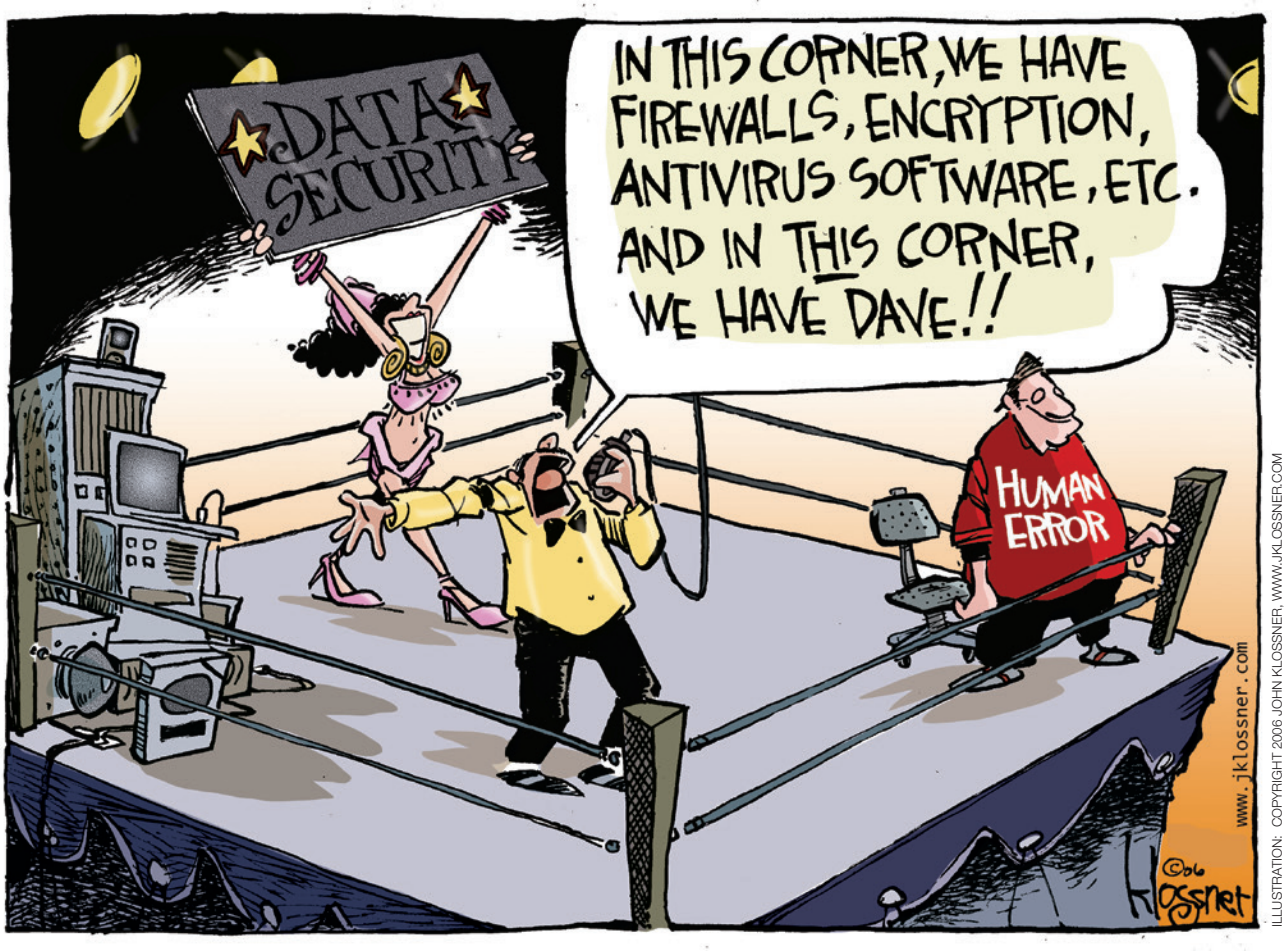




# SECURITY Awareness and the HUMAN Firewall

## Five ways to protect your organization from disaster

A midsize retailer's recent email phishing test revealed how susceptible companies can be to hackers. Employees received an email disguised as a threat of termination from their human resources department for accessing prohibited sites on the job. It included instructions to click a link in the message to see a list of sites they allegedly visited.

