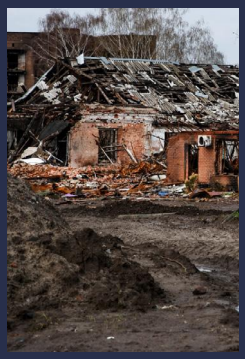
ASIS INTERNATIONAL® JAMAICA CHAPTER
Jamaica Chapter # 74
www.asisjachapter.org, Volume 27, March 2026
The Informer
The Official Newsletter of ASIS Jamaica Chapter #74

IN FOCUS

EMPOWERMENT THROUGH CERTIFICATION AND KNOWLEDGE SHARING

Disaster Readiness in a Hybrid Threat Era: Rethinking Proactive Security in Jamaica

In Jamaica, the maritime industry supports economic stability and tourism accounts for around one-third of foreign exchange revenues, a significant climate catastrophe might result in both strategic risk and economic disruption. By upsetting economies, destroying infrastructure, and undermining public confidence in times of crisis, it can exacerbate hybrid threats. - *Page 2*



Physical Security After a Disaster

Security systems will be compromised during a disaster such as Hurricane Melissa, doors may malfunction, alarms disabled, interrupted power supply, and lack of connectivity between systems will negatively impact electronic access control. - *Page 11*

ASIS INTERNATIONAL®
JAMAICA CHAPTER

Contents

MESSAGE FROM THE IMMEDIATE PAST CHAIRMAN:

BUILDING PARTNERSHIPS, ADVANCING SECURITY: OUR 2026 STRATEGIC ROADMAP

Jason Robinson, PCI, PSP

> ***Under the leadership of myself and Vice-Chairman Suzanne Scarlett, PSP and your Business Management Committee we have developed a five-pillar strategic plan which sets out the road map.***

Dear valued Members and Friends, As we embark on a new year together, I am committed to ensuring that our Chapter remains a diverse but unified space for all. We will continue to make an impact in the wider security industry, by delivering educational programs, raising awareness, and advocating for the profession.

Under the leadership of myself and Vice-Chairman Suzanne Scarlett, PSP and your Business Management Committee we have developed a five-pillar strategic plan which sets out the road map to:

- Build partnerships
- Increase member value
- Continue global expansion
- Advance the profession
- Optimize digital transformation

As we continue to build our Chapter, I would like to thank you for your dedication and commitment. Remember, our success is a shared responsibility – please get involved!

Let's work together to make 2026 a memorable year for the Chapter

Photo courtesy of: https://averyhall.com/what-should-be-in-your-hurricane-preparedness-kit/

DISASTER READINESS IN A HYBRID THREAT ERA:

RETHINKING PROACTIVE SECURITY IN JAMAICA

THE MARITIME INDUSTRY SUPPORTS ECONOMIC STABILITY AND TOURISM

By Angilee Baboram, NextGen Liaison

Jamaica's geostrategic location, astride major shipping lanes and serving as a transshipment bridge between North and South America, places it within a dynamic global security corridor. In 2026, that geography intersects with climate volatility, transnational organized crime, digital threat actors, and information manipulation.

In Jamaica, the maritime industry supports economic stability and tourism accounts for around one-third of foreign exchange revenues, a significant climate catastrophe might result in both strategic risk and economic disruption. By upsetting economies, destroying infrastructure, and undermining public confidence in times of crisis, it can exacerbate hybrid threats. Additionally, it can lead to increased organized crime, operational loopholes, digital exploitation, and stress on security systems.

The psychological aspect is also crucial. Such events may result in increased anxiety, rumors, and institutional mistrust post disaster, according to United Nations Office for Disaster Risk Reduction (UNDRR 2025), From a forensic psychology perspective, crisis situations intensify cognitive bias, fear-based thinking, and vulnerability to misinformation, all of which hybrid actors take advantage of.

> ***A significant climate catastrophe might result in both strategic risk and economic disruption. By upsetting economies, destroying infrastructure, and undermining public confidence in times of crisis, it can exacerbate hybrid threats.***

> ***ASIS International's Jamaica Chapter NextGen, intends to be proactive in educating the next generation of security professionals capable of operating in hybrid-threat environments. The NextGen represents a critical incubator for leaders who can interpret global intelligence***

Global intelligence assessments reinforce this multi-domain convergence. The U.S. Annual Threat Assessment (2025), Israel's National Security Outlook, Danish Defense Intelligence Service Intelligence Outlook (2025), and NATO's Strategic Foresight Analysis all emphasize multi-domain hybrid warfare, where cyber operations, disinformation campaigns, proxy violence, economic coercion, and terrorism-inspired acts intersect. The information gathered from these assessments can be used as learning centers for development and customized use in the current threat landscape.

Growing evidence points to climate change as a threat multiplier that exacerbates instability and increases the likelihood of radicalization in susceptible areas. These cognitive vulnerabilities are real for an economy that is small, open, and digitally connected, with over 80% of people using the internet.

Against this backdrop, the need for trained proactive security professionals is paramount. ASIS International's Jamaica Chapter NextGen, intends to be proactive in educating the next generation of security professionals capable of operating in hybrid-threat environments. NextGen represents a critical incubator for leaders who can interpret global intelligence, anticipate convergence across climate, crime (physical and digital), and terrorism vectors, and act proactively rather than reactively.

