BLACK & VEATCH

Agent CISO: Mission Critical— Cybersecurity for New Construction

There are New “Bad Guys” on the Scene. Are You Ready?

Cyber adversaries are evolving—targeting not only our digital world of data, but also the physical world of operations. Growing stronger is a group of cyberattackers working towards their own devious ambitions: Operation Blackout. These rogue saboteurs aspire to take down critical infrastructure worldwide. No facilities are immune to their “bad guy” tricks and these nefarious activities are forcing modern organizations to reshape their approach to cybersecurity.

Information Technology (IT) and Operational Technology (OT) used to be viewed in their own silos. Previously, IT experts were focused on protecting essential business functions against cyberattackers aiming to steal, falsify, or destroy data—while OT systems at the heart of these functions were largely overlooked.

Today, all of that has changed as new technologies are adversely used to better-equip cyberattackers. Integrations, automations, and digitization bring incredible benefits, but also expands the attack surface, increasing exposure and vulnerabilities, as lines blur between IT and OT. Many organizations are operating under a false sense of security, as the concept of being “air gapped” has become obsolete. While traditional cybersecurity strategies are collapsing under threats from Operation Blackout, the stakes are higher than ever.

Agent CISO

The team back at Mission Control will be behind you every step of the way. You’ve been armed with all the knowledge, skills and tools you need to achieve your three main mission objectives. When you’re ready to get started, proceed to Mission Objective 1.

Your Mission, Should You Choose to Accept It...

This is where YOU come in. To the rest of the world, your professional title is Chief Information Security Officer (CISO)...but to your cybersecurity expert peers, you also have a secret identity as **Agent CISO.** Throughout this mission, you’ll be collaborating with **The Client,** who embodies all critical infrastructure organizations across the globe. The Client is relying on you to get ahead of Operation Blackout’s insidious plot to take control and bring down the power grid, water treatment facilities, hospitals, data centers, military bases, vessels, ports, pipelines, airports, and everything else that keeps our world safe and functional.

CLASSIFIED

Mission Objective 1: Outsmart Cyber Adversaries During Facility Design

The cyber adversaries behind Operation Blackout are gaining malicious intelligence on how to infiltrate The Client's facilities around the world. Luckily, you can stay ahead of the emerging threat landscape by designing new facilities that are optimized for cybersecurity. Although bringing on a cybersecurity expert like you historically hasn't been part of the design-build process, adding your expertise is now a huge differentiator for The Client's engineering and construction teams.

Review Your Mission Brief

When it comes to cybersecurity, The Client's existing facilities face a distinct set of challenges that make cybersecurity integrations and updates far more costly and complex:

- **Legacy Systems and Technology.** Many older facilities rely on legacy systems that weren't designed with modern cybersecurity in mind—utilizing outdated software, hardware, and communication protocols that can't be efficiently upgraded or patched. Compatibility issues between old and new systems may create weak links in the cybersecurity "armor" for Operation Blackout to find and exploit.
- **Operational Disruptions.** The installations and updates needed to introduce cybersecurity to an existing facility often require system downtime, therefore disrupting critical operations.
- **Physical Constraints.** The Client's older facilities weren't designed to accommodate secure server or ICS control system rooms and other cyber-physical best practices, creating space limitations for new hardware.
- **Organizational Culture and Resistance.** Employees have grown accustomed to the same processes they've been following for years; some may be resistant to changes in security protocols. This lack of buy-in could hinder the effectiveness of new cybersecurity measures.

While these legacy challenges are being addressed by other agents in the field, The Client has asked you to advise on the design and construction of their new facilities—opening up opportunities for seamless industrial cybersecurity integration. Cybersecurity can be "built in" from the start, leading to more secure and resilient facilities in the long run:

- **Modern and Scalable Systems.** The Client's new facilities can leverage the latest hardware and software solutions, adaptable to future needs. This will create more secure and flexible OT environments that can easily incorporate new technologies as they come to market.
- **Reduced Operational Disruptions.** Cybersecurity solutions and measures can be implemented during construction—reducing the risk of downtime or operational delays when facilities are up and running.
- **Better Network Design.** The Client's network architecture can be designed with secure zoning, architecture that reduces the deployment of duplicated network devices, proper segmentation between IT and OT networks, and robust firewalls to minimize ways for Operation Blackout agents to sneak in.
- **Organizational Alignment.** Starting fresh with a new facility is the perfect opportunity to launch a cybersecurity-conscious work culture, building effective operational habits from the beginning.
- **Regulatory Compliance.** The Client's new facilities can be designed to comply with the latest cybersecurity regulations and internationally recognized industry standards, avoiding potential penalties and shutdowns in the future. (More on this in Mission Objective 2!)

