Assessing the Effectiveness of a Cybersecurity Program

Lynn D. Shiang
Delta Risk LLC, A Chertoff Group Company

Objectives

- Understand control frameworks, assessment structures and scoping of detailed reviews
- Understand practical steps for assessing the Cybersecurity Program
- Understand that…'It' CAN happen or… it MAY have already happened

Commercial vs. Industrial Networks

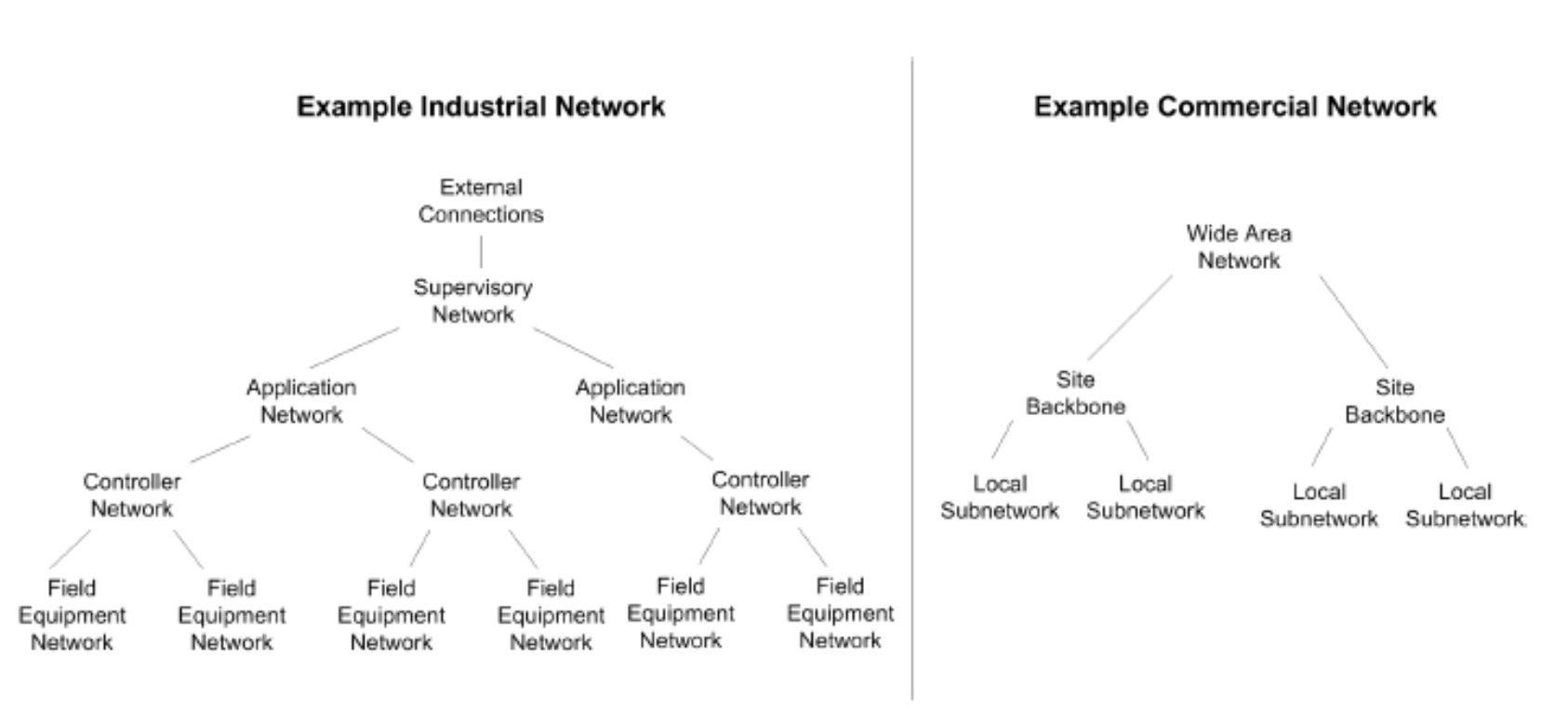
Commercial Networks

- Failure could have financial impact on XYZ Co. and its business partners, shareholders, brand reputation, etc.
- Cyber-terrorists, hackers, industry competitors pose well-known threats to commercial networks
- XYZ Co. may incur fines, penalties or lawsuits

Industrial Networks
(especially critical infrastructure organizations)

- Failure could have severe, regional or nation-wide health and safety effects
- Cyber-terrorists organizations pose a great threat to industrial networks (especially critical infrastructure systems)
- Fines/penalties may be the least of the organization's worries

Network Comparisons



Drawing obtained from: *Introduction to Industrial Control Networks*, Galloway, Brendan & Hancke, Gerhard, 2012

Security Issues for SCADA Systems

"The reliable function of SCADA systems in our modern infrastructure is crucial to public health and safety."

