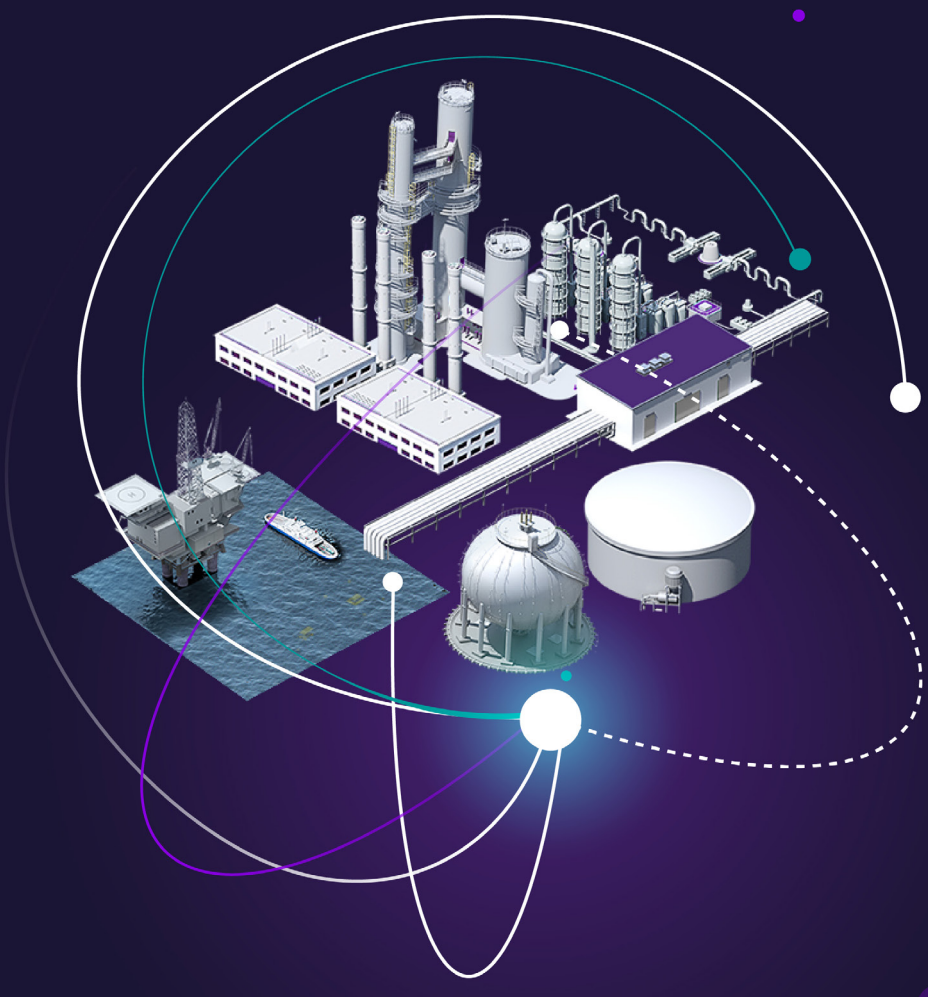
SIEMENS energy

Simulating a Cyberattack on the Energy Industry

A PLAYBOOK FOR INCIDENT RESPONSE



Foreword

Today's cybersecurity environment brings attacks to the utility sector with increased frequency and sophistication – and many are struggling to adapt to the new normal. We can no longer treat cybersecurity as though attacks are rare, one-off events. Instead, utilities need to plan for resilience against the backdrop of constant siege. The best way to approach this new threat environment is to develop an incident response (IR) plan to better detect, contain and eliminate cyberattacks with minimal impact on operations.

In the same way the physical safety of a plant depends on many people understanding their roles and responsibilities to ensure the availability and safety of operations, cybersecurity is a collective undertaking. Teams that have built and practiced an IR playbook in advance of a breach will perform better than teams forced to improvise every time.

