Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ISSUE BRIEF

Supply Chain in the Software Era

MAY 2018 BEAU WOODS AND ANDY BOCHMAN

Executive Summary

This issue brief analyzes cyber supply-chain risk across the energy sector, ranging from oil and gas to electricity, renewables, and nuclear.[1] Operational practices and supply chains, while not identical across all of these segments, are similar enough to support a common analysis. While there is already a large body of work, key aspects of cyber supply-chain risk in the energy sector remain underexamined. After an extensive review of existing literature, the research focus narrowed to a much-overlooked significant aspect of the energy sector—flaws in software components unintentionally built into products in design or implementation. These flaws are called *"unintended taint,"* as distinct from both counterfeit—substituting lesser quality or imitation products—and "*malicious taint*," which is intentional supply-chain subversion.

Bookending the research between 2015 and 2017, two high-profile cyberattacks in Ukraine and Saudi Arabia leveraged supply-chain vulnerabilities to impact operations at two energy sector organizations. In December 2015, hundreds of thousands of Ukrainian homes were temporarily plunged into darkness in the first confirmed cyberattack against an electric grid.[2] In August 2017, a cyberattack halted operations at Saudi Aramco.[3] In both cases, improvements in the security of supply-chain components would have halted the attacks.[4]

1 In addition to energy systems, other industrial sectors (e.g., transportation, heavy manufacturing, chemical, water, and waste water) depend on similar equipment from the same suppliers who support energy sector operations.

2 Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

3 Elias Groll, "Cyberattack Targets Safety System at Saudi Aramco," *Foreign Policy*, December 21, 2017, http://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/.

4 In the Ukrainian case, software update mechanisms were abused to gain access to grid control systems. In the Saudi Arabia case, avoiding default, hardcoded credentials provided remote access to the plant control systems network.

A Saudi Aramco in Jubail, Saudi Arabia. *Photo credit:* Suresh Babunai (http://creativecommons.org/licenses/by/4.0/).

Cyber supply-chain security has become a prominent issue in the energy sector, and the attempts to address it are growing. For instance, the North American Electric Reliability Corporation (NERC) is updating its Critical Infrastructure Protection (CIP) standards to include supply-chain protections.[5] Additionally, companies like BitSight,[6] Security Scorecard,[7] and Sir-Track (in Germany),[8] which measure "digital exhaust," are increasingly used to measure public, observable artifacts of third-party suppliers' Information Technology (IT) and IT security practices. However, gaps still exist—NERC-CIP applies to only a subset of systems and components that impact safety and reliability at a subset of electric utilities, and measuring Internet-facing security is (at best) an indirect bellwether of the technology used in energy sector control systems.

Several alternative courses of action are recommended to address these issues.

- Apply Existing Frameworks Across the Energy Sector—Energy sector companies or the Department of Energy (DOE) can leverage existing frameworks, particularly the NERC-CIP standard and the DOE's Cybersecurity Capability Maturity Model,[9] as blueprints for improving security across the energy sector, including third-party suppliers.

- Incentivize Trusted IT Practices to Avoid Unintended Taint in the Energy Sector—Congress, the DOE, and energy sector companies can increase awareness and adoption of practices that are known to be effective, and avoid those that are known to be ineffective, through reduction of regulatory burden, use of buying power, or other incentives.

- Vulnerability Monitoring, Coordination, and Sharing—The DOE, the Department of Homeland Security (DHS),

5 "Cyber Security – Supply Chain Risk Management Number CIP-013-1," NERC, accessed March 25, 2018, http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf.

6 BitSight, accessed March 25, 2028, https://www.bitsighttech.com/.

7 Security Scorecard, accessed March 25, 2018, http://securityscorecard.com.

8 A sample of Sir-Track findings relevant to the energy sector, accessed March 25, 2018, https://sir-track.com/beispielrankings.html#energy.

9 "Cybersecurity Capability Maturity Model (C2M2) Program," Energy.gov, accessed March 25, 2018, https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program.

and industry organizations can increase awareness and understanding of existing software vulnerabilities across the sector to reduce information asymmetry among organizations affected by the same or similar issues.

- Examine Other Models of Operation, Liability, and Regulation—Congress, the DOE, and DHS, as well as other affected stakeholders should identify and analyze alternative approaches to operation, liability, and regulation, which may increase safety, security, and reliability across the energy sector.

