USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association

Corporate Security Culture

View from the Top

What do we mean by Corporate Culture?

- Refers to the shared values, attitudes, standards, and beliefs that characterize members of an organization and define its nature
- Rooted in an organization's goals, strategies, structure, and approaches to labor, customers, investors, and the greater community.
- An essential component in any business's ultimate success or failure.

https://www.inc.com/encyclopedia/corporate-culture.html

USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association

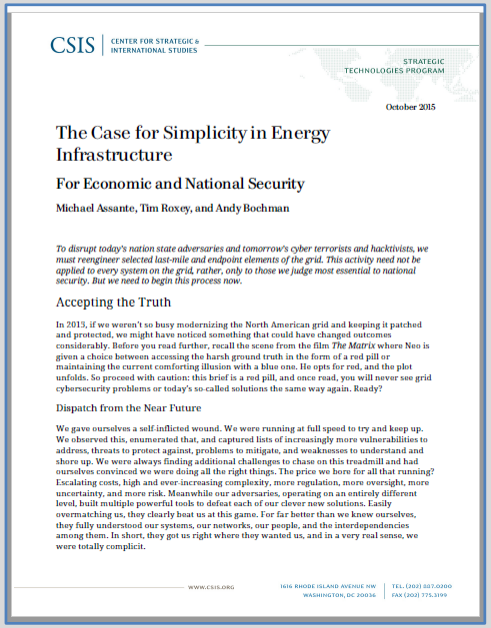
Context

U.S. AIR FORCE

IBM

THE CHERTOFF GROUP

INL
Idaho National Laboratory


CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

STRATEGIC TECHNOLOGIES PROGRAM

October 2015

The Case for Simplicity in Energy Infrastructure

For Economic and National Security

Michael Assante, Tim Roxey, and Andy Bochman

To disrupt today's nation state adversaries and tomorrow's cyber terrorists and hacktivists, we must reengineer selected last-mile and endpoint elements of the grid. This activity need not be applied to every system on the grid, rather, only to those we judge most essential to national security. But we need to begin this process now.

Accepting the Truth

In 2013, if we weren't so busy modernizing the North American grid and keeping it patched and protected, we might have noticed something that could have changed outcomes considerably. Before you read further, recall the scene from the film *The Matrix* where Neo is given a choice between accessing the harsh ground truth in the form of a red pill or maintaining the current comforting illusion with a blue one. He opts for red, and the plot unfolds. So proceed with caution: this brief is a red pill, and once read, you will never see grid cybersecurity problems or today's so-called solutions the same way again. Ready?

