



# National Electric Sector Cybersecurity Organization

TOWN HALL

August 17, 2011

## Measurable Security

Post Event Overview

A considerable amount of money and time are being expended by utilities on efforts to improve security and comply with related regulatory mandates. The town hall discussion focused on the functional and financial measurements that are needed to effectively measure the cost, benefit, and efficacy of those security efforts.

### The Security Landscape

The National Electric Sector Cybersecurity Organization partnered with IANS Research to conduct a security benchmarking study, the results of which were used to kick-off the town hall discussion. The study revealed that security spending is trending up slightly while spending on compliance to the North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards is trending up sharply. This was not a surprise to most of the attendees. The study also suggested that most companies were converting existing security staff over to CIP compliance efforts rather than hiring new staff. This was also confirmed by the asset owners in the room (*full results of the study are available on the EnergySec wiki - see link at the end of this summary*).

*“What we are trying to accomplish is elusive - it is a bit like eating soup with chopsticks”*

In trying to further establish the landscape, Moderator Brandon Dunlap (Brightfly) asked the question *“Is this the new normal - or is history simply repeating itself?”* He referenced an interesting video discussion on the topic from Agovia Consulting [http://www.youtube.com/watch?v=9sgU-3uu\\_Sg&feature=player\\_embedded](http://www.youtube.com/watch?v=9sgU-3uu_Sg&feature=player_embedded)

### Why we need Security Metrics

If our job as security practitioners is not to protect the company, but rather to facilitate better risk decisions, then the question becomes *“How do we improve the quality of the decision support we provide?”* Risk is cumulative. As our networks get more complex and our risk goes up, so should the level of supporting data for those risk decisions.

*“As security practitioners our job isn't to protect the company, but rather to facilitate better risk decisions”*

The electric sector is overflowing with metrics related to operations but when it comes to security the industry is struggling. According to Brent Rowe (RTI International) the industry is missing key data and seems to struggle with knowing the difference between good and bad data. If companies rely too heavily on the wrong data to make important decisions it can actually be worse than having no data at all.

### What Metrics Do and Don't Tell Us

Metrics really aren't about numbers; rather, they are about increasing knowledge and creating awareness. The number is almost never what you are looking for. What you are really looking for are the insights that you discover along the way while you are looking for the numbers. Numbers by themselves don't offer much value.

*“The number is almost never what you are looking for. What you are really looking for are the insights that you discover along the way while you are looking for the numbers”*

One thing metrics cannot tell us is exactly how secure we are today versus tomorrow. Security just doesn't work that way. But, metrics can tell

us about changes and trends which in turn allows us to make better risk decisions.

### **The Mechanics of a Metric**

A good metric helps to sift through mountains of data, extract the points of significance, and summarize them in a meaningful way. A metric should not be designed to “keep score”. Too often people are focusing on the number. To use a sports analogy, metrics should not be about tracking wins vs. losses but rather they should measure how good we are at playing the game.

*“It’s not whether you won or lost. It’s about how well you played.”*

Value is created when data is parsed in a significant way, analyzed, and then monitored and trended over time. The experts in the room all agreed that the foundation of creating a good metric is asking the right kinds of questions. Good questions help to ensure that the metrics measure the right things. If metrics will be used

*“Vulnerability management is almost a hygiene issue. Figuring out what people are actually trying to do is where it starts to get interesting.”*

to determine spending and staffing levels then they need to reflect trends that will support appropriate levels of spending and staffing. Focusing on what kinds of decisions the metric needs to support is important to consider in the design.

One of the suggestions from Mike Hamilton (City of Seattle) was to look for security metrics that help you to determine intent.

The number of desktop spam malware removed every month may be useful, but determining that there had been an increase in key-logger malware found is likely more significant. Monitoring network traffic for any attack is important, but sifting through that traffic to find potential targeted attacks is more important. Using metrics to monitor the state of your network provides you awareness, and lends support to risk decisions.

Cyber security is a very fast paced discipline. Thus metrics must reflect how quickly things change. It is critical to respect the element of

time and somehow represent it in each metric we develop.

