



ASIS IN FOCUS

EMPOWERMENT THROUGH CERTIFICATION

CPP, PCI or PSP: Which ASIS Certification Fits Your Security Career?

Does certification really make a difference in a security career? For many practitioners, it can. Experience builds competence, but a recognised credential can validate that experience, deepen knowledge and signal readiness for greater responsibility.

- Page 7



Executive Protection as a Risk Management Discipline

There is a moment that still defines how most people picture executive protection: a principal steps from a vehicle, a protector at their shoulder, moving as one toward the door.

- Page 10

LEVEL UP YOUR SECURITY CAREER

APPLY FOR PSP

Physical Security Professional (PSP®)

The Physical Security Professional (PSP®) certification shows your mastery of physical security assessments, designs, applications.



**MODERNIZING
SECURITY WITH
ROBOTICS PROCESS
AUTOMATION
READ MORE**



Contents

Editor's Note	3
ASIS International Jamaica Chapter Makes Courtesy Calls	4
CPP, PCI or PSP: Which ASIS Certification fits Your Security Career?	7
Executive Protection as a Risk Management Discipline	10
The Invisible Load-Bearing Wall: Physical System Availability as the Foundation of Organizational Resilience	12
Artificial Intelligence and the Future of Physical Security: Preparing Jamaica for the Next Generation of Risks	15
ASIS International Jamaica Chapter Makes its Mark at GSX 2026	17
Experience is not Enough in Modern Security	20
Technology, AI, and the Future of Guarding in the Caribbean	22
When the Security Provider Becomes the Risk	24
Are our Facilities Physically Hardened?	27
Are we Designing Crime Into our Communities?	28
Data Analytics in Security: Using Data to Guide Security Strategy and Operations	30
Men's Mental Health Webinar: Analytics for BEYOND "I'M FINE"	32
Knowledge Shared, Security Strengthened: Learning Across ASIS International Jamaica Chapter	33



The Informer is published by the Jamaica Chapter of ASIS International. All views, opinions and conclusions expressed in this newsletter are those of the authors, and do not necessarily reflect the opinion and/or policy of ASIS International or its leadership. References in this newsletter to any specific commercial products, process or services by trade name, trademark, manufacturer or otherwise, do not necessarily constitute or imply endorsement, recommendation or favouring by ASIS International or its leadership.



Editor's Note

Growing Together as Security Professionals

As I worked through the articles and stories in this issue of The Informer, one thought kept returning to me: **security is changing, and we have to be willing to change with it.**

Our theme, “**Empowerment Through Certification,**” is not simply about adding letters after our names. Certification represents a commitment to learning, professional standards and continuous improvement. Experience remains valuable, but in a profession that is becoming more complex, we must continue to build on that experience.

Throughout this issue, we look at some of the forces shaping our profession, from artificial intelligence, data analytics and advanced surveillance technologies to physical resilience, facility hardening and the changing role of security officers. **What connects these subjects is the need for security professionals to understand not only what is changing, but why it matters.**

I am also reminded that technology and systems are only part of the picture. Our profession is ultimately about people: the people we protect, the teams we lead, the colleagues from whom we learn and the communities we serve. The Chapter's activities, our participation at GSX 2026, Women-In-Security initiatives and member knowledge-sharing all demonstrate the value of learning together.

My hope is that you will not simply read this issue, but find something in it that makes you pause, question an existing practice, learn something new or consider your own professional journey.

Carlos Pipher, CPP, PCI, PSP
Newsletter Editor

“

Throughout this issue, we look at some of the forces shaping our profession, from artificial intelligence, data analytics and advanced surveillance technologies to physical resilience.



Courtesy call by Women-in-Security (WIS) on the CDS, Vice Admiral Antonette Wemyss-Gorman, CD, ADC, JP, MSc, psc (n) (centre) on July 28, 2026.

Women-In-Security Pays Courtesy Call on JDF Chief of Defence Staff

By The Informer Editorial Team

On July 28, 2026, members of the ASIS International Jamaica Chapter Women-In-Security (WIS) paid a courtesy call on Chief of Defence Staff Vice Admiral Antonette Wemyss-Gorman, CD, ADC, JP, MSc, psc (n) at Jamaica Defence Force Headquarters, Up Park Camp. Vice Admiral Wemyss-Gorman, who became the first woman to lead the JDF in January 2022, has more than three decades of military service and was the JDF's first female officer to attain flag rank.