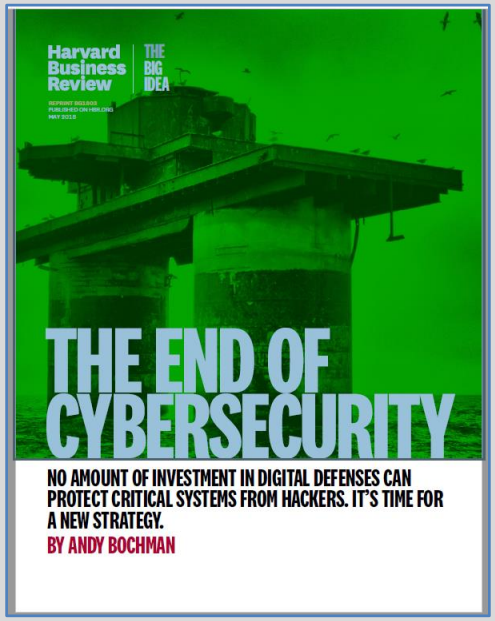
Dispatch from the Near Future

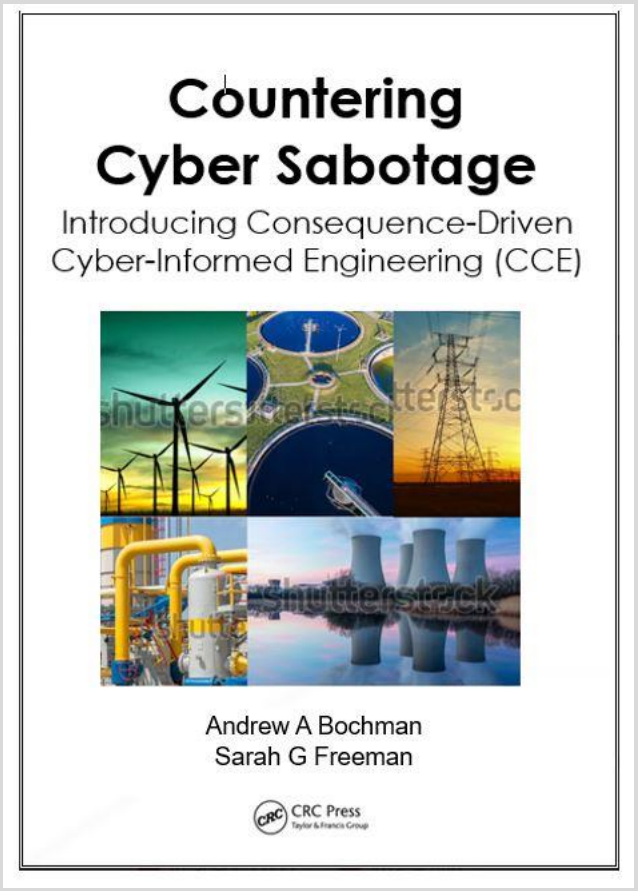
We gave ourselves a self-inflicted wound. We were running at full speed to try and keep up. We observed this, enumerated that, and captured lists of increasingly more vulnerabilities to address, threats to protect against, problems to mitigate, and weaknesses to understand and shore up. We were always finding additional challenges to chase on this treadmill and had ourselves convinced we were doing all the right things. The price we bore for all that running? Escalating costs, high and ever-increasing complexity, more regulation, more oversight, more uncertainty, and more risk. Meanwhile our adversaries, operating on an entirely different level, built multiple powerful tools to defeat each of our clever new solutions. Easily overmatching us, they clearly beat us at this game. For far better than we knew ourselves, they fully understood our systems, our networks, our people, and the interdependencies among them. In short, they got us right where they wanted us, and in a very real sense, we were totally complicit.

WWW.CSIS.ORG

1616 RHODE ISLAND AVENUE NW
WASHINGTON, DC 20036

TEL. (202) 887-0200
FAX (202) 775-3199





Context (cont.)

US Department of Energy: Idaho National Lab

- **Cyber-Physical Grid Protection**
- **Critical Infrastructure Assessments**
- **US & International Security Policy & Guidance**
- **International Nuclear Cybersecurity**

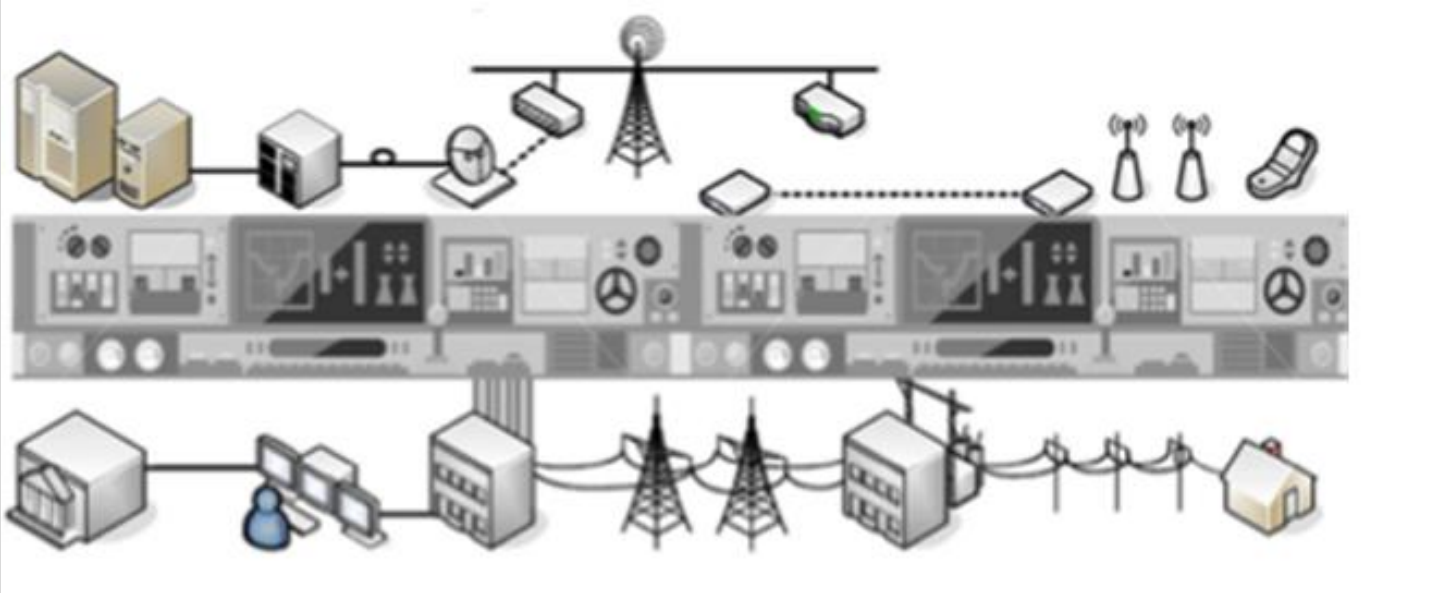


Shortest History: Tech Evolution

IT Infrastructure

Operational Technology (OT) Infrastructure

Power Infrastructure



Operational systems were analog and protected by isolation. They were not digital, not networked, and not automated. All of that has changed.

