GOVERNANCE POLICIES & PROCEDURES for THIRD PARTY CYBERSECURITY RISK MANAGEMENT

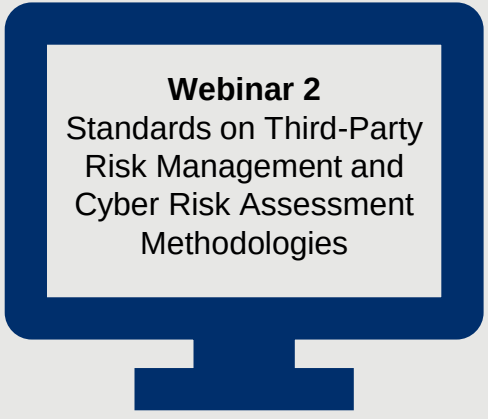
Cybersecurity and Digitalization:
Supply Chain Risks in the Electricity Sector

OBJECTIVES

- Focus on organizational cybersecurity governance and the best practices on policies and procedures to address supply chain risk management
- Highlight:
  - Typical models for managing cybersecurity (e.g., the role of a CISO or CSO) and
  - Level of visibility into cybersecurity risks from the senior management to technical staff
- Discuss strategies and approaches to communicating not only within an organization about cyber risks, but also with regulatory authorities
  - Support the review and approval of CAPEX and OPEX cyber investments

ASSUMPTIONS

- The following USEA-USAID Webinar Topics are considered foundational to this presentation and should be well understood & recommendations implemented:



HOW TO GET STARTED

Leverage Existing Company Governance Models

- Code of Business Conduct
- Company-level Compliance Department/Committee
- Regulatory Affairs

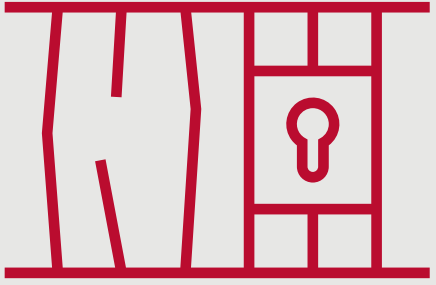
Set up a Charter – review and agree amongst the stakeholders

- Mission
- Purpose
- Responsibilities
- Scope
- Guidelines

Build

- Executive/Senior Sponsorship
- Director-level Steering
- Working Group – Subject Matter Experts(SMEs)/Leads/Managers

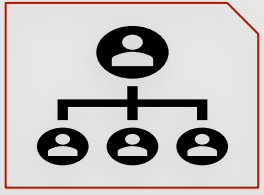
HOW TO GET STARTED – What Can Go Wrong?



- Minimal Existing Governance
- No Centralized Procurement
- Organizational Culture –
  - ambiguity (vague goals or actions in conflict with policy)
  - inconsistency (even and fair application of policies)
  - lack of communication
  - weak leadership (people won't follow management they don't respect)
- Lack of Executive Buy-in

COMMON STAKEHOLDERS

- Who in the company utilizes third parties or suppliers?
- Who manages the third parties and/or suppliers' work?
- Who makes decisions about the third party and supplier work and program(s)?
- Who needs to know about the third party and supplier work program?
- Who can benefit from the success of the third party and supplier work program?
- Who can be harmed from the failure of the third party and supplier work and/or program?
- Who can influence the third party and supplier work culture?



ORGANIZATION

Functional Areas

GEOGRAPHY

Multi-sites within city, state, and/or nation, multi-affiliates and/or territories

KEY DECISION MAKERS

KEY INFLUENCERS

Subject Matter Opinion Leader

INVOLVEMENT ASPECTS

RACI

ONGOING ENGAGEMENT PLAN

Organizational Change Management, Dept. Goals

COMMON STAKEHOLDERS – What Can Go Wrong?

- Missing Stakeholder(s)
- Lack of Consensus
- Prioritization Issues
- Identifying "Opinion Leaders"
- Third-party Inclusion (and When)
- Multi-country and Parent/Affiliate Company Cultural Differences
- Keeping Governance/Stakeholders Up-to-Date
    - through organizational change to implement, operationalize, and maintain

EXECUTIVE BUY-IN

Regulations are usually easier

- Still need to have the conversation

Anyone could start the conversation

- Generally brought forward by CISO and/or Legal

Audience - Senior Leadership such as:

- CISO
- CIO
- Legal Officer
- Officer/Executive responsible for Procurement
- Business Officer(s)

Becomes the governance top tier

Determine relevant risks for the executive level audience

- focus on risks that would lead to loss of revenue (e.g., loss of business ops and associated likelihood)

Gain agreement to proceed

- may need to utilize phased approach

EXECUTIVE BUY-IN – What Can Go Wrong?