Led by Shanna Shirley, CPP, PSP, the delegation included Angilee Baboram, Carlene Clacken-Reid, Superintendent of Police Michelle Campbell, Mollie Plummer-Henry and Shanique Hudson, PCI. The visit gave WIS members an opportunity to engage directly with the Chief of Defence Staff on leadership and the security profession.

The conversation touched on leadership in traditionally male-dominated spaces, remaining grounded in purpose and protecting the environment for future generations. During the exchange, Shirley asked Vice Admiral

Wemyss-Gorman what advice she would give to women serving in the JDF.

“Don’t be fixated on your gender. It doesn’t do your work for you. Once you have earned that respect, it will push that barrier down eventually.”

Reflecting on the courtesy call, Vice Admiral Wemyss-Gorman also emphasised the value of women creating space to learn from, support and inspire one another. WIS members had also prepared questions on professional certification, continuing education, public- and private-sector support for national security, and stronger knowledge-sharing between ASIS International and the JDF.

The courtesy call concluded with an exchange of publications. The delegation presented Vice Admiral Wemyss-Gorman with a copy of *The Informer*, while members received copies of her memoir, *Life, Duty and Command*.



ASIS International Jamaica Chapter members made a courtesy call on Ambassador Rocky Meade, CD, JP, PhD (fourth from left) at the Office of the Prime Minister on July 31, 2026.

Chapter Members Pay Courtesy Call on OPM Permanent Secretary

By Capt. Basil Bewry, CPP, PCI, PSP

On Friday, July 31, 2026, a delegation consisting of Capt. Basil Bewry, CPP, PCI, PSP; Maj. Andrew Lamb; Wayne Ballen, CPP, PCI, PSP; Carlos Pipher, CPP, PCI, PSP; Angilee Baboram; and Carleen Clacken-Reid from the ASIS International Jamaica Chapter paid a courtesy call on Ambassador Rocky Meade, CD, JP, PhD, Permanent Secretary in the Office of the Prime Minister.

The engagement provided an opportunity to formally introduce the Chapter's leadership, outline the mandate and professional objectives of ASIS International, and highlight the Chapter's contribution to advancing professional security management and standards in Jamaica.

Discussions focused on Jamaica's evolving national security environment and the potential contribution of the private security sector to the country's broader security and resilience objectives. Particular emphasis was placed on professional standards, continuous education and professional development, knowledge exchange, and collaboration among key stakeholders.

The Chapter welcomed Ambassador Meade's guidance on the importance of developing strategic partnerships with the HEART/NSTA Trust and the Jamaica Defence Force's Department of Veterans' Affairs, as well as exploring opportunities for greater collaboration between the private sector and the Jamaica Constabulary Force.

The Chapter was also encouraged to undertake research to determine how many former members of the Jamaica National Service Corps have secured employment in Jamaica's private security industry. The findings could provide valuable insight into the programme's contribution to workforce development and identify opportunities for further collaboration with national stakeholders.

The meeting was highly constructive and established a foundation for continued engagement between the ASIS Jamaica Chapter and the Office of the Prime Minister. The Chapter looks forward to advancing the opportunities identified and strengthening collaboration in support of professionalism and excellence within Jamaica's security industry.



Chapter Family Fun Day!

Chapter family fun day at
Jamaica Officers' Club on July 12, 2026.



Chapter Meeting at Curphey Barracks, Up Park Camp on July 29, 2026.



As part of the courtesy call, the Chapter's 50th Anniversary magazine and Q2 Newsletter, *The Informer*, was presented to Amb Dr. Meade by Carlos Pipher, CPP, PCI, PSP, Newsletter Editor.

CPP, PCI or PSP: Which ASIS Certification Fits Your Security Career?

By The Informer Editorial Team



Does certification really make a difference in a security career? For many practitioners, it can. Experience builds competence, but a recognised credential can validate that experience, deepen knowledge and signal readiness for greater responsibility.

ASIS certification already has a strong presence within the Jamaica Chapter, with members holding credentials across different areas of security practice. The more useful question for practitioners today is not whether these certifications exist, but which one best fits the direction of their career.

