Anthelio Healthcare Solutions
Global Information Security Group
Security Awareness Bulletin - Vol. 6

anthelio®

A higher aim. A newer standard.

Data Backup and Recovery - Data Backup Practices

A subject that has recently gained prominence and garnered attention at all levels, from corporate boardrooms to news media outlets (and more importantly in the health care industry) is the importance of having a Data Backup Strategy.

“Is there a data-backup of all the required information and data? How old is the last full data-backup? How quickly can the data be recovered from the data-backup?”

These familiar questions may look elementary but the emerging risk of the new generation malware(s) and variations (including Cryptoware and other Ransomware) has turned the spotlight back on the Data Backup Strategy.

Organizations that subscribed to the “we will do it later” strategy for data-backups have come to realize that it can be a fatal decision. For some healthcare organizations severely impacted by Ransomware threat recently, it was just too late. The urgency and need to implement a sound data-backup strategy and process is now. Experts advocate that the only reliable, fast, cost-effective and secure solution to recover from data loss from malware attack(s) is if the organization had implemented and maintained a sound data-backup solution.

The information security principle of Confidentiality, Integrity and Availability looks to ensure that back-up data is safe, protected and available at time of need, and a well-implemented data-backup strategy plays a key role in supporting this principle. This newsletter provides some common data-backup and recovery practices and suggestions.

DO ✓

- Encrypt the critical data before backup.
- Consider performing a Full Backup of critical data periodically.
- Backup often; a lot can happen in a week/day.
- Keep multiple backup copies.
- Automate and/or set reminders for the backups.
- Verify the backups to make sure files are retrievable.
- Before discarding, securely sanitize or destroy the backups

DON’T

- Wait or postpone the backup of files and data; instead take a little time now to set up the backups.
- Always perform full backup; instead consider incremental backups of critical data more frequently.
- Run backup tasks during business hours; instead consider rescheduling the backup during non-business hours to minimize business impact.
- Ignore or discard backup files that are old and obsolete.
- Assume that backup-data will be corruption-free; instead verify data retrieval procedures periodically.