they focus exclusively on external constituencies, rely on other technical groups outside of their organization to get their job done, their membership changes with each advisory, and their effectiveness is not easy to assess.

High Performance in Contemporary Work Groups: In a three-hour class (or over two 90-minute sessions), showing all four parts provides support for development of internal and external process models of group performance.

I. Making a Team Decision: The Sniffer Incident (a.k.a. CERT: Working on an Advisory)

There has been an attack on the Internet. It has been invaded by a "password sniffer" which can identify user IDs and passwords. Over 45,000 hosts are involved. The CERT team is responsible for sending out an advisory to Internet users that allows them to protect themselves from this attack. Should an advisory be sent out? If so, the team's task is twofold: to help those users not yet affected to prevent an attack, and to help those who are already affected to recover. They must decide on whether to issue an advisory, its content, and the timing of their announcement.

Key Words

"... bigger than the Internet worm"
"... makes us look bad"
"Long-term and short-term, we will need to respond."
"We have to have better words."
"The interface is in promiscuous mode."

Some best practices the class will observe include:

- Use of the board
- Role of team leader as a facilitator
- Active participation by all members
- Problem identification
- Building on each other's ideas
- Role of opposition member (devil's advocate)
- Check for consensus
- Get problem statement agreed to and shared
- Use of summarization as a consensus-building technique
- Putting names by action items

It may be useful to:

a. Show the class the first few minutes to be sure they understand what you want them to do to answer this question. Then rewind and start again.

b. Draw a picture of the group after you show the first few minutes so you have a way to talk to people:

Member 2 Member 1

Member 3 Team Leader
(Public Relations Manager)

Member 4 Member 6
(Public Relations)
Member 5

2. What information do they use to make their decision?

- past experience
- vendors
- reporters
- other teams via e-mail
- service providers
- users

Note: Some of this information is gathered before the meeting, but some is also gathered in the two hours set aside after the meeting.

II. Describing the CERT Team: What can the CERT team tell us about new forms of groups?

After the meeting, CERT team members describe their experiences in working together. Each member is an expert with a high degree of respect for their team members.

Key Words

"When we come to the table, there is nothing there."
"Conflicts get resolved in this room."
"Everyone believes their opinion is the right one."
"...high stress levels..."

Before viewing Part II, ask the class:

1. What adjectives would you use to describe the CERT team? The CERT team describes itself as: creative, hardworking, eclectic, diverse, busy, chaotic.

2. What other groups are like CERT teams? Fire-fighting and other trouble shooting groups. Task forces (e.g., for strategic planning)

New forms of work groups are increasingly ad hoc, temporary, cross-functional, empowered, and under high pressure from external constituencies (e.g., customers) for quality results.

Critical features for success in such groups (Meyerson, Weick, and Kramer, 1996) include:

- Diversity in skills.
- Overlapping social networks or limited labor pools.
- Complex tasks involving interdependent work.
- Deadlines.
- Tasks are non-routine and not well understood.
- Tasks are consequential.
- High level of respect of skills competencies of each other
- Reputation of individual as well as group is on the line.

III. Factors Leading to Team Effectiveness

We asked the CERT team to describe a situation where the group really had worked well together. The Sniffer Advisory Incident in Part I was their chosen example of high performance. CERT team members debrief their experiences during the Sniffer Advisory Incident.

Key Words
"Every time they send communications out on the Internet, their reputation is on the line."
"...getting beaten up privately instead of publicly..."
"Sum is greater than the individual parts."

1. How do you learn to be in a cross-functional group that only meets occasionally and when there is a crisis?

- mentoring
- know someone before joining
- parties
- step back and laugh
- become friends with each other outside of CERT meetings

2. What approach to tasks do members of this group take? What is their approach to building social relations with each other?

Team members attribute their success, particularly in the Sniffer Incident, to:

- always collecting information
- paying attention to individual members (including James's objections
- valuing opposition relevant to the task
- spreading work out across all team member so everyone contributes
- coordinating with other teams

IV. Assessing Group Effectiveness

This section concerns group effectiveness criteria.

1. How do we know that the CERT team is effective? Members tell that the following indicators are important:

- renewal of funding
- user feedback via e-mail and at conferences
- referrals from knowledgeable users in the area

2. What are critical criteria, both intermediate and final, for group effectiveness?