Natural Gas Utility Threat Analysis Elements & Mitigations – Cyber

[insert company name]

August, 2014

Introduction & Disclaimer

This product is intended to serve as a guidance or template for AGA member company cybersecurity professionals to use to engage their corporate senior leadership in discussion of leading cyber-based threats to the gas utility industry as of the date of this product release and as identified by the AGA Board-appointed Cybersecurity Strategy Task Force. The identified threats are not listed in any particular order or ranking. This product identifies industry practices employed at various points of incident mitigation and measures a company may/may not choose to employ. Due to the extent of operational diversity across the natural gas utility industry, the content of this slide deck is intentionally presented at a high-level; deferring to the presenter to interject company-specific actions and measures.

Threat & Elements

Coordinated Physical & Cyber Attack

Description:

A coordinated campaign of cyber and physical attacks on multiple natural gas targets that may rapidly bring the systems and the operators beyond their capability to effectively assess, prevent, respond to, or recover from the combined effects of the attacks. The attacks could also be timed to coincide with another wide-scale impacting event such as natural disasters or accidents to maximize the disruption or increase the attacks' likelihood of success.

Impact of Successful Compromise:

A successful campaign could potentially reach across multiple owner-operator entities causing disruption and/or destruction of storage, transportation, or delivery of natural gas through the system. Attacks could negatively impact reliability, safety, profitability, or reputation of a company or the natural gas industry. This could lead to elongated loss of gas supplies, injury, or loss of life.

Target Types:

- Control Systems
- Physical Infrastructure (e.g., city gate stations, compressor stations, LNG facilities, pipelines)
- Communication Systems (e.g., voice and data)
- Key Company Personnel

Threat Actors:

- Nation States
- Terrorists
- "Hactivists"
- Criminal Cyber Actors
- Insiders, including Employees and/or Contractors

Attack Vectors:

- Denial of Service
- Social Engineering
- Sabotage
- Disruption of Communications
- System Vulnerabilities (e.g., Missing Patches, Malware, Insecure Coding)

General Mitigation Actions

Coordinated Physical & Cyber Attack

PHASE	MITIGATION
Preparedness	• Training – Cyber and physical security awareness • Incident Response Plan (IRP) tabletop exercises, including law enforcement contacts • Situational Awareness – Information sharing, intelligence gathering, background checks • Assessments – Vulnerability, penetration, risk
Prevention	• Governance • Overpressurization prevention hardware • Cyber and physical event logs monitoring • Controls audit and testing • Control systems access and authorization
Response	• IRP execution • Reporting to regulatory government agencies • Voluntary sharing of information with trusted entities
Recovery	• Business Continuity Plan / Disaster Recovery (BCP/DR) implementation and remediation • After Action Plan (AAP) – Governance review, Root Cause Analysis and Lessons Learned; Implement Preparedness, Prevention, and/or Response Improvements

Threat & Elements

Information Theft, Loss, or Misuse

Description:

Intentional or inadvertent loss of information, i.e., copied or taken, including personally identifiable information, corporate information, and/or intellectual property. The following factors can contribute to information loss:

- Increased amounts of sensitive data
- Economics of hacking and cybercrime
- Systems complexity, new technologies, and the accompanying vulnerabilities
- Use of devices or resources outside the control of a business

Impact of Successful Compromise:

The breach, theft, or loss of proprietary and confidential information can have costly and immediate consequences, ranging from regulatory fines, lost business opportunities, fraudulent use of the information, damage to brand, and/or loss of customer confidence.

Target Types:

- Personally Identifiable Information (e.g., Name, Address, SS#, Credit/Banking Card)
- Business Plans
- Financials
- Intellectual Property

Threat Actors:

- Nation States
- "Hactivists"
- Criminal Cyber Actors
- Insiders, including Employees and/or Contractors

Vectors:

- Social Engineering
- System Vulnerabilities (e.g., Missing Patches, Malware, Insecure Coding)
- Intentional/Unintentional Data Loss
- Device Loss or Theft (e.g., Laptops, Smartphones, Back-up Media, Servers, Removable Media)
- Third Party or Business Partners

General Mitigation Actions

Information Theft, Loss, or Misuse

PHASE	MITIGATION
Preparedness	• Governance – Information protection policies and procedures; contract clauses with business partners • Awareness – Information classification and protection • IRP – Exercises, cyber insurance, credit monitoring, background checks, notification plans, contracts
Prevention	• Governance • Monitoring – Log management, security event monitoring, data loss prevention system, vendor contract management by business owner • Perimeter Security – Intrusion prevention/detection, demilitarized zone (DMZ), firewalls • Risk Management – Risk assessment, security testing, patch management • Access Policy – Data classification, physical and cyber access controls, encryption, Least Privilege Access
Response	• IRP execution • Communications – Management, customers, media, law enforcement, regulators, etc.
Recovery	• Impacted System Integrity • AAP – Governance review, Root Cause Analysis and Lessons Learned; Implement Preparedness, Prevention, and/or Response Improvements • Remediation Plan

Threat & Elements

Cybersecurity Breach of Critical Natural Gas Infrastructure

Description:

Unauthorized access and compromise of one or more components of SCADA, Industrial Control Systems, or Compressor Station systems to disrupt access to real-time data from field equipment resulting in loss of control and situational awareness of field operations.

