Cybermap 360 is very intuitive and should not require too many explanations. To have a good start with Cybermap 360, follow theses steps.

1. Change the admin user

First, make sure you change the admin user password and store it in a safe place. To change the admin password, your must be logged in as the admin (username: admin, password: admin) and you must use the top right menu and select *Change Password*.

In addition to the Admin user, that no one should actually be using, we recommend to have only one other admin user. To avoid issues while defining setup parameters. Future versions will better support multiple admin users.

2. Create users

Create your users through the *Users* setup menu. An *Administrator* can do everything, including managing users and accessing logs. A *Power User* can use all features but managing users and logs. A *Viewer* can consult Cybermap 360, but not make any change.

3. Go through the setup

Go though the different setup menus and configure Cybermap 360 to your needs, especially the data map. We strongly suggest that you create a generic employee's role, and a generic internal employee.

4. Create your providers

Create as many providers as possible upfront, including their employees. We suggest that you create your own IT department as a provider. Create a generic employee for each provider.

5. Enter your systems

Start entering your systems.

Dashboard

The dashboard is based on the Firm Risk Assessment, which is mandatory for each system, and let to your firm's discretion.

Adding a system

Before adding a system to Cybermap 360, first create the Provider, the provider's contacts (employees), as well as your internal employees who have a role (e.g., business stakeholder or IT stakeholder). Then create the new system.

Security assessment

The security assessment measures along five dimensions (level of business continuity readiness, signon method, two factor authentication, data encryption at rest and data encryption in transit), taking into consideration the hosting and criticality of the data and system, if a given system is a low, moderate or high risk system for the firm.

Hacking assessment

The hacking assessment measures the impact if the system would be hacked.

Firm risk assessment

The firm risk assessment is the assessment used for the dashboard and is defined by the firm. It should be done reflecting the results of the security assessment, hacking assessment, and particularities of the system and its setup.

* * * * *

This is the first version of Cybermap 360. We have many more ideas which we are going to develop and launch over the coming months. We are also very happy to read your suggestions, so do not hesitate to contact us at admin@cybermap360.com.