What should your cyber security director be telling you?

Gary Dodd

Chief Information Security Officer,
Bonneville Power Administration,
Office of Cyber Security
1. **What is our overall Cyber Security Strategy?**

Don’t be surprised if you don’t have one. Cyber security professionals, even good ones, don’t always have that skillset or know how. Writing a real strategy is something your cyber team will likely need help with, but let them drive it.

2. **Have we had an independent or self-assessment of our enterprise cyber security program?**

Not just IT, and not just intrusion detection systems and firewalls, but the whole program. Choose a framework that is comprehensive and covers governance and roles, and all technology (ES-C2M2 or NIST rather than NERC CIP; SANS Top 20 rather than PCI).
3. **Do we approach the risk of cyber attack as an enterprise or is it an IT issue?**

- Ensure both the cyber security director and senior management understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue. It's not just an OT issue either.

- Cyber attacks on utilities are an increasingly likely occurrence. Often the equipment used to monitor, control and protect the electric grid and distribution networks are IT stuff, but not controlled by IT.

- The Risk to the enterprise is not an IT issue. IT doesn’t understand the impact of a data breach or cyber attack. Only the business does. The cyber risk needs to be communicated and brought together with the mission/business impact. NIST Risk Management Framework and the DOE Risk Management Framework both provide examples of how to structure this.
4. **What do you think we/I need to know about? What’s your biggest concern?**

- Senior managers/boards should have access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on meeting agendas.

- It may take a few tries before a CISO or cyber security Director and a board or senior management team work out how to communicate; what they need from each other – be patient. Most organizations are not good at this when it comes to cyber. Metaphors fail, and comparisons often aren’t quite right.
5. Do we feel we have an enterprise-wide risk management framework with adequate staffing and budget?
   • What framework are we using?
   • Operating a risk management framework requires staffing proportional to the number of persons putting in new functionality and operating IT and OT.

6. What risks are we accepting now and can you explain why you think this is one of our bigger concerns?
   • Regardless of framework, senior managers should know what risks are being avoided, accepted, mitigated, or transferred through insurance, as well as specific plans associated with each approach. Ultimately they aren’t cyber risks, there are risks to operations, of non-compliance, legal and regulatory, etc. The cyber security Director or CISO can tell you what a bad guy could get to and what they might do, but she’d be guessing at the impact.
SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.

Mike Henson
Chief Security Officer,
Northwest Open Access Network
Employee are the Keys to the Kingdom

What’s the most dangerous social engineering threat to organizations?

- Lack of Employee Awareness: 56%
- Phishing: 21%
- Criminals: 12%
- Vishing: 5%
- Other: 6%
Fear and Free Stuff!

You are eligible to receive one of our FREE Giftcards

Complete the steps below to be able to get your free gift card

Packages remaining: 387

Step 1: Pin It

Final step: Click Here

Warning: You’re TOTALLY infected!!

Call Now! 888-ITS-FAKE

Cyber Security Panel: Gary Dodd, BPA - Mike Henson, NOANET - Dean Kovacs, EN
What do these companies and yours have in common?
Your Employees!

Email use and employees 2015...

- 44% of email recipients made at least one purchase based on a promotional email
- 33% of recipients open an email based on subject line
- Subject lines fewer than 10 characters had an open rate of 58%
- 70% of people say they made use of a coupon or discount from an email
- Email that includes social sharing buttons have a 158% higher click through rate

- 61% reuse passwords
- 54% have only five passwords or less
- 44% change their password only once a year or less
- 89% feel secure with their current password management and use habits
- 21% have had an online account hacked

http://www.csid.com
Digital Systems: The Case for Vigilance

Dean Kovacs

Chief Information Officer,
Energy Northwest
Two good reasons to invest in protecting your digital systems:

Compliance & Consequence
But that’s not why you should invest in security.
You should invest in security because your digital adversaries have so many advantages:

- Distance
- Time
- Motivation
- Coordination
DISTANCE
Your attacker never has to set foot in
your facility
or even
this country

Digital attacks can be planned, scouted, and executed remotely

Cyber Security Panel: Gary Dodd, BPA  -  Mike Henson, NOANET  -  Dean Kovacs, EN
TIME
Not only can digital attacks be planned well in advance but

Once your systems have been compromised, attackers often quietly monitor and map your systems rather than execute an attack immediately

sometimes for months or years
Motivation

Critical Infrastructure attackers often have significant motivations that are supported by substantial resources or ideological teams:

- Criminal entrepreneurs
- Nation-states
- Hacktivists
COORDINATION

Attackers are showing increasing coordination to create broad impacts

- Ukrainian power outage – December 2015
- East Coast Internet Outage – October 2016
- NERC Alert – Internet of Things (IoT) Attacks
We cannot guarantee that we won’t be compromised but

We can be prepared to:

*NIST Cyber Security Framework