Committee on Critical Infrastructure
Committee on Critical Infrastructure and Task Force on Innovation and Cybersecurity – Exploring the Relationship Between New Technology and New Risks
Cyber Security in a Connected Grid

S&C Electric Company
S&C Products and Applications

Overhead Distribution

Underground Distribution

Automation and Grid Control

Energy Storage Systems

Microgrid Controls

Substations

Global Services
Computers and Communications

- Overhead Distribution
- Underground Distribution
- Automation and Grid Control
- Global Services
- Energy Storage Systems
- Microgrid Controls
FPL Grid Recovers in 4 days!
SMART Devices are just like Computers on a Network

PROTECT
Secure Platform
Secure Communications

DETECT
Secure User Access
Monitoring and Logging

RECOVER
Patch Management
Secure Backup
If we can beat this....

We can beat this....
Innovation and Cybersecurity

Steven Martin – VP, CDO
@martin_stevenb

Confidential. Not to be copied, distributed, or reproduced without prior approval.
How did I end up here?

\[ y^2 = x^3 + ax + b \]
86% Renewables Additions
18% Intermittent Power
8 GW Coal Plant Closures
€104n Asset Write Downs
2.5 BN Urbanizing

40 M Electric Cars

50% Less CO₂

32 GW Prosumer DERs

Peer2Peer

Vehicle2Grid

Energy Efficiency

MicroGrid

Beyond the Electron
Cloud computing - lessons learned

1. The internet will always win
2. The myth of non-connected security
3. Beware the keyboard and the seat
4. Hack yourself
The Next Generation of Grid Software

1. Seamlessly manage Transmission <-> Distribution
2. Hierarchical by design
3. Consume additional inputs
4. Micro-optimization
5. Energy generation + storage in single layer
6. Multiple deployment options

Solutions for the next 25 years
Grid Automation
Cyber security, situational awareness and resilience

Joe Doetzl, Cyber Security Practice Leader, ABB Grid Automation
Important notices

This presentation includes forward-looking information and statements including statements concerning the outlook for our businesses. These statements are based on current expectations, estimates and projections about the factors that may affect our future performance, including global economic conditions, and the economic conditions of the regions and industries that are major markets for ABB Ltd. These expectations, estimates and projections are generally identifiable by statements containing words such as “expects,” “believes,” “estimates,” “targets,” “plans,” “outlook” or similar expressions.

There are numerous risks and uncertainties, many of which are beyond our control, that could cause our actual results to differ materially from the forward-looking information and statements made in this presentation and which could affect our ability to achieve any or all of our stated targets. The important factors that could cause such differences include, among others:

- business risks associated with the volatile global economic environment and political conditions
- costs associated with compliance activities
- market acceptance of new products and services
- changes in governmental regulations and currency exchange rates, and
- such other factors as may be discussed from time to time in ABB Ltd's filings with the U.S. Securities and Exchange Commission, including its Annual Reports on Form 20-F.

Although ABB Ltd believes that its expectations reflected in any such forward-looking statement are based upon reasonable assumptions, it can give no assurance that those expectations will be achieved.

This presentation contains non-GAAP measures of performance. Definitions of these measures and reconciliations between these measures and their US GAAP counterparts can be found in the ‘Supplemental reconciliations and definitions’ section of “Financial Information” under “Quarterly results and annual reports” on our website at www.abb.com/investorrelations
Addressing the IoT Security Gap
THE ISOLATED ENTERPRISE
RISK FROM THE IoT SECURITY GAP IS EXPLODING

- 24B
  24 BILLION
  INTERNET
  CONNECTED
  DEVICES BY
  2020.

- 25%
  BY 2020, MORE
  THAN 25% OF
  ENTERPRISE ATTACKS
  WILL INVOLVE
  IoT DEVICES.

- 92%
  CONNECTED
  DEVICE THREATS
  WILL BE A MAJOR
  SECURITY ISSUE
  IN 2017.
Security = $\frac{1}{\text{Convenience}}$

Market forces dominate sound security principles
Mission: To Find and Distribute what is Valuable and Trusted
THANK YOU
Committee on Critical Infrastructure