The focus of cyberattacks against the energy industry has shifted from targeting information technologies (IT) toward operating technologies (OT). Instead of seeking to extract information like credit card numbers or business practices, attackers aim to disrupt service or damage critical infrastructure. Detecting and responding to these events require cybersecurity, IT, and OT experts to work together in a crisis.

Leaders will need to choose between competing interests during cyber incidents and make decisions with partial information in high-stress situations. Continuing plant operations may preclude investigation of anomalies or make it more difficult to preserve evidence. Someone in the organization will need to decide when – and how – to engage with partners, vendors, regulators, and the public. All these issues require thoughtful consideration before a crisis.

With a more than a 170 year legacy of building and securing critical infrastructure, Siemens stands ready to assist utilities in enhancing their security, detecting anomalies, and responding to threats before damage occurs. This white paper offers an example of an attack against a fictional electric utility, as it manages an unfolding crisis and illustrates how IR planning can make a difference in reaching the least disruptive outcome.

We hope it will help your team prepare.

Leo Simonovich
Global Head
Industrial Cyber and Digital Security,
Siemens Energy, Inc.

Introduction

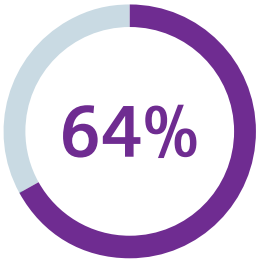
This paper will examine an incident response scenario, using specific examples drawn from a recent interactive session held in the United Kingdom (UK). The exercise simulated an attack, which caused a blackout at the main electric utility, ACMEPower, in a fictional city called ACME-City. While this particular exercise was held jointly by the cybersecurity group of the UK Energy Emergency Executive (E3CC) and the UK Department for Business, Energy and Industrial Strategy (BEIS), its lessons are broadly applicable for regulators, utilities, and operational technology (OT) or information technology (IT) security experts anywhere in the world.

Tabletop exercises can help utilities evaluate their cybersecurity strengths and weaknesses, and generate insights that shape their IR detection and prevention strategies. They bring abstract concepts to life and enable participants to connect the what-if incident response steps with day-to-day jobs. Done well, exercises can help key personnel preview problems likely to arise from real-life challenges.

IR planning is especially relevant today because industrial cyberattacks are on the rise, and the nature of these attacks is changing with increased connectivity and penetration of digital energy assets. Digitalization brings a convergence of IT and OT connectivity, so that data can travel from the field to the control room, and to the enterprise network; with that evolution also comes opportunity and risk.

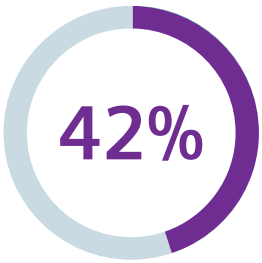
of global utilities expect an OT attack in the next 12 months, according to an independent study conducted by the Ponemon Institute.

The Poneman Institute found that utility OT infrastructure is significantly more vulnerable to a cyberattack than utility IT networks; breaches also have a more destructive impact on operations. In other words, OT – which is everything outside the enterprise network – is the new frontier for cyberthreats against critical infrastructure.



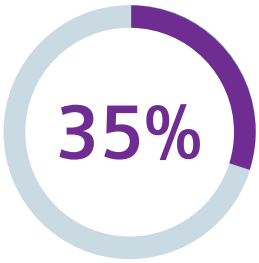
of global utilities expect an OT attack in the next 12 months, according to an independent study conducted by the Ponemon Institute.

Cyberattacks on the energy industry have escalated in recent years, both in volume and sophistication. In 2010 Stuxnet was the first known case of malware specifically designed to attack industrial control systems. Then, in 2017, the widely reported Wannacry ransomware virus affected organizations across the world, including computers at the West Bengal power distribution company in India. More recently, in March 2018, the US Department of Homeland Security reported that critical infrastructure sectors had been intentionally targeted by hackers to cause widespread destruction. These, and other high-profile examples, have made utilities acutely aware of the new and destructive risks.



of utilities rate their own readiness and response to cyberattacks as high.

