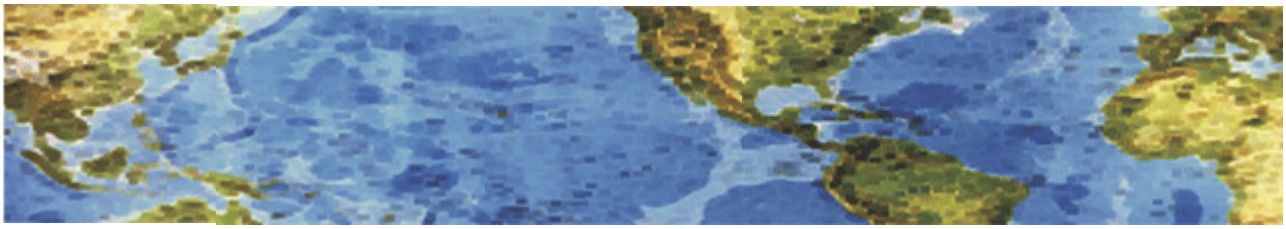
HALL ASSOCIATES



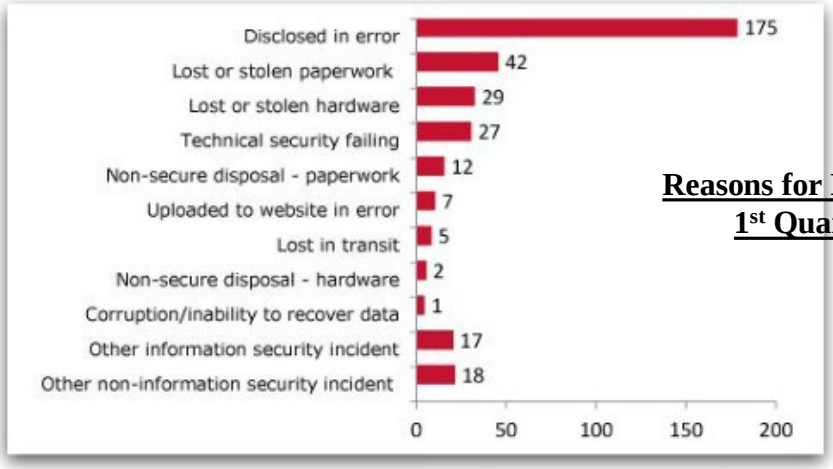
Risk-Based Decision Making Commentary
17 September 2013 Newsletter

When is Enforcement of Security Policies Effective?

When is enforcement of security policies effective? **When it serves as an enabler of the right behavior.** For that to happen, usually three conditions need to be met. First, enforcement has to be visible, meaning the entire workforce has to be aware of it. Second, it needs to be meaningful, meaning there has to be a real consequence. Third, it needs to be persistent, meaning it has to be visible long enough to shape new behavior.

In recent months, when reading about and talking with folks about security incidents and breaches, a common theme that has repeated itself over and over again is that termination of personnel was often the action taken in response to a data breach. But that action normally only temporarily stemmed the number of incidents. **Terminations have not been as effective as one might expect to effect long-term behavior modification**.

Is Termination Visible? For an action to change behavior it must be visible, meaning others must be aware of it - not only that it happened, but the circumstances that led to it. This is problematic because many companies/organizations are hesitant to discuss punitive actions. They are also hesitant to acknowledge that a data breach occurred. As a result, only a few employees may be aware, and depending on their perception, the story told to others may be skewed. Behavioral change is helped by learned retention, and termination has a short shelf-life when it comes to retention.



Reasons for Data Breaches
1st Quarter 2013

HALL ASSOCIATES

Is there Meaningful Consequence? Termination has personal, professional and financial consequences. It alone may actually modify behavior for those aware of what happened. If the goal is long-term change, then termination alone is not likely to achieve that result and might actually be counterproductive.

Is It Persistent? Termination eliminates certain awareness opportunities for long-term learning because the person terminated is gone and the people involved don't discuss it. Individuals who have been punished, but remain in the workforce, can testify to others firsthand that certain behaviors are destructive. In fact, individuals that are given a second chance can become positive influences with other personnel - particularly if they perceive the consequences they're handed were fair. Termination is still an appropriate consequence depending upon the circumstances. It should be reserved, though, for the repeat offender, the individual who shows a total disregard for the rules, the person who seeks to harm another, or the most egregious incidents. But it should not be a standard response for every data breach in which an employee had some responsibility. It is also necessary for you to have specific policies stating what an employee can be terminated for.

Privacy and security, both individually and for the company, are every person's responsibility. You hear this over and over again, yet many companies and organizations seem to be very reluctant to set privacy and security performance criteria for their workforce. **Have you set privacy and security performance criteria for your workforce?** Is data security identified in job descriptions and included as part of performance evaluations? Establishing privacy and security performance criteria for all employees should make everyone in the organization personally aware of their individual and collective responsibility to protect your (and their) sensitive information.

Also note that often companies are held responsible for the actions of their employees in various ways - legal, regulatory, reputational and business. **Everyone needs to provide workforce training and make sure that they emphasize that their personnel's actions have consequences.** The point is that even good workers sometimes make mistakes or have lapses of judgment. That does not necessarily mean they are not good employees or are not capable of doing better. An incident or even a lapse of judgment, depending on circumstance, should not be grounds for automatic dismissal. Sometimes the person who makes the mistake and suffers the consequences, but is not terminated, is far more effective at shaping others' behavior than the one who disappears and is soon forgotten.

Tying privacy and security to individual performance plans and then enforcing it fairly can have a profound effect on behavior, and therefore, culture. It has consequences, it's visible and persistent, and if applied consistently, will be perceived as fair. More importantly, it will contribute to **awareness and learning** and should assist in reducing the number and effects of future incidents.

These links are some useful ideas about establishing and enforcing an effective security policy. There are many, many more available.
http://www.darkreading.com/management/writing-and-enforcing-an-effective-emplo/240142264
http://www.isaca.org/Journal/Past-Issues/2005/Volume-6/Documents/jopdf-0506-creating-enforcing.pdf
http://www.sans.org/reading-room/whitepapers/policyissues/developing-effective-information-systems-security-policies-491?show=developing-effective-information-systems-security-policies-491&cat=policyissues
http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-503131.html