

THIRD EDITION



CRITICAL INFRASTRUCTURE PROTECTION

THEMES AND LESSONS LEARNED

MITIGATING RISKS BEHIND THE CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

2024





PREAMBLE AND LIMITATION OF PURPOSE

Through their compliance monitoring, enforcement, outreach, and other activities, the North American Electric Reliability Corporation (NERC), ReliabilityFirst Corporation (RF), Southeast Reliability Corporation (SERC), Western Electricity Coordinating Council (WECC), Midwest Reliability Organization (MRO), Texas Reliability Entity (Texas RE), and the Northeast Power Coordinating Council (NPCC) (collectively, the ERO Enterprise) have identified risk themes that have made it difficult for some entities to mitigate risks associated with the NERC Critical Infrastructure Protection (CIP) Reliability Standards.[1] The purpose of this report is to communicate these themes (and possible resolutions to them) so that we can work together to continuously assure the reliability of the Bulk Electric System (BES). While there are many discrete valuable lessons learned published by the ERO Enterprise to promote strong CIP performance, this report is intended to identify and share broader themes.

The suggestions for possible resolutions in this report are not, and should not be construed as, mandatory directives to industry. Rather, most of these possible resolutions are merely approaches that have been successful for certain entities. However, these possible resolutions may not be the best approach for every entity because the impact of the resolutions is largely driven by variables such as an entity's size, structure, workforce, technology, culture, and other factors.

[1] The power industry is subject to mandatory Reliability Standards for CIP. The entities discussed in this report have worked with, or are working with, the ERO Enterprise to resolve and mitigate any noncompliance with the CIP Reliability Standards.



TABLE OF CONTENTS



04

EXECUTIVE SUMMARY

05



LATENT VULNERABILITIES

The importance of internal detective controls

09



INSUFFICIENT COMMITMENT TO LOW IMPACT PROGRAMS

The need to revisit approaches to CIP-003 R2

13



SHORTAGES OF LABOR AND SKILLSETS

Challenges in workforce and succession planning

16



PERFORMANCE DRIFT

Physical security issues as markers of performance drift and apathy

20

CONCLUSION



EXECUTIVE SUMMARY

The ERO Enterprise pursues its mission of ensuring the effective and efficient reduction of risks to the reliability and security of the Bulk Power System. Through targeted engagement and outreach, the ERO Enterprise communicates themes, lessons learned, and best practices throughout each year.

It is also important for the ERO Enterprise to step back, evaluate broader themes over a longer period, and share those themes with industry, along with possible resolutions. To that end, this report is the third installment of “CIP Themes and Lessons Learned,” with prior iterations having been released in 2015 and 2018. While industry excels at many aspects of cyber security, the intention of this report is to outline areas for improvement with the goal of driving continued progress toward our shared mission of ensuring a reliable power system.

In this report, the ERO Enterprise strives to balance the importance of protecting entity information and security while still providing actionable examples of common or significant issues. Accordingly, the ERO Enterprise included high level fact patterns from open and closed cases in this report while at the same time avoiding the inclusion of information that, if released publicly, could jeopardize the security of the BES or be useful in planning an attack on energy infrastructure.

The four main themes the ERO Enterprise has identified are:

- Latent vulnerabilities;
- Insufficient commitment to low impact CIP programs;
- Shortages of labor and skillsets; and
- Performance drift.

Each of these themes is explored in more detail on the following pages, including suggestions to better address underlying issues and mitigate cyber security risks to the BES.

LATENT VULNERABILITIES

The importance of internal detective controls

THEME
1

Observations

In the years since the implementation of CIP version 5, the ERO Enterprise has observed many entities with medium or high impact BES Cyber Systems mature their approach to cyber security and CIP compliance, including notable advancements in internal controls programs. As a result, the nature of noteworthy CIP violations has fundamentally changed.

Latent Vulnerabilities
Long-standing, higher risk issues that evade detection and persist within entities' environments.

For instance, there are far fewer examples of entities running medium or high impact CIP programs with widespread, programmatic issues.[2] These types of cyber security “fall downs” were relatively common during, and in the years following, the implementation of CIP version 5. They were hallmarked by significant violations across several areas [3] with overlapping durations and root causes, many of which could be tied back to themes outlined in prior iterations of this report (i.e., organizational silos, disassociation between compliance and security, lack of awareness, and inadequate tools or ineffective use of tools).