Reactive response alone will not characterize Jamaica's security position in 2026 and beyond. It will depend on how well-prepared, nimble, and forward-thinking its upcoming security professionals are. More than just a security network, ASIS Jamaica Chapter NextGen is a calculated investment in the resiliency of the country.

Hurricane Kit Checklist

INCIDENT MANAGEMENT:

- Laminated evacuation plan
- Laminated shelter in place plan

PROTECTION AND SHELTER:

- Face masks
- Emergency thermal blankets
- Emergency ponchos
- Roll plastic sheeting
- Roll duct tape

TURNING OFF UTILITIES AND OTHER TASKS

- Multifunction tools including pliers, wire cutter, screwdriver, can opener, bottle opener, utility knife, etc.
- Pair leather-palmed work gloves

COMMUNICATION AND LIGHT

- Metal whistles with lanyard
- AM/FM radio with two sets of AAA batteries
- Flashlight with two sets of D batteries
- 12-hour light sticks
- LED Safety Signal
- NotepadPen
- Waterproof document pouch

HYDRATION AND NUTRITION

- Water bag for carrying, purifying, and storing water (1 gallon per person)
- High-calorie food bars (at least 6 per person)
- Emergency water pouches
- Water purification tablets

MEDICAL, HYGIENE AND SANITATION

- Personal First Aid packets
- Family First Aid kit
- First Aid Guide
- Biohazard bags
- Toilet paper roll
- Moist towelettes
- Vinyl gloves

EVACUATION

- Portable backpack with the following items packed inside
- Face mask
- Thermal blanket
- Emergency poncho
- Bodywarmers
- Flashlight
- Metal whistle with lanyard
- Weather-resistant flashlight12-hour light sticks
- LED Safety Signal
- Water filtration bottle
- Emergency water pouches
- High-calorie food bars
- First aid kit
- Vinyl gloves
- Toilet paper roll
- Moist towelettes
- Biohazard bags

"DUTY CALL"

Aldean Campbell
Legislative Chairperson

> ***These developments remind us that legislation is not a distant concept, but it is the environment in which we make it to be and operate every day. When the law changes, our responsibilities change, and so do the risks and opportunities before us.***

Colleagues,

As we move further into the year, I want to reaffirm the purpose of the Chapter's legislative arm, our mandate is to ensure that the members remain informed, prepared and confident.

Over the past quarter, we have witnessed meaningful changes in national discussions concerning security governance, compliance expectations, and the modernization of regulatory agendas to include licensing standards, training requirements, compliance and expectations. These developments remind us that legislation is not a distant concept, but it is the environment in which we make it to be and operate every day. When the law changes, our responsibilities change, and so do the risks and opportunities before us.

In the coming months, the Legislative Committee will continue to:

1. Track and interpret emerging policies that affect private security operations, corporate governance, and protective services.
2. Provide clear, accessible summaries so members can understand not just what has changed, but why it matters.
3. Support the Chapter's training and professional development efforts by aligning legal updates with practical application.
4. Strengthen our partnerships with national agencies and industry stakeholders to promote transparency, accountability, and best practice standards.

Therefore, our goal is to make legislative awareness a tool of empowerment, not intimidation. When practitioners understand the framework, they work within, they lead with greater confidence, make better decisions, and contribute to a safer, more resilient Chapter and country. Consequently, we are not just monitoring laws, we are helping the Chapter to stay aligned with national regulatory requirements and best practices.

I encourage you to be supportive, stay engaged, ask questions, and share insights from your own areas of practice. The strength of this Chapter has always been its members, professionals who are committed to excellence, integrity, continuous learning, and shared knowledge.

Thank you for your ongoing support and for the work you do every day to elevate the standards of security across our island and the diaspora. Let us work for the greater good, knowing that the Chapter rises when its members rise together.

> ***I encourage you to be supportive, stay engaged, ask questions, and share insights from your own areas of practice. The strength of this Chapter has always been its members, professionals who are committed to excellence.***

BEYOND COMPLIANCE:

The Strategic Value of Pre-Employment Screening Programmes

By Keron Thomas, MSc., PCI, PSP
Chapter Secretary

Laws and regulations impose organisational obligation to maintain safe working environment and prevent harmful acts/actions of employees. The introduction and maintenance of a robust pre-employment screening program by an entity can be worth its weight in gold. Many lessons have been learnt locally and internationally for the lapse of this essential onboarding step, from the case(s) of high-powered CEOs claiming unearned qualifications/ experience, to line staff omitting their criminal antecedents, all for the same outcome- employment.

Organisations being conscious of these nondisclosures that are easily enabled/enhanced with AI, are increasingly recognizing this strategic responsibility and have been investing in risk reduction strategies that prevent negligent hiring, and civil suits. While the mitigative action is evident, a word of caution is necessary: pre-employment screening should not be treated as mere obligatory checks, but rather as deeper checks to unearth misrepresentation and omissions. This hardline prevents financial losses, increases brand protection, and satisfy stakeholders.

ASIS Pre-employment Background Screening Guideline asserts that pre-employee screenings are done to make the right hiring decision and/or provide a safe working environment. Admittedly, while pre-employment screening is not a panacea for risks, it is statistically beneficial to organisations and therefore adds value to organisations.