ASIS International currently offers four board certifications, including the **Associate Protection Professional (APP®)**. This article focuses on three established credentials: the **Certified Protection Professional (CPP®)**, **Professional Certified Investigator (PCI®)**, and **Physical Security Professional (PSP®)**.

The right choice depends on your responsibilities and the expertise you want to build.

CPP Security Management and Leadership: is aimed at experienced security managers and leaders whose responsibilities span several areas of the security function. Its body of knowledge covers seven broad areas: security principles and practices, business principles and practices, investigations, personnel security, physical security, information security and crisis management. The CPP is especially relevant to those moving into senior management, consultancy or strategic roles, where security decisions must support organisational risk priorities and broader business needs.

PCI Professional Investigations: Focuses on investigations and is suited to practitioners involved in corporate investigations, fraud, misconduct, loss prevention, security intelligence and related



Certification does not have to be pursued in isolation. ASIS International gives members access to educational resources, standards and guidelines, webinars, conferences, subject-area communities, networking opportunities and certification support.

assignments. The certification covers three primary areas: professional responsibility, investigative techniques and procedures, and case presentation.

Investigative work requires sound judgement, proper documentation, objective analysis and the ability to gather and present information clearly. The PCI provides an internationally recognised benchmark for those competencies.

PSP Physical Security Expertise: Is designed for practitioners whose work centres on physical security assessment and the design, application and implementation of security systems. In practice, this may involve electronic access control, CCTV, intrusion-detection, systems, protective design, security surveys, system integration and risk assessment.

Physical security now demands far more technical knowledge than it once did. Practitioners are expected to understand how people, procedures, technology and the built environment work together to protect personnel, facilities, assets and operations.

Which Certification Fits You?

For some practitioners, one credential is only the beginning. Additional certifications may follow as responsibilities broaden, expertise deepens and career goals change.

What Should You Know Before Applying?

Choosing a certification also means looking realistically at eligibility, preparation and the commitment required to maintain it.

Requirements vary according to the certification and, in some cases, educational background. CPP requires

substantial security-management experience, including experience in responsible charge of a security function. PCI requires relevant investigations experience, including case-management responsibility. PSP requires practical experience in physical security.

The examinations require serious preparation. Field experience provides an important foundation, but structured study is still necessary because each certification is assessed against a defined body of knowledge rather than day-to-day experience alone.

Earning the credential also carries an ongoing commitment. CPP, PCI and PSP holders must complete 60 hours of continuing professional education during each three-year certification cycle to maintain their certification.

Candidates should review the current eligibility, examination and recertification requirements published by ASIS International before applying.

The Value of the ASIS Community

Certification does not have to be pursued in isolation. ASIS International gives members access to educational resources, standards and guidelines, webinars, conferences, subject-area communities, networking opportunities and certification support.

That network becomes especially useful when security challenges cross disciplines. A physical security issue may involve technology. An investigation may require input from legal, human resources or compliance teams. A leadership role may demand a broader understanding of resilience, risk and organisational priorities.

Access to practitioners with different experiences can help members see problems differently, test ideas and learn from approaches they may not encounter in their own workplace.

The Jamaica Chapter Connection

For practitioners in Jamaica, the ASIS Jamaica Chapter brings that wider network closer to home.

The Chapter has supported certification study efforts and provides opportunities for members to exchange knowledge, build relationships and learn from others working across physical security, investigations,

corporate security, law enforcement, government, cybersecurity and risk management.

Those relationships often prove useful in practice. An emerging practitioner may find a mentor. A certification candidate can learn from members who have already completed the process. A manager facing an unfamiliar challenge may gain insight from someone who has dealt with a similar issue.

For Jamaican practitioners wondering whether these credentials are achievable, the Jamaica Chapter boasts the largest number of triple certificants in Latin America and the Caribbean.

ASIS International has highlighted Jamaican security professional Selbourne Webb, CPP, PCI, PSP, whose certification journey began with support from a CPP study group organised through the Jamaica Chapter. He later earned all three credentials, completing what ASIS refers to as the Triple Crown. His journey shows that

“

For Jamaican practitioners wondering whether these credentials are achievable, the Jamaica Chapter boasts the largest number of triple certificants in Latin America and the Caribbean.

certification can be supported by more than individual study. Peer encouragement, chapter involvement and persistence can all play a part in getting there.

