Prepare for a Catastrophic Event

Data theft and blackmail via ransomware are common everyday events. These crimes are preventable even when a system computer becomes compromised. A team of people is a model for how a system of computers can work together to prevent crime and survive a catastrophic event.

Work is divided into tasks where a basic task is performed by one worker (person or computer). Work is performed, inspected, and audited by different workers to find a defect, prevent success of most crime attempts, and detect a successful crime.

Workers at multiple locations can survive a catastrophic event such as a power failure, successful cyber-attack, fire, or flood. They can be prepared and available to perform needed tasks. A manager assigns tasks to workers based on ability, availability, and maximizing work performed at minimal cost.

A “Cloud” can be part of a solution. A cloud provides leased low-cost storage and computing that is accessible via the Internet.

Ideally a computerized system has a multilayered defense. A computer is located within an enclosure, room, and building that provides a suitable environment including physical means to limit access. Information is encrypted into what appears to be random or white noise to an unauthorized observer. A user is authenticated via a username and password or multifactor authentication combining something a user knows with something a user possesses. Another user can be required to approve user access to a critical function. A plan can require reviewers to approve before implementation.

A system of computers should distribute work among computers at several locations. Corruption of a computer interfacing to a user must be prevented from spreading to a server computer storing data and performing critical work. Defensive functions such as authentication and access approval to a function are performed on an isolated server computer. Multiple instances of user interface and server software exist on different computers at several locations to survive a catastrophic event. Ideally in progress work of a server is recovered upon a failure without requiring a user action.

A communication infrastructure should help a system of computers and applications to work as a team of people. Communication infrastructure requirements in software terminology include:

- Minimize effort to create applications that distribute, isolate, and recover work.
- Provide reasonable cost and performance.
- Enable applications to converse peer to peer, client to server, or publisher to subscriber.
- Encrypt application conversations.
- Enable a client to server conversation to be recoverable.
- Help to ensure and prove software corruption cannot spread.
- Enable an administrator to control and audit data flowing between applications.
- Enable change during operation by supporting multiple simultaneous versions and ensuring conversing parties are the same version.

An existing communication infrastructure likely does not and almost certainly cannot achieve all these goals. Join in to devise a new and radically different infrastructure needed to achieve these requirements. Visit web site SoftEcoSDK.com or send an email to SoftEcoSDK@gmail.com to learn about, discuss, research, and build a new kind of application communication infrastructure.