Supply Chain in the Software Era

Since the beginning of the industrial revolution in the early 19th century, achieving and maintaining a high level of competence in supply-chain management has been a necessity for all companies, both large and small. Software is increasingly an integrated supply-chain component.

Depending on the good or service being sourced, suppliers remain valued for a number of familiar attributes, including reliability, speed, quality, safety, price, compliance with standards, energy efficiency, and in some domains, innovation. The supply chain for energy sector equipment increasingly includes digital components: hardware, firmware, and software—lots and lots of software. Software is now deployed on local servers and other devices, as well as from faraway data centers that are most often hosted by third parties offering application delivery, data storage, and computing power as services. In the electricity sector, "smart grids" and "smart meters" are computer-controlled, network-connected versions of their traditional counterparts.

While silicon is the substrate of this new smartness, the story is almost entirely propelled by software. Software is what animates the machines, determines which messages are passed (or broadcast) between machines, generates, and is, in various forms, the content of those messages. It is truly the most vital enabler of the modern world, in general, and the revolution in connected devices, now known as the "Internet of Things" (IoT), in particular. Furthermore, software as a raw material is extremely malleable under pressure from the right combination of finger strokes, which can bring both strategic advantages and weaknesses when embedded in the world through dependence on connected technology.

Properties of software components, which confer cost, safety, and efficiency benefits, are less reliable than those they are replacing. Traditional isolated mechanical and electrical components can be made provably reliable and safe through well-understood concepts and practices. However, the malleability of general-purpose computing components provides pathways for accidents and for adversaries to undermine their reliability and safety.[10]

Software security vulnerabilities are a natural result of the development process and—despite best efforts—cannot be fully eliminated. Each year, more than 10,000 security vulnerabilities are discovered in common off-the-shelf (COTS) components.[11] They show up in global cyber supply chains, including those of the energy sector; and weaknesses and vulnerabilities in software design and implementation accrue along the multistep journey through the supply chain, whether intentional or accidental. When vulnerabilities are passed through the supply chain, which is a common occurrence, a single software component can compromise the operational integrity of critical systems. For instance, hardcoded default passwords—a known class of supply-chain vulnerabilities—in a safety-instrumented-systems component facilitated a shutdown of Saudi Aramco operations in December 2017.[12] As the industry stands ready to reap benefits from IoT, cloud, mobile, and others, these technologies also increase the size, depth, and complexity of the supply chain. This confluence of factors has driven cybersecurity to become one of the most pressing concerns of the energy sector.[13]

In particular, cloud-dependent processes cede safety and security decisions to third parties who rarely pass along details about risk-management processes and thresholds that are sufficient for energy sector compa-

10 While the concept of provable software security is under active development in academic and government research communities, successes seem to be limited to certain practices or components, such as cryptography, and do not seem to scale to the size and complexity of energy sector systems.

11 CVE Details, accessed March 8, 2018, http://www.cvedetails.com/top-50-products.php?year=2016.

12 Robert M. Lee, "Trisis," Dragos Blog, December 14, 2017, https://dragos.com/blog/trisis/index.html.

13 The power sector, for instance, rated "physical and/or cyber grid security" as the number one issue according to immediate importance to the company. UtilityDive, 2017 State of the Electricity Utility Survey, accessed March 8, 2018, https://www.utilitydive.com/news/why-utilities-dont-think-trump-will-stop-the-clean-energy-transition/439138/.

A high performance computing center in Stuttgart, Germany. *Photo credit:* Julian Herzog (http://creativecommons.org/licenses/by/4.0/).

nies to fully understand the implications. The need for real-time, always-on connectivity increases the number of partners through which a cyber incident might flow. Additionally, cloud data practices can cause uncertainty and delay in understanding operational implications of a cloud data breach. Finally, as decision making is automated and highly augmented through machine learning or artificial intelligence, traditional protections from human-in-the-loop processes may become absent.

Impacts to Safety, Security, and Reliability

In the energy sector, cybersecurity poses risks not just to financial or data assets, but also life-threatening physical damage or destruction of equipment from successful attacks on operational technology (OT) systems. Impacts to energy sector systems could cause prolonged disruptions to the energy supply—oil, gas, and electricity—which have the potential to wreak havoc on other sectors and to affect citizens in their homes as well. The government and the electric sector have developed and implemented several controls to reduce the supply-chain risks, including current NERC-CIP efforts.[14]

Most industrial equipment is protected by safety systems that are designed to safely shut down processes when something out of the ordinary is detected. In pursuit of efficiency, cost savings, and convenience, former mechanical safety systems are now increasingly driven by software and automation. Yet, software engineers have been aware of the dangers of "reliance on software to perform safety-critical checks"[15] since the 1980s, when a medical device killed and maimed several people because of unintended software defects. Further connecting these systems to corporate networks and the Internet increases their susceptibility to hazardous and hostile conditions from accidents and adversaries.