**Jim Kandrac** is president and founder of UCG Technologies.

Over 48 percent of employees clicked on the link, despite the fact that the sender's email address was from an unknown source and the link clearly led to a destination outside the firewall. This may be an extreme example of how companies can fall prey to phishing, but it's not unusual. In my experience, between 20 and 45 percent of employees are deceived by email ploys. A single click to a malicious site can infect a user's computer with malware that compromises the entire corporate network.

Many experts believe breaches are so common that the issue is no longer whether organizations will be attacked but when. Consider this:

- The Ponemon Institute found that nearly 90 percent of

healthcare organizations were hit by a data breach in the past two years (bit.ly/1UZtSu2)
- Intel's McAfee Security division reported a nearly eightfold increase in ransomware attacks over the past year (intel.ly/2a3myue). Imagine if an attacker held servers hostage; you could be down for days.
- An analysis of 11 million stolen passwords for cloud services conducted by Skyhigh Networks found that 20 passwords constitute 10.3 percent of all passwords in use, with "123456" used by 4.1 percent of compromised accounts (bit.ly/1YCMcc5)
- Ponemon reported that the average consolidated total cost of a data breach is now $4 million (ibm.co/1AA4djh)

## Five Steps for Protection

Organizations can take the following steps to protect themselves:

**1. Use encrypted data protection in two data centers.** It's nearly impossible to keep determined attackers from breaching your defenses, so the best course of action is to make the data useless to them. Using redundant data centers gives you an extra layer of protection in case of failure or breach. Strong data encryption protects you from damage even if you are hacked. Be sure to keep encryption keys in your possession and encrypt data both at rest and in transit.

**2. Conduct regular phishing tests.** The finest firewalls, encryption and anti-virus software can't compete against one uneducated user who falls prey to a phishing scam. In my experience, even the most security-aware companies experience click-through rates of 15 to 20 percent on phishing email tests. According to SC Magazine, 82 percent of 298 IT security professionals surveyed worry that their high-ranking executives are vulnerable to phishing scams, but only 45 percent provide cybersecurity training to all employees (bit.ly/29aX0L5). This is one of the cheapest and easiest vulnerabilities to address. By conducting tests regularly, you can determine your level of susceptibility and identify employees who need additional education.

**3. Conduct ongoing security training.** Experts have long agreed that the most serious vulnerability companies face is their staff's lack of knowledge. Security training isn't difficult or time-consuming. However, siloed organizational structures prevent many companies from taking a coordinated approach to security awareness. The people in charge of backup and disaster recovery (DR) may have no security responsibilities. Executives may regard security training as a waste of time. The good news is that security awareness works. For example, when security education firm KnowBe4 partnered with UCG Technologies, the percentage of employees susceptible to phishing emails dropped to 1.3 percent 12 months after awareness training began (bit.ly/29KBEWS).

**4. Develop an incident response plan.** Many customers mistakenly believe their problems are solved once they sign up with a DR provider, but no one can guarantee absolute protection. Organizations must have their own processes in place to ensure quick and full recovery from a breach or outage. IT staff and business users must know what's expected of them during a disaster. Test the plan by conducting a mock recovery once a year. It's amazing how many details are overlooked, even in carefully thought-out plans.

**$4 million:** The average consolidated total cost of a data breach, according to a Ponemon Institute study

**5. Calculate recovery time and recovery point objectives.** Knowing how long your business could survive an outage and how current your information should be to continue conducting business can save a lot of money. Not every business needs to be back online within one hour. If you can survive 24 hours of downtime, you can save significantly on DR costs. Similarly, knowing the maximum age of files that must be recovered from backup for normal operations to resume helps you calculate your backup windows. The need to have files current to within one hour, for example, drives many decisions about service levels, storage media and personnel. If you can get by with two-day-old files, your backup window is more open and your costs are less. This information also should be incorporated into your DR plan.

## Partner Up

Managed service providers are an option for effective security and DR planning. It's about taking shared responsibility for customer success and protecting the customer at all levels. Be prepared to ask them how they will work with you on each of these five steps. If you don't like the answer you get, there are plenty of other options. P