Dr. Markus Braendle, Head of Cyber Security, ABB Group

10 Steps on the Road to a Successful Cyber Security Program

Asia Pacific ICS Security SUMMIT
A global leader in power and automation technologies
Leading market positions in main businesses

- 145,000 employees in about 100 countries
- $39 billion in revenue (2012)
- Formed in 1988 merger of Swiss and Swedish engineering companies
- Predecessors founded in 1883 and 1891
- Publicly owned company with head office in Switzerland
Just to be clear …
A bit of ABB terminology

**Internal (i.e. IT Security)**
Protecting ABB IT infrastructure against unauthorized access, computer based threats and attacks

Responsibility of Group Function Information Systems (GF-IS)

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

Responsibility of Group Cyber Security Council and ABB Business
1. Management support

How do you get top management involved?
- Use FUD*?
- Show how easy “it” is?
- Talk about APT**, threats & vulnerabilities?
- Talk about technology & solutions?

... might get them to listen **but** not get them involved, **better**
- Show why cyber security is directly relevant to them, their business, their customers, their targets, ....
- Linking cyber security to company strategy
- Talk about the real, non-technical consequences

A hacker could exploit the 0day, elevate his privileges and then own the system

VS.

We would loose operational control and would have to stop production

---

* Fear Uncertainty and Doubt
** Advanced Persistent Threat
1. Management support
ABB example: linking cyber security to the ABB strategy

Show how cyber security connects to company strategy!

2015 Strategy overview
Strategy for the next 3 years – We will...

1. Drive competitiveness
   and stay relevant in our current markets
   - Continue to drive cost and quality competitiveness
   - Invest in technology leadership
   - Efficient use of assets: cash, people, IP & brand
   - People development: and investment

2. Capitalize on mega trends
3. Aggressively expand core business
4. Disciplined M&A
5. Exploit disruptive opportunities

Source: ABB Capital Markets Day
ABB recognizes the importance of cyber security in control-based systems and solutions for infrastructure and industry, and is working closely with our customers to address the new challenges.

Ulrich Spiesshofer, CEO ABB
2. Cross-functional teams
It’s not just about “IT security”

Cyber security is

- **not** an isolated topic
- **not** just about technology
- **not** something that “cyber ninjas” can take care of
- **not** either OT or IT

... so why do we treat it that way?

Cyber security is very broad in scope and requires teams that cover **all** aspects, e.g.:

- Human resources
- Legal
- Quality
- Technology
2. Cross-functional teams
ABB example: Group Cyber Security Council

- Formally established organization at group level
- Covering all aspect of cyber security
- Reporting to ABB EC members, ABB CIO, business unit managers and senior R&D management
3. People, Awareness, & Training

Might be the most important piece in the entire puzzle but more on this tomorrow:

- **Dream Team: Building the Perfect ICS Team**
  Tuesday 9:00 – 9:45

- **Going Global: Global ICS Professional Certification**
  Tuesday 16:15 – 17:00
Different awareness programs and trainings depending on roles

- General IT security awareness program for all employees
- General and specific training for developers
- General and specific training for engineers
- Customers
- …

3. People, Awareness, & Training

ABB example: ABB university
4. Integration into the entire lifecycle

Cyber security
- is not a “do-once-activity”
  
  "Security is a process, not a product” Bruce Schneier

- is not just relevant at a single point in the lifecycle
- should be integrated into the entire lifecycle

→ Effective cyber security program should thus consider the entire lifecycle (also those parts that are outside your direct responsibility)
5. Long term targets & short term goals

Building up a cyber security program is very complex and takes time
- You won’t solve all your problems in one iteration

A good security program should have clear long term targets broken down into small goals

Both long term targets and small goals must be clearly communicated

Use a maturity model / security level approach, e.g.
- NIST Cybersecurity Framework
- ISA / IEC 62443
- Building Security In Maturity Model (BSIMM)
- OpenSAMM