Best practice dictates that pre-employment screening begins with a detailed employee application form containing volunteered information. The information should be collected at the earliest, and cover at a minimum, an applicant's bio details, employment

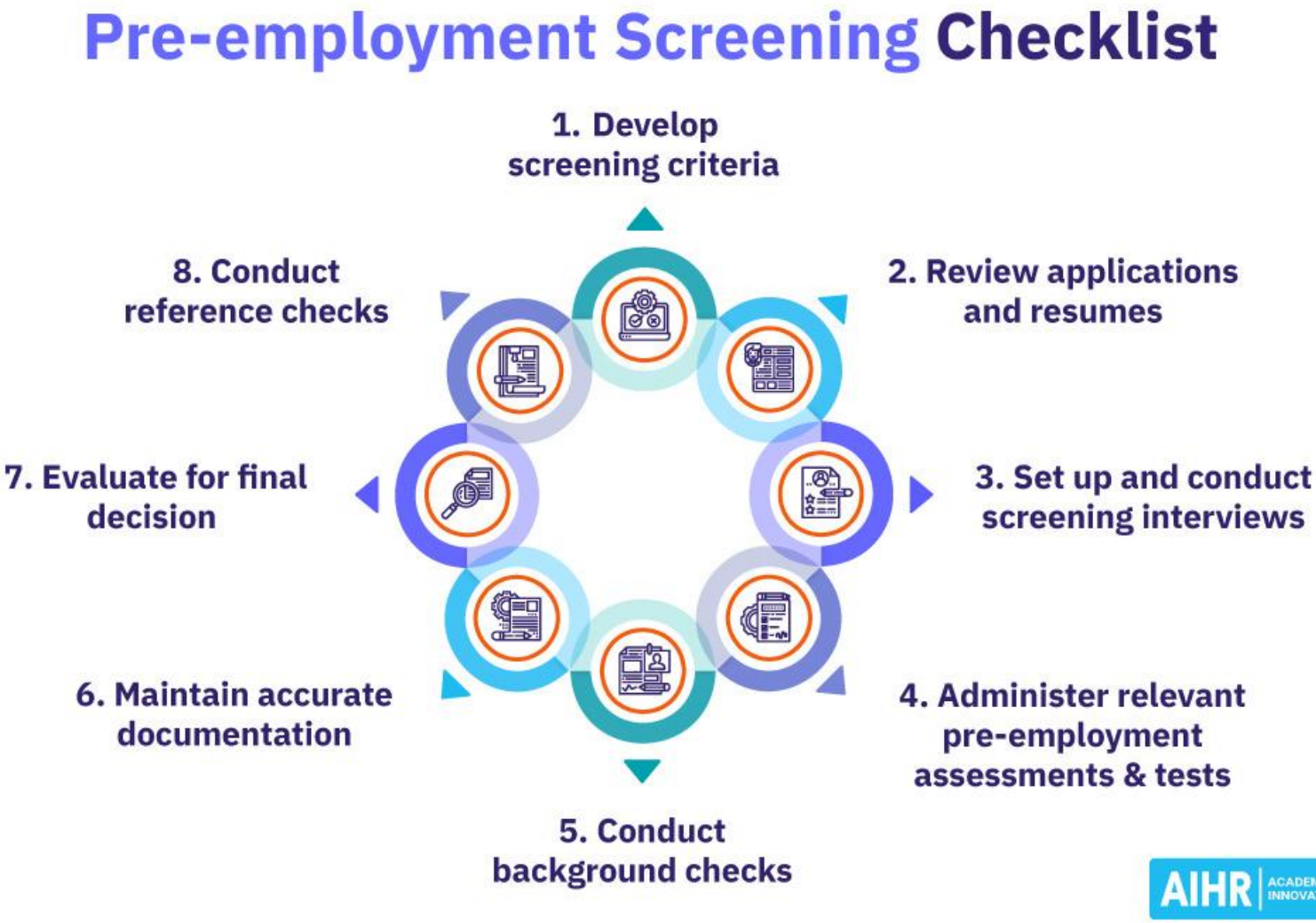
> ***Organisations can decide on the screening process being either an in-house or a delegated function, so long as it is understood that the buck stops with them. Care is therefore required in observance of data collection laws by whomever conducts these checks.***

> ***The strategic value will be manifested through reduced risks as verification checks are done on identity, stakeholders are reassured through criminal checks, turnover is reduced or the cultural fit of an applicant is determined through reference checks.***

history, qualifications and training records, credit and financial history, references (independent), and criminal history. Attention must be given to framing questions around the contentious issues of an applicant's age, religion, marital status, disability, sexual orientations, political leanings etc. because of the risk of inferring/ implying prejudice. Organisations can decide on the screening process being either an in-house or a delegated function, so long as it is understood that the buck stops with them. Care is therefore required in observance of data collection laws by whomever conducts these checks, as lawsuits can easily arise where negligence or prejudice can be proven.

Simple ways of implementing pre-employment screening strategically to improve the organisations governance framework, includes making it standard for all new hires, scaling to the applicant's risk level, transparency and applying periodic re-screening for employees in sensitive roles and positions. The strategic value will be manifested through reduced risks as verification checks are done on identity, stakeholders are reassured through criminal checks, turnover is reduced or the cultural fit of an applicant is determined through reference checks.

