TCIPG

ANNUAL INDUSTRY WORKSHOP
NOVEMBER 12-13, 2014

Challenges of Cyber Security Economics in Distribution Systems

Industry Panel

November 12, 2014

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

Please Note

- Where a specific IBM product or service is mentioned, IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

- The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

Economics Depend on Goal

- Security is the Bond Between Digital and Reality

- Malware is a Software Terrorist
  - So apply DHS principles
    - Avoid fragmented security
    - Recognize increased attack surfaces
  - Resulting in
    - Monitor and distill information
    - Correlate and predict threats
    - Take adaptive and pre-emptive approach
- It is not all cyber

Energy and utilities attacks – impact scenarios

Reliability impacts

a potential brown/black out of a large geographical area/or concentrated at an area where other critical infrastructures depend on power, water treatment plants, transportation centers, etc.

Safety impacts

potential harms to utility personnel and/or customers - re-energize systems where maintenance crews are deployed or exploding transformers with hazardous waste

Productivity impacts

Risks to utilities' capacity, delivery and overall ability to provide a consistent product/service to their customer base

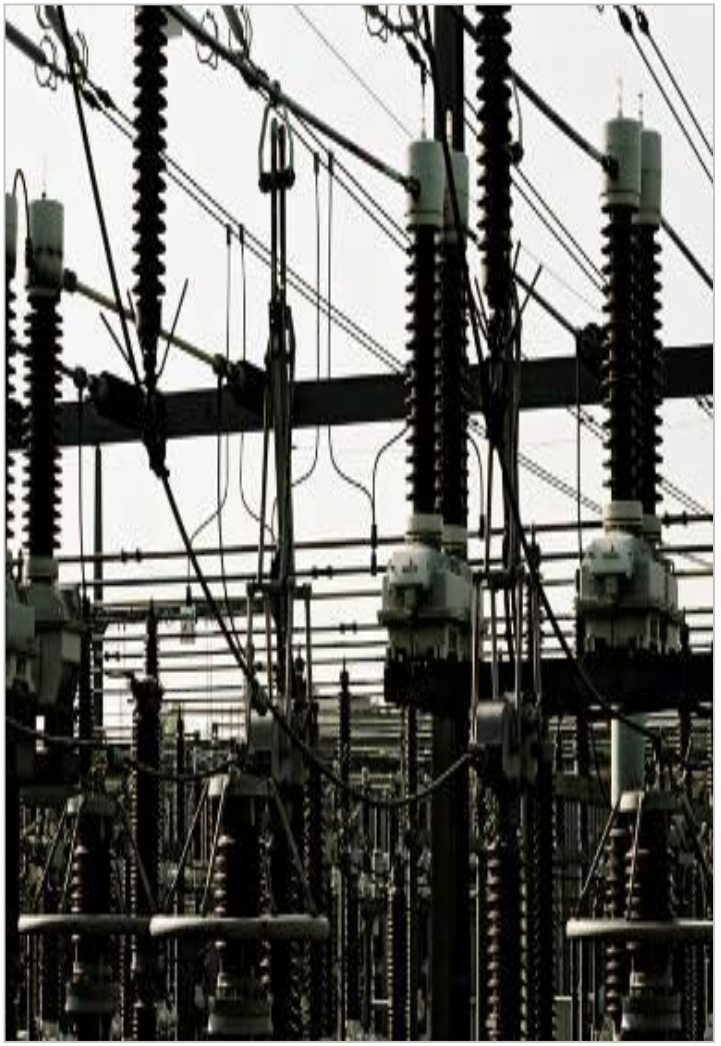
Reputation impacts

exposure of sensitive customer data (e.g., usage info, SSN, credit card, etc.) - extraction of such data, including union employee healthcare data

The balance of risk for energy and utilities organizations is unique, economics of scale and operational capability are real challenges if *"End to End Cyber Security"* is your mandate for distribution networks