### **How to Choose a Metric**

The number of metrics to choose from is limited only by imagination. Some that we discussed include: cost per incident, severity of incidents, recovery time, level of spending, compliance, efficiency and reliability to name a few. Determining which one is the right one in a given situation can be challenging at best. Reliability and spending were discussed at length so they are included here.

#### Reliability as a Metric

Reliability as a metric received quite a bit of air time. It is used heavily in the operational areas of the sector, and it is well understood, which makes it an appealing metric. However, the hesitancy in using it is related to the exceptionally high reliability of the system now. The power grid is both the largest machine ever built and the most reliable one. Increasing the reliability of the grid may be subject to the law of diminishing returns and thus may not be a realistic metric. On the flip-side, the law of diminishing returns goes away immediately if there is a serious incident. Using reliability related security metrics to enhance reliability, enable better business controls, and promote operational efficiencies seemed to be the “sweet spot” for the discussion.

*“The power grid is the largest machine ever built. It is also the most reliable.”*

#### Spending as a Metric

Whether or not spending levels provide value as a metric was a hotly-debated topic. Some declared “absolutely,” while others held steadfastly to “definitely not,” but most attendees were firmly in the camp of “it depends.”

It appeared that one key to using spending as a metric is that an element of quality must be included. If I spend less because I am more efficient and do a better job than my neighbor, then the level of spending, in and of itself, is not necessarily an effective metric. Another example provided was the purchase of an expensive anti-

virus solution for the purpose of meeting a compliance regulation. If it meets compliance but doesn't work as an anti-virus solution then spending alone is a bad metric.

Russell Thomas (Meritology) suggested that some recent research on network security spending levels gets at that element of "quality." Rather than focusing on what the right level of security spending is, it evaluates the current level of spending against whether it helps to meet the corporate security goals. Measuring any considered shifts in spending against the impact to those same goals.

### Framing the Metrics

There are a number of existing risk models in various industries. The discussion focused on whether one of the existing frameworks might work or if an entirely industry specific model were needed. The group was split on what was on this point. Some felt all of the existing frameworks are similar enough - so just pick one and go with it. Others felt like we were unique enough to need our own framework, even if it were just pulled together from elements of existing models. Another factor to be considered is maturity. It was pointed out that the reason PCI (mostly) works is that the hard work has been done. The assets to be protected have been clearly defined (cardholder data) the impact is defined as well (loss of card holder data). The electric sector just isn't there yet.

*"Numbers are great. But what are we supposed to do with them?"*

### Moving Forward

It was a great morning of exploration on the topic of security and metrics. There were some excellent take-aways from the event, recommendations on things we do right now, as well as ongoing discussion on the wiki. Here are a few items to consider:

#### Measure Your Maturity

In looking for a place to start, measure your organization's maturity related to security. Then take actions that are appropriate at that level rather than trying to reach for the stars immediately. Taking appropriate steps forward

provides incremental benefits whereas reaching too far almost always ensures failure.

#### Shift your Mindset

Stop thinking about what we do as protecting the company and start thinking about it as enabling appropriate risk decisions. If we can provide the right information to the decision makers, our resource needs will likely be met, and our level of security improved.

#### Measure what you can Manage

Ensure that what we are measuring is the right thing. Metrics should help inform the decisions that we can manage rather than measure things we have no control over. If we are to provide good decision support we need to measure things that will enable us to make good decisions.

### Summary

One attendee summarized the objective with a wry smile, "It's simple really - we just need to be reliable, safe, efficient, and secure." Admittedly, this perfect balance is difficult to achieve. However, having good metrics is certainly a step in the right direction.

### Thank you to our panelists and presenters for sharing your insights and expertise.

William Bryan  
US Dept. of Energy

Brandon Dunlap  
Brightfly

Michael Hamilton  
City of Seattle

Russell Thomas  
Meritology

Ed Moyle  
IANS

Brent Rowe  
RTI International

Steve Parker  
EnergySec

Check out our wiki for recommended reading, additional discussion, and copies of presentation materials.  
<http://bit.ly/o3LMjz>

**See you next time!**

follow us on twitter @NESCOtweet

PLUG INTO THE DISCUSSION AT: [WWW.ENERGYSEC.ORG/JOIN](http://WWW.ENERGYSEC.ORG/JOIN)