National Institute of
Standards and Technology
U.S. Department of Commerce

CASE STUDIES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Observations from Industry

Anonymous Renewable Energy Company

February 4, 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.02042020-4

Jon Boyens
Celia Paulsen
Computer Security Division
Information Technology Laboratory

Nadya Bartol
Kris Winkler
James Gimbi
Boston Consulting Group

SERIES DESCRIPTION

The *Case Studies in Cyber Supply Chain Risk Management* series engaged with several companies that are mature in managing cyber supply chain risk. These case studies build on the Best Practices in Cyber Supply Chain Risk Management case studies originally published in 2015 with the goals of covering new organizations in new industries and bringing to light any changes in cyber supply chain risk management practices.

For information on NIST's Cyber Supply Chain Risk Management project, see https://csrc.nist.gov/projects/cyber-supply-chain-risk-management.

DISCLAIMER

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose.

Contents

Company Overview

The Renewable Energy Company is a vertically integrated solar power company headquartered in the United States. The company is one of the largest solar panel manufacturers in the United States and operates photovoltaic (PV) power plants all over the world. As research from the company and other manufacturers makes solar power more accessible, the market share of solar energy in the power supply landscape continues to grow.

Risk Profile

The Renewable Energy Company operates two separate business lines. The manufacturing business produces solar panels used all over the world. These products require components and materials from suppliers operating in disparate regions with different levels of cybersecurity and supply chain risk management maturity. The second business line—energy services—builds, acquires, and operates PV power plants. Operating critical infrastructure introduces stringent compliance requirements, and the impact of power disruptions on downstream customers obliges the Renewable Energy Company to develop and maintain robust and consistent risk management processes.

Highlighted Practices in Cyber Supply Chain Management

- **Consolidate global regulatory requirements into common processes.** Critical infrastructure operations invoke different compliance obligations from region to region. The Renewable Energy Company is consolidating these cybersecurity and supply chain obligations into a single set of requirements to be applied globally. This is expected to simplify compliance and supplier management while enhancing the company's global security posture.
- **Include access requirements when evaluating criticality.** Traditional criticality assessments may not capture the full scope of a supplier's potential impact. Consider attack-surface factors, such as a supplier's access to information technology (IT) networks or physical facilities, to more accurately evaluate supplier criticality.
- **Limit unnecessary access to sensitive systems.** Apply the principle of least privilege to acquired businesses and suppliers with access to Information Technology (IT)/Operational Technology (OT) networks. The Renewable Energy Company isolates newly acquired PV power plants until they replace existing systems with controlled, mature systems that can be safely integrated with the company's infrastructure.

Organizational Approach to Supply Chain Risk and Cybersecurity

The Renewable Energy Company's manufacturing and energy services businesses have separate operations and supply requirements. However, their vertical alignment allows a single supply chain team to handle governance and supply chain risk management for the entire company. The global supply chain team consists of over a dozen full-time employees under the Vice President of Supply Chain Global and Value Chain and works closely with the information and cybersecurity team to identify the spectrum of cyber risks facing the supply chain. These teams perform joint, post-incident reviews and hold an annual internal conference to discuss developments in the threat landscape.

The Board of Directors has become more involved in cyber supply chain risk management (C-SCRM) in recent years. The Director of IT Security meets with the Board on a quarterly basis to keep the members apprised of the Renewable Energy Company's efforts and challenges in the C-SCRM space.

Supplier Management

Key Aspects of Managing Supplier Relationships

Contractual requirements conformant with cyber hygiene best practices are the Renewable Energy Company's principal tool for managing cyber supply chain risks. When a new supplier is engaged or an existing contract is renewed, the supplier must provide assurances that account for cybersecurity controls and cyber insurance. Suppliers must also demonstrate compliance with relevant privacy and critical infrastructure regulations, such as the European Union's General Data Protection Regulation (GDPR) and the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP), which is enforced by the Federal Energy Regulatory Commission (FERC). These contracts are refined on an ongoing basis and give the Renewable Energy Company the right to audit vendor processes and practices.

Global supply line management introduces unique regulatory challenges. The Renewable Energy Company's vendors operate in several countries, each with separate standards and compliance obligations. This complicates the development of contract requirements, as well the company's own cybersecurity and supply conformance practices. To account for this complexity, contract requirements are written assuming the widest possible interpretation of regulatory obligations.

The Renewable Energy Company acknowledges that these contract requirements can be difficult to satisfy. Over 30 % of their suppliers are specialized small businesses which depend on the Renewable Energy Company to stay in business. These firms often struggle to develop the type of mature cybersecurity capabilities that are more common at larger companies. Other suppliers are simply not aware of the cybersecurity and supply chain risks they face, which impedes the cultural shift necessary to improve their practices. But the Renewable Energy Company's intimate supplier relationships allow them to manage a supplier's cybersecurity risks on an individual level. The company often provides guidance to elevate a supplier's cybersecurity capabilities and implements specialized monitoring practices to account for unresolvable gaps. The company has, at times, augmented smaller suppliers' response for cybersecurity incidents. In one instance, a vendor fell victim to a series of business email compromise attacks. The Renewable Energy Company guided the vendor's response and recovery, minimizing the impact on both companies.

Measuring Supplier Risk

The Renewable Energy Company's key driver for cyber supply chain risk management is mitigating the negative business impacts of supply disruptions and component compromise. These impacts can lead to the inability to deliver products and services, additional cyber attacks on the company and downstream customers, or noncompliance with regulatory requirements. Compliance violations can be particularly impactful; direct fines from FERC for NERC CIP violations have been as high as $10 million and can accrue additional penalties of up to $1 million each day[i].