14 "Cyber Security – Supply Chain Risk."

15 David Rice, *Geekonomics: The Real Cost of Insecure Software* (New Jersey: Addison-Wesley, 2007), 142.

Most of these systems are "insecure by design."[16] Industrial control systems (ICS) engineers tend to design systems in such a way that they fail safely in predictable contexts. For instance, hardcoded passwords ensure that engineers can access systems in emergencies without regard for complex, unique credentials. At the same time, adversaries can also access and use these systems if they are connected to the Internet. This design undermines security, which can impact safety, and lowers the bar such that anyone who can search the Internet for the default password can potentially cause harm. These design patterns have manifested in high-profile incidents across the energy sector. (See breakout box for examples.) Yet, despite knowledge of the dangers and of more secure failsafe methods, "insecure by design" controls systems[17] are exposed to the Internet.[18]

If the energy sector cannot reconcile cybersecurity with reliability and safety, it may realize neither. When the consequences of failure impact the infrastructure that supports the global economy and national security, like the energy sector, a higher standard of care is merited for managing cyber supply-chain risk. This is why the energy sector has placed so much emphasis on ensuring the integrity of supply-chain partners and components.

Much of the cyber supply-chain landscape is well-worn. While these challenges are by no means solved in theory or in practice, it would do a disservice to the volumes of material in mature areas of cyber supply-chain risk to try to cover them extensively. Instead, this issue brief defines and focuses on unintended taint, particularly known, but unmitigated, vulnerabilities, which are less well represented in public policy documentation. A rough framing will provide context and clarify scope.

- **Supplier-Facilitated Risk**: Cybersecurity of third-party partners who can influence energy-sector operations. For instance, systems integrators who design and implement products into energy-sector operations environments, as well as other vendors who have physical or network access.

- **Counterfeit**: Components that come through an unauthorized channel, are not authentic, and would fail a sufficiently rigorous validation. Counterfeiters are typically motivated by financial gain, buying inexpensive components and passing them off as more expensive ones. Negative impacts on energy operations are often an unintended consequence.

- **Malicious Taint**: Components that often come through authorized channels, are authentic, and pass highly rigorous validation. Nonetheless, these components have some unintended functionality when placed intentionally by an adversary, which has negative implications on reliability, security, and safety. Typically, introducing malicious taint requires very high-level capabilities and resources, such as those a nation-state may possess.

- **Unintended Taint**: Components that come through authorized channels, are authentic, and pass highly rigorous validation. Nonetheless, these components contain quality defects in the form of software flaws or vulnerabilities, which may be known or unknown to the producer at the time of implementation.

Global work on this topic has been rare compared with attention given to other forms of supply-chain security, even in other sectors. Yet, solving this issue may resolve many of the undesirable supply-chain security issues. Unintended taint is often a key step in a cyber-kill chain that permits adversaries to do harm, and known treatments tend to be less costly and more easily measured than other supply-chain issues.

Understanding Unintended Taint in Cyber Supply Chains

Assembling systems from COTS hardware and software components can reduce cost and time to market, while increasing standardization and interoperability, as compared with building all of the computing hardware and software from scratch. The same characteristics that drove sectors to adopt these technologies into their corporate IT environments are also driving adoption into the OT environment. For instance, many OT systems increasingly use COTS hardware and software components from mainstream technology, software, and telecom-

16 Dale Peterson, "Insecure by Design / Secure by Design," Digital Bond Blog, November 4, 2013, http://www.digitalbond.com/blog/2013/11/04/insecure-by-design-secure-by-design/.

17 Ralph Langner, Twitter post, January 28, 2018, 8:36, a.m., "PoC from 2008, no insider knowledge needed to mess up Siemens S7-300/400, just push some buttons. Back in the days I considered announcing to release the software on the Internet in ten years, but decided against it." https://twitter.com/langnergroup/status/957653547675475969.