- Lack of attention to security, availability, integrity, change management and authentication in design, testing, deployment and operation of some existing SCADA networks and applications
- Belief that SCADA systems have the benefit of "security through obscurity" through the use of specialized protocols and proprietary interfaces
- Belief that SCADA networks are secure because they are physically secured
- Belief that SCADA networks are secure because they are disconnected from the Internet
- Industrial Control Systems (ICS) were not designed or built for security

Popular Control Frameworks

- NIST SP 800-53 rev. 4 (CSF)
- CoBIT
- ISO 2700x family
- SANS Critical Security Controls (CSC)

Choosing a Framework

Considerations:

- Industry ‘best practices’
- Regulatory requirements
- Intellectual property or critical information values
- Quantity, location, criticality of business critical systems
- Nation-wide critical infrastructure relevance (DHS)
- Current maturity vs desired maturity

ISO 27002 Domains

1. Information security policies
2. Organization of information security
3. Human resource security
4. Asset management
5. Access control
6. Cryptography
7. Physical & environmental sec
8. Operations security
9. Communications security
10. System acquisition, development & maintenance
11. Supplier relationships
12. Information security incident management
13. Information security aspects of business continuity management
14. Compliance

NIST CSF Framework
(SCADA)

1. Asset Management
2. Business Environment
3. Governance
4. Risk Assessment
5. Risk Management Strategy
6. Access Control
7. Awareness & Training
8. Data Security
9. Information Protection Processes & Procedures
10. Maintenance
11. Protective Technology
12. Anomalies & Events
13. Security Continuous Monitoring
14. Detection Processes
15. Response Planning
16. Communications
17. Analysis
18. Mitigation
19. Improvements
20. Recovery Planning

SANS Common Security Controls (CSC)

1. Inventory of devices
2. Inventory of software
3. Security configurations (hardware, software, servers, workstations)
4. Continuous vulnerability assessment & remediation
5. Malware defenses
6. Application software security
7. Wireless device control
8. Data recovery capability
9. Security skills assessment & training
10. Secure configurations for network devices (firewalls, routers, switches)
11. Limits & controls on network ports, protocols, and services
12. Controlled use of admin privileges
13. Boundary defense
14. Maintenance, monitoring and analysis of security audit logs
15. Controlled access based on need-to-know
16. Account monitoring and control
17. Data loss prevention
18. Incident response management
19. Secure network engineering
20. Penetration tests and red team exercises

Implementing a Framework

- Asset protection (information security) is a journey
- Consistent improvement is the realistic goal
- Figure out where you are in the journey (baseline assessment)
- Determine where you *should* be (baseline "to do's")
- Define the reasonable and realistic (12-18 mos.) strategic, tactical, operational and educational plans to get there (Management Action Plan - MAP)
- Check progress of efforts no less than annually; ideally quarterly
- Educate on risks and report risk management progress to C-level committees and Board of Directors quarterly

Assessing Information Security Capabilities

- **Who?**
  - Who performs the assessment?
    - Defined by scope and objectives
    - External, qualified information security consulting firm
    - Continuous self-assessment
    - Internal Audit

Assessing Information Security Capabilities

- **What?**
  - What gets assessed?
    - Administrative Processes, or
    - Technical Safeguards, or
    - Physical Safeguards, or
    - Full Information Security Management System, or
    - Newly mitigated audit/assessment findings, or
    - …

Assessing Information Security Capabilities

- **When?**
  - When should an assessment occur?
    - Self assessment – continually
    - External program assessment – every two years
    - Internal program assessment – yearly
    - Specialized program area assessments – twice yearly
    - Specialty topics – as necessary

Assessing Information Security Capabilities

- **Why?**
  - Why should an assessment occur?
    - Regular risk & compliance management process
    - SCADA conformance
    - Focused problem areas (e.g., validation of mitigation of previous audit or breach findings)
    - SSAE 16 completion for service organizations
    - Board of Directors, Shareholders, stakeholders

Structuring the Assessment

Determine:

- Scope (e.g., one division, policies, firewalls, etc.)
- Assessment objectives
- Provider (in-house or external)
- Assessment Project Leader (accountable manager)
- Framework of record (ISO 27002, NIST, CSC, etc.)
- Results reporting content & format (define "presence" & "effectiveness" or maturity ratings)
- Closure processes, schedules, logistics, etc.

Methodology A

- **Full ISMS Assessment approach** (not all-inclusive)
  - Review documentation (e.g., policies, procedures, configurations, network drawings, security program structure, committee charters, etc.)
  - Interview stakeholders, accountable managers, Legal, Audit, C-level leadership, etc.)
  - Rate each framework element or domain (CMMI?)
  - Correlate data and develop prioritized recommendations (based on risk, quick win, other strategies, etc.)