Will this address the APT risk? vs. Will this improve our situation?
5. Long term targets & short term goals
ABB example: Security Development Lifecycle

Inspired by Microsoft SDL but tailored to our environment
- Start with most important elements that can be implemented “quickly”

Combination of mandatory and advanced requirements
- All units must fulfill mandatory requirements
- Many units also already fulfill advanced ones

Implementation according to multi-year roadmap
- Advanced requirements become mandatory
- New requirements are introduced

Example: Minimum Cyber Security Product Requirements
- Must be fulfilled by all products
- Set a minimum baseline
- Not perfect but provide a solid foundation
- Exceeded by many products
6. Finding the right balance

- Security vs. cost
- Change
- Own capabilities vs. external expectations

A “perfect” plan will fail without the right balance!
7. Be prepared to respond

Everyone agrees that there is no such thing as 100% security but we still seem to struggle when things go wrong

→ Need for a more humble approach

1. Accept that things will go wrong
   - Vendors: someone will find a vulnerability in your product!
   - Asset owners: someone will hack into your systems!

2. Develop and document plans, processes and policies
   (Get management support & involve e.g. legal, communications, etc.)

3. Exercise those plans, processes or policies

4. Follow your plans, processes and policies

5. Update your plans, process and policies

[1 – 5] Communicate
   - expectations & needs (prior)
   - request help & inform others (during)
   - Information, resolutions, or lessons learned (after)

All of us need to do much better here!
7. Be prepared to respond
ABB examples

Patch Management: documented and executed processes

Vulnerability Handling: mandatory policy

Participation in external exercises
- Cyber Storm III
- GridEx I & II
8. Test, review, validate & verify

**Everything** should be tested **regularly** by **everyone**!

- What: People, Processes & Technology
- Who: Suppliers, Integrators, Asset owners, Service providers, etc.
8. Test, review, validate & verify

ABB example: Device Security Assurance Center

- Formally established and independent security test center
- Leveraging state-of-the-art open source, commercial and proprietary robustness and vulnerability analysis tools
- Close collaboration with ABB developers providing in-depth analysis and recommendations
- First vendor lab to be accredited by Wurldtech
9. Investment into the future

- Easy to get caught up in everyday problems
- Cyber security environment keeps changing very fast
- Importance of IT and software will increase
  - Use of COTS components
  - Cloud based offerings
  - Wireless technologies
  - Mobile devices
  - ...

→ Cyber security should become part of research initiatives
  - Industry: internal research organizations
  - Academia: new areas of research
  - Governments: funded research programs
9. Investment into the future

ABB Example: Corporate Research

- Develops forward-looking cyber security concepts and technology
  - Authentication, remote access, security monitoring, security engineering, product/system security assessments, tracking market trends, ...
- Evaluates security relevant technologies
- Adapts enterprise security to industrial control systems context

Energy Department Announces New Investments of Over $30 Million to Better Protect the Nation’s Critical Infrastructure from Cyber Attack

**ABB, Inc. – Cary, NC**

ABB will develop a system that allows substation devices to work together to validate the integrity of communications, such as commands to change a protective relay’s configuration, and assess the potential impact on grid operations.
Collaborations, partnerships and information exchange are a **must** for effective cyber security solutions

- Open discussions and involvement between different stakeholders (requires a certain level of trust)
- International standardization efforts (e.g. ISA S99)
- Information exchange initiatives (CPNI.NL, ICSJWG)
- Involvement of “IT” companies (e.g. telecommunication)
- ...
Summary & Conclusions

1. Management support
2. Cross functional teams
3. People, awareness & training
4. Integration into the entire lifecycle
5. Long term targets & short term goals
6. Finding the right balance
7. Be prepared to respond
8. Test, review, validate & verify
9. Investment into the future
10. Collaboration

Are just 10 steps in a very long journey …
your journey might look very different …
Contact information
Questions, Comments, etc.

cybersecurity@ch.abb.com

www.abb.com/cybersecurity
Power and productivity for a better world™