Finally, pre-employment screening should be viewed as more than meeting compliance objectives, and more of risk-reducing objectives that add value to an organisation's mission and vision.



BEYOND THE BOTTOM LINE:

Scaling Security Partnerships In Jamaica's Evolving Landscape

Capt. Garth Gray, CPP, PCI, PSP
ASIS Member

In Jamaica's evolving business environment, facility security is no longer a back-office function—it is a frontline enabler of continuity, reputation, and growth. For management teams and entrepreneurs alike, the difference between resilience and vulnerability often lies not in the hardware itself, but in the quality of the partnership behind it.

Too often, organizations accept mediocrity in service delivery, tolerating late responses, vague explanations, or transactional attitudes from providers. But in a market where supply chains are fragile, the industry is tightly knit, and the tropical climate punishes equipment, mediocrity is not just inconvenient—it is dangerous. High service-level expectations must be the baseline. Anything less undermines both the business and the security function.

The "Honey-Moon" Trap and Early Red Flags

Procurement's riskiest stage is the bedding-down period. Managers and entrepreneurs focus on technical specifications and customs clearances, while subtle signs of a failing partnership slip by. Red flags rarely appear as catastrophic failures. They show up as reactive inertia: a provider who only calls when an invoice is due, or a technician who patches a sensor without explaining how salt air or heavy rain triggered it. If a provider cannot articulate a three-year roadmap, blames logistics for every delay, or resists open-platform integration, the issue is not technical—it is philosophical. You want a strategic partner; they want a sale.

The Trap of Enterprise Lock-In

Enterprise brands oftentimes rely on proprietary protocols that lock you into their ecosystem—and their exclusive local distributor. For managers, this creates operational rigidity. For entrepreneurs, it stifles scalability. If the relationship sours, you face a grim choice: endure poor service to protect your investment, or rip and replace hardware with years of functional life left. As facilities expand, this risk compounds. Bolting on secondary systems to compensate creates

a "Frankenstein" architecture—disjointed platforms, longer mean time to respond (MTTR), and doubled training costs for your guard force.

The ROI Gap: The Cost of Severing Ties Early

Breaking ties too soon is financially punishing. In Jamaica, foreign exchange and importation costs magnify the impact. NVRs, controllers, and specialized sensors depreciate over five to seven years. Ending a relationship in year two means abandoning most of your ROI.

Switching costs are steep:

- De-installation and Re-installation: Double labor at premium rates.
- Knowledge Gap: Losing site-specific history and configuration nuances.
- Operational Downtime: Vulnerability windows during transition.

For management, these costs erode budgets. For entrepreneurs, they erode competitiveness.

Recommendations for "Marriage-Ready" Procurement

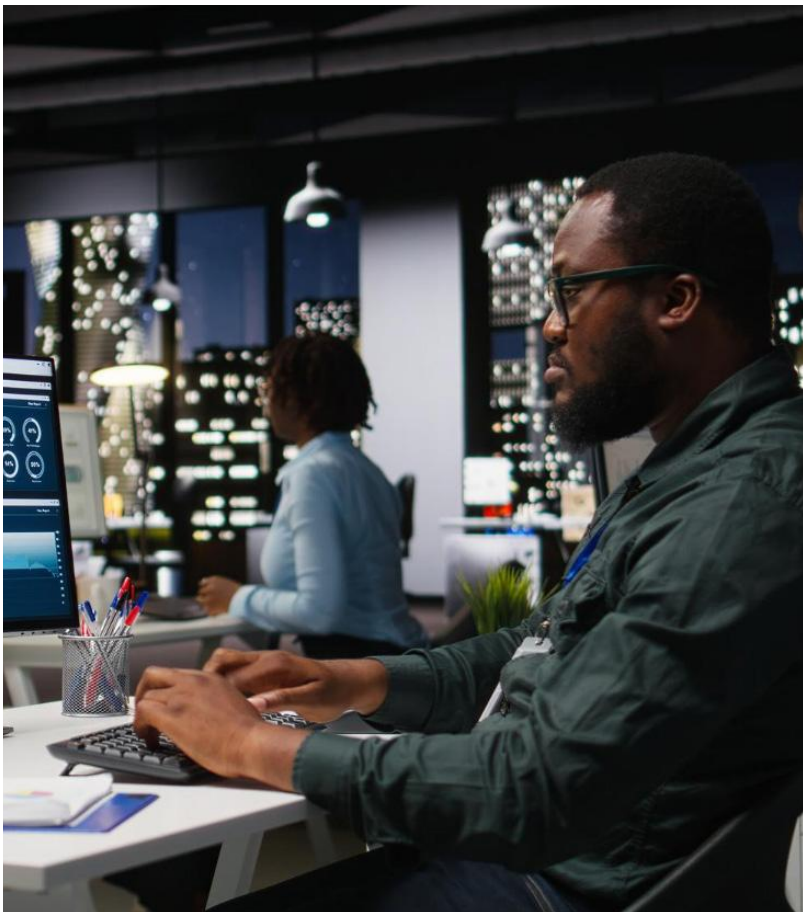
To elevate industry standards, procurement must shift from product-focused to partnership-focused. Alignment between business objectives, the security function, and the provider is non-negotiable.