When choosing your next step, a useful starting point is to look honestly at the work you are doing now, the responsibilities you want to take on next and the knowledge you still want to build.

Then ask yourself: where do I want my security career to go next? The answer may point you towards CPP, PCI or PSP.

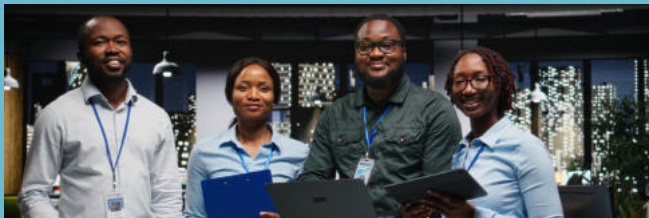


Hosted by



The Value of an ASIS CERTIFICATION

MASTERY OF SECURITY PRINCIPLES | IMPROVED LEADERSHIP SKILLS
INCREASED EMPLOYABILITY | PROFESSIONAL GROWTH



Apply for 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](#)



Executive Protection as a Risk Management Discipline

WHY THE MODERN PROTECTION PROFESSIONAL MUST THINK LIKE A RISK MANAGER, NOT JUST A RESPONDER

By Jerome Lawrence | *Foundation Liaison*

There is a moment that still defines how most people picture executive protection: a principal steps from a vehicle, a protector at their shoulder, moving as one toward the door. It's a compelling image, but an incomplete one. By the time that door opens, the work that matters most is largely finished. The route was chosen days earlier. The venue was assessed, the access points identified, the emergency response confirmed. If protection begins when the principal steps out of the vehicle, it has already started too late.

Ask an experienced protection professional what actually keeps a principal safe, and the honest answer is rarely the person standing closest to them. It's the decisions made days or weeks before: which routes to avoid, which venues need a second look, which risks are worth escalating and which aren't. That is risk management, an approach reflected in ASIS International's Enterprise Security Risk Management framework. Executive protection is simply that thinking applied to a person instead of a building or a

network. This risk-based approach is also reflected in ASIS International's Executive Protection Standard, which emphasizes threat assessment, planning, and the structured management of protective services.

I have seen an advance team quietly shift an arrival time by ninety minutes after learning a scheduled protest would push a motorcade through a predictable bottleneck. No one outside the team ever knew; nothing happened that day. That is the point.

“

Ask an experienced protection professional what actually keeps a principal safe, and the honest answer is rarely the person standing closest to them. It's the decisions made days or weeks before: which routes to avoid, which venues need a second look, which risks are worth escalating and which aren't.

“

A well-run protection program keeps leadership functioning, keeps decisions being made, and keeps a company's name out of tomorrow's headlines.

Risk rarely comes from the principal alone. It comes from the residence, the daily commute, the family, the digital footprint, the whole ecosystem surrounding them. Protect only the individual and you are managing half the problem. And the person standing closest to the principal is only one layer of that protection. Intelligence, route planning, access control, and coordination with local authorities usually do more work than anyone realizes, long before a hand ever reaches for a door.

Information tells you what is happening. Intelligence tells you what it means. Behavioral threat assessment can help identify concerning patterns or warning behaviors before targeted violence occurs, turning raw information into a decision made early enough to matter.

None of this is really about one person's safety. A well-run protection program keeps leadership functioning, keeps decisions being made, and keeps a company's name out of tomorrow's headlines. Boards are beginning to understand this: executive protection is not a security expense. It is a form of continuity protection for the organization itself.

The best protection operations are usually invisible, not because nothing was happening, but because someone was managing the risk long before anyone noticed there was one.



ASIS International Volunteers pose for a picture at GSX 2026 Volunteers' Day.



THE INVISIBLE LOAD-BEARING WALL:

Physical System Availability as the Foundation of Organizational Resilience

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

A warehouse camera once had an uptime of 99.9% over a three-year period. For the security department, this was a remarkable demonstration of system resilience, but one fateful day, a single unexplained power loss changed that. Following the reviews and investigations, the failure was identified as an unauthorised rewiring of the power source. Not a cyber breach, not a sophisticated attack. It was an interruption of power that compromised the invisible load-bearing wall of the critical infrastructure.