Shortest History: Notable Attacks

Security Governance

The missing chief security officer

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

Andy Bochman
Feb 20, 2018 · 5 min read

https://medium.com/cxo-magazine/the-missing-chief-security-officer-11979a54fbf9

CSOs vs CISOs

- "It's time for organizations to appoint CSOs with both technical and business leadership attributes. Most CISOs are far too pigeonholed to effectively deal with the material nature of attacks and help CEOs navigate these turbulent times. Yesterday's governance models don't live up to today's business realities."

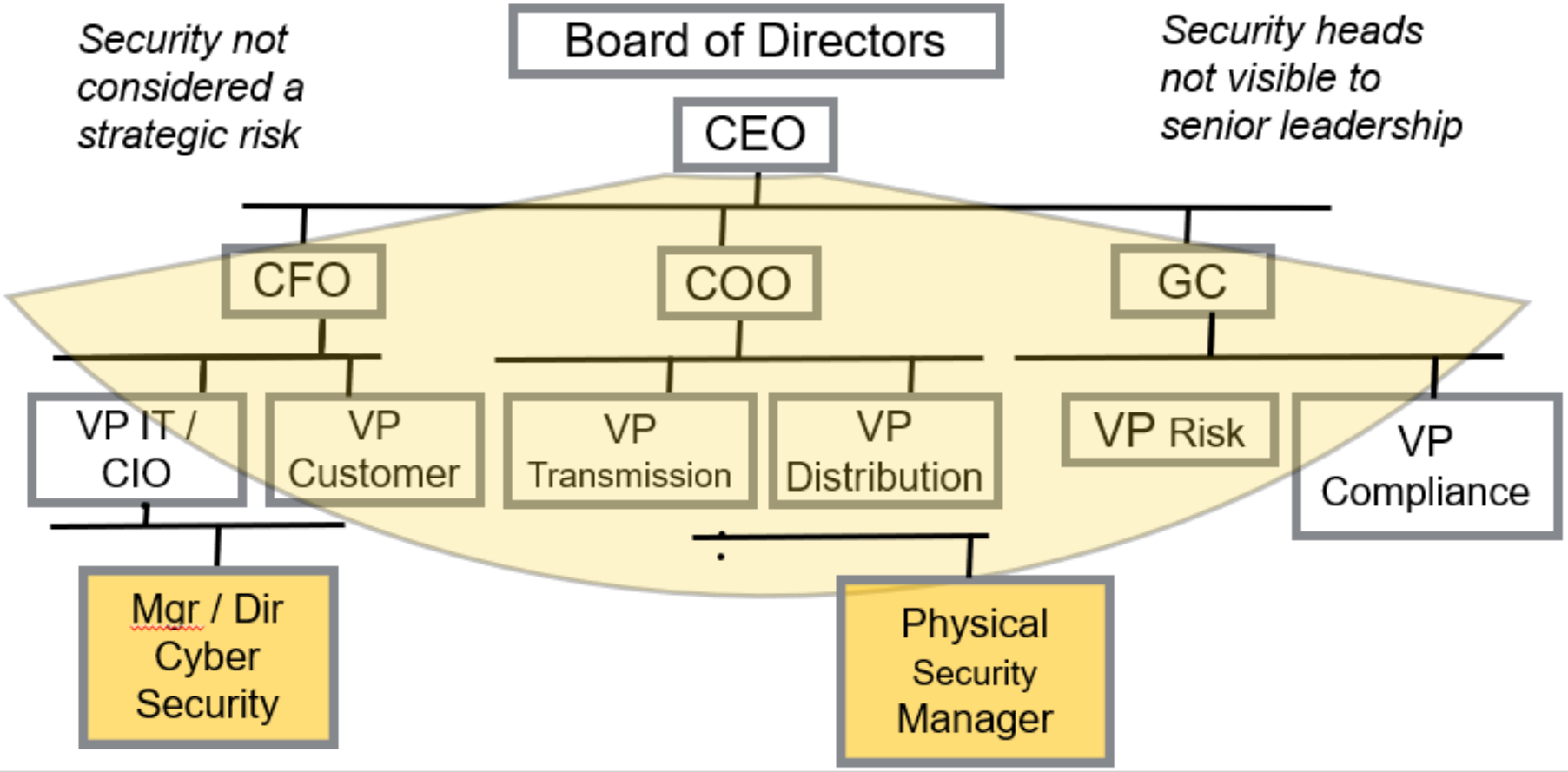
-- Michael Assante, (RIP), former director of critical infrastructure and ICS at SANS Institute and former CSO of American Electric Power.