Given the escalating threat environment, utilities should evaluate: how to protect their own systems from attack; how to better detect security breaches; and what response plan they would follow if an attack against OT systems succeeds – either in part or in whole. Too many utilities have yet to take this basic step.



of utilities have no response plan in place.

Incident Response Steps

Whether an organization is creating its first IR plan or building on existing capabilities, a clear OT response framework will help build a culture of continuous improvement and constant vigilance. Strong cybersecurity IR begins before an incident occurs and continues long after normal operations have been restored. The following steps are distinct and crucial aspects of IR decision-making and are intended to form a feedback cycle.

Preparation – practicing a methodical response to a wide variety of threats. To prepare, IR teams should build and maintain an industrial forensic toolkit. An organization should also identify which staff will centrally manage a crisis, define roles, and educate plant personnel. This team will be responsible for rebooting equipment, restoring operations and eliminating vulnerabilities during an incident.

Identification – identifying a cyberattack is underway. An initial signal might come in the form of an operational abnormality or more directly as ransomware. Field personnel are especially important in helping distinguish between security and process control system abnormalities. An investigative playbook can help diagnose, triage and activate responders in assessing the impact and determining appropriate next steps.

Containment – ensuring the incident causes no further damage. The overarching priority is to isolate infections, maintain production, and above all, ensure actions do not further jeopardize plant safety or operations. In an OT context, containment can be difficult; utilities must isolate the source of an attack and determine when to apply a built-for-purpose passive forensic tool to remove malware from production networks or limit unnecessary data transfers.

Eradication – removing the threat. The forensics team must ensure that essential operations are backed up should challenges arise with restoration. Possible methods could range from system patching or rebuilds to full architecture redesign. The team should preserve evidence, which may range from mapping of employee change control to full system image capture.

Recovery – enacting a phased recovery plan to restore full strength operations. This requires focusing on restoring critical systems first – or operating in analog mode – until there is confidence in system-level performance. An environmental and safety check should be done in parallel to control for unintended performance impacts of restoration.

Lessons learned – documenting lessons learned from the incident. The lessons learned process is an ongoing activity that must not only capture the immediate impacts of an incident, but also the long-term improvements of plant security. This could range from a better designed process control system and stand-up of a physical command response center, to enhancing an organization's monitoring capabilities. This response system should include utility peers, vendors, authorities, and the security community.

The Scenario

Consider a fictional city called ACMECity in 2020. With a population of 15 million in a dense metropolitan area, ACMECity relies on a central electric network to provide nearly all the region's power.

ACMEPower, a public utility, is the sole power operator for the city. The company owns two combined cycle power plants but has recently committed to shifting 40 percent of power generation to renewables over the next six years. This strategic shift has left ACMEPower exposed to new threats that come with IT, OT and IoT integration.

On September 4th at 21:10, a major blackout affects the ACMECity metropolitan area the night before state and city government elections. ACMEPower's CEO, Joe Provolone, receives a phone call from the governor with a requirement to restore power in time for the next day's election. She tells Mr. Provolone that he has 12 hours to determine the root cause. The CEO states that he will call the governor back immediately after getting an update from the operations team on duty.

Development 1

Blackout in ACMECITY

The Scenario

Here is what ACMEPower knows so far. On September 4th, 2020 at 21:02, immediately after a supervising operator shift change, the distributed control system (DCS) master server is rebooted, switching operations to the backup Human Machine Interface (HMI).

Three minutes later, at 21:05, the SCADA alarm history indicates a critical failure on a control system which showed thermal stress on generation Unit 1. A similar event is observed at the other generating unit, Unit 2, five minutes later.

