19 March 2013

From: Steve Dougherty and Andy Bochman, both of IBM

Subject: Suggestions for Business-Oriented Security Metrics for Utilities

To: NIST for its initiative - Framework for Reducing Cyber Risks to Critical Infrastructure

## I. Introduction

In order to run cybersecurity as a true enterprise function, management needs a framework, such as one NIST is developing here, with which to establish a baseline for current security programs, understand the context and critical interdependencies, and set priorities accordingly. The framework also is used to identify gaps and monitor progress in filling them, and achieve other strategic security objectives while ensuring security programs are fully coordinated with the utility's core business objectives and initiatives.

Frameworks and maturity models can help organizations identify their strengths and weaknesses and compare them against current industry best practices. Such approaches are widely used to improve performance, efficiency and quality.

Utilities' business and organizational structures vary widely, and not all frameworks, maturity models or metrics will be appropriate. To account for the unique requirements of individual utilities, some customization is required. When new cyber security metrics are being considered, there are three characteristics IBM considers essential for the metrics to be of maximum value to senior utility leadership. Cyber security metrics must be:

1. Easy to obtain - with no expensive tools or overly labor-intensive processes needed to acquire data.
2. Easy to understand - so a business person can easily understand the connection between what is being measured and what it indicates about the organization's risk management, reliability, safety or other performance objectives
3. Easy to share - such that the information gathered should not be so sensitive that it can't be shared among internal organizations and depending on the metrics, outside the utility with oversight and stakeholder organizations

Below find high-level structural elements we're suggesting, in conjunction with  could form the basis for the development of metrics to help utilities baseline their current security postures, identify relative strengths and weaknesses, and then roadmap to desired future states with demonstrable improvements.

## II. Security Measurement Prerequisites/Preliminary Steps

1. Identify your key / most critical business processes
2. Understand the threat scenarios to those processes
3. Identify the key controls for the threats to those processes
4. Once you have that these things, then you can establish what you to measure

## III. Initial Security Metrics Categories

Organization and People
Data
Applications
Infrastructure
Security Situational Awareness
Resilience

**IV. People and Organization**

Is there a security governance board?
What is highest ranking person in company with security in their title and ...
Do they have authority to set and enforce security policy enterprise-wide
% completing refresher training course
# or % phishing events (how many employees clicked on dangerous links)
% of key employees using social media and/or portable media BYOD devices
Help Desk stats/measures - Security related tickets called in such as:
-- # of locked/forgotten password/malware infection
-- # of tickets resolved
-- # of tickets still open and under investigation

**V. Data**

% critical databases protected
% total databases protected
Data loss related incidents:
-- # of lost/stolen devices (e.g., unencrypted laptops, smart phones, USB drives)
-- # of unauthorized data disclosures
-- # of data loss near misses
% of system administrators with access to root or PII information without audit capabilities

**VI. Applications**

Does the company have a current inventory of all the applications (built and bought) it depends on
Access controls:
-- # of applications using multi-factor authentication
-- # applications using web security (HTTPS, TLS-SSL)
% applications in portfolio scanned for security vulnerabilities in year
of apps scanned, avg # of high severity vulnerabilities per million lines of code
time between application vulnerability awareness and patching

**VII. Infrastructure**

IT/OT downtime for planned security updates
IT/OT downtime for unplanned security tasks
# of infected PCs, phones, meters, etc. detected and cleansed
time between system vulnerability notice and patching or mitigation

**VIII. Security Situational Awareness**

% of critical IT/OT systems instrumented ... logs being continuously analyzed
% of network segments protected by firewalls and IDS/IPS
% up-time and availability of network against DDoS and other network attacks
# of ICS/CERT alerts relevant to client

**IX. Resilience**

# of security and / or privacy breach exercises per year

Performance of teams re: incident response, rapid recovery, forensics, etc.

Maturity capability rating of people, processes and technologies performing the key controls for both of the above

# of critical servers/databases with root password and key escrow and without

Contact Info:


Andy Bochman
Energy Security Lead, IBM
bochman@us.ibm.com
+1 781-962-6845

Steven Dougherty
Global Cyber Security Leader, IBM
sdougherty@us.ibm.com
+1 916-849-1954