CSO = Chief Security Officer
CISO = Chief Information Security Officer

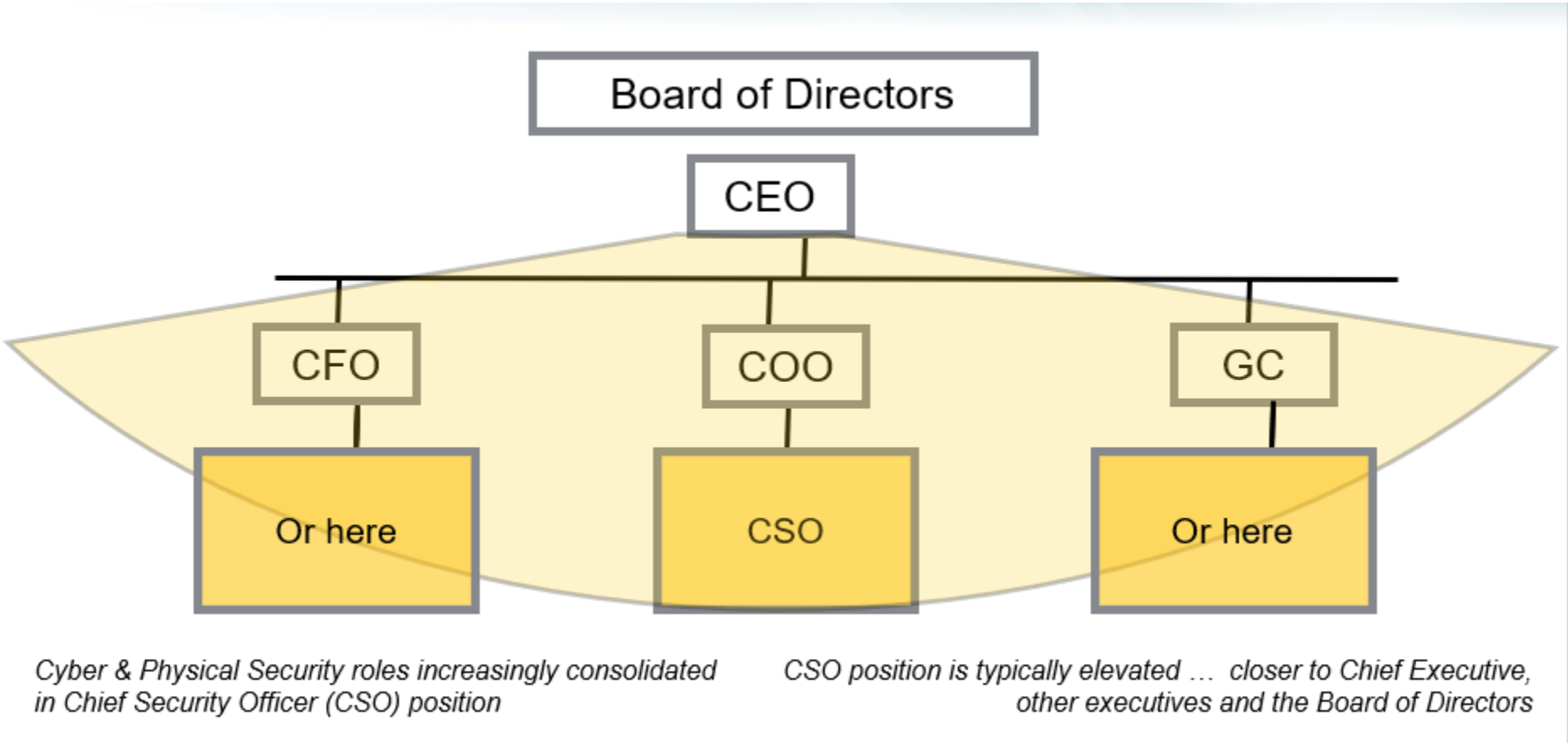
Problems When CISO Reports to CIO

1. Inevitable conflicts with their boss (the CIO), whose principal job is to deploy new technologies that drive profits and efficiencies
2. CISOs under CIOs aren't in the position to align security priorities with the company's other strategic business goals
3. CEOs and board members need constant and regular interaction with their company's cybersecurity expert to build trust and rapport. They don't get that from people far down the organizational chart

Utility Org Chart for Cybersecurity Environment (1)



Utility Org Chart for Cybersecurity Environment (11)



Cyber & Physical Security roles increasingly consolidated in Chief Security Officer (CSO) position

CSO position is typically elevated … closer to Chief Executive, other executives and the Board of Directors

An Exemplar – How to Measure Success

- First year at previous utility, socialized security staff with OT operators and maintainers
- Now at Xcel – responsible for all aspects of security
  - OT/IT
  - Cyber/Physical
  - Safety
  - NERC CIPs

Thanks for your attention.

Happy to get your questions.