18 Sean Gallagher, "Vulnerable Industrial Controls Directly Connected to the Internet? Why Not?" Ars Technica, January 26, 2018, https://arstechnica.com/information-technology/2018/01/the-internet-of-omg-vulnerable-factory-and-power-grid-controls-on-internet/.

Examples of Cyber Supply-Chain Issues

- **Havex.** In March 2014, security researchers reported an attack campaign targeting energy sector companies by spreading malware (dubbed Havex) through several supply-chain vectors. Attackers compromised the websites of an energy sector law firm and several energy companies themselves, distributing Havex to site visitors. In at least one case, malware was inserted into software updates hosted on a supply-chain vendor's site, tempting operators to install the malware directly on ICS systems. This allowed adversaries to gain footholds in energy operators' IT and OT environments, with payloads that allowed them to enumerate OT systems and capabilities. This malware is modular, and it could be easily modified to cause damage instead.[1]

- **WannaCry/NotPetya.** In May 2017, and then again in June 2017, hundreds of companies worldwide were impacted when malware caused their computers to stop working. Energy sector companies that were impacted include Bashneft and Rosneft in Russia, Ukrenergo Electric in Ukraine, Gas Natural Fenosa and Iberdrola in Spain, as well as oil and gas shipping companies when ports were impacted. The malware spread rapidly across affected organizations through a set of known vulnerabilities in design, implementation, and maintenance of these systems.

1 "Advisory (ICSA-14-178-01): ICS Focused Malware," ICS-CERT, July 1, 2014, https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01.

munications providers. Therefore, hardware and software vulnerabilities in these systems end up in the energy sector cyber supply chain as unintended taint.

All systems fail; complex systems fail in complex ways. Software has a defect rate measured in the number of flaws per 1,000 lines of code. Energy sector systems comprise dozens, hundreds, or thousands of software components that come from different suppliers of varying integrity. As a result, energy sector systems may have tens of millions of lines of code representing thousands of potential vulnerabilities. Vulnerabilities in these constituent components are continually discovered, remediated, and made public.

Fixed-design elements can also represent unintended taint in systems and components; the most common is hardcoded passwords. Energy companies often need to manage systems remotely, and manufacturers often facilitate access through hardcoded credentials, such as default passwords that cannot be changed. Capabilities in the hands of an operator, working in good faith, can be used for harm in the hands of an adversary or an unskilled individual. To effectively gate access, these passwords must remain secret; yet, to provide access for defenders, they must be widely distributed and are often published in operating manuals. As a recent panelist testified before Congress, "a hardcoded password effectively means you have no password."[19]

One of the best capabilities to improve cybersecurity is tracking and sharing publicly known vulnerabilities. The National Vulnerability Database, for instance, catalogues tens of thousands of vulnerabilities; others have more. This capability allows for operators and manufacturers to identify specific vulnerabilities within their products and infrastructure, as well as address practices that led to the flaw. This allows defenders to enjoy a permanent advantage, giving them easy access to information commonly shared by adversaries.

Executive Order 13800[20] states that "known but unmitigated vulnerabilities [e.g., Unintended Taint] are among the highest cybersecurity risks" faced by the government. Unintended taint dramatically lowers the capabilities necessary to gain access to affected

19 *Cybersecurity of the Internet of Things*, Subcommittee on Information Technology Hearing, October 3, 2017, (testimony of Ray O'Farrell, WMware chief technology officer; 1:16:52), https://oversight.house.gov/hearing/cybersecurity-internet-things/.

20 "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017, https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

systems. In short, unintended taint through software vulnerabilities makes supply-chain subversion easier for all adversarial classes, from highly resourced and capable nation-states, to "hacktivists" with a basic understanding of IT or OT systems.

Therefore, risk from unintended taint accrues over time as more vulnerabilities in a system become public knowledge, unless it is eliminated across the deployed infrastructure. Capabilities to update software, rather than replace it, and to apply updates are a critical part of reducing risk by eliminating taint. As Xcel Energy CEO Ben Fowke said, "The great lesson for us [from recent breaches] is doing timely patches and basic cyber hygiene."[21] Organizations that are able to identify and eliminate known vulnerabilities in their environments can more quickly and thoroughly enjoy an advantage in reduced incidence of unintentional taint.

