Davide Zanetti, ABB / Jano Bermudes, KPMG

How do you know if you are doing enough?
It all started with a simple question …
… by a board member

“Are we doing enough and are we moving fast enough?”
Understanding the environment

A bit of ABB terminology

Internal (i.e. IT Security)

Protecting ABB IT infrastructure against unauthorized access, computer based threats and attacks

External (i.e. Cyber Security)

Helping ABB customers protect their assets (e.g. energy networks or automation plants) against unauthorized access, computer based threats and attacks

Our focus
Defining the scope

Life cycle

Product
- Design, Implementation, Verification, Release, Support

Project
- Design, Engineering, FAT, Commissioning, SAT

Plant
- Operation, Maintenance, Review, Upgrade, Services

Areas

- Organization
  - Structure, staffing, setup, funding

- Governance
  - Mandate, reporting, leadership

- Content and subject matter
  - Policies, guidelines, standards, support

- Internal services
  - Awareness, training, tools, consulting

- Global roll-out & implementation
  - Staffing, compliance, maturity, technology

Focus on the foundation
Cyber Security does not exist by or for itself - a solid business context is key for success!
Methodology

The biggest risk in 2016

1. The **threats are changing** as technology and know how opens up new criminal opportunities

2. Existing **threat actors are constantly changing** their attack techniques to keep ahead of the game

3. The **full extent of attacks is unknown**; often unknown even to the victims, leading to a confused and confusing media picture

4. Like any risk, there is **no complete solution**; only varying degrees of risk reduction

5. The **landscape is constantly changing**; convergence to enable cloud and analytics means connectivity, exposing previously isolated assets to a wider set of threats.

This is a “wicked” problem – **the biggest issue is a business problem**, that you spend in the wrong areas and fail to reduce your risk profile.
Methodology
The spiral of waste
Methodology
The gravity intrinsic within the spiral

LACK OF CONTINUOUS ASSURANCE means capability isn’t sustained

POOR UNDERSTANDING (assets, intelligence, regulatory etc) leads to over controlled low risk assets

INADEQUATE GOVERNANCE STRUCTURE leads to poor decision making

LACK OF OWNERSHIP and accountability leads to ad hoc and incomplete capability insertion

TACTICAL STICKING PLASTER + New Incident = Requirement for New Sticking Plaster

‘GOLF COURSE’ CONVERSATIONS leads to Board solutioneering directing technology based Interventions

SECURITY PROGRAMME uncovers issues wherever it looks, that challenge priorities

INSUFFICIENT RISK DEFINITION causes tactical incidents to overtake larger and more strategic mitigations

POOR BUSINESS UNDERSTANDING leads to broken capability when business changes

NO OBJECTIVE JUSTIFICATION for plans causes priorities to be reset ‘on the fly’

CONFIDENCE IN SECURITY PLANS UNDERMINED by each tactical incident-driven change

LACK OF CONTINUOUS ASSURANCE means capability isn’t sustained

POOR UNDERSTANDING (assets, intelligence, regulatory etc) leads to over controlled low risk assets

INADEQUATE GOVERNANCE STRUCTURE leads to poor decision making

LACK OF OWNERSHIP and accountability leads to ad hoc and incomplete capability insertion

TACTICAL STICKING PLASTER + New Incident = Requirement for New Sticking Plaster

‘GOLF COURSE’ CONVERSATIONS leads to Board solutioneering directing technology based Interventions

SECURITY PROGRAMME uncovers issues wherever it looks, that challenge priorities

INSUFFICIENT RISK DEFINITION causes tactical incidents to overtake larger and more strategic mitigations

POOR BUSINESS UNDERSTANDING leads to broken capability when business changes

NO OBJECTIVE JUSTIFICATION for plans causes priorities to be reset ‘on the fly’

CONFIDENCE IN SECURITY PLANS UNDERMINED by each tactical incident-driven change
As engineers we need to need to “earn the right” to talk about People, Process & Technology:

1. **Understand business strategy** and objectives
2. **Cyber** security strategy alignment to business objectives
3. **Ensure solid foundational aspects** e.g. funding and sponsorship
4. **Prioritize delivery and control** e.g. people, change and risk management
Methodology
Tailoring to specific needs

<table>
<thead>
<tr>
<th>Domain</th>
<th>Focus Area</th>
<th>Key Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic Direction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advisory Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Model</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Methodology