While these broad-spectrum misses were not acceptable, growing pains were expected as large entities were trying to implement complex security protocols across multiple business units (and sometimes affiliates) and many assets. Industry responded to these issues and focused on building sustainable, scalable CIP programs with improved internal controls. The result has been a decline in widespread, programmatic failures, and entities have made strides in (a) preventing widespread issues before they start and (b) developing strong, routine detective controls to quickly identify most issues that do arise.

Even though there has been a decline in programmatic failures, the ERO Enterprise is still seeing long-standing, higher risk issues that evade detection and persist within entities' environments.[4] For the purposes of this report, the ERO Enterprise is going to refer to these issues as “latent vulnerabilities.”

[2] As outlined later in this report, some of these broader issues are still occurring at entities with low impact programs.

[3] For example, access management and revocation, electronic security perimeters, interactive remote access, physical security plans, ports and services, security patch management, security event monitoring, configuration change management, configuration monitoring, vulnerability assessments, transient cyber asset and removable media management, and information protection.

[4] On a positive note, these violations have been more isolated in nature. But the point of this theme is to highlight the negative aspects of these cases in an effort to drive continuous improvement and further eradicate cyber security risks to the BES.

LATENT VULNERABILITIES

Examples of Latent Vulnerabilities

In a case involving a physical security issue, an entity failed to monitor physical access points to substations. The entity implemented alarms and alerts to monitor for unauthorized access, which created a false sense of security that monitoring was occurring, but failed to recognize that configurations utilized during construction of the substations effectively eliminated the alarms and alerts. After evading detection for nearly three years, the vulnerability (i.e., lack of monitoring of physical access points) was finally discovered in preparation for an internal audit.



There are multiple examples of significant failures related to managing electronic access:

- An entity discovered that thousands of unauthorized users had improper access to BES Cyber System Information (BCSI) for nearly six years due to an inherited and overlooked configuration. The issue was discovered by happenstance. While helping a successor navigate files, a transferred employee realized that she had remaining unauthorized access to files, and further investigation uncovered the full extent of the issue. A quarterly detective control (access reviews) consistently failed to identify the issue because the user group/configuration causing the improper access capabilities was not included in the test population and access lists were not being pulled from the best source.
- More than 100 administrators had unauthorized access to BCSi repositories for over eight years. The issue dated back to the effective date of CIP version 5, and the entity failed to consider the type of access at issue when designing and executing its access management procedures and controls. The issue was discovered by happenstance when a subject matter expert completing other work noticed the potential error.
- Multiple user groups had unauthorized and unmanaged backend access to BCSi repositories due to an entity's lack of understanding of the technical architecture of its systems. The issues spanned several years and were discovered only when the entity was working on a new initiative.

LATENT VULNERABILITIES

- An entity failed to identify and manage four shared accounts, leading to the failure of Energy Management System (EMS) hosts and a loss of Supervisory Control and Data Acquisition (SCADA) visibility. The loss of visibility was attributed to two of the accounts automatically locking out following password expiration. The issue dated back to the effective date of CIP version 5 and was not discovered until the system outage investigation. An extent of condition review uncovered issues with additional shared accounts, and the violation spanned nearly three years.

A final representative case involves a patching issue discovered during a compliance audit conducted by a Regional Entity. An entity failed to accurately identify a patch source for a critical system application. The entity had identified a legitimate, albeit incorrect, patch source with a name very similar to the correct patch source, which contributed to the delayed discovery of the issue. As a result of relying on an incorrect patch source, security patches for the critical system application were not evaluated or applied for over three years.

Many entities dealing with such latent vulnerabilities have mature CIP programs with well-designed and strong internal controls, and the existence of these issues does not necessarily prove otherwise. But it does suggest that entities should consider utilizing additional or different tools or methods to identify latent vulnerabilities that may exist in their environments. As demonstrated in the examples above, failing to do so may allow significant issues to persist unidentified and uncorrected until: (a) someone accidentally discovers and reports them; (b) audit activities uncover them; or (c) a latent vulnerability reveals itself or is leveraged adversely, thereby causing operational issues.