- **Prioritize Open Architecture:** Hardware must not be locked to a single dealer. If you fire the provider, another vendor in Kingston or Montego Bay should be able to manage the same equipment.
- **Conduct a "Pre-Nup" Audit:** Interview their support desk. Speak to long-term local clients. Ask about performance and parts availability in years three to five, not just the honeymoon phase.
- **Philosophical Vetting:** Ask, "What happens when our local needs outpace your current software?" A scalable partner will show API integration paths, not push a full system replacement.
- **Define Exit Strategies:** Build knowledge-transfer clauses into SLAs. Ensure programming codes, administrative passwords, and system maps remain your property if the relationship ends.

Conclusion

For managers the lesson is clear, demand high service levels and strategic alignment. For entrepreneurs, the takeaway is equally critical: choose partners who scale with your vision, not just your current footprint.

Facility security is not about locks and cameras—it is about business continuity. By rejecting mediocrity and insisting on alignment between business, security, and provider, you ensure your enterprise grows without the costly heartbreak of starting from scratch.



> ***For managers the lesson is clear, demand high service levels and strategic alignment. For entrepreneurs, the takeaway is equally critical: choose partners who scale with your vision, not just your current footprint.***

The Hidden Danger of Unqualified Close Protection Officers

Ian Roberts, PSP
Treasurer

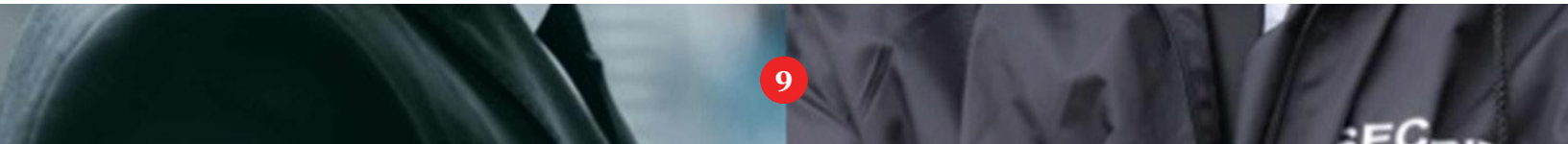
An unqualified person posing as a Close Protection Officer (CPO) is not just ineffective, it is dangerous, unlawful, and an increasingly prevalent risk in the personal protection industry. Often labelled as "gym-muscle" bodyguards or "rent-a-cops," these individuals lack the specialized training, discipline, and judgment required to safeguard high-profile clients. Instead of reducing risk, they frequently introduce new and avoidable threats.

Key risks associated with unqualified CPOs:

- **False Sense of Security:** Clients may believe they are protected, when in reality they are more exposed and vulnerable to harm.
- **Failure in Threat Detection:** Without proper training in threat assessment and advance work, these individuals are unlikely to identify or prevent dangers such as ambushes, snatch-and-grab incidents, or kidnappings.

> ***An unqualified person posing as a Close Protection Officer is dangerous, illegal, and is increasingly a common issue in personal protection.***

- **Poor Situational Awareness:** An inability to read environments or anticipate risks can escalate otherwise manageable situations.
- **Lack of Planning and Preparation:** Effective protection relies on research—routes, locations, culture, and contingencies. Unqualified individuals often neglect this entirely.
- **Breakdown in Team Coordination:** Close protection is a team discipline. Inexperienced personnel create gaps in coverage, especially in dynamic or crowded environments.



Common warning signs:

- **Unprofessional Demeanour:** Nervous, overly aggressive, or visibly uncomfortable when not in close proximity to the client—lacking composure and control.
- **Questionable Credentials:** Limited or non-accredited training, often with backgrounds unrelated to professional close protection.
- **Overreliance on Physical Presence:** Emphasis on size or strength rather than intelligence, planning, and tactical competence.
- **Poor Positioning:** Standing in vulnerable positions, turning their back on crowds, or failing to control the client's immediate environment.
- **Inadequate Response Capability:** In a crisis, hesitation or improper reaction can leave the client dangerously exposed.

Chapter members participated in the Health and Wellness Unit in Collaboration with ACP PSTEB 5K Run Walk.

Physical Security After a Disaster

This article was first published in the Jamaica Gleaner on Thursday January 22, 2026

Carlos Pipher, CPP, PCI, PSP
Newsletter Editor

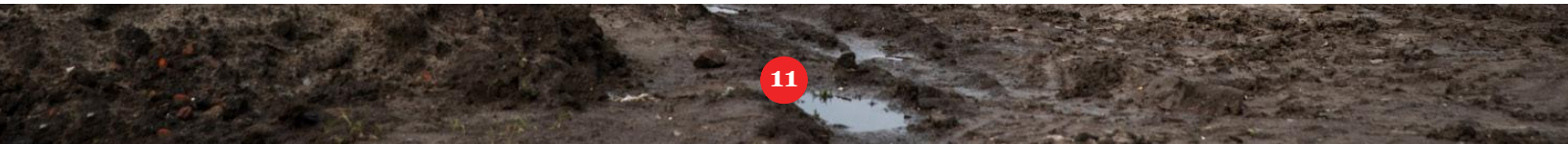
> ***Security systems will be compromised during a disaster such as Hurricane Melissa, doors may malfunction, alarms disabled, power destroyed, and lack of connectivity between systems will negatively impact electronic access.***

The immediate concern after a disaster is rescue operations and humanitarian aid. However, physical security which mandates the protection of assets, tangible and intangible, are most times overlooked. Disasters often leave buildings damaged, fences destroyed, lighting disabled, communication blackout, and surveillance systems offline. These conditions create opportunities for nefarious activities, such as looting; vandalism; theft of proprietary information; and unauthorised access, particularly at commercial sites, warehouses, and critical infrastructure facilities. The post-disaster period can be just as dangerous as the disaster itself if security controls are not swiftly put in place.