- Clarity of cost/loss of revenue
- Clarity of funding type – depends upon local accounting regulations/terms
  - CAPEX (capital expenditure) vs. OPEX (operating & maintenance expenditure)
- Clarity of what happens if we *don't implement* (i.e., not just the cyber risks) –
  - Reputational harm
  - 3rd party relationship damage
  - Potentially breach of contract
  - Regulatory penalties (if applicable)
- Other priorities
- Lack of consensus

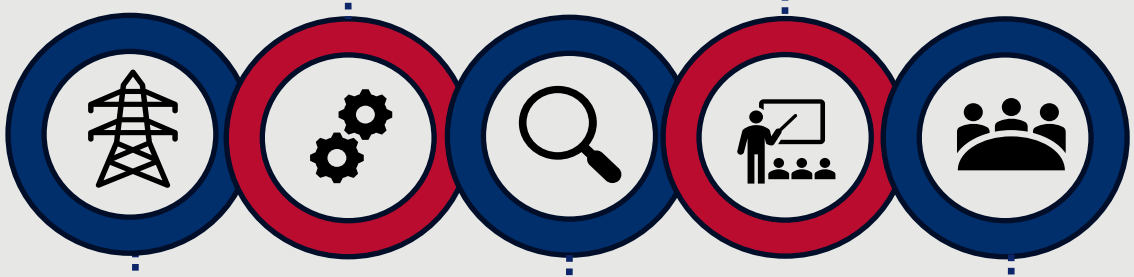
OCM & CULTURE CHANGE

ORGANIZATIONAL CHANGE MANAGEMENT (OCM)
Example: PROSCI/ADKAR

- AWARENESS
- DESIRE
- KNOWLEDGE
- ABILITY
- REINFORCEMENT

HOW DO WE DO IT?
SME Collaboration
SME Training
Ongoing: New SME Orientation

VARIED LEARNING APPROACHES & POLICY
Process training/courses (record/store on LMS)
Lunch & Learns
1-1s, Surveys
Policy Review/Update (e.g., annual)
End-to-end process reviews
Assessments/Mock audits



WHY ARE WE DOING THIS & WHY IS IT IMPORTANT?
What's in it for me? Why are we doing it this way?
Why now? What if we don't do it?
What are we really protecting?
"Awaring" isn't Caring → Pathos ← Use Stories
+ External Stakeholders – Vendors, Regulators +

WHERE CAN I FIND MORE INFORMATION?
Program/Process/Procedures location/evidence site
Regulation/standards website
Your GRC or Compliance team

MAINTAINING INTEREST
What's going on in the world of Third-party Risk Management that the SMEs may want to know about?
REINFORCE: Validate processes/ & controls

Upcoming standards
Local workshops

DIMENSIONS OF SECURITY CULTURE
Carpenter/Roer

- Attitudes
- Behaviors
- Cognition
- Communications
- Compliance
- Norms
- Responsibilities

LEVERAGING ORGANIZATIONAL CHANGE MANAGEMENT (OCM) – What Can Go Wrong?

- Hard to maintain momentum / higher priorities after "go live“
- Resistance
- Easy to start thinking tactically
- Lack of sustainability
- Changes in organizational structure and impacts to messaging
- Cultural differences
- Attitude
- Lack of motivation
- Listening skills
- Written communication and quality
- Appropriate communication tools
- Oversharing

- Delays in contracting with third parties
  - Not following risk management processes
  - Missed milestones,
  - Re-work from not identifying issues upfront
  - Loss of work by project team
  - Other unexpected obstacles

TYPICAL MODELS: LEVELS OF VISIBILITY

- Technical Staff – involved in the risk identification and remediation, including deviations from policies/standards
- Cyber/Compliance Staff – risk identification translation into business terms, mitigation/remediation tracking, review triggers, exceptions management
- CISO/CSO – must sign-off on high-level residual risks
    - Periodically review all the residual risks in the Third-Party Risk register (exceptions)
- Business Leaders – risk sign-off, organizational level dependent upon level of residual risk
- C-Suite/BoD – major risks awareness in context of all enterprise risks/risk register

SEE WEBINAR - 2. Standards on Third-Party Risk Management and Cyber Risk Assessment Methodologies

TYPICAL MODELS: LEVELS OF VISIBILITY – What Can Go Wrong?

- Risk identification issues
- Risk communication issues
- Inappropriate business approvals
- Lack of tracking and follow-up to implement agreed remediations
- Lack of or poorly documented methodologies for deviations from internal standards
- Rigid processes that don't allow for flexibility and conversely, lax and inconsistent processes

SUPPORTING REVIEW AND APPROVAL OF CYBER INVESTMENTS

- Address fundamental questions in business language
  - Why?
  - Why now?
  - Why this way?
  - What if we don't do it?

- Focus on Cost of Ownership
  - Assessment tool subscription, procurement labor, security labor, risk management, IT/OT management review
  - Consideration of post-project non-CAPEX costs, including vendor support & maintenance, internal training, efforts to operationalize, manage and maintain (e.g., headcount)

SUPPORTING REVIEW AND APPROVAL OF CYBER INVESTMENTS – What Can Go Wrong?

- Didn't answer the fundamental questions in business terms – what is the true VALUE
- Incorrect financial assumptions
- Incorrect/challengeable financial calculations
- Didn’t understand the true effort to implement and associated costs
- Didn’t include all of the needed stakeholders
- Didn’t understand the ongoing impacts to day-to-day operations to manage, support, and maintain

QUESTIONS and ANSWERS

Terri Khalil
www.linkedin.com/in/terrikhalil
tkhalil@amperesec.com

Roland Miller III
www.linkedin.com/in/roland-miller-iii

USAID FROM THE AMERICAN PEOPLE

USEA United States Energy Association