



### *How to Prepare, Prevent, and Respond to Cyber-Attacks in the Energy Sector: Three Lessons*

The core foundation of the global energy sector is ensuring reliable energy to homes and businesses 24/7/365. Yet, as energy suppliers endeavor to meet the energy needs of seven billion people, cybersecurity often falls to the wayside.

Meanwhile, the rapid digitalization of the energy industry has provided more avenues for cybercriminals to permeate through an organization's security barriers. As the U.S. Energy Association's (USEA) Executive Director Sheila Hollis always says, "[Energy never sleeps...](#)" and neither does cyber-crime. This is especially concerning for utilities in developing countries that lack cybersecurity policies, standards, or don't consider cyber risks on a regular basis.

To fill this critical need gap U.S. Agency for International Development (USAID) collaborated with USEA to lead a webinar series on Digitalization and Cybersecurity in the Energy Sector hosted by the Bureau of Economic Growth, Education and Environment (E3). The 15-part Cybersecurity and Digitalization Webinar Series that commenced this summer educated global utilities on cyber standards, trends, and best practices. The series hosted leading cybersecurity experts from domestic and international utilities, covering topics including: [utility assessment tools](#), [data protection](#), [elements of trusted collaboration](#), and [the importance of supply chain security](#).

In case you missed the series, here are the top 3 lessons on how to be better prepare for cyber-attacks in the energy sector:

#### **1. Prepare: Appoint and empower a Chief Security Officer (CSO)**

In the fifth webinar on “[The Corporate Culture and Importance of Cyber Hygiene](#),” [Idaho National Lab](#) Senior Grid Strategist Andy Bochman, suggests that many utilities don’t prioritize cybersecurity because most of them haven’t had a destructive, catastrophic attack yet. Bochman says, “At a time when corporate dependency on digital technologies is now nearly complete, sticking with a business-as-usual structure is outdated and unwise.” His [article](#) on *Medium* argues the most important C-suite position doesn’t even exist at most companies and states that only [15 percent of corporate boards](#) are completely satisfied with the level of cybersecurity reporting they’re getting from management.

## The missing chief security officer

The most important C-suite position doesn't even exist at most companies. Here's why it should.

Andy BochmanFollow



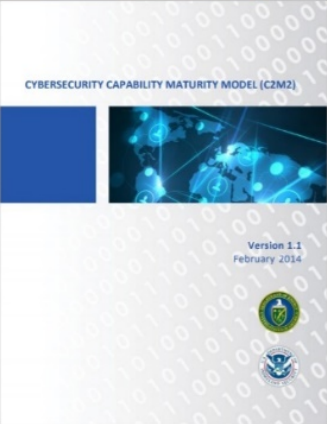
Feb 20, 2018 · 5 min read

## 2. Prevent: By establishing a cybersecurity plan and constantly self-assess

The [Cybersecurity Capability Maturity Model \(C2M2\)](#) is one of the most important tools for assessing the cybersecurity posture of the energy sector organizations and enhancing their cybersecurity capabilities. In the sixth webinar on “[Introduction to the C2M2](#)” Galen Rasche from the [Electric Power Research Institute \(EPRI\)](#) and Christopher Taylor from [Southern Company](#) demonstrated how voluntary practices such as the [NIST Cybersecurity Framework](#), [C2M2](#), and [EPRI’s Technical Assessment Methodology \(TAM\)](#) help build, maintain, and mature a cybersecurity program. By creating and continuously revisiting your cybersecurity plan, you can easily assess and prevent cyber risks.

### Cybersecurity Capability Maturity Model (C2M2)

- Voluntary practices for building, maintaining, and maturing a cybersecurity program
- C2M2 is a model and assessment for both IT and OT
- Objectives
  - Strengthen cybersecurity capabilities
  - Consistent assessment and benchmarking
  - Share knowledge and best practices
  - Enable prioritized actions and investments
- Developed by utilities and for utilities in 2012 under the US Department of Energy, updated in 2014 (v1.1)
- New version (v2.0) to be released in 2021

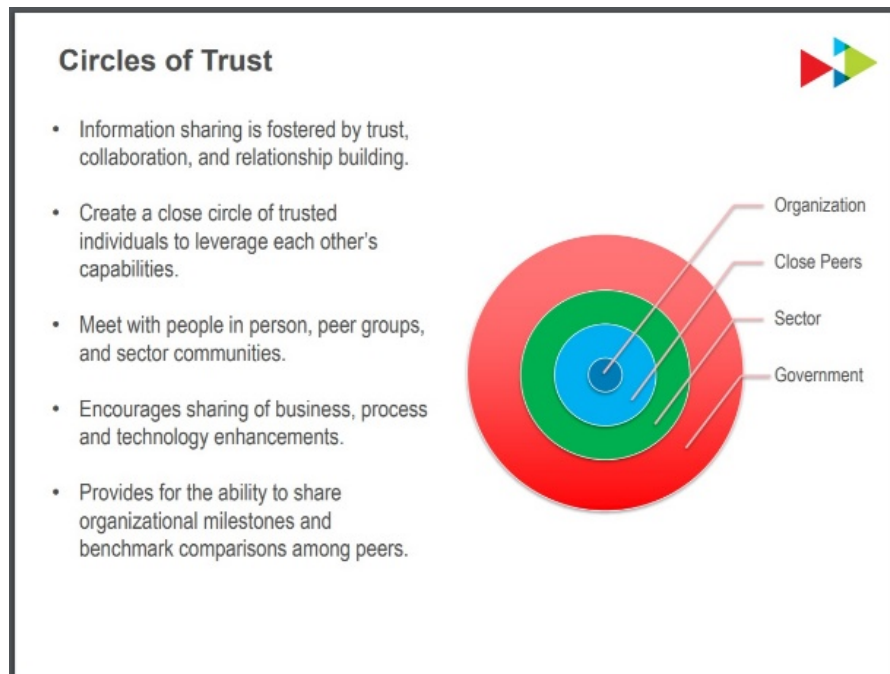


Version 1.1  
February 2014

3

## 3. Respond: By establishing and fostering a circle of trust

A recurring theme of the webinars was to create a close circle of trusted individuals to leverage each other's capabilities by sharing information and benchmarks among peers. In the fourteenth webinar on "[Key Elements of Trusted Collaboration and Information Sharing](#)," Frank Honkus from the [Electricity Information Sharing and Analysis Center \(E-ISAC\)](#) and Tom Wilson from [Southern Company](#) demonstrate how information sharing can allow organizations to detect threats sooner, increase situational awareness, and create a discussion for best practices/lessons learned. Notably, Frank and Tom provided an overview of how developing countries can create information sharing centers and utilize best practices for information sharing.



*This blog was written by [Jake Swanson](#), Program Coordinator, USEA. To learn more about the Cybersecurity and Digitalization Webinar Series write to me: [jswanson@usea.org](mailto:jswanson@usea.org) or follow us on [LinkedIn](#) and [Twitter](#).*