Security systems will be compromised during a disaster such as Hurricane Melissa, doors may malfunction, alarms disabled, interrupted power supply, and lack of connectivity between systems will negatively impact electronic access control. Temporary security measures is essential to secure damaged facilities and to assist in business continuity. This includes restricting access to facility, cordon off unsafe areas, accounting for personnel, and accounting and securing hazardous materials that may have become exposed, especially products that are of dual use. Erect temporary fencing where vulnerability exits, use mobile lighting towers to monitor perimeter fence and high-value areas, and security patrols to deter criminal activity.

Prioritized Treatment

Government facilities are subjected to heightened risks, some more than others because of their nature of operation. Their damage often disrupt essential services, making them attractive targets for theft or sabotage. Facilities should factor physical security assessments in their emergency response plans, so that breaches to the physical protection systems can be identified in order



to apply prioritised treatment to protect assets. Physical security is the platform for all security systems.

Following recovery, the aim should be to restore the physical protection system (PPS) to normality or upgrade to more robust measures of protection. Security systems should be repaired/replaced with urgency, badges audited, and lessons learnt should be annexed in security plans. Facilities with well-developed physical protection systems and trained staff recover faster.

Let us not forget security guards, who may be required to work in conditions that are not hospitable and safe. Security providers should ensure that their guards are given the necessary personal protective equipment for the disaster environment.

> ***Security systems should be repaired/replaced with urgency, badges audited, and lessons learnt should be annexed in security plans.***

Disasters test organisational leadership, organisations and private enterprises that integrate physical security into their disaster recovery plan are better positioned to protect lives, and assets.

Managing Converging Risks in Energy Infrastructure

Dr. Oswald Smiley, CPP, PSP, PMP
Community Liaison, *ASIS Jamaica*

Energy Infrastructure: The Hidden Security Battleground

In today's borderless risk environment, cyber threats, geopolitical instability, supply chain disruptions, and climate-driven disasters are converging to create unprecedented challenges for organizations. Energy infrastructure sits at the centre of this convergence, powering everything from healthcare and finance to logistics and communications. Vulnerabilities in centralized grids can lead to cascading failures, making energy resilience a core component of corporate and national security.

JPS launching an Emergency Mobile Power Generator Unit in Bethel Town February 21,2026. Serving over 800 customers to include critical facilities such as Clinics, Police Stations & Communication Cell Sites in Bethel town following the passage of Hurricane Melissa in October 2025.

Microgrids and the 5-P Integration Model

Microgrids and distributed energy resources offer a practical solution by providing localized generation and "islanding" capability, ensuring operational continuity during grid disruptions. However, technology alone is not enough. The effectiveness of these solutions depends on how well they are integrated into an organization's broader security and risk management strategy.

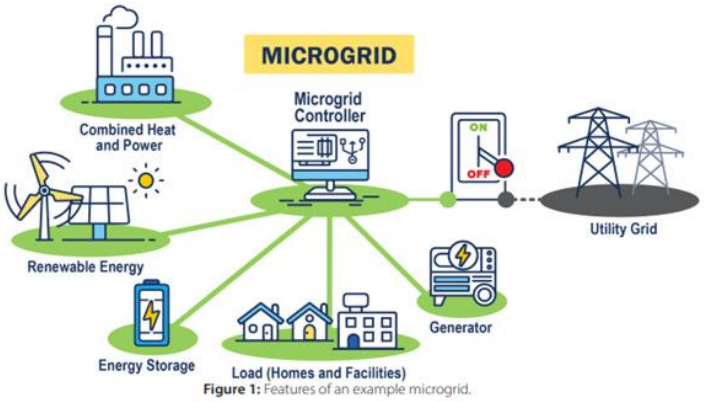


Figure 1: Features of an example microgrid.

This is where the 5-P Integration Model becomes essential. By structuring energy resilience around Policy, Protection, Preparedness, Partnership, and Positioning, the model ensures a comprehensive and coordinated approach:

- Policy establishes governance, standards, and accountability, ensuring energy resilience is embedded at the strategic level.
- Protection focuses on safeguarding critical infrastructure against physical and cyber threats.

- Preparedness ensures organizations have the plans, training, and resources to respond effectively to disruptions.
- Partnership emphasizes collaboration with government agencies, utilities, and private-sector stakeholders to strengthen collective resilience.
- Positioning enables organizations to anticipate future risks and align investments to maintain a competitive and security advantage.

Together, these pillars transform energy resilience from a technical function into a strategic capability, one that supports continuity, reduces vulnerability, and enhances decision-making at the executive level. The 5-P Integration Model therefore provides a practical roadmap for organizations to move beyond reactive measures and adopt a proactive, intelligence-led approach to risk management.