Map Out Your Strategy

When designing The Client's facility to optimize cybersecurity, it's essential to build a strong foundation of tactics that address both physical and digital vulnerabilities. It's up to you, Agent CISO—how many steps of this mission can you accomplish in the allotted time to outsmart Operation Blackout during facility design? (Mission Control encourages you to complete all three steps for maximum impact!)

- **Step 1: Optimize Physical Layout.** Design The Client's new facilities with multiple layers of perimeter defense such as controlled entry points, fences, and other barriers—reducing the risk of physical intrusions from Operation Blackout that could compromise cybersecurity. Create zones with different levels of access controls based on the sensitivity of The Client's information or IT/OT systems within each zone. Designate specific areas or facilities for secure disposal of hardware, ensuring that sensitive data is properly destroyed as intended. Physically segregate guest Wi-Fi networks from sensitive networks used by IT, OT, and financial departments. Future-proof The Client's facilities by leaving space for additional server racks and other hardware upgrades to stay ahead of Operation Blackout's evolving cybersecurity threats.
- **Step 2: Secure IIoT and OT Devices.** Secure each "smart" Industrial Internet of Things (IIoT) device used to control HVAC, lighting, locks, cameras, and alarms with unique credentials, firewalls, Programmable Logic Controllers (PLCs), human machine interfaces (HMIs), and other control systems. Use modern access controls like biometrics or keycards to restrict Operation Blackout's entry to sensitive areas. Install dedicated, encrypted communication lines for The Client's incident response teams to maintain coordination during cybersecurity events. Execute device hardening tailored to clients' needs to minimize inherent vulnerabilities. Remove default passwords to prevent ease of access to systems. Protect critical areas like server rooms with fire suppression, flood protection, and controlled ventilation to prevent tampering.
- **Step 3: Establish Redundant and Backup Systems.** Isolate the power supplies of critical IT and OT infrastructures from general building systems to minimize the risk of tampering or power-related attacks from Operation Blackout. Design The Client's facilities with uninterruptible power supplies (UPS) and backup generators to ensure that critical cybersecurity systems continue to operate during power outages. For buildings that host data centers, design redundant data storage solutions on-site or off-site to ensure that cybersecurity incidents do not lead to irreversible data loss or unintended network activities.

Agent CISO

You did a great job ensuring the future safety of The Client's new facility by swooping in during the construction phase, but your mission has only begun. Proceed to Mission Objective 2 to help The Client protect the continuity of their critical operations.

Latest Intel from Mission Control

While you've been in the field working on Mission Objective 1, the team back at Mission Control just compiled the latest intel on how to implement cybersecurity strategies for The Client in the most cost-effective ways. Consider how you can weave the following tactics into your current approach:

- **Prioritize critical, high-risk systems** and expand protections in phases as budget and resources allow.
- **Leverage scalable, modular, and cloud-based solutions** that allow for incremental upgrades over time.
- **Integrate automated and AI-enabled security monitoring tools** to detect and respond to threats with minimal manual efforts.
- **Train employees on cybersecurity best practices** and foster a cyber-aware culture to proactively mitigate costly mistakes from human error.
- **Invest in energy-efficient and compliant systems** to reduce long-term operational and regulatory costs.
- **Implement policies and procedures** like an Incident Response Plan (IRP) to ensure effective remediation and reduced recovery time after a cyberattack.
- **Integrate concepts such as Cyber-Informed Engineering (CIE) and Cyber Risk Quantification** to add cyber principles into the design process and account for overall risk appetite.