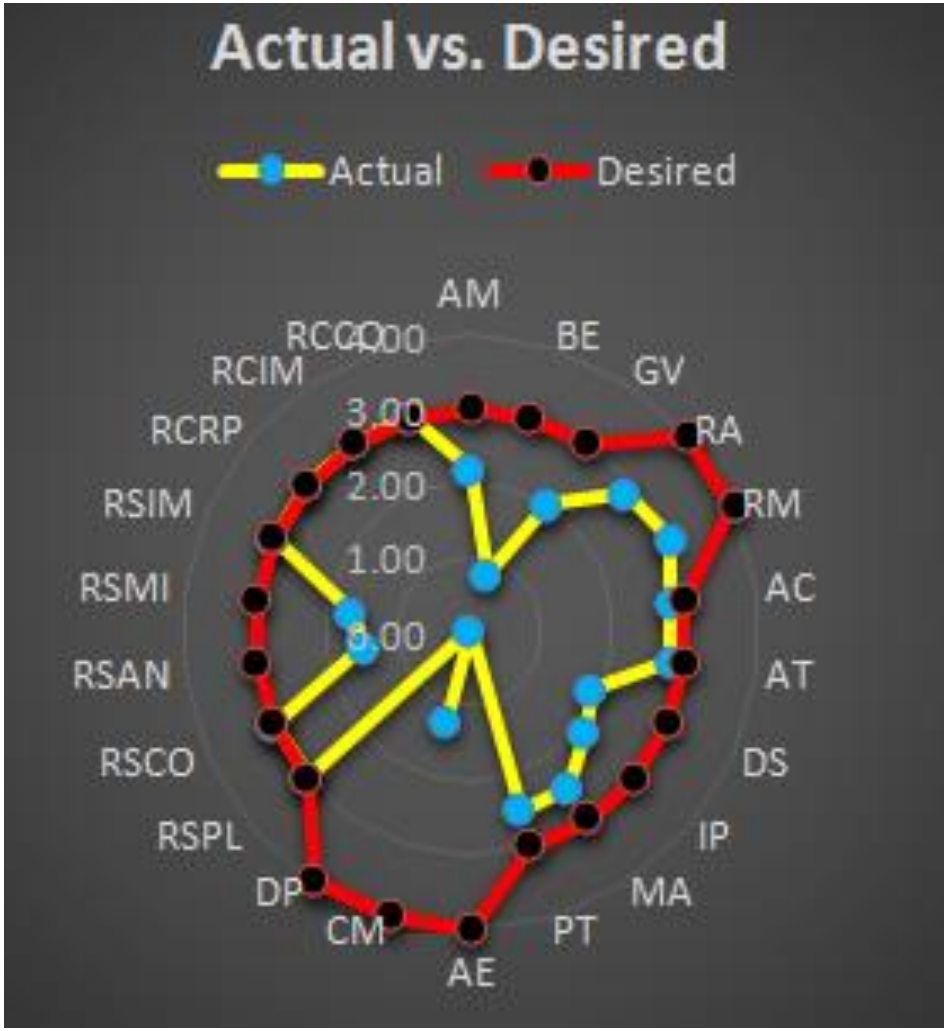
Challenges are not unique to North America

- A Government initiative in the Middle East has a goal of a secure 2020 Smart City grid
- A Utility is considered National Critical Infrastructure
- Scope of Smart City program has 500 transmission stations and 22,000 distribution substations to secure, requiring a threat and risk management approach as numbers and scale too large for a traditional approach.
- Security capability, maturity and threat modeling in use.



NIST CSF Distribution Maturity Roadmap

- Current state of distribution systems and threat modeling show gaps and opportunities for investments in:
  - Cyber security governance (BE)
  - Anomalies and Events (AE)
  - Continuous Monitoring (CM)
  - Detection Processes & Procedures (DP)
  - Respond Analysis (RSAN)
  - Respond Mitigation (RSMI)
- While threat modeling warranted investment into substation and device hardening, increased monitoring and response showed greatest benefits



From NIST CSF v 1.0 of 2-12-14, Appendix A, table 1

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify		
ID.AM	Asset Management		
ID.BE	Business Environment		
ID.GV	Governance		
ID.RA	Risk Assessment		
ID.RM	Risk Management Strategy		
PR	Protect		
PR.AC	Access Control		
PR.AT	Awareness and Training		
PR.DS	Data Security		
PR.IP	Information Protection Processes and Procedures		
PR.MA	Maintenance		
PR.PT	Protective Technology		
DE	Detect		
DE.AE	Anomalies and Events		
DE.CM	Security Continuous Monitoring		
DE.DP	Detection Processes		
RS	Respond		
RS.RP	Response Planning		
RS.CO	Communications		
RS.AN	Analysis		
RS.MI	Mitigation		
RS.IM	Improvements		
RC	Recover		
RC.RP	Recovery Planning		
RC.IM	Improvements		
RC.CO	Communications		

Acknowledgements and Disclaimers

Availability. References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates.

The workshops, sessions and materials have been prepared by IBM or the session speakers and reflect their own views. They are provided for informational purposes only, and are neither intended to, nor shall have the effect of being, legal or other guidance or advice to any participant. While efforts were made to verify the completeness and accuracy of the information contained in this presentation, it is provided AS-IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this presentation or any other materials. Nothing contained in this presentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

— Please update paragraph below for the particular product or family brand trademarks you mention such as Web Sphere, DB2,Maximo, Clear Case, Lotus, etc.

IBM, the IBM logo, ibm.com, [IBM Brand, if trademarked], and [IBM Product, if trademarked] are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or TM), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at

•"Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

•If you have mentioned trademarks that are not from IBM, please update and add the following lines:[Insert any special 3rd party trademark names/attributions here]

•Other company, product, or service names may be trademarks or service marks of others.