Impact of Successful Compromise:

A successful cyber attack could cause disruption and/or destruction of storage, transportation, or delivery of natural gas. An incident could negatively impact reliability, safety, profitability, or reputation of the company and could lead to elongated loss of gas supplies, injury, or loss of life.

Target Types:

- SCADA Systems
- Control Systems
- Communications Systems

Threat Actors:

- Nation States
- Terrorist
- "Hactivists"
- Insiders, including Employees and/or Contractors

Vectors:

- Social Engineering
- Sabotage
- Disruption of Communications
- System Vulnerabilities (e.g., Missing Patches, Malware, Insecure Coding)
- Removable Media
- Third Party or Business Partners

General Mitigation Actions

Cybersecurity Breach of Critical Infrastructure

PHASE	MITIGATION
Preparedness	• Training – Security awareness and user training • Situational Awareness – Information sharing, intelligence gathering • Redundancy – BCP/DR • IRP table top exercises, BCP/DR exercises
Prevention	• Governance • Overpressurization prevention hardware • Monitoring and Threat Analytics • Hardening/Patching • Assessments – Vulnerability and penetration testing • Network Segmentation
Response	• IRP – BCP, investigation, impact, safety review • Situational Awareness – Bidirectional information sharing with peers • Communications – Management, customers, media, law enforcement, regulators, etc.
Recovery	• DR – Invoke if warranted • Remediation, reinstallation, service restoration from backups • AAP – Document findings and Lessons Learned

Threat & Elements

Dependency on Telecommunication Infrastructure

Description:

Disruption of the telecommunications systems and associated infrastructure and services that serve as the backbone for many critical infrastructure components dependent on these systems to perform their missions. Organizational response relies on telecommunications; making it a target for a coordinated attack timed to coincide with another wide-scale impacting event.

Impact of Successful Compromise:

A successful campaign could impede a company's management and support of SCADA and other critical business systems, i.e., situational awareness. The inability to communicate with key personnel and/or first responders could risk safety and negatively impact response efforts. Reduction of communications could result in adverse public reaction (e.g., customer, regulator, and shareholders) and negatively impact company reputation.

Target Types:

- Communication Systems, (e.g., voice and data)

Threat Actors:

- Nation States
- Terrorist
- "Hactivists"
- Criminal Cyber Actors
- Insiders, including Employees and/or Contractors

Attack Vectors:

- Denial of Service
- Sabotage
- Malware

General Mitigation Actions

Dependency on Telecommunication Infrastructure

PHASE	MITIGATION
Preparedness	• Training – Cybersecurity awareness, cyber education • IRP tabletop exercises, BCP/DR exercises • Situational Awareness – Information sharing, intelligence gathering • Assessments – Vulnerability, risk, network reliability and failover
Prevention	• Governance • Telecommunication systems monitoring • Telecommunication equipment and facilities security • Telecommunication equipment patching • Telecommunication redundancy, (e.g., multiple channels) • Carrier and technology diversity
Response	• BCP/DR Implementation • Situational Awareness • Managed public relations, corporate reputation and messaging • Alternative Internal Communications • Redundant systems and equipment
Recovery	• Remediation, reinstallation, service restoration • AAP – Governance review, Root Cause Analysis and Lessons Learned; Implement Preparedness, Prevention, and/or Response Improvements

Threat & Elements

Lack of Employee Understanding and/or Awareness of Cybersecurity

Description:

Many cybersecurity attacks and compromises can be traced back to a human action or inaction as part of the initiating event. People are both the largest vector to introduce threats into the environment as well as the best defensive technique to prevent the threats. An enterprise cybersecurity program requires an aware and well-trained workforce in addition to the technology layers for a mature strategy.

Impact of Successful Compromise:

Attackers may gain control or access to a company computer, move laterally within the network to discover more vulnerabilities, gain access to or steal company data (including intellectual property), and disrupt business operations. This threat is typically an initiating event to one of the other threat scenarios. This compromise may also negatively impact business reputation.

Target Types:

- Executives
- Employees
- Contractors
- Third Party or Business Partners
- Customers

Threat Actors:

- Nation States
- Terrorists
- “Hactivists”
- Criminal Cyber Actors
- Insiders, including Employees and/or Contractors

Vectors:

- Social Engineering
- Spearphishing
- Vulnerability Management
- Intentional/Unintentional Employee Error
- Personal Devices (e.g., Laptops, Smartphones, Removable Media)
- Third Party or Business Partners

General Mitigation Actions

Lack of Employee Understanding and/or Awareness of Cybersecurity

PHASE	MITIGATION
Preparedness	• Training – Cybersecurity awareness; management understanding of impact; incident reporting/response • Security policy maintenance and updates • Situational Awareness – Information sharing and incident reporting
Prevention	• Governance • Security policy monitoring and enforcement • Situational Awareness – Threat assessment • Periodic and new employee training • Reward and recognition program • Social engineering testing exercises
Response	• BCP/DR Implementation • Employee cybersecurity awareness metrics • Security incidents reporting to management • Security policy enforcement
Recovery	• Root cause analysis • Employee and supervisor awareness of non-compliance • Security policy and partner contracts review

Glossary of Acronyms

AAP	After Action Plan
BCP	Business Continuity Plan
DMZ	Demilitarized Zone
DR	Disaster Recovery
IRP	Incident Recovery Plan
LNG	Liquified Natural Gas
SCADA	Supervisory Control And Data Acquisition
SS#	Social Security Number

[insert presenter contact information]