Understanding CrowdStrike & Other Security Threats to the Energy Industry

Adam Stahl, Avangrid, Chief of Staff (Corporate Security & Resilience)

Avangrid Corporate Security & Resilience

Avangrid
A member of the Iberdrola Group

Corporate Security & Resilience

Table of Contents

Crowdstrike Incident (Background)

- **Incident**: Global IT outrage (July 15) disrupting populations across multiple sectors (commercial + air travel)
- **Crowdstrike**: Company provides security software products for businesses, designed to protect endpoints (computers, servers, phones, etc.) from cyber attacks
- **Cause**: Faulty software update to software (buried within Microsoft Office operating systems) on Windows PCs and servers
- **Applicable Systems**: Systems running Windows 10 and Windows 11 (primarily on non-personal devices)
- **Result**: System “crashes” (Reboot loop, invalid page vault)
- **Remedy**: Forced reboot (connect to network), large percentage machines required
- **Devices Impacted**: ~8.5 million devices (>1% Microsoft devices)

CrowdStrike Incident (Impacts by the #s)

Corporate Security & Resilience

Significant commercial/travel impacts, *but* little disruption to critical operations (safety, security, reliability)

Commerce/Travel

- **49 million** customers impacted (directly and indirectly)
- Air Transportation: **2,000+** flights canceled, **9,200** delayed
- Healthcare: 12 Hospitals impacted (only elective surgery delays **$1.94B**)
- Financial Sector: Select, temporary bank (TD Bank), payment service (PayPal, Venmo) disruption
- Air Freight: Air cargo transit times **+25%,** no impact
- Fortune 500 Financial Impact: **$5.4 billion**

Critical Operations

- Energy Delivery: No impact (customer support disrupt)
- Hospital: Critical surgeries/functions interrupted
- Telecom Connectivity: No impact
- Emergency Services: Three states (IP-enabled dispatch system manual operation)

Key Lessons

CROWDSTRIKE INCIDENT (MICRO)

While only debilitating commercially/financially, **extremely fortunate** no acute reliability impacts to critical services (limited duration and scope, remediation)

- Strengthen Software Testing/Deployment Requirements
- Risks of Vendor Monopolization
- Robust Contingency Planning

BIG PICTURE (MACRO)

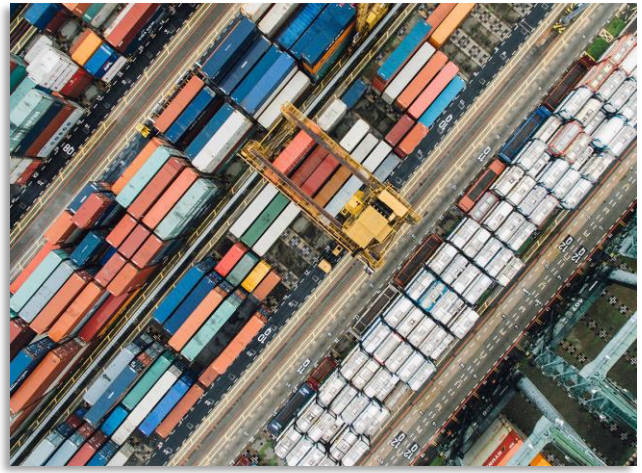
Spotlights supply-chain fragility in a global, digitalized, and interconnected world (acute security, safety impacts in sustained event)

Understanding the Supply-Chain Threat (Evolution)

Corporate Security & Resilience

CURRENT ENVIRONMENT:

- More dynamic, automated, and interconnected than ever before, introducing efficiencies and risks (IT/Communication and Energy)



KEY DRIVERS:

- **Geopolitics**
  - Economic Volatility (Trade Wars, Tariffs)
  - War (Russia-Ukraine, Middle East, Indo-Pacific)

- **Changing Weather Patterns**
  - Rising Sea Levels, Wildfire Increasing

- **Technological Advances**
  - IoT Deployment, Software (OT/IT Convergence)
  - Data Analytic Advancements: Cloud technology, AI