Suggestions to Address Latent Vulnerabilities

To address latent vulnerabilities, the ERO Enterprise encourages entities to revisit their approach to detective controls. Entities should consider, without limitation, whether they are:

1. Dedicating sufficient resources to the development, implementation, testing, and execution of detective controls.
2. Conducting regular and sufficient testing of detective controls. Considering some of the examples above, testing to ensure that alarms and alerts from the substations functioned from end-to-end could have uncovered that issue much sooner. In some of the electronic access cases, access reviews failed to uncover the issues because the entities were using insufficient lists to compare access to authorization records. As part of testing controls, entities should ask whether

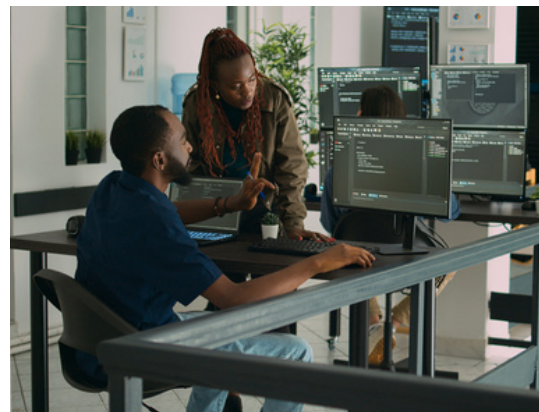
LATENT VULNERABILITIES

the detective control is relying on the best evidence and source records, as opposed to summaries, manually populated reports, or other records that carry a risk of being incomplete or inaccurate.

3. Periodically scrutinizing the design of existing detective controls and contemplating scenarios that those controls may not address.
4. Conducting appropriate internal audits and assessments, and preferably not just in the months leading up to a compliance audit conducted by a Regional Entity as (a) there may be years between such engagements, (b) external compliance audits are sample-driven and may not uncover latent vulnerabilities, and (c) entities should be more proactive in their pursuit of identifying and correcting cyber security risk.

The ERO Enterprise recognizes that resource constraints and practical realities prevent in-depth, detailed internal audits of every aspect of a medium or high impact CIP program, but they should not prevent entities from thinking critically, ranking the biggest risks to their environment based on several factors, and periodically and heavily scrutinizing those areas.

In addition to formal internal audits, entities could train internal subject matter experts to periodically search for latent vulnerabilities. At registered entities, the point person responsible for CIP-004 detective controls may not be a technical expert familiar with implementing, configuring, and provisioning access to BCSI. In this scenario, it might make sense to leverage an internal expert to conduct a review of configurations and access privileges and search for latent vulnerabilities.



Even if the hypothetical CIP-004 point person is a technical expert, bringing in a fresh set of eyes to conduct a peer review may be optimal to avoid a situation where a person is so close to something that they miss an obvious issue.

5. Leveraging and acting on internal vulnerability assessments, third party security assessments, penetration testing, and other activities designed to catch and correct latent vulnerabilities before they are exploited.

INSUFFICIENT COMMITMENT TO LOW IMPACT PROGRAMS

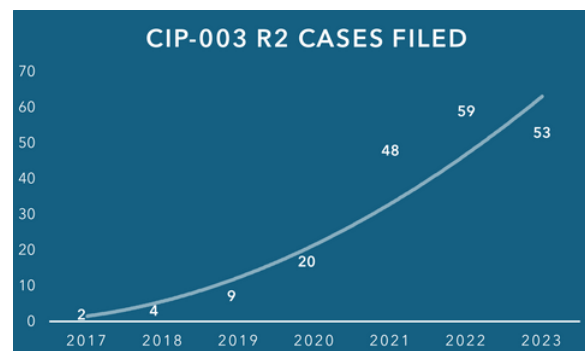
The need to revisit approaches to CIP-003 R2

THEME
2

Observations

In a vacuum, individual assets containing low impact BES Cyber Systems (sometimes referred to herein as “low impact assets”) may not pose a significant risk to the overall BES. Nevertheless, compromise of such assets could create localized issues, and an individual low impact asset could (a) serve as a channel to attack other assets or (b) be used to conduct reconnaissance. And the potential risk to the BES multiplies in scenarios where several low impact assets are compromised in a coordinated attack.

