

The Bulletin

Technical Tips

By Tom Snyder Ph.D.

Policies and Procedures – the Missing Piece of the Security Puzzle

New technologies have emerged that allow unprecedented efficiency, freedom and functionality e.g. the internet, mobile computing, the convergence of voice and data, etc. However, they also introduce new risks that are harder to control and have higher impacts when something goes wrong. Technical measures, such as back ups, virus protection, and firewalls, are important for maintaining security. They are only a part of the puzzle though. They don't protect organizations from: employees who take customer lists or erase hard drives when they leave, internet downloads that slow internet connections or computers to a crawl, systems administrators who peak at email and electronic files containing HR or financial information or photo and music software that crash computers or other software. Policies and procedures can.

While there is no such thing as 100% security, the following in combination with appropriate technical measures will provide organizations with a very effective level of security.

- Ensure that staff knows security do's and don'ts

- Ensure that staff has sufficient resources and skills to exercise its security responsibilities

- Ensure that staff knows what to do in case critical IT services are unavailable

- Ensure that security is considered in job performance appraisals and result in appropriate rewards and disciplinary measures

- Ensure that staff has been vetted, especially staff in sensitive roles

- Ensure that the organization is not dependent on one individual for any key security task

- Ensure that privacy and intellectual property rights as well as other legal, regulatory, contractual and insurance requirements have been identified with respect to security

- Ensure that security aspects have been considered in all service level agreements and the security competence of the service providers has

been assessed

Ensure that security guidance and contractual obligations for e-commerce and electronic payment exist

Ensure that applicable security measures have been implemented, tested and kept up to date (e.g. back up, access control, virus protection, firewalls, insurance, etc.)

Ensure that archiving, back up, virus protection, firewall and software patch installation and maintenance procedures are followed

Ensure that access control and connectivity rules for internal and external users have been implemented based in business need and risk

Ensure that important computer equipment is safe from theft or damage (e.g. lock computer rooms, take back up tapes offsite, use operating systems with encryption on laptops)

Ensure that security is an integral part of the application development process

Ensure that a business continuity program is established, tested and kept up to date

Ensure that there is a security strategy in place based on risk, gap analysis and performance monitoring

If the bottom line is higher on your priority list than security or reputation, policies 1, 2, 4-6, 11 and 15 can prevent many of your more expensive support incidents. For sample policies or more information, feel free to contact us at 866.926.8746 or contactus@xantrion.com.

===== If you have questions or concerns about your particular situation, please e-mail me at tpsnyder@xantrion.com. I will use your input to direct future columns. =====