While many of the Renewable Energy Company's suppliers provide commodity products, the company relies on a small number of critical suppliers that provide complex digital components or specialized materials. The Renewable Energy Company considers two factors when determining a given supplier's criticality. First is the supplier's level of access to the company's network and facilities. For instance, an external robotics programmer would require physical access to the manufacturing floor and OT network and may require access to the larger IT network. The second factor to consider is the potential business impact of failure or compromise. The Renewable Energy Company prioritizes suppliers with high potential impacts on the power grid and proactively monitors them at the Security Operations Center.

The Renewable Energy Company regularly evaluates existing supplier relationships for opportunities to improve visibility and constructive influence over critical manufacturing processes. Beyond strict cybersecurity requirements, the company considers each supplier's business baseline and bankability. This includes evaluating balance sheets to determine a vendor's stability and long-term viability.

Quality Management and Continuous Improvement

When the energy services business acquires new solar power plants, the Renewable Energy Company assumes unknowable risks due to the sparse or non-existent visibility into the plant's production. To better understand and manage the risks presented by newly acquired power plants, the company is building an internal capability for assessing technical cybersecurity controls and NERC CIP compliance on subsidiary sites. Alongside technical controls, the Renewable Energy Company's legal team is also working to limit the company's exposure to these risks in purchasing agreements.

The cybersecurity posture of these acquired plants varies widely. Some are quite mature while others lack vulnerability management and antivirus implementations. The Renewable Energy Company isolates new plants with an additional access control layer while it identifies and mitigates risks posed by the new assets. The acquired network is monitored and studied by the

Renewable Energy Company's Security Operations Team, and over time, a dedicated team replaces the existing systems at the acquired plant with controlled, mature systems that can be safely integrated with the company's infrastructure.

Every region of the power grid is controlled and coordinated by separate regional transmission organizations (RTO), independent system operators (ISO), and other global equivalents. Each region's RTO or ISO may establish regulations unique to their region. Power providers, such as the Renewable Energy Company, are responsible for making sure their entire supply chain is compliant with the requirements in a particular region. The company is working to merge these requirements into a unified minimum standard across all suppliers regardless of region. This robust standard would simplify compliance and supplier management while enabling the global cybersecurity posture of the Renewable Energy Company and its suppliers to exceed any one given requirement.

Because power systems are a vital part of critical infrastructure, product reliability and integrity are paramount. The Renewable Energy Company must test for flawed or deliberately compromised hardware and software as well as traditional supply chain risk management functions involved in logistics, materials, and assembly. The company is investing in more thorough and advanced component integrity inspections to mitigate potential supply chain attacks by advanced threat groups. Recognizing the operational and compliance complexity of critical infrastructure logistics, the Renewable Energy Company outsources transit logistics to specialized providers.

Recycling is a valuable piece of the Renewable Energy Company's manufacturing business. Components from end-of-life products are often installed in new units, eliminating unnecessary cost and waste. Each component is inspected for potential integrity issues before it can be used in new products. To ensure that only safe and high quality components are recycled, the Renewable Energy Company only accepts materials from products they produced and only from the original purchaser. This policy gives the company thorough control of material integrity and does not significantly impact their recycling intake.

Incident Response and Recovery

The Renewable Energy Company's solar panel production leverages a "just-in-time" manufacturing workflow, lowering operation costs and delivering consistent quality control. However, this lean workflow is inherently vulnerable to supply disruptions. The company tracks potential causes of disruption and maintains response plans for potential supply line incidents. Manual processes are in place as fallback for automated procedures. Moreover, the Renewable Energy Company secures contracts with alternate suppliers in the event of an emergency, which enables continued production at a premium. The company stays ahead of potential supply disruptions by paying for premium assurances from suppliers whenever they are available.

Every cybersecurity-related incident is managed through a comprehensive incident response plan (IRP). The IRP requires the Renewable Energy Company to perform a review after an incident is resolved to improve their detection and response processes. These improvements may also be augmented by input from suppliers.

The Renewable Energy Company's predominant supply security issue is site-level physical security. In the past, theft of solar panels and other components was relatively common. All components are now outfitted with barcodes for tracking, and the Renewable Energy Company is investing in radio-frequency identification (RFID) tagging for more capabilities. Further, components are manually inspected on-site for evidence of tampering or quality concerns, and incidents of theft and destruction are promptly reported to local police. The company also inspects all billing records for evidence of theft or fraud.

International supply lines may be impacted by broader economic and geopolitical risks as well as operational complexity. Future escalations in trade tensions, such as tariffs and sanctions, may add uncertainty to continued operations. The Renewable Energy Company is preemptively developing plans to navigate any disruptions to existing supplier relationships. Importantly, the company secures alternate vendors for every component whenever possible. However, there are a few critical components only offered by a handful of manufacturers. To mitigate the impact of disruptions for those suppliers, the Renewable Energy Company maintains a quantity of those products in reserve.

Lessons Learned and Improvement Opportunities

The Renewable Energy Company recommends that companies interested in maturing or developing new C-SCRM programs should focus on uplifting the cyber hygiene practices of their vendors. Instead of focusing exclusively on manufacturing or logistics processes, companies and vendors should work together to improve their entire security posture, allowing them to fully appreciate and benefit from mechanisms such as multi-factor authentication and logical segmentation.

The Renewable Energy Company is also investing in emerging production security solutions, such as machine learning-powered monitors for the manufacturing floor designed to highlight predictive indicators. This technology is expected to improve business operations by enabling better understanding of the product lifecycle, improving manufacturing processes, and informing better warrantee offerings.

References

[i] Enforcement Actions 2019, North American Electric Reliability Corporation (NERC), https://www.nerc.com/pa/comp/CE/Pages/Actions_2019/Enforcement-Actions-2019.aspx, (retrieved September 16, 2019)