Cyber Risk Management Program

Methodology:

The Phoenix 2.0 Cyber Risk Management program is based on The NIST Cybersecurity Framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to manage, prevent, detect, and respond to cyber risk and attacks. For each phase of the framework we have a list of recommended tools, polices, solutions that all organizations should have in place. We derive a risk score of their existing security posture as measured against security industry best practices. All of this is easily turned into a dynamic Cyber-Risk Management Playbook, which in turn rolls up into an organization's Business Continuity Plan

Cybersecurity Framework's five Functions

- Identify
- Protect
- Detect
- Respond
- Recover

Basic best practices:

1. **Identify:** Risk assessment (simulated phishing campaign, e.g. penetration & vulnerability/ethical hacking testing)
2. **Protect**: End-Point Protection (anti-malware engine), Password management & multi-factor auth., device encryption
3. **Detect**: firewall, IPS/IDS Intrusion Detection System
4. **Respond**: Cyber Incident Response Plan, User security awareness training
5. **Recover**: Backups, Cyber Liability coverage