CLASSIFIED

Mission Objective 2: Build in Regulatory Compliance for Resilient Future Operations

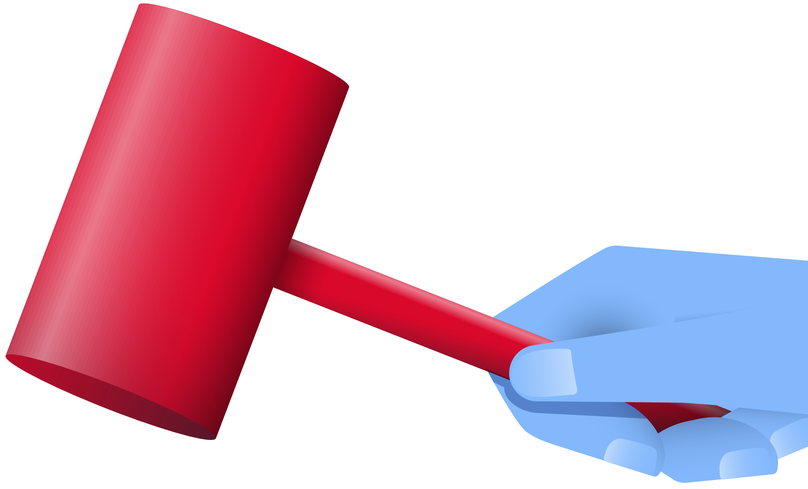
Now that you've successfully executed "cybersecurity by design" methods, it's time to ensure robust security without jeopardizing The Client's operations. This part of the mission will be especially challenging—not only are the bad guys from Operation Blackout still trying to undermine your efforts at every turn, but there's another influential force to consider. **The Regulator** represents all regulatory bodies and government agencies that set standards and oversee compliance with cybersecurity policies. The Regulator has the power to halt critical operations at the hint of non-compliance; with regulations evolving as quickly as Operation Blackout's threats, guaranteeing compliance can be harder than it sounds.

Review Your Mission Brief

The Regulator enforces cybersecurity regulations from local and national agencies. Recently, The Regulator has announced a few major changes to improve the overall cybersecurity posture of organizations across the world:

- NIST has updated its frameworks to establish privacy standards for cybersecurity programs, ensuring organizations are appropriately handling sensitive data.
- CISA's role has expanded with the introduction of mandatory incident reporting requirements for critical infrastructure owners and operators.
- The SEC recently proposed new rules for companies to report cybersecurity incidents within four business days of discovery and to disclose their cybersecurity risk management programs.
- ISA/IEC 62443 introduced a security model for IACS in Europe to evaluate requirements to help organizations assess their cybersecurity capabilities and identify areas for improvements.
- The NIS2 Directive, an update of the NIS Directive, establishes the cybersecurity requirements of OT and digital service providers and emphasizes risk management and incident reporting.
- The European Union Agency for Cybersecurity (ENISA) published guidelines and recommendations for securing critical infrastructure.

The Client's resource allocation and budget constraints pose additional obstacles here, as allocating sufficient investments for cybersecurity initiatives and compliance (and getting spending approval from stakeholders) while managing operational costs requires a delicate balance. It is imperative to have a seat at the table to drive a Capital Expenditure (CapEx) investment, secure resources for implementation, and ensure top-down compliance adoption as part of your mission. Don't forget to utilize the cost-saving measures you learned from Mission Control's latest intel.



Map Out Your Strategy

Ensuring The Client's compliance with various cybersecurity regulations can be tough to navigate due to the broad range of laws and standards that must be followed. It's up to you, Agent CISO—how many steps of the mission can you execute to protect ongoing operations? (Mission Control encourages you to complete all three steps for maximum impact!)

- **Step 1: Implement Comprehensive Policies.** Develop cybersecurity best practices for password management, data encryption, access control, incident response, and data privacy—making sure these policies align with The Regulator's mandates. Implement procedures such as NIST Cybersecurity Framework, IEC 62443, or NIST SP 800-82, which provide proven and structured approaches for managing risks. Advise The Client to require multifactor authentication (MFA) to access sensitive systems or data, which ensures that even if credentials are compromised, additional authentication prompts will prevent Operation Blackout agents from breaking in. Embed privacy measures and encrypt sensitive data in case it's intercepted when transmitting over networks. Ensure OT systems are segmented for optimal security posture. Implement a patch management program to push regular updates and close any security gaps before Operation Blackout finds them.
- **Step 2: Train and Empower Personnel.** Provide regular training on phishing attacks, social engineering, password hygiene, OT management and usage, and data privacy to The Client's employees. Serve as The Client's compliance consultant to ensure they're aware of any changes in The Regulator's national and local industry-specific requirements. Develop and maintain an incident response plan that outlines procedures for detecting, reporting, and mitigating cyber incidents in IT and OT systems, and conduct regular tabletop exercises with The Client to test the plan's effectiveness.
- **Step 3: Monitor Risks and Report Incidents.** Regularly assess risks in The Client's OT environment and evaluate how sensitive data is stored, transmitted, and processed. Use automated systems to manage and monitor networks 24/7 for anomalies and conduct regular audits to ensure that policies and controls are functioning properly. Keep thorough records of cybersecurity practices, risk assessments, incident response activities, training, and compliance reviews. Documentation ensures that you can prove The Client is meeting The Regulator's strict requirements.