Methodology B

- **Technical approaches** (not all-inclusive)
  - Network vulnerability assessment
  - Application security assessment
  - Exercises and red team activities
  - Penetration testing
  - PMO management of information security inside the SDLC
  - Log management and aggregation assessment
  - Firewall placement and configurations

Methodology C

- **Administrative approaches** (not all-inclusive)
  - Governance & information security organization
  - Policies, framework & lifecycle management
  - Change management program
  - User lifecycle management
  - Human Resources processes
  - Security awareness & education programs

Methodology D

- **Physical Security approaches** (not all-inclusive)
  - Social engineering
  - Awareness testing
  - Monitoring & surveillance infrastructure
  - Guard competency
  - Incident response & recovery capabilities

Real-World Events

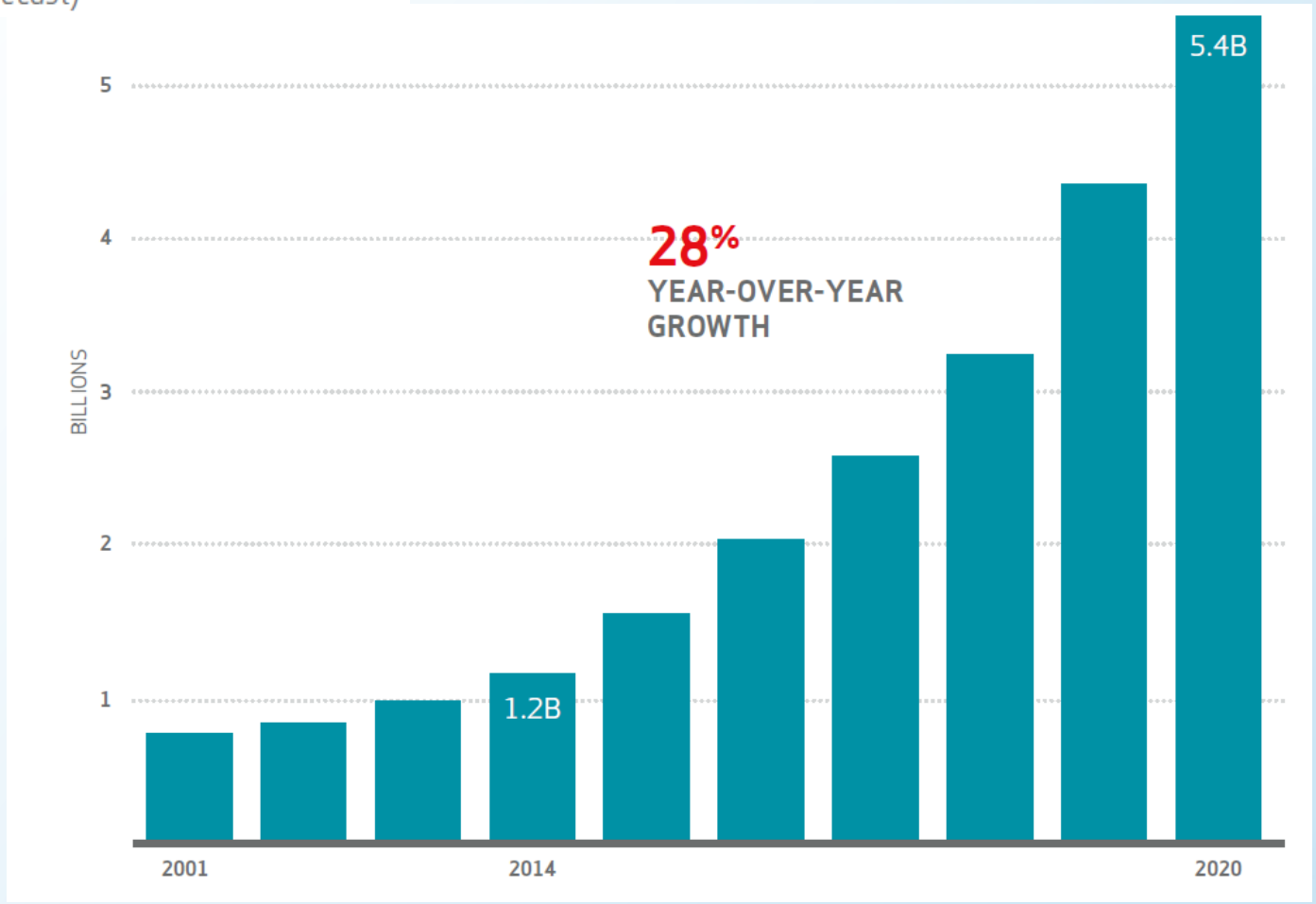
- Social engineering
- Distributed Denial of Service (DDoS)
- “Data Integrity” hacking
- un-Awareness
- Lack of policies & processes
- Carelessly restricted ‘system admin’ privileges

An unidentified group of hackers targeting natural gas pipeline companies gained access to the corporate systems of several of their targets and "exfiltrated" -- that's security-speak for "stole" -- data on how their control systems work. (CNN news – 2012)

Verizon's 2015 DBIR

Figure 44.

B2B Internet of Things connections, 2011 to 2020 (forecast)



Thank You

Lynn D. Shiang
Delta Risk LLC, A Chertoff Group Company
O: 314.918.7499
C: 314.650.4498
www.delta-risk.net