CIP-003 R2 contains the majority of low impact cyber security requirements with a focus on cyber security awareness, physical security controls, electronic access controls, cyber security incident response, Transient Cyber Asset (TCA) and removable media malicious code risk mitigation, and now as part of CIP-003-9, vendor electronic remote access security controls.[5] Between 2017 and 2023, the ERO Enterprise processed a steadily increasing volume of noncompliances with CIP-003 R2.



The ERO Enterprise does not expect this trend to reverse in the next few years because: (a) CIP-003 R2 violation intake—including compliance monitoring findings—and inventory remain at high levels; (b) the ERO Enterprise anticipates that the number of entities with low impact assets will continue to grow (e.g., ongoing efforts relating to registration of inverter-based resources); and (c) new and future requirements are raising the bar as it relates to low impact security obligations (e.g., the above-referenced incorporation of vendor electronic remote access security controls into CIP-003-9).

The ERO Enterprise has observed concerning trends in these violations. Nearly two-thirds of the violations involve examples of low impact entities that:

- misunderstand CIP obligations and security objectives;
- have an insufficient understanding of their cyber environment and struggle to effectively manage electronic access (i.e., inbound/outbound access); or
- struggle to implement effective TCA plans.

[5] In addition, CIP-012 requires all entities, including those running only low impact programs, to protect certain communications between Control Centers.

INSUFFICIENT COMMITMENT TO LOW IMPACT PROGRAMS

Some individual cases involve a blend of these issues, as detailed in the next section, but a majority of the failures involve the second trend (insufficient understanding of cyber environment and struggling to manage electronic access).

Examples of Insufficient Commitment to Low Impact Programs

As it relates to the first trend (misunderstanding of CIP obligations and security objectives), there are two main types of cases. First, there are many examples of improper or limited training of personnel responsible for completing requirements (e.g., staff misinterpreting requirements, lack of understanding of expectations, and lack of familiarity with documented policies, processes, and procedures). Second, there are many examples of low impact sites experiencing changeover in ownership, leadership, operations management, or compliance oversight (sometimes successive and frequent changeover at one site). In this second type of case, the ERO Enterprise has seen an increased frequency of entities ignoring, or taking a complacent approach to, the security objectives of CIP-003 R2.

The second trend involves two failures that often go hand-in-hand (insufficient understanding of cyber environment and struggling to manage electronic access). Certainly, it can be difficult to manage electronic access in and out of an environment without an adequate understanding of what is in that environment and how it is configured. There are many examples of entities: (a) with incomplete or inaccurate network diagrams; or (b) failing to identify, understand, or secure potential connections in and out of the environment. Many of these scenarios involve an added layer of coordination with third party vendors.

Cases involving the third trend (struggling to implement effective TCA plans) often have some overlap with the first trend (misunderstanding CIP obligations and security objectives). In many of these cases, the entity has a documented TCA and removable media malicious code risk mitigation plan but little or no evidence that staff are observing and executing the plan. For example, one entity's process required completion of a form and the capture of evidence demonstrating that a TCA had been scanned for malicious code prior to each use. Even though the entity confirmed that TCAs had been used, they could



INSUFFICIENT COMMITMENT TO LOW IMPACT PROGRAMS

not locate a single completed form and had no evidence of scanning for malicious code prior to use. Another entity could not identify how many TCAs were in use, let alone provide evidence showing management of those TCAs to reduce the risk of introducing malicious code in the environment.

Suggestions to Address Insufficient Commitment to Low Impact Programs

The ERO Enterprise has seen entities run their own low impact programs, rely exclusively on third parties, or use a hybrid approach. As an added layer and regardless of approach, many of these entities rely on vendors to varying degrees to handle specific activities within their program. The ERO Enterprise is not implying that any one approach is better than the others. The suggestions below are relevant to all low impact program types.