## Tailoring to specific needs

<table>
<thead>
<tr>
<th>Domain</th>
<th>Focus Area</th>
<th>Key Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic Direction</td>
<td>Maturity</td>
<td>Alignment to business</td>
</tr>
<tr>
<td>Governance Services</td>
<td>Policy framework</td>
<td></td>
</tr>
<tr>
<td>Advisory Services</td>
<td></td>
<td>Direction and support from leadership</td>
</tr>
<tr>
<td>Operating Model</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Methodology
Tailoring to specific needs

<table>
<thead>
<tr>
<th>Domain</th>
<th>Focus Area</th>
<th>Key Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic Direction</td>
<td>Maturity</td>
<td>Cyber security strategy</td>
</tr>
<tr>
<td>Governance Services</td>
<td>Alignment to business</td>
<td>Communication</td>
</tr>
<tr>
<td>Advisory Services</td>
<td>Policy framework</td>
<td>Procedures and standards</td>
</tr>
<tr>
<td>Operating Model</td>
<td>Direction and support from leadership</td>
<td>Communication Coverage</td>
</tr>
</tbody>
</table>
## Methodology
### Making it measurable

<table>
<thead>
<tr>
<th>Score</th>
<th>Tagline</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Non existent</td>
<td>Missing <strong>all</strong> the key components necessary for particular focus area.</td>
</tr>
<tr>
<td>1</td>
<td>Partial</td>
<td>Missing <strong>one or more</strong> key components necessary for the particular focus area.</td>
</tr>
<tr>
<td>2</td>
<td>Defined</td>
<td><strong>All</strong> key components for the particular focus area are defined or implemented to some degree. But, at least <strong>one is not mature</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Established</td>
<td>All key components for the particular focus area are defined or implemented; <strong>all are mature</strong> (e.g. evidence of well-defined and standardized processes are in place to support the implementation of all key components).</td>
</tr>
<tr>
<td>4</td>
<td>Adaptive</td>
<td>All key components for the particular focus area are defined or implemented; all are mature and **for each key component a process to maintain the maturity level over time is in place.</td>
</tr>
</tbody>
</table>
# Methodology

Making it measurable and **repeatable**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Focus area</th>
<th>Key component</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strategic Direction</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maturity</td>
<td>Cyber security strategy</td>
<td>• Documented assessments of the challenges that the strategy sets out to deal with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Guiding policy that specifies the approach to dealing with the obstacles called out in the diagnosis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Action plan that includes resource commitments, funding structure and target timelines and deliverables designed to carry out the guiding policy.</td>
</tr>
<tr>
<td>Communication</td>
<td></td>
<td>• Documented plan that identifies stakeholders types needs/challenges</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Identified appropriate communication channels</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Articulated timelines, resource participation requirements and some form of measurement of effectiveness</td>
</tr>
<tr>
<td></td>
<td>Procedures and standards</td>
<td>A set of guidelines, procedures and standards that explain what needs to be done and supports how implementation needs to be performed. Includes measurement of risk and compliance and translates cyber risk into business terms such as financial or brand impact.</td>
</tr>
<tr>
<td>Policy framework</td>
<td>Communication</td>
<td>A documented communication strategy for the dissemination of the policy framework is available. The communication strategy includes at least:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• identification of stakeholders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• definition of channels of communication to reach the target audience</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• a cohesive plan to disseminate information</td>
</tr>
<tr>
<td>Coverage</td>
<td></td>
<td>Based on risk assessment by appropriately skilled individuals, business needs analysis and outside sources of intelligence on threats.</td>
</tr>
</tbody>
</table>
Assessing the current status
“How we did it”

1. **Internal stakeholder review**
   - ~100 interviews
   - All levels in the organization
   - Global footprint
   - Cross-functional
   - Fair representation of the business (e.g. mature and less mature)
   - **Full access provided to external experts**

2. **Document review**
   - Cyber security policies, standards, guidelines etc.
   - Business documents
   - **Full access provided to external experts**

3. **External stakeholder review**
   - Direct through customer discussions
   - Indirect through expertise and know-how of external experts
Charts are good but what do they mean for management?

Need to use business language that is relevant for senior leadership, e.g.:

- Smarter deployment of organizational resources (“cost”)
- Reduced costs for poor quality
- Increased productivity

Bring the discussion back to the board room
1. **Cyber** security is best as a business **enabler and not a gate keeper**. Leave that to audit!

2. Having a mature cyber security capability is not about having the highest castle walls the deepest moats or the biggest bazooka, it is about having:
   - Visibility
   - Control
   - Agility

3. We do this by adapting our overall approach to cyber to be:
   - Risk based
   - Decision focused and integrated
   - Linked to business imperatives
   - Cost appropriate

4. As engineers we need to “**earn the right**” to talk people, process and technology by first understanding and aligning to the business
Power and productivity for a better world™