> ***Together, these pillars transform energy resilience from a technical function into a strategic capability, one that supports continuity, reduces vulnerability, and enhances decision-making***

Strategic Imperative for Corporate Security

Energy resilience is no longer merely a technical or sustainability consideration; it is a strategic security imperative. By understanding and mitigating converging risks, corporate leaders can protect critical services, reduce systemic exposure, and strengthen regional security. ASIS Jamaica remains committed to equipping security professionals with the knowledge and tools needed to navigate this complex landscape, ensuring that organizations and communities remain resilient in the face of evolving threats.

MITIGATING ATTRITION AS AN OPERATIONAL RISK:

Engineering Stability in Guarding Enterprises

Conroy Samuda CPP, PCI, FIoL, CPOI
ASIS Member

Workforce attrition is one of the most underestimated operational risks in the private security industry. Guarding firms carefully track overtime, incident rates, and contract margins, yet often overlook the quiet loss of institutional knowledge when employees depart. In a service model built on consistency and trust, frontline instability is not a staffing inconvenience—it is a structural vulnerability within the organization's risk framework.

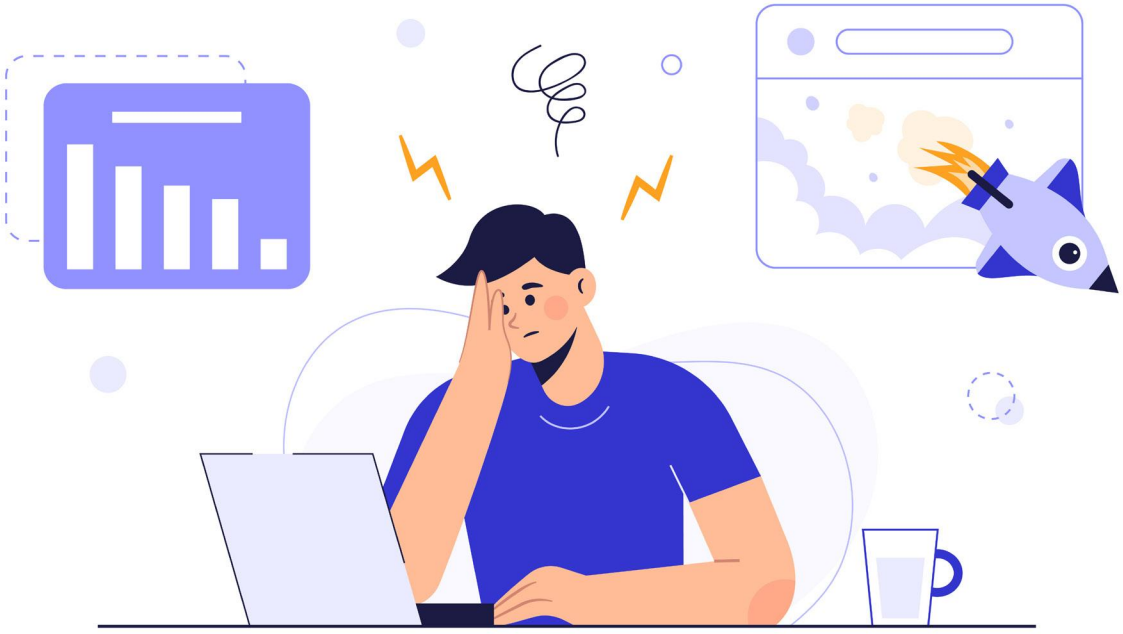
When experienced officers leave, they take more than salaries and equipment. They carry site-specific intelligence, knowledge of client dynamics, emergency response familiarity, and procedural memory that cannot be replicated in a short onboarding cycle. Replacements create productivity lags, supervisory strain, and heightened exposure during transition periods.

A review of post-incident analyses across several guarding environments shows error rates and procedural deviations are highest within the first 60 days of new officer deployment. The pattern is predictable: experience is not easily replaced, and transition windows generate measurable operational risk.

In a mid-sized firm with 150 officers, a 25% annual attrition rate can conservatively produce six-figure operational leakage when recruitment, vetting, uniforms, overtime backfill, and training costs are combined. More critically, visible turnover at premium or regulated sites erodes client confidence and increases service-level agreement exposure.

Under risk management principles aligned with ISO 31000, workforce volatility should be assessed for likelihood, impact, and control effectiveness. Similarly,

> ***When experienced officers leave, they take more than salaries and equipment. They carry site-specific intelligence, knowledge of client dynamics, emergency response familiarity, and procedural memory.***



ISO 9001 quality management standards emphasize reducing process variability—including variability in frontline performance. Addressing security "brain drain" therefore requires governance architecture, not simply accelerated recruitment.

Strategic actions include formally classifying officer turnover as an operational risk with defined tolerance thresholds and escalation triggers; implementing a talent continuity charter with documented succession plans for supervisors and operations leaders; producing annual cost-of-attrition reports to quantify financial impact; institutionalizing knowledge capture through structured site intelligence briefs, cross-training, digital post-order updates, and after-action reviews; aligning career pathways with competency benchmarks and professional certifications; and deploying workforce stability dashboards to monitor promotion ratios, vacancy days, tenure by site, and incident frequency within the first 90 days of deployment.