This theme highlights the need for improvements in attention to detail, planning, and execution to achieve security objectives at low impact sites. Entities with low impact BES Cyber Systems should consider revisiting their approach to achieving security objectives, evaluate whether personnel responsible for executing the program understand expectations and how to meet those security objectives, and ensure that personnel understand their cyber environment. Similarly, entities purchasing (i.e., buyers) or otherwise taking over the management of (i.e., operations and management or compliance management companies) existing low impact sites should engage in the same evaluation.

As part of this evaluation, entities should:

1. Understand what technology makes the facility work (what they own, what technology is in their environment, and what is running, or capable of running, their facility). The ERO Enterprise acknowledges that CIP-002.5.1a R1, P1.3 states that “a discrete list of low impact BES Cyber Systems is not required[,]” and a note in the current version of CIP-003 R2 provides that “[a]n inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.” But these statements do not excuse entities’ obligations to protect those systems and assets under CIP-003 R2. Indeed, it may be very difficult to achieve the security objectives of CIP-003 R2 without such inventories and lists, so entities should strongly consider developing and maintaining them.
2. Understand how that technology is configured and how they are protecting it.

INSUFFICIENT COMMITMENT TO LOW IMPACT PROGRAMS

3. Ensure that their program includes sufficient and consistent training and education on security practices and objectives.
4. Ensure that channels of communication between staff and leadership are open for the identification and mitigation of security vulnerabilities.
5. Ensure that their program clearly delineates roles and responsibilities at the facility and operations level (be sure to account for third party responsibilities, if any).
6. Identify ways to regularly verify execution of the program to achieve desired results.

Throughout this process, entities should identify areas for improvement and strive to implement a program that focuses on security posture and security objectives as opposed to treating CIP-003 compliance as a set of “check the box” activities.

Entities with Medium or High Impact BES Cyber Systems

Up to this point, this theme has predominantly been written from the perspective of an entity that has low impact BES Cyber Systems only. But that is not to say that entities that also have, or traditionally had, medium or high impact BES Cyber Systems haven’t encountered issues managing low impact BES Cyber Systems. In fact, there is one sub-theme that entities in this category should be aware of: staff may be unfamiliar with low impact obligations and expectations.

As examples at low impact sites, the ERO Enterprise has seen experienced staff: (a) remotely unlocking doors for unauthorized individuals; (b) neglecting to secure doors and manage keys; and (c) generally failing to identify a need to create or apply security plans to new sites or sites transitioning from medium/high to low impact.

Root causes in these cases often point to ineffective training and lack of direction or guidance, which can result in staff treating low impact sites as functionally out of scope for NERC CIP purposes, which in turn can increase the frequency of less-than-desirable security decisions. Entities in this category may be able to adapt many of their existing policies, processes, procedures, and practices to encompass their low impact BES Cyber Systems, and the ERO Enterprise encourages them to reengage staff executing responsibilities for low impact BES Cyber Systems to ensure expectations are clear.

SHORTAGES OF LABOR AND SKILLSETS

Challenges in workforce and succession planning

Observations

The gap between the number of cyber security workers needed and the number available has increased 12.6% year over year.

[6] This significant increase represents a growing unmet demand for cyber security labor. And this is occurring at a time when (a) 70% of organizations in the energy/power/utilities industry report a shortage of cyber security staff,[7] (b) 79% of organizations in this industry view the current threat landscape as the most challenging it has been in the past five years,[8] and (c) there have been reports of substantial skills gaps in the cyber security workforce.[9]

Tying this back to the CIP Reliability Standards, the ERO Enterprise often sees noncompliances that result, at least in part, from entities losing skilled labor (e.g., voluntary separation for new employment, retirement, etc.) and failing to successfully transition the underlying job responsibilities to new or existing staff (e.g., succession planning). For example, one registered entity has requested lengthy mitigation extensions in several cases due to issues restructuring and reassigning work following employee departures.

Sometimes the failure is attributable to knowledge transfer issues, and other times it is attributable to entities struggling to find knowledgeable and experienced individuals who are capable of adapting to the evolving electric and cyber security industries.

At the same time, the ERO Enterprise is seeing entities struggle to provide new and existing staff with the tools and resources necessary to strengthen their understanding of the nuanced issues and difficulties that arise in this space. Over time, the issues above can limit an entity's ability to (a) design and operate successful and sustainable security and compliance programs and (b) prevent, detect, and respond to cyberattacks.