- **Growing Energy Reliance**
  - Demand/consumption increases (e.g., AI revolution), Electrification

Dissecting the Supply-Chain Threat (Physical)

Malicious Events (Man-made)

- Supply-chain Weaponization (Embargos)
  - Russia: Ukraine Gas Wars (2009, 2014, Present)
  - China: Raw Material/Resource consolidation (e.g., Chips, EV batteries)
  - Middle East: Houthi Attacks in Red Sea
- Firmware (Huawei)
- Counterfeits (safety, reliability impacts)

Accidental Events (Man-made)

- Transportation accidents (Suez Canal, Francis Scott Key Bridge)
- Fire events (Semiconductor Fire in Taiwan)

Wildfires, Floods, Hurricanes (Natural)

- Winter Storm Uri (2021): Collapsed Energy Grid, Disrupted Fuel Access (161 deaths)

Dissecting the Supply-Chain Threat (Cybersecurity, Software)

Malicious (Intended)

- Third-Party Cyber Vendor Attacks
  - Operational, Business Disruptions (e.g., Ransomware, Phishing)
  - Software Supply-Chain Infiltration (SolarWinds)

Unintentional

- System Crashes: Faulty Software Updates (e.g., Crowdstrike incident)
- Security Vulnerabilities: Outdated Software, Misconfigured Systems (e.g., Zero Day vulnerabilities)

Ongoing Efforts (Public, Private Sectors)

Corporate Security & Resilience

Regulatory/Legislative Actions (Physical, Cyber)

- Critical Resource/Mineral “Onshoring”/“Nearshoring” (IRA, Solar Tariffs, CHIPS Act)
- Cybersecurity Vendor Standards (Executive Order 14028)

Supply-Chain Forecasting/Modeling (Physical)

- Public Sector Research Centers (DHS Supply Chain Resilience Center, DOE Manufacturing & Energy Supply Chain Office)

Intelligence Collaboratives (Cyber)

- Real-time intelligence sharing, including supply-chain information
  - Joint Cyber Defense Collaborative, CISA (cross-sector)
  - Energy Threat Analysis Center, DOE (oil, gas, electricity)

Supply-Chain Risk Illumination Tools/Initiatives

- Vendor Scoring Tools
- Supply-Chain Inventories (Hardware/Software Bill of Materials)
- Software/Physical Vulnerability Testing (CyTRICS, CISA scanning and testing)

Avangrid's Supply-Chain Risk Management Approach

Corporate Security & Resilience

Assessing supply-chain risk management through an operational reliability, business continuity lens

Vendor Vetting, Risk Vulnerability Analysis

- Understand where vendor resides in enterprise asset, function criticality.
- Assess Vendor
  - questionnaire
  - security history
  - cyber hygiene ratings
  - risk scoping (geopolitical, geographic, regulatory),
  - supply-chain mapping (1st, 2nd, 3rd tier)
- Additional Factors (Risk Appetite, Vendor diversity)

Mitigation, Resiliency Measures

- Controls
  - Governance (Policies, Standards, Tools)
  - Contractual Documentation (Data Security riders)
  - Cyber Insurance
  - Beta Testing (OT software sandbox)
- Incident Response, Business Continuity Plans (drilling)
  - Cyber forensics
- Secure Operational Redundancies (alternative suppliers)

Persistent Monitoring

- Threat, Cyber Intelligence monitoring
  - Tools (Dark web monitoring, OT/IT sensors)
  - Partnerships (Federal, State, ISACs)
- Frequent Reviews (high risk, critical vendors, audits)

Conclusion: Key Challenges, Takeaways

Supply-Chain Security is a shared, whole-of-society responsibility (Industry, Government, Consumers)

Companies can take proactive measure to strengthen resiliencies in an increasingly volatile supply-chain landscape, including:

- Robust vendor vetting
- Incident Response, Business Continuity Planning
- Partnership Building (intra-Company and with Public and Private sector partners)

Companies must look at vendor costs beyond the “price tag”


Avangrid
A member of the
Iberdrola Group
Corporate Security
& Resilience