Recommendations

Apply Existing Frameworks Across the Energy Sector

The NERC-CIP Reliability Standards are a set of domain-specific regulations for the electricity segment. Because the equipment, vulnerabilities, and threats to the oil and gas industry are so similar, these standards could provide an ideal blueprint for improving the security of the oil and gas segment without increasing regulation.

Applying these requirements to suppliers could further increase energy sector reliability. Operators can require adherence and attestation, with appropriate incentives, through contractual obligations. Other industry standards and regulations, such as the Payment Card Industry Data Security Standard in the finance sector or the Health Insurance Portability and Accountability Act (HIPAA) in the healthcare sector, require similar supply-chain adherence, to varying degrees of success. The specificity of NERC-CIP, as well as the close-knit nature of the energy sector, helps avoid some of the pitfalls of HIPAA, where it is largely a paperwork exercise.

Viewing partners' security programs through a NERC-CIP framing will also reveal greater distinctions. For instance, many cloud providers have very high-level physical security programs, with auditable evidence-capture. On the other hand, some services work only when comingling data across all of their clients.[22]

Incentivize Trusted IT Practices to Avoid Unintentional Taint in the Energy Sector

The software and IT industry were first to encounter issues of unintentional taint, and the lessons learned can be instructive. Several practices, cited below, have been found highly effective in addressing the root causes and effects by those who have implemented them in similar sectors like healthcare and automotive. Taken together, they can increase reliability and decrease energy-sector cost, but only after galvanizing the political and organizational will to adopt them. Time is of the essence; with each new system that is designed and implemented that does not have these capabilities, it will take decades to replace it with one that does.

- Secure Software Development Lifecycles: Often called security by design or cyber safety by design, this approach anticipates and builds in capabilities that operators will need for the lifetime of the system, rather than requiring most of these capabilities to be bolted on later, often at a much greater expense.

- Software Bill of Materials: Sometimes called software composition analysis or software transparency, this is an inventory of software components in a system that can reveal complexity, flaws, and other potential issues. (See breakout box for more details.)

- Coordinated Vulnerability Disclosure Policies: Positions by manufacturers or operators that clarify how external parties can report potential security issues, so they can be investigated and addressed.

- Software Updatability:[23] Capabilities of systems that allow for a prompt and agile remediation of discovered software flaws without requiring the more expensive replacement of hardware components.

Procurement transparency reveals distinctions among alternative providers and products, and it makes more

21 Ben Fowke, Twitter post, October 18, 2017, 7:16 a.m., https://twitter.com/montaelkins/status/920654948597141505.

22 Tom Alrich, "A Break in the Cloud(s)? – Part 1," Tom Alrich's Blog, February 19, 2017, http://tomalrichblog.blogspot.com/2017/02/a-break-in-clouds-part-i.html.

23 Michael Assante, Tim Roxey, and Andy Bochman, *The Case for Simplicity in Energy Infrastructure*, CSIS, October 20, 2015, https://www.csis.org/analysis/case-simplicity-energy-infrastructure.

A Software Bill of Materials

Inside and outside of the energy sector, software applications and systems are increasingly assembled from software components rather than being developed from whole cloth. Applications run on COTS hardware and software, procured against a standard set of requirements, with a standard set of components. In this way, software manufacturing methods are coming to more closely resemble traditional manufactured goods, such as cars. This resemblance has led organizations like Netflix and DHS[1] to apply traditional supply-chain approaches to improving quality, resilience, agility, and cost of their cyber supply chains. These practices also allowed them to reduce software defects and respond quickly to head-off operational impacts. Increasingly, software development is coming to resemble lean manufacturing principles.

A simple and increasingly common approach is to track software composition across the supply chain. Procurement language across many sectors now mandates the disclosure of commercial and open-source, third-party software components through a software bill of materials (SBOM), as well as specifying and justifying defects that are publicly listed in reference databases.[2] This provides observable measures that can be used to evaluate the number and the reliability of suppliers and components, as well as the number and severity of known software defects. By limiting the transparency to only third-party and open-source components, intellectual property concerns are dampened. In the energy sector, Exxon has begun asking vendors to supply a SBOM,[3] the National Cybersecurity Center of Excellence Energy Sector Supply Chain Security Sub Working Group holds SBOM as one of its tenets,[4] and this recommendation was part of formational discussions on the NERC-CIP 013-1 guidance.[5]