BY THE NUMBERS

Gap between cyber security workers needed and number available increasing

12.6%

Year over year growth



70%

Of organizations in the energy/power/utilities industry report a shortage of cyber security staff

79%

Of organizations in the energy/power/utilities industry view the current threat landscape as the most challenging it has been in the past five years



Source: ISC2 Cybersecurity Workforce Study (2023)

[6] ISC2 Cybersecurity Workforce Study, p. 5 (2023)

[7] ISC2 Cybersecurity Workforce Study, p. 18 (2023)

[8] ISC2 Cybersecurity Workforce Study, p. 66 (2023)

[9] ISC2 Cybersecurity Workforce Study, p. 20 (2023)



SHORTAGES OF LABOR AND SKILLSETS

Large entities are complex, with hundreds of individual technology systems, cloud services, suppliers, processes, and interfaces making the identification of, and training on, critical skillsets essential. This complexity makes it extremely difficult to gauge what tools, resources, and staffing are needed to support a large entity's program or specific areas of the program. Defining roles in large organizations is necessary and essential to ensuring there are personnel assigned and aware of their responsibilities. In large organizations, there are often several individuals or groups touching the same set of assets, and clearly defining roles assists in eliminating uncertainty and creating accountability. In one case, an entity failed to clearly define roles and responsibilities among separate information technology groups and lacked an overarching control to manage organizational changes. This resulted in failures to (a) execute password changes for newly-commissioned devices, (b) fully inventory all known default or generic accounts, and (c) identify individuals authorized to access shared accounts.

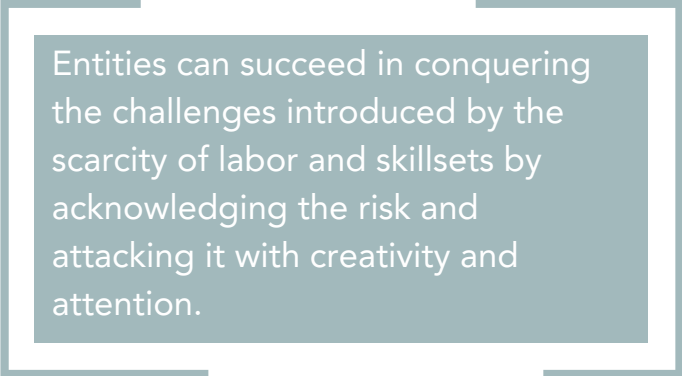
Small entities are also complex and often working with limited resources and tools, which can create barriers to effectively maintaining their own program, especially without third party assistance. Often, staff of small entities must gain expertise in multiple technology systems due to limited resources. The loss of a single employee can be significantly more disruptive to a small entity's security planning and posture because that single individual may represent a larger proportion of the entity's overall cyber security and compliance workforce. Small entities often rely on fewer employees, which can make any loss more impactful.



Suggestions to Address Shortages of Labor and Skillsets

Entities should consider the following suggestions as they navigate issues relating to shortages of labor and skillsets:

1. Sources of skilled staff include existing employees with the required skills and experience, hiring new staff with the needed skills and experience, or training and mentoring new or existing staff to gain the desired skills and experience.



Entities can succeed in conquering the challenges introduced by the scarcity of labor and skillsets by acknowledging the risk and attacking it with creativity and attention.

The industry as a whole will continue dealing with the departure of a large and skilled generation from the workforce. While these experienced individuals are still in the workforce, entities should take the opportunity to hire new staff and use their experienced staff to educate and train their successors.



SHORTAGES OF LABOR AND SKILLSETS

Existing knowledge must be shared with and expanded upon by new employees. As availability of skilled and experienced staff remains at low levels, training and mentoring may be the best option for increasing or maintaining appropriate levels of skilled staff.