As physical security professionals, we understand perfectly the many layers that security provides through robust overlays of deterrence, detection, delay, and response controls. However, often overlooked in the sequence are the dependent and interdependent relationships that must exist to prevent assumptions of actual system(s) availability when the threat occurs. In the case of the blinded cameras, an effective deterrent could be the organisational policies guiding maintenance procedures that are augmented by periodic detection strategies of system log and time stamp reviews.

Part of the challenge with availability is that it is often viewed as an IT metric since it forms such a crucial

part of the CIA Triad (Confidentiality, Integrity and Availability). To correct this misconception, a non-negotiable understanding of the criticality of physical security availability is necessary to ensure that hardware, environmental controls, and infrastructure access remain fully operational and accessible to authorised personnel without interruption. Considered another way, system availability resilience when done correctly prevents protection illusion or false fronts.

System Availability as The Nervous System of the Organization

Think of the organization as a living organism. The access control reader that denies an adversary entry, the PIR sensor that detects movement, and camera that records theft form the nervous system. Similarly, the

“

As physical security professionals, we understand perfectly the many layers that security provides through robust overlays of deterrence, detection, delay, and response controls.

guard force and response protocols form the immune system. When a camera fails or a door controller loses communication, the response system is effectively offline, no matter how well trained or staffed the organisation may be. This is where the lines of system availability and organizational resilience intersect. Resilience is therefore the capacity to absorb a shock and endure the risk (ANSI/ASIS ORM.1-2017) without hemorrhaging stakeholder trust, profit, or productivity. Availability, on the other hand is the precondition for that absorption, and so it must be accepted that a resilient organization cannot adapt to an event it never detected.

“

In many audits the expensive software is rarely the problem, as the chain usually breaks at the physical layer: an unprotected access point, a VMS with no power redundancy, a camera with obscured lens or whose power supply is shared with non-critical loads.

The Availability Continuum

Physical system availability is a chain, and it is only as strong as its weakest link. In many audits the expensive software is rarely the problem, as the chain usually breaks at the physical layer: an unprotected access point, a VMS with no power redundancy, a camera with obscured lens or whose power supply is shared with non-critical loads. Each link, be it the human monitoring, or maintenance plans must be verified. Risk managers to verify that the UPS is tested under load or if video retention is calculated to support redundancy, and if power source is unshared and secured from tampering?

The Business Impact

For security managers, availability failures carry hard costs, because like doctors, when errors are made, lives may be lost. Furthermore, regulators and executives expect continuous protection and monitoring. Here is a challenge for every security professional reading this. Walk down to your security closet and inspect the system, then ask yourself: if the power blips, what happens? If a network switch fails, which doors unlock or lock? If the camera goes dark, who knows and how fast? If you do not know the answer, you do not have resilience nor availability, you have security through obscurity.

TOP QUESTIONS TO ASK YOUR SECURITY CAMERA INSTALLER

- What type of cameras do you recommend?
- How many cameras do I need? **2**
- What are the installation costs?
- How do I access footage remotely?
- Is there a warranty?
- What is the coverage area?

BENEFITS OF COMMERCIAL SECURITY CAMERA SYSTEMS

- 80% CRIME REDUCTION**
- REMOTE MONITORING**
Monitors proactively
- EMPLOYEE SAFETY**
Detects compliance
- COST SAVINGS**
Drives planes
- BUSINESS INSIGHTS**
Analyzes flow analysis

2025

Security Camera King, Inc.
www.securitycameraking.com



“

For security managers, availability failures carry hard costs, because like doctors, when errors are made, lives may be lost. Furthermore, regulators and executives expect continuous protection and monitoring.

HOW MANY CERTIFIED SECURITY PROFESSIONALS ARE ON YOUR TEAM?



Certified professionals bring internationally recognized expertise to your security team.



BUILD CAPABILITY

Professional certification strengthens your organization's ability to manage risk, protect assets and respond to evolving security threats.



INVEST IN YOUR PEOPLE

Support your security professionals in earning internationally recognized ASIS certifications.



STRENGTHEN YOUR TEAM

Partner with ASIS Jamaica Chapter to develop stronger, more capable security professionals across Jamaica.



CPP[®]

PCI[®]

PSP[®]

Globally recognized professional certifications for security practitioners.

