CLARITY technology solutions

5 Reasons Your Employees Don't Care About Your Information

Your organization spent months archiving, refining and testing your business continuity plan. No doubt it is amazing, with a great deal of stone solid disaster recovery measures and wonderful documentation for getting back on course following a meltdown of significant systems. But, there is one element that may sink your lovely plan before it ever gets an opportunity to shine. It's not fire or tsunami, it's varying levels of end user frustration, apathy and general ignorance.

1. They do not have any concept that a strategy exists.

Believe it or not, the typical employee does not devote a good deal of time wondering how the company will survive in case a giant Godzilla-like monster rises from the closest body of water. They simply assume someone will take care of things and usually make a hand wave about backups and possibly even cite cloud computing. They do not know their functions in getting the company back on its feet – since they haven't been granted roles or training.

Best Practice: Engage your users

Use a broad-spectrum awareness policy, such as what they need to do if they cannot perform their jobs. This should contain explicit printed directions for remote working and the way to report an outage if the email server is down. Oh, and it should go without saying that you must check your BC/DR plan frequently. If you want to be a stickler, consider the system down as part of an evaluation on a weekend and then see how well the ordinary user addresses the calamity.

2. They do not know the significance of "disaster."

Hollywood has taught us that disasters imply a great deal of special effects and perhaps Dwayne "The Rock" Johnson swooping in with a couple witty quips and a huge plan to save the day. Nonetheless, it's not like sharknado and zombie outbreaks occur daily, or perhaps occasionally. Disaster recovery more frequently entails electricity outages due to different terrestrial reasons, or information loss from malware, or merely general clumsiness from personnel destroying data unintentionally. These are not one-time occasions but rather things that are certainly likely to occur – maybe not now, maybe not next week, but you can bank on it. The IT staff knows, but your employees do not.

Best Practice: Be crystal clear about everything

"Disaster" means – less smoke and laser beams and more visions of being attacked by malware or somebody inadvertently deleting a directory. Include several sample situations that people can understand are high likelihood and in their best interest to prepare against.

3. They are creating new places for business-critical data outside of the strategy.

You understand rogue IT is out there. You might even guiltily do it yourself, whether "it" is a stash of business documents on Dropbox. Even if your policy mandates optimal security methods, there is probably a group out there sourcing all its files up on Google Drive because staff members do not understand the consequences of free cloud storage. While there are many reasons this activity may not be copasetic to your business, that's a conversation separate from the necessity to work those procedures into your business continuity program.

Best practice: Use detective work to combat rogue IT

When there's a group out there that's spartan with its own file storage, then consider it a red flag – virtually nobody practices pristine information hygiene. They are saving their information somewhere, and when it is not in your covered systems, where is it? Expect reluctance to talk about, but with an assurance that you are not attempting to hamper their efforts, but rather working to safeguard them, you should have the ability to break down silos. At a minimum, get it on record that the offer was made.

4. They were not even considered in the strategy.

We have all experienced the continuing battle to align IT with the business. The writers of a business continuity strategy neglect business-critical processes simply because they did not recognize that they were essential. Can you really blame employees who do not care about a strategy that does not protect them? This is a large problem, and typically these procedures aren't captured until the true disaster strikes and it's too late.

Best practice: IT has an opportunity for outreach

To get IT alignment, your organization must conquer the processes and find out just what users do to drive company business. Keep tabs on all vital systems and ask questions, especially as it might pertain to "what-if" situations around your business continuity program. Yes, it is easier said than done, however, IT wants to remain on top of what is mission essential this week.

5. They have their own tragedy in the home.

In the event of a hurricane, flooding, or the zombie apocalypse, your employees are suffering the exact same environmental effect as your company. Consider, for example, Hurricane Sandy – the residents of the affected regions were concerned first and foremost about their loved ones and property and their own safety. If your company recovery situation depends on a couple of key people who understand the passwords and procedures to get systems back online, you are taking a tremendous gamble that they are likely to concentrate on the requirements of the business during a period of catastrophe.

Best practice: Great vs. Good businesses

Great businesses provide for the creature comforts and work-life equilibrium of the employees. Ensuring your employees have what they need to perform their tasks is an often-overlooked feature of business recovery. Ensure that your business continuity plan includes recommendations for emergency housing and meals, and allows your employees the time they will need to take care of business – both yours and theirs.