Frontline exodus rarely ends at scheduling gaps. Its effects extend to performance, efficiency, client confidence, operational resilience, and business continuity. Attrition is not merely a human resources issue—it carries measurable implications for service reliability and contractual stability. A structured, systems-based approach to reducing both its frequency and impact decreases reliance on constant recruitment and strengthens the bottom line. In an industry built on trust, stability signals professionalism and delivers competitive advantage.

The Importance of the Supervisor Role in Modern Security Operations

Tania Rhoden, CPP, PSP
Placement Chairperson

Security officers are the most visible part of security guard services.

Security officers are the most visible part of security guard services, therefore the effectiveness of security operations depend largely on the quality of its supervision. Supervisors ensure that people, processes, and standards align with organisational and client expectations. As security environments become more complex and risk-sensitive, the need for capable, well-trained supervisors continues to grow.

Supervisors are the operational bridge between management and frontline teams. They translate policies into daily practice and maintain consistency across shifts, sites, and personnel. Their close oversight of routine activity allows them to identify emerging risks, compliance gaps, and performance issues early, preventing minor concerns from escalating. Without strong supervision, even well-designed procedures lose impact.

Professional competence is fundamental to supervisory effectiveness. Training equips supervisors to interpret policy correctly, manage incidents appropriately, and ensure compliance with legal and contractual obligations. In high-pressure situations, this competence supports sound judgment and confident decision-making. Well-trained supervisors also strengthen reporting, escalation, documentation, and communication processes, critical areas for accountability, audit readiness, and client assurance. Their professionalism reduces operational risk and safeguards organisational reputation.

Supervisors set expectations, address underperformance constructively, resolve conflict, and support officer wellbeing. Those who communicate clearly and lead by example foster trust, accountability, and professionalism, this improves morale, engagement, and adherence to standards. Effective supervision

> ***Supervisors are the operational bridge between management and frontline teams. They translate policies into daily practice and maintain consistency across shifts, sites, and personnel.***

contributes significantly to staff retention, officers who feel supported and valued are more likely to remain with the organisation. In an industry where retention is a persistent challenge, strong supervision delivers measurable operational stability.

Beyond managing individuals, supervisors ensure consistent adherence to SOP's, site instructions, and client-specific requirements. By monitoring performance and correcting deviations, they maintain service quality and contractual compliance. Their role in onboarding and ongoing coaching ensures new officers integrate smoothly and understand expectations, which will strengthen overall operational reliability.

For these reasons, companies must invest in structured development programmes for supervisors rather than relying solely on experience or tenure. Promotion without leadership training often results in stress, inconsistency, and avoidable errors. Comprehensive development programmes, covering leadership, communication, incident management, risk awareness, and operational planning prepare supervisors for the full scope of their responsibilities.

The return on investment is tangible. Improved supervision leads to fewer incidents, reduced liability exposure, stronger client satisfaction, higher retention rates, and more consistent service delivery. It also builds an internal leadership pipeline, reducing future recruitment costs and strengthening organisational resilience.

Ultimately, investing in supervisor development is not an expense but a strategic decision that enhances performance, mitigates risk, and secures long-term commercial success.

ASIS International:

GRC and Physical Security: Strengthening Strategic Resilience Through Integrated Risk Management | By Eric Davoine, CPP, and Abhijeet Sinha | 30 March 2026

The fusion of physical and digital security has transformed enterprise risk environments. While the traditional guards, gates, and guns framework laid the groundwork, this model no longer suffices amid today's overlapping cyber-physical threats, regulatory demands, and operational continuity challenges.

Governance, risk, and compliance (GRC) frameworks—originally designed for IT and finance—now offer physical security professionals strategic tools to demonstrate measurable business value. This elevates security's role from reactive responder to proactive risk management partner. Today's complex and interconnected threats require a holistic approach that aligns security's efforts with organizational objectives.

Click Here to Read More

Advance Your Security Career

Enhance your expertise in key areas of security through ASIS certificate courses. These focused learning programs are designed to build and reinforce professional competencies, whether you're new to the field or a seasoned practitioner. Successful completion earns you Continuing Professional Education (CPE) credits.

Click Here to Read More

GAIN EVERY ADVANTAGE

More possibilities.
More responsibilities.
More trust.

An ASIS International certification offers limitless opportunities to advance in your career. Whether you're new to the field or a security management veteran, you can find a credential that aligns with your objectives and raises your profile among our global community of security professionals. Our four certifications are widely recognized symbols of excellence that establish your mastery. This expertise gives you an unmatched advantage in your threat-prevention strategies—and in the marketplace.

JOIN TODAY

ASIS INTERNATIONAL® JAMAICA CHAPTER

Congratulations

Julian Nelson, PSP

The Executive and Members of ASIS International Jamaica Chapter proudly congratulates

Julian Nelson, PSP

For his recent Exam Success.

Julian was successful in the PSP exam on March 2, 2026.

Steps to Certification

When you earn an ASIS board certification, you have a visible acknowledgment of a mastery of core security principles.

Click Here to Read More

ASIS INTERNATIONAL® JAMAICA CHAPTER | Jamaica Chapter

For Information on ASIS International Jamaica Chapter, Contact:

Chairman: suzanne.scarlett@yahoo.com
Treasurer: dapsbusiness@gmail.com
Latin America and Caribbean Regional Board Director: bewryba@gmail.com
Newsletter Editor: carlospipher@gmail.com