2. Entities might have to reassess their human resources approach to navigate an increasingly competitive field to induce employees to join and stay at an entity. They may also need to rework and reimagine their recruiting efforts, from colleges and high schools to job fairs, to build awareness around the importance of the energy sector and the opportunity for security professionals to make an impact on such an essential and foundational service.
3. When implementing new processes or internal controls, entities should ensure adequate resources to execute the process or internal control without overly tasking existing staff. They should develop processes or internal controls in coordination with the staff responsible for executing them. Further, they should ensure that said staff have a way to share feedback on unmanageable processes or internal controls to management (before such unmanageable processes or internal controls lead to failure or burnout).
4. When considering new vendor technology, entities should take advantage of and ensure that responsible personnel engage in demonstrations and training offered by the vendor prior to implementation.
5. Entities should implement succession plans for staff who support technology solutions, processes, or internal controls. The departure of single employees should not lead to process or internal control failures or an inability to manage a technological solution. Succession planning is critically important for staff with unique responsibilities. Entities should: (a) strive to identify unique technical tasks and prioritize those tasks based upon risk; (b) document those tasks thoroughly (e.g., procedures, work instructions, job aids); and (c) implement short- and long-term plans to handle these tasks in the event of primary staff departure.
6. Where possible, entities should create process, internal control, and technology commonalities between departments, business units, or affiliates as it can increase the available staff who may be able to address workforce and skillset shortage issues.
7. The ERO Enterprise is working hard to help highlight the critical skillsets needed and assist industry in continuing to develop and maintain these critical skillsets across their workforce. Many different tools and resources are available to help entities optimize their security and compliance cultures, such as training, workshops, seminars, webinars, e-learning modules, and articles on best practices and lessons learned regarding emerging cyber security risks.

PERFORMANCE DRIFT

Physical security issues as markers of performance drift and apathy

Observations

Physical security has long been a focal point for the ERO Enterprise, originating with NERC Urgent Action Cyber Security Standards 1205 (Physical Security Perimeter), 1206 (Physical Security Controls), and 1208 (Monitoring Physical Access) and continuing today through CIP-006-6 (Physical Security of BES Cyber Systems),^[10] CIP-014-3 (Physical Security),^[11] and CIP-003-9 R2, Attachment 1, Section 2 (Physical Security Controls).^[12] Protecting grid assets from physical breach, misuse, and damage is a long-standing and continuous responsibility. But even where there are time-honored and well-communicated expectations, strong programs can slip and decline due to a variety of factors. This theme highlights examples of apathy, circumvention, complacency, inattentiveness, and other types of “performance drift” in physical security programs at entities of every size and type.

One of the many challenges of executing a physical security program is managing tasks that require repetitive behavior over significant periods of time, as there is increased potential for personnel to lose focus on the performance of an individual act or forget the importance of the act itself. Acknowledging this challenge does not authorize process adherence failures, especially when the stakes are high (i.e., poor decisions in NERC-scoped physical security programs can endanger the reliable and secure operation of the BES). The ERO Enterprise has seen increased failure with these repetitive behaviors when disciplined execution becomes inconvenient or uncomfortable.

People often conceive of the BES as a collection of wires, breakers, switches, and turbines. The BES is all of that, but it is also a tremendously intricate system operated by thousands of human beings. Human beings rely on assumptions and frequently operate with social norms, or commonly shared manners, one even being holding the door for others. Of course, in the context of physically protecting low, medium, and high impact BES Cyber Systems, certain assumptions and social norms must be set aside.

[10] CIP-006-6 applies in medium and high impact programs.

[11] CIP-014-3 applies in medium and high impact programs.

[12] CIP-003-9 R2, Attachment 1, Section 2 applies in low impact programs.

PERFORMANCE DRIFT

Examples of Performance Drift

The ERO Enterprise has observed entity staff letting individuals into secure areas when those individuals forgot (or never or no longer had) credentials. In multiple instances, an employee who was running late to a shift, without their badge, was able to talk their way through multiple barriers and into a Physical Security Perimeter (PSP). Similarly, individuals returning from leave had their credentials deactivated while on leave, but they were let in regardless after speaking with a security guard who failed to follow security protocols.

There are related cases involving access revocations due to expired background checks or incomplete annual training. In one case, staff witnessed an individual unsuccessfully attempting to badge in and assumed there must have been a technical issue with the badge reader or door; therefore, they opened the door or lent a badge to the individual when, in reality, a security control was functioning as intended to prohibit said access.