- **Manufacturers** can track software components used in their products and use the software or audits to trace components where they do not maintain such a manifest, and they can require the same practices from their suppliers. Manufacturers benefit from increased reliability of components and reduced costs when discovering and addressing quality issues. Manufacturers can provide the SBOMs to internal teams (for support or license review), customers, insurers, regulators, and others based on business need.
- **Operators** can evaluate the information provided by manufacturers and systems integrators, or the inability or unwillingness to provide it, in order to improve the information available for decision making and then validate the information once it is acquired. Furthermore, operators can catalogue and maintain these SBOMs, permitting faster, less expensive, and more reliable identification and response to new public vulnerabilities. When these become publicly known, operators can instantly know which systems are affected, rather than conducting inventories and assessments that can take weeks and tend to be more disruptive.
- **Regulators and Industry Associations** can build capabilities to understand risks across the entire sector from known, but unmitigated, vulnerabilities. This can provide insight into actual and potential cybersecurity risks in the event of targeted attacks or Internet worms, such as WannaCry and NotPetya. This centralized, sector-wide oversight can play a critical role in dampening the likelihood and impact of harm caused by cyber supply-chain issues.
- **Insurers** can use SBOMs to understand levels of potential risk to more precisely determine the scope and size of a cybersecurity risk through objective and observable information. How well a company acquires, maintains, and uses this information is an indicator of how well it can reduce its potential attack surface, manage change in its environment, and how quickly it can respond to the changing security landscape.

---

1 "Software and Supply Chain Assurance (SSCA) & WG," GSA Interact, accessed March 25, 2018, https://interact.gsa.gov/group/software-and-supply-chain-assurance-ssca-forum-wg.

2 Public examples of this include: the Cyber Supply Chain Management and Transparency Act of 2014, the Mayo Clinic's procurement guidance, the Financial Services Information Sharing and Analysis Center procurement guidance, and the Financial Services Sector Coordinating Committee guidance for issuing cyber insurance products.

3 Dan Perrin, "A New Narrative on Cybersecurity," The Hill, May 4, 2016, http://thehill.com/blogs/congress-blog/technology/278712-a-new-narrative-on-cyber-security.

4 "National Cybersecurity Center of Excellence (NCCoE) Energy Sector Supply Chain SWG Energy Provider Community of Interest," NIST, January 13, 2017, https://nccoe.nist.gov/sites/default/files/library/coi/es-scswg-20170113.pdf.

5 "Technical Reference [Draft] DRAFT CIP-013-1 – Cyber Security – Supply Chain Management," NERC, November 2, 2016, http://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Mana1/Tech_Conf_Discussion_Only_CIP-013-1%20Guidance_Draft.pdf.

information available for buyers to evaluate the true cost of a product and its associated risk. These traits unlock market forces that match available choices to preferences for quality, cost, etc. This level of transparency also permits sector- or government-led responses in the same way that product recalls can for traditional supply-chain components. Finally, insurance markets can improve their ability to forecast risk and shape better practices through free-market forces.

Regulators or industry associations can set goals and thresholds for remediation of unintended taint and attach carrots and sticks. The US Food and Drug Administration has done this in the healthcare industry,[24] raising the bar for security, while reducing regulatory burden for companies that do so. Their approach is to tie a recall avoidance mechanism to practices that reduce and allow for a prompt and agile response to unintended taint. This has driven medical device makers to innovate new approaches to isolate and contain impacts to patients, as well as improve their agility in addressing newly discovered vulnerabilities. The DOE should evaluate whether similar approaches may help assess and manage risk across the energy sector.

Vulnerability Monitoring, Coordination, and Sharing

Much of the technical infrastructure across the energy sector relies on the same software, hardware, and firmware components. Computing chips, operating systems, platforms, libraries, and other common components cut across the entire sector, allowing for issues from unintended taint that impact one manufacturer or operator to impact others. The sooner a vulnerability is known, the sooner it can be addressed across an entire sector.

Individual companies, sector associations, and the government all have a role to play in accepting, distributing, and addressing newly discovered software vulnerabilities. Coordinated vulnerability disclosure policy guidance, such as that put forward by the International Organization for Standardization,[25] the National Telecommunications and Information Administration,[26] and the Department of Justice,[27] allow individual companies to accept reports from security researchers and others acting in good faith. This is already standard practice for Siemens, Philips, GE, and many other manufacturers. This information can be shared among industry organizations, such as the Electricity Information Sharing and Analysis Center (E-ISAC) and other ISACs and sector coordinating councils. Additionally, government, through Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and US-CERT, can help manage the process of making issues publicly known, by assigning them unique identifiers, communicating with affected stakeholders, mediating disagreements, and collaborating with other government agencies.

