



Citi-SecureWare Assessment

Anonemis Research
Símenona Martínez
AnonemisResearch.com

Citi-SecureWare Assessment

Determine the company's current framework and structure of cyber-security.

- *What is in place and what needs to be established.* Reviewing any and all information of prior attacks and conducting thorough meeting with IT department and upper management.

Organizing implementation and assessment meeting with the staff.

- Assess company size and employee capabilities to delegate functions in the event a cyber-attack or breach.
- Assess cyber-security knowledge based on testing questionnaire custom to each department.
- Review results.
- Provide a cohesive presentation:
 - Introduction in Office Cybersecurity Procedures
- Provided secure online tutorial custom to each department. Overseen by myself and IT, with brief follow-up meeting for questions.

Prepare cyber-security drill to assess Cyber-Security Breach Response in both, staff and software/hardware. Providing each employee with a skill assessment report, containing improvements needed and/or efficiency not met. Management will receive a more cohesive and detailed evaluation. IT department will receive the overview of this report as it relates to expected duties.

Formulate the best course of action depending upon budget and necessity. Prior research of previous attacks within industry would be incorporated in conceiving a cohesive procedural structure.

Training remotely training to monitor and continually assess staff efficiency will be delegated by a trained IT professional and overseen by cyber-security operations management company.

Routine Management

System will prohibit employees from unlocking computer, accessing the network, if employee has failed to meet required multi-encryptions. Digital signatures and additional encryptions required after executing high-risk actions such as, file and content alterations