The Way Forward with Cyber Security Target Operating Models

A Plan of Approach for Senior Executives
“Process and People first, THEN Technology” will always be at the heart of the winning formula.

Technology comes in support of a structured set of processes, that enable people to protect the business from cyber threats.

The selection of the necessary TECHNOLOGY products and service providers should come in support of alignment action plans: PROCESS and PEOPLE first, then TECHNOLOGY.
**OBJECTIVE:**
Assess the strengths and weaknesses of the current cyber security operating model situation

Engaging with all stakeholders and getting them onboard from the start is key, as going forward THEY will have to live the values of the TOM and make it happen in real life.
The TOM Design Phase

OBJECTIVES:

- Produce a high-level description of the cyber security operational PROCESSES which need to be in place across the organisation
- Validate the new TOM with key senior stakeholders

Keep things simple and achievable: Simplicity, clarity and transparency of objectives are always the best success factors in any new operating model initiative

Three Key Steps

- Building the new TOM from expectations and requirements of key stakeholders
- Iterating with the sponsor and key stakeholders through workshops
- Estimating the costs involved in delivering & operating the new TOM

As collected as part of the DISCOVERY phase

Compared to the current cyber security cost base
The Organisational Model Design & Implementation Phase

OBJECTIVES:

Produce a set of specific roles and role descriptions
AND an overall RACI mapping detailing specific accountabilities and responsibilities
for all the PEOPLE involved in the delivery of the TOM.

Validate the new organisational model with key senior stakeholders including HR

Involve HR throughout and communicate around organisational changes with staff in line with internal practices and policies, and ONLY when sufficient endorsement has been obtained from HR, stakeholders and other parties
The Execution Phase

OBJECTIVES:
Ensure that the new Leadership team - resulting from the new organisational model - brings its cyber security practices in line with the new TOM

The selection of the necessary TECHNOLOGY products and service providers should come in support of alignment action plans: PROCESS and PEOPLE first, then TECHNOLOGY

Three Key Steps

- Defining action plans to deliver on the actual process content of the TOM
- Sequencing of the required TOM alignment work across the different teams
- Selecting and evaluating technology platforms and service providers

To avoid conflicts, work duplication and adverse dependencies, in line with budgetary resources potentially available during the current financial year and the following ones

This is a task for the new leadership structure resulting from the new organisational model, for each of their practice area

As identified by the new leadership structure resulting from the new organisational model in support the delivery of the content of the TOM
Summary of Key Points

- Technology comes last, not first,
- It comes in support of alignment plans and new process and organisational structures

- Process is key and comes first; that’s the backbone of the TOM
- Security Processes need to align with stakeholders expectations and the objectives of the business at large around cyber security

- Focus on clear, consistent, realistic role descriptions and RACI model aligned to Security Processes
- Involve key stakeholders throughout, including HR and the relevant employees representatives where necessary
Please be in touch to discuss further

jcgaillard@corixpartners.com
+44 (0) 7733 001 530
www.corixpartners.com
@Corix_JC
@CorixPartners