During the following emergency meeting, Mr. Provolone solicits advice from his senior staff and receives inconsistent recommendations on how to proceed. Knowing he has little time to waste, Mr. Provolone considers four different courses of action:

The Options

Option 1: Scan ACMEPower's plant networks to determine when the incident occurred and what caused the shutdown.

Option 2: Begin an investigation from the Digital Forensics Incident Response (DFIR) team and start the acquisition of forensic artifacts.

Option 3: Given the urgency of restoring power before the election, contact vendors to begin acquiring new equipment immediately.

Option 4: Begin an internal investigation of all ACMEPower's departments – both related and unrelated to the shutdown. This would help determine if other OT or IT systems were compromised and if any personnel failed to follow procedures. The investigation could include examining building control systems, operator workstations, computer networks, or physical security breaches.

To successfully execute an IR plan, it is critical that leaders act on verified facts, not emotion, to find the root cause of the incident.

The Challenge

Leaders must rely on their team to make quick but well-informed decisions based on the best information available. As is the case with most executives, Mr. Provolone is faced with a common IR challenge; the CEO must rapidly corroborate facts, consider expert recommendations, evaluate competing priorities, and based on this information, develop a comprehensive plan with clear team actions. The most challenging aspect of emergency response is that leaders could face multiple choices that will determine success or failure early on in the effort. These conditions tend to sway leaders as they chart a course of action. To successfully execute an IR plan, it is critical that leaders act on verified facts, not emotion, to find the root cause of the incident. And here it is important to have a playbook or set of procedures to follow.

The Best Practice

What would you do? Does your organization have a playbook with clear tie-ins to both corporate and field operations?

As ACMEPower triages the incident, the logical choice is to immediately reconcile operational and network data to determine if it's dealing with a cyber event. ACMEPower should also pursue additional options in parallel, such as launching an internal investigation and beginning to contact vendors in case new equipment needs to be acquired to restore service. All responder activities should be documented from the start, in a timeline, to preserve the chain-of-custody.

Development 2

Security Incident Declared

The Scenario

At 21:43, following the examination of network and operational data and interviews with personnel, ACMEPower uncovers clear evidence of malicious activity in the control network. In an unrelated action, the automation vendor received an urgent request for replacement equipment outside of the standard procurement process; the vendor confirmed the order with estimated delivery of two weeks.

The analysis revealed that a malicious actor was on the network looking for a host with an open port. This vector serves as an ideal entry point for an intruder trying to hack into a network because it enables applications and services to communicate and share files.

This discovery is an important first step in the investigation, but significant gaps in confirming the root cause of the incident remain. With incomplete facts, ACMEPower is contemplating whether to inform relevant government agencies – including its regulators.

Shortly after receiving the first data points, additional information begins to come in.

At 21:50, additional suspicious network activity is detected by the Intrusion Detection System (IDS), which is reported to ACMEPower's leadership; this evidence further points to a potential malicious breach. Based on this information, Mr. Provolone calls the governor and declares that the utility has found evidence of malicious activity on its networks, and asks for local law enforcements' help.

At 21:54, following Mr. Provolone's call to the governor's office, local law enforcement officials contact Mr. Provolone to inform him that one of his operator staff – who was on duty the night of the incident – has been reported missing by his spouse.

At 22:01, the vendor calls the procurement department to confirm ACMEPower's request to source one of the components that might need replacement; however, the phone call comes as a surprise to Mr. Provolone who is unaware that the request was made.

The Challenge

With the possibility of a malicious intrusion, the potential of a missing employee, and some evidence of a compromised supply chain, the CEO must determine what to do next. Mr. Provolone reconvenes his core team to understand the linkages between the three possible pathways a malicious actor could have used to breach plant security and asks for recommendations about what to do next.

The Options

Option 1: Deepen the investigation by sending a team of automation, network, and security experts into the field to conduct further forensics, preserve evidence, and authorize containment; meanwhile maintain operations and share all information with government officials.

Option 2: Launch an internal investigation to find out who placed the order with the vendor for new equipment; wait until this investigation is complete before taking further action.