Staff have also allowed unauthorized and unknown individuals into secure areas for reasons that can only be described as “they seemed like they were supposed to be there.” Examples here include: (a) allowing a truck to enter and roam a site for over a half hour because it was believed to be an authorized delivery truck; and (b) allowing an unknown individual into a secure area because he was dressed in work coveralls and claimed to be with a vendor. There are more examples of impermissibly propping doors, ignoring alarms, allowing visitors to roam freely, accidentally leaving doors and gates open, sharing badges and personal identification numbers (PINS), and engaging in other poor security practices.

Even worse, there are cases of intentional circumvention and weakening of security controls. In one case, a long-tenured contractor became increasingly frustrated waiting for an escort to begin work in a secure area, so the contractor used available tools to leverage the door open to the area. The contractor was familiar with the importance of access restrictions and the need for escorting within the facility but felt comfortable enough to force entry due to a slight delay in escort availability. This sort of attitude around physical security suggests that culture-driven performance drift could be on the rise.

PERFORMANCE DRIFT

Suggestions to Address Performance Drift

To some extent, individuals performing physical security tasks appear to have lost sight of the purpose of access controls and fall into the trap of viewing them as impediments to their role. Some of the failures described above can seem understandable, and maybe even innocuous, but when it comes to the security of the BES, they are unacceptable. It is this sort of complacency and performance drift that will lead to an entity letting the wrong person in on the wrong day with potentially dire consequences. The physical security threat level remains high. As set forth in the E-ISAC 2023 End-of-Year Report, there were “more than 2,800 physical security incidents shared with E-ISAC [in 2023.]”[13]

With elements of social engineering and human error present in most cyber security incidents, the ERO Enterprise encourages entities to refocus on (a) eliminating poor physical security practices and (b) driving discipline in physical security programs. Ideally, entities are not fostering an environment where people are substituting individual judgment calls in place of security protocols.

Given the examples above, it is not difficult to imagine a scenario in which a terminated individual or someone posing as an employee or contractor attempts to exploit human instincts, including the proclivity for blind trust, to access and harm the BES.

This theme underscores that even the oldest and most fundamental security practices in the CIP space require organizational attention. An entity can have cutting edge tools and well-conceived physical security policies yet still experience performance drift.

Ideally, entities are not fostering an environment where people are substituting individual judgment calls in place of security protocols.

To combat performance drift, the ERO Enterprise recommends that entities consider:

1. Testing their organization for potential performance drift on the physical security side. Consider periodic physical penetration testing. Communicate anonymized testing results to staff where failures are identified to create awareness of how simple acts and situations can be leveraged by a bad actor.

[13] Electricity Information Sharing and Analysis Center (E-ISAC) 2023 End-of-Year Report, p. 4 (2023) (<https://www.nerc.com/pa/CI/ESISAC/Documents/2023%20E-ISAC%20End-of-Year%20Report.pdf>).

PERFORMANCE DRIFT

A security program with continuous internal skepticism is necessary to fight the risk of performance drift. Indeed, the need for skepticism in physical security has only been heightened as remote work and turnover have increased, resulting in staff becoming increasingly unfamiliar with colleagues and other departments.

2. Emphasizing and reinforcing through training and other means why process adherence and individual acts matter. Sometimes the execution of an act can become mindless, and the purpose of an act can become lost. It is imperative to highlight real-world examples of the importance of process adherence in physical security. CIP-004-7 R1, CIP-004-7 R2, and CIP-003-9 R2, Attachment 1, Section 1[14] training and awareness activities provide outstanding opportunities for entities to refresh employees in this area.

3. Constructing incentive programs aligned with corporate values to both promote process adherence and whistleblowing when processes are ignored.

[14] CIP-004-7 applies in medium and high impact programs; CIP-003-9 applies in low impact programs.



CONCLUSION



Cyber security is an ongoing process, and there is always room for improvement. The ERO Enterprise hopes that by shining a light on the topics outlined herein, entities will continue the conversations within their organizations and with their peers and will reach out to staff at the Regional Entities for more tailored conversations regarding entity-specific questions and issues.