Examine Other Models of Operation, Liability, and Regulation

Attacks against the energy sector may cause substantial impact to global prosperity and national security. As adversaries demonstrate an increasing capability and intent to cause harm through cyberattacks, market-driven solutions may fail to respond as necessary. The possibility of a single high-profile incident affecting markets or national security requires policy makers to react swiftly. Equipping them to take a well-reasoned response serves to heighten confidence that the solution will be the right one, not just the one close at hand.

In light of the severe consequences of cybersecurity failure in the energy sector, Congress, DOE, and DHS, along with other relevant public and private sector stakeholders, should initiate a study (convene, research, workshop) to determine appropriate measures, mandates, thresholds, and timelines for very high-risk environments (e.g., nuclear and/or critical infrastructure at greatest risk)[28] that are dynamic enough to anticipate

24 Through their post market guidance for cybersecurity of medical devices. "Post Market Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff," FDA, accessed March 26, 2018, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

25 "ISO/IEC 29147:2014," ISO, accessed March 26, 2018, https://www.iso.org/standard/45170.html.

26 "Multistakeholder Process: Cybersecurity Vulnerabilities," National Telecommunications and Information Administration, December 15, 2016, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

27 "A Framework for a Vulnerability Disclosure Program for Online Systems," U.S. Department of Justice Cybersecurity Unit, July 2017, https://www.justice.gov/criminal-ccips/page/file/983996/download.

28 This could be enacted under Section 9 of Executive Order 13636, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity; or Section 2 of Executive Order 13800, https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

and respond to imminent threats to public safety, not just the bottom line. Starting points for alternate approaches can be pulled from existing practices in other countries, such as strict liability, government operation of some energy sector environments, increased regulatory regimes, etc. It might be that some approaches have no advocates today, but the process of analysis gives us options and foresight.

Fail Safe Capabilities and Training

Manual processes using exclusively mechanical and electrical technologies reduce cyber dependency during times when these components are under attack or are otherwise unreliable. As older equipment and engineers retire from service, capabilities are expected to go back to manual operations atrophy. The industry should investigate the costs and efficacy of preserving and enhancing manual fail-safe capabilities, including older equipment, regular education and training for engineers, etc. These activities will prove valuable for multiple energy-sector reliability threats, not just threats to the supply chain.

Accountability and Responsibility for Unintended Taint

Energy sector cybersecurity is a shared responsibility across supply chains and operators. While much of the accountability for safe operations falls to the operator, their options to do so are, in large part, dependent on capabilities built into the device. This includes their ability to build a defensible environment, as well as respond to vulnerabilities and threats once they become known. At the same time, manufacturers who have developed robust capabilities often see them unused by operators, thereby reducing the benefit of their investments and exposing their brand to reputational damage if involved in a high-profile incident. A broad examination of roles, responsibilities, and liability for different aspects of cyber supply-chain security can identify the gaps and inefficiencies in preserving security, safety, and reliability across the sector.

Conclusion

While energy sector cyber supply-chain issues have been recognized and studied for several years, they still persist. This research outlines a taxonomy for understanding certain energy sector risks, such as unintended taint, and defines concrete and exploratory recommendations for equipping policy makers and the private sector. While some of the options may be unattractive to some, others are comparatively easy, if the will exists. The much less attractive option is to continue down the current road, providing the pathways for accidents and for adversaries to undermine energy operations, which would have a much more profound effect on the sector, the global economy, and national and international security.

Beau Woods is a cyber safety innovation fellow with the Atlantic Council, a leader with the I Am The Cavalry grassroots initiative, and founder/CEO of Stratigos Security. His focus is the intersection of cybersecurity and the human condition, primarily around cyber safety, ensuring connected technology that can impact life and safety is worthy of our trust.

Andy Bochman is senior grid strategist for Idaho National Lab's National and Homeland Security directorate. Prior to joining INL, he founded a strategic energy sector security consulting firm, was an advisor on energy security matters at the Chertoff Group in Washington, D.C., and was the security lead for IBM's global energy and utilities business.

This issue brief is part of a partnership between the Atlantic Council's Scowcroft Center for Strategy and Security and Saab North America.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org