Option 3: Prioritize the search for the missing employee, offer support to the family, and discourage law enforcement contact until the family is comfortable with the investigation.

Option 4: Expand the investigation into ACMEPower's supply chain. Ask local law enforcement to contact the vendor re-supplying parts to determine the sequence of events and any potential wrongdoing. Simultaneously, initiate an internal data call to find out if employees and other suppliers have either received or made similar requests for new parts.

The Best Practice

What would you do? Would you limit or expand the scope of the investigation, and who would you include or exclude?

The recommended best practice is Option 1: deepen the investigation by collecting additional evidence from the field and validating assumptions through a diverse group of experts. The known intrusion may not be the only malicious activity underway, hence other possible attack pathways must be investigated. The investigation should remain focused on what the hacker is likely to do moving forward; narrowing the scope of the investigation too early might compromise critical information needed to uncover ongoing threats. Maintaining a focused investigation can be especially challenging when new but unrelated information comes to light, challenging the CEO's primary assumptions. If criminal or nation-state activities are detected or suspected, it is essential to work hand-in-hand with appropriate law enforcement officials.

Development 3

Infection has been eradicated

The Scenario

Mr. Provolone has decided to deepen ACMEPower's investigation to validate all possible pathways of attack and contain active threats.

At 13:00 – approximately 36 hours after the attack was first identified – an internal investigation confirms its origins. A hacker found an unpatched vulnerability in Unit 1's control system. To mask his path, the attacker manipulated firewall rules to bypass the DCS's intrusion detection system. Unknowingly, the attacker triggered a signature alarm. At the same time, the plant operator noticed an unauthorized configuration change in plant operations. A subsequent inventory scan showed a new device on the network.

A few days later, on September 7th at 03:30, a joint investigation by ACMEPower, the industrial control system (ICS) vendor, and law enforcement concluded that ACMEPower was the victim of an adversary attack focused on embedding malicious code into ICS hardware components. Law enforcement interviews with an ACMEPower plant employee revealed that 48 hours ago he received a package with control system vendor labeling, which contained a USB with instructions to update the PDF workflow viewer. Even though the plant employee thought receiving updates on a USB was unusual, the package looked legitimate and he plugged the USB into the DCS.

On September 10th at 09:05, the missing operator has been located; his disappearance was unrelated to the incident.

At 11:25, Mr. Provolone instructed his executive team to focus their investigation on eradication and phased recovery. The team began work in forensics and attribution, regulatory and public notification, and lessons learned.

On average, responses to past malware days attacks took

after an outage. Smaller organizations took longer (88.5 days) than larger organizations (62.6 days).

ACMEPower now has the opportunity to learn from the incident, improve its protocols, and fix vulnerabilities discovered during the investigation. Mr. Provolone's executive team once again offers competing advice on how best to prepare for future incidents.

The Options

Option 1: Establish a team to address cyber supply chain management and halt all vendor orders until a full review has been initiated.

Option 2: Develop new rules and regulations for all portable media and hardware components introduced into the plant environment.

Option 3: Establish an IR command center that will serve as a hub for all plant monitoring and crisis management.

Option 4: Immediately issue a press release and inform the public about the incident, including open aspects of the investigation.

The Challenge

What would you do? What is the best way to put a comprehensive IR playbook in place?

The most impactful decision is to set up a permanent IR command center. The center will convene experts and vendors to monitor daily plant operations, gather stakeholders for regular exercises, and manage future crises. This command center will house the IR playbook and help all relevant responders make better decisions during future incidents.

Establishing a command center can also help organizations proactively shore up defenses. In today's environment, it is safe to assume that an adversary is already within a utilities' network planning the next attack. Too often utilities only refresh security programs based on the last incident.

The Best Practice

We believe that the most important action organizations can take to make their operations resilient is to develop and implement an IR playbook. Resiliency is based on three key concepts: visibility, relationships, and speed. These elements are fundamental to developing a forward-looking IR playbook that brings together intelligence and leaders under a single umbrella.

