Physical Security and Disaster Preparedness

Often over-looked is that "Cyber Security" is, and must be, part of total business security. You can't be Cyber Secure if items are lacking from either Physical Access or from Disaster Planning.

Here are some example items you can use to start a conversation with your staff.

1 Physical Control Examples

_____ Is access to your computing area controlled?

_____ Are visitors escorted into and out of controlled areas?

_____ Are your PCs inaccessible to unauthorized users (e.g. located away from public areas)?

_____ Is your computing area and equipment physically secured?

_____ Are there procedures in place to prevent computers from being left in a logged-on state?

_____ Are there areas and facilities identified that need to be sealed off immediately in case of an emergency?

_____ Are key personnel aware of which areas and facilities need to be sealed off and how?

2 Disaster Response Plan (DRP) Examples

_____ Do you have a current Business Continuity Plan (BCP) and related Disaster response Plan (DRP)?

_____ Is there a process for creating retrievable backup and archival copies of critical information?

_____ Do you have an emergency/incident management communications plan?

_____ Does your procedure identify who should be contacted, including contact information?

_____ Does your procedure identify who should make the contacts?

_____ Have you identified who will speak to the press/public in the case of an emergency or an incident?

Interested in more checklists and resources?
www.radiusbridge.com or info@radiusbridge.com