FT.com
FINANCIAL TIMES

A Cyber Security Health Check

If cyber crime was a nation, it would have the world's 27th largest GDP at $445 billion. So how good are your company's controls at preventing, detecting and reacting to this threat? Well, a good start would be to assess your controls against one of the following frameworks:

1) **International Standards Organisation ISO27001 (2013).** This describes 114 controls in 14 categories. Organisations which meet the standard may gain an official certification issued by an independent and accredited certification body on successful completion of a formal audit process.
2) **National Institute for Science & Technology (2014).** The NIST Cybersecurity Framework SP 800-53 offers a set of measurements to assess to what degree an organization has implemented the core activities and benchmark how prepared they are to protect systems against an attack (the "Implementation Tiers"); A "Profile" that can be used to identify opportunities for improving an organization's cyber security posture by comparing a current profile with a target profile.
   Compliance with NIST guidelines has become an accepted defense in the USA against shareholder lawsuits in cases of data breaches.
3) **Cybersecurity Capability Maturity Model (2014).** The C2M2 provides a more detailed, granular and actionable framework than the high level NIST guidelines. The C2M2 is organized into 10 domains, with each being a logical grouping of cybersecurity practices. The Risk Management domain comprises three objectives: Establish Cybersecurity Risk Management Strategy; Manage Cybersecurity Risk; Management Practices
4) **Innovation Value Institute (2015)**. IVI is a non-profit organization based in Ireland. They have created an Information Security Management framework used by hundreds of large companies worldwide to conduct a self-assessment and then compare their scores with other companies. This represents the nearest approach to "benchmarking" available for cyber security.
5) **Critical Security Controls (V5, 2013).** Managed by the Center for Internet Security, these 20 controls are recognized by Law Institutes as providing the basis for compliance with legal requirements.

It could take about a month of effort to calibrate your company against one of these frameworks. That is just the first step in a process that consists of:

(1) Discovery; (2) Results; (3) Interpretation; (4) Interventions

Think of the process like going to your doctor for a health check. The doctor will arrange for a set of lab tests (*discovery*). When the *results* come back, they are meaningless without expert *interpretation*. And then the doctor will recommend *interventions* to take corrective action (medication, exercise…).

The same is true for a cyber security health check. Apply one of the frameworks above for discovery, and you will get hundreds of data points (results). Then it takes an expert to assess the materiality of these findings, and make recommendations for corrective action. The cure is not painless, but it certainly beats a long illness!