Visibility means that utilities can see and understand the complexities of their systems – continuously monitoring and investigating potential threats.

Relationships matter in a crisis. The ability to share information throughout a common supply chain with trusted vendors make the difference in getting to a resolution. Relationships need to work at all levels of the organization with a clearly defined escalation path.

Speed becomes critical during a crisis. Incident response requires system operators to quickly and accurately understand, contain and recover from an attack before its full impact can cause outages or spread to other systems.

Takeaway Lessons

This simulation offers several key lessons for utilities and regulators seeking to bolster their IR capabilities. In the scenario, Mr. Provolone did many things well, but could have significantly benefited from a strategic plan. He recognized the importance of factual information and the need to remain open to multiple investigative pathways before making a decision.

With the benefit of hindsight, we can also identify opportunities for ACMEPower to detect the attack earlier and resolve the incident more quickly. Working backward from the attack, ACMEPower had the opportunity to identify:

The commands that caused thermal stress fatigue. Commands that cause damage to equipment may closely resemble legitimate commands. An operator, or an automated system, may be able to use context to identify commands that will cause damage. Both vigilance and detailed system knowledge are required to detect this type of attack.

The behavior of the intruder in the network. In the exercise, the intrusion was confirmed by examining the logs and discovering that an intruder had been looking for an open port. Human operators and automated Artificial Intelligence (AI) monitoring may have exposed the intrusion at this stage. Plant operators need the relevant tools and discretion to investigate anomalies.

The malware. Signature-based monitoring can detect malware if it uses code that has been identified by other organizations. Security teams need monitoring software, access to sources of threat intelligence, and to ensure monitoring covers all pathways into the OT environment.

The USB device that introduced the malware. Practices that eliminate portable storage devices in operating environments would prevent this type of threat. All personnel must understand portable media policies, as well as broader security measures, to address a wide range of insider threats.

The malicious firmware embedded in new equipment. Establishing a common set of cybersecurity standards across all vendors can improve the overall security posture in the supply chain.

In this scenario, ACMEPower had these five opportunities to detect and block the attack before a blackout could occur. Capitalizing on any of these opportunities depends on establishing the right procedures to triage, diagnose and act on an established set of IR procedures.

The sophistication of attacks mean that organizations should assume an intruder has already breached defences.

While this specific exercise involved just one malicious actor attacking multiple vectors, attackers can attempt thousands of potential pathways to disrupt an organization's operations. Many organizations would benefit from increased situational awareness through monitoring of their control systems. Even in isolated production environments, the sophistication of attacks means that organizations should assume an intruder has already breached defenses. Identifying and testing against all possible attack scenarios should be a routine task in all cybersecurity planning.

At Siemens Energy, we believe strong relationships with our customers, backed by rapidly enacting joint response plans, are essential for cybersecurity in the ever-changing environment. As a vendor with expertise in developing and deploying digital and industrial cyber equipment in the utility sector, Siemens has solutions to help organizations like ACMEPower detect, prevent, and recover from cyberattacks.

Strong relationships with our customers, backed by rapidly enacting joint response plans, are essential for cybersecurity in the ever-changing environment.

We partner with customers to develop incident response plans and provide expert OT support – both remote and in the field. Siemens Energy develops built-for-purpose solutions, including IR forensic and monitoring tools, to contain and eradicate malware on plant's critical systems.

In this new environment, no one can treat cybersecurity as a responsibility that stops with a core IR team. Resilient organizations must ensure every person understands – and contributes – to a culture of situational awareness, active response, and continuous improvement.

Siemens Energy, Inc.
15375 Memorial Dr #700,
Houston, TX 77079
+1 (832) 679-8500

For more information, please visit our website:
https://www.siemens-energy.com/global/en/offerings/services/digital-services/cybersecurity.html