Agent CISO

The Client is grateful that you continued to fend off Operation Blackout's attempts to bring everything to a screeching halt—all while keeping The Regulator happy with your compliance solutions! Now it's time to take extra measures about going on defense. Please proceed to Mission Objective 3.

Latest Intel from Mission Control

The team back at Mission Control just received the latest intel on an innovative approach to cybersecurity called the "CALM" model. Mission Control has informed you that this proprietary approach came from a trusted source who must be kept confidential for now…but they will be revealed at the end of your mission.

The Cyber Asset Lifecycle Management **(CALM)** model is built on three core concepts, which you'll leverage for The Client in Mission Objective 3:

- **Holistic Lifecycle Approach.** CALM accounts for unique cybersecurity requirements throughout the asset lifecycle—enabling critical infrastructure organizations to proactively minimize risk and cost from construction all the way through decommissioning.
- **Business-Driven Cybersecurity.** CALM facilitates data-driven decision-making, enabling cybersecurity leaders (like you, Agent CISO!) to future-proof operations in response to evolving threats.
- **Consequence-Focused Cybersecurity.** This model has been adapted to the cyber-physical nature of Operation Blackout's attacks on critical infrastructure. CALM ranks the impact on safety and up-time from minor to catastrophic, reducing the fallout of cyber-attacks.

CLASSIFIED

Mission Objective 3: Initiate Robust Physical Defensive Measures

You've already gotten two steps ahead of Operation Blackout by successfully guiding The Client through design, construction, and compliance. While the bad guys are lurking in the shadows planning their next move, it's time to implement additional defensive measures you learned from the CALM model. At this stage, threats from Operation Blackout extend beyond digital and financial consequences—they also have the power to endanger environmental, human, and community safety, and more. Keep your guard up, Agent CISO!

Review Your Mission Brief

Many of The Client's critical infrastructure systems—including power grids, water treatment facilities, and transportation networks—are now connected through internet-enabled devices, making them more susceptible than ever to cyberattacks.

The Client is struggling to keep up with these technological advancements and their associated physical security considerations in OT environments. They need your expert guidance on identifying and mitigating their physical weaknesses before the opportunistic bad guys from Operation Blackout use them to weasel their way in. Be on the lookout for the following potential weaknesses as you assess the state of The Client's cybersecurity program:

- **Unauthorized Physical Access.** Attackers from Operation Blackout could install malware, steal sensitive data, or disrupt critical systems by gaining physical access to The Client's hardware.
- **Inadequate Surveillance and Monitoring.** Without the proper monitoring solution, physical and digital intrusions may go undetected, allowing cyber adversaries to manipulate equipment or steal data.
- **Poorly Secured Entry Points.** Spies from Operation Blackout could bypass entry security by exploiting poorly secured doors, gates, windows, and remote access points—gaining access to The Client's sensitive systems and data.
- **Lack of Device Security.** Unsecured physical access to devices with open USB ports or other external connection points entices cyberattackers to install malware or extract data from mobile devices, laptops, unattended workstations, and poorly discarded hardware.
- **Lack of Physical Redundancy.** Without multiple backup systems, a single point of failure initiated by Operation Blackout (such as a power outage or damage to a critical server) will cause major disruptions and prevent recovery.
- **Insider Threats.** Insider threats can be difficult to detect, especially when employees abuse their physical access privileges to steal data, damage systems, or bypass security measures. Be on the lookout for Operation Blackout spies trying to take down The Client from the inside, and alert Mission Control of any suspicious behavior.

Choose Your Approach

Addressing physical vulnerabilities is critical to a holistic cybersecurity strategy, as Operation Blackout is constantly looking to exploit The Client's weaknesses and bypass virtual barriers. It's up to you, Agent CISO—which of the following approaches will you take to initiate robust defensive measures? (If time and resources allow, Mission Control encourages you to choose more than one!)