BUILD A STRONGER SECURITY WORKFORCE.

Partner with ASIS Jamaica Chapter.



LEARN MORE:

asisjachapter.org



CONTACT:

asisjachapter@gmail.com



ARTIFICIAL INTELLIGENCE AND THE FUTURE OF PHYSICAL SECURITY: **Preparing Jamaica for the Next Generation of Risks**

Oswald J. Smiley, PhD, CPP, PSP, PMP, FMP
ASIS Professional Development Steering Committee

The security profession is undergoing one of the most significant transformations in its history. Artificial Intelligence (AI) is reshaping how organizations protect people, assets, information and critical infrastructure. For security professionals across Jamaica and the Caribbean, the question is no longer whether AI will affect security, but how effectively we adapt to its opportunities and risks.

Criminal organizations are already using AI to support phishing, deepfakes, synthetic identities and targeted social engineering. At the same time, security teams are adopting intelligent video analytics, automated access control, AI-supported threat detection and advanced Security Operations Centers capable of identifying unusual activity in real time.

For Jamaica, these developments bring both opportunity and responsibility. Airports, seaports, hospitals, financial institutions, utilities and telecommunications networks increasingly depend on interconnected physical and digital systems. Protecting these assets requires security strategies that integrate physical security, cybersecurity and operational resilience.

AI should enhance professional judgment, not replace it. Technology cannot substitute for ethical leadership, sound policies, trained personnel or effective governance. Security professionals must still investigate incidents thoroughly, assess context and ensure that AI-enabled systems are used responsibly and transparently.

AI Applications Transforming Physical Security



AI-Enabled Drone Surveillance for Critical Infrastructure Inspection and Security.

AI is already supporting physical security in several practical areas. Intelligent video analytics can detect

“

Organizations face a multifaceted risk landscape that includes internal misconduct, fraud, workplace violence, operational disruptions, and data breaches. In this context, security must be understood not merely as a protective service, but as an integrated component.

suspicious behavior, abandoned objects, perimeter breaches and crowd anomalies. Facial recognition and access-control technologies can strengthen identity verification when supported by appropriate privacy safeguards, testing and human oversight. Predictive risk analysis can identify patterns and indicators that may signal emerging or elevated risk. Drones and robotic platforms can extend surveillance in large or hazardous environments, while AI-enabled threat intelligence can combine information from multiple systems to improve situational awareness.

The growing convergence of physical and cyber security makes this especially important. A cyberattack can disable cameras, access-control systems or other

“

As security professionals, our greatest asset has never been technology; it has always been our ability to anticipate risk, adapt to change and lead with integrity. AI will transform the profession, but its value will ultimately depend on knowledgeable professionals

essential systems, creating direct physical consequences. Security leaders therefore need an Enterprise Security Risk Management (ESRM) approach that treats security as an integrated business function supporting resilience.

Preparing Jamaica for Responsible AI Adoption

Preparing Jamaica for responsible AI adoption will require more than purchasing new technology. Organizations should strengthen AI governance, workforce training, cybersecurity controls, data management, human oversight and system testing.

Procurement decisions should also consider reliability, privacy, resilience and the ability to maintain operations when automated systems fail.

The ASIS International Jamaica Chapter has an important role to play through professional development, certification, knowledge sharing and regional collaboration. These efforts can help practitioners understand emerging technologies while maintaining professional and ethical standards.

As security professionals, our greatest asset has never been technology; it has always been our ability to anticipate risk, adapt to change and lead with integrity. AI will transform the profession, but its value will ultimately depend on knowledgeable professionals who know when to trust technology, when to question it and when human judgment must prevail.

On-demand Webinar

1 in 3 security professionals were unsure how to leverage AI. Is that still true?

One Year On: How AI Adoption Reshaped Security Operations

See how security teams are using AI today to move faster on investigations, reduce operational friction, and keep pace with rising expectations — without adding complexity.

WATCH NOW

ASIS International Jamaica Chapter Makes its Mark at GSX 2026

By The Informer Editorial Team



Members of the ASIS International Jamaica Chapter delegation at the Global Security Exchange (GSX) 2026 in Atlanta, Georgia.