- **Plan A: Implement Consequence-Focused Cybersecurity.** Consequence-focused cybersecurity reduces the potential impacts of cyber-attacks rather than solely focusing on prevention. Regarding The Client's critical infrastructure, a lack of preparation means a cyberattack could have severe, far-reaching consequences. Proactively minimize the damage of Operation Blackout's security breaches by implementing impact assessments, resilience strategies, and incident response plans—ensuring that The Client is well-equipped to recover swiftly and effectively.
- **Plan B: Leverage the Physical Impact Principle.** The physical impact principle refers to Operation Blackout's potential to cause real-world, tangible damage to physical systems, infrastructure, and human safety. This principle emphasizes the importance of safeguarding not only digital assets, but also The Client's physical assets that rely on interconnected technology. Keeping the physical impact principle top of mind, develop best practices to shield The Client's employees, OT equipment and devices, and cyber-physical systems from Operation Blackout's malicious interventions.
- **Plan C: Double-Down on Regulatory Mitigation Strategies.** Fortunately, you already deployed many mitigation strategies proven to address physical vulnerabilities when ensuring regulatory compliance in Mission Objective 2. However, it certainly doesn't hurt to bolster these security measures even further. Take a closer look and see how The Client can improve their access control systems, 24/7 monitoring, environmental controls, device hardening, redundant power and connectivity, employee training programs, and physical security audits.

Agent CISO

You've achieved Mission Objective 3; it's time to head back to Mission Control for a debrief!

Mission Complete! …or is it?

Congratulations, Agent CISO—you've completed all three mission objectives! You saved The Client by successfully implementing "cybersecurity by design" strategies, ensuring regulatory compliance, addressing physical vulnerabilities, leveraging the CALM model, and protecting system uptime in cost-effective ways. The Client even wrote you a glowing review to add to your mission debrief file:

Mission Debrief

"Agent CISO fostered a culture of cybersecurity awareness throughout our organization, embedding best practices before the facility was even built. Beyond facility design and construction, Agent CISO continuously improved our organization's security measures to keep up with Operation Blackout's evolving schemes to take down our critical infrastructure—all while meeting the demands of The Regulator. Agent CISO saved us millions of dollars by avoiding Operation Blackout's hefty ransom or losing operational control. Thank you, Agent CISO, for developing a robust plan to maintain operational continuity despite relentless virtual and physical threats."

You certainly deserve to celebrate a job well done, but Mission Control wants to remind you not to get too comfortable… we never know what Operation Blackout has planned next!

Agent CISO—You don't have to do this alone!

As you know, the next mission in protecting the world from cyber-attacks is always looming. For your next task, Mission Control has decided to bring in a partner for you—**Agent EPC,** who also happens to be the confidential source of the CALM model revealed in Mission Objective 2.

Agent EPC's skills are complementary to your own; outside of their secret agent identity, Agent EPC works for an industry-leading engineering, procurement, consulting, and construction firm specializing in delivering critical infrastructure worldwide. Agent EPC is ready to support you no matter where these missions take you throughout the infrastructure asset lifecycle, and take on any cybersecurity obstacles, together.

Let’s Talk Cyber

Increasing attacks to industrial operations have disrupted the traditional cyber model that used to separate the two worlds of IT and OT. Today, companies need to account for cyber impacts on **safety, operational continuity, liability, and national security.**

In response to the evolving threat environment and the increased operational and safety risks, critical infrastructure organizations are working to integrate compliance measures, industry best practices, and past experiences to safeguard their OT assets long-term and develop solid cybersecurity risk management programs.

From design-build to decommissioning, we help clients, like you, to keep their OT assets running safely through Cyber Asset Lifecycle Management (CALM). We work with you in the design, development, and implementation of cyber programs that optimize operations, maximize efficiencies, and minimize costs.

No matter where you are in your cybersecurity journey, our team of experts can customize a solution to fit your needs.

Powering Success:
A Strategic Guide to Energy Utilities' Top Boardroom Priorities
Private LTE:
Bridging the Data Gap in the Energy Transition

Read our other eBooks and Reports to stay resilient and secure from threats

Set up communications with your new partner, Agent EPC, to start your next mission!

Contact us