From member recognition and chapter leadership, to international recognition and the ASIS Foundation Fitness Challenge, the Jamaica Chapter's presence in Atlanta reflected a strong contribution to the wider ASIS Community.

The Jamaica Chapter of ASIS International was represented in Atlanta, Georgia, at the Global Security Exchange (GSX) 2026, with Chapter Chair Suzanne Scarlett, PSP, and members of the Jamaica delegation taking part in one of the security profession's major international gatherings.

GSX brings together security professionals, chapter leaders, solution providers and industry representatives from around the world. For the Jamaica Chapter, the conference provided an opportunity to exchange ideas, strengthen professional relationships and identify approaches that can support the security profession at home.

CLICK TO READ MORE ON GSX 2026

Sharing a Jamaican Idea on the Global Stage



The Jamaica Chapter's Member Recognition Strategy was featured during a GSX Chapter leadership session.

A notable moment came during a chapter-focused session, where Chapter Chair Suzanne Scarlett, PSP, shared the Jamaica Chapter's Member Recognition

Strategy as a practical idea that other chapters could consider. The initiative acknowledges members who make meaningful contributions throughout the year.

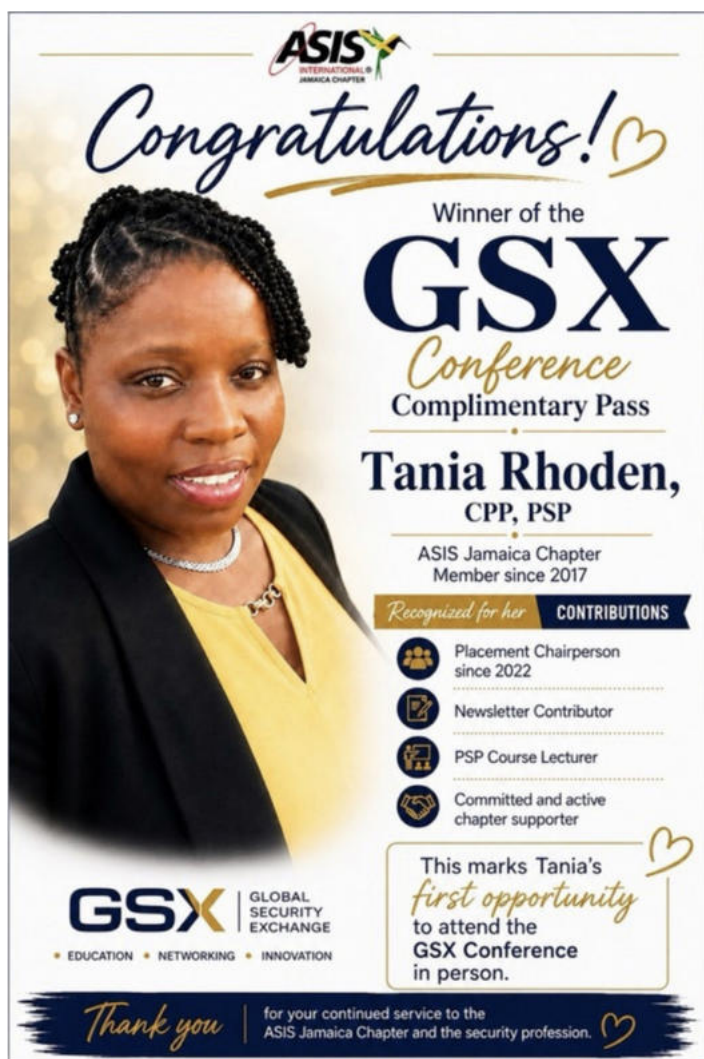
The strategy includes Member of the Quarter and Member of the Year recognition, helping to celebrate volunteer service, increase member visibility and encourage continued participation.

Recognition is not only about awards; it is about showing members that their contribution matters.



ASIS International Jamaica Chapter Chair Suzanne Scarlett, PSP speaking during a GSX session.

Recognition in Practice: Tania Rhoden, CPP, PSP



One example of this approach was the selection of Tania Rhoden, CPP, PSP, to receive the Chapter's GSX Complimentary All-Access Pass in appreciation of her service and commitment.

Rhoden has served as Placement Chairperson since 2022, supporting members in identifying employment opportunities. She has also contributed to charitable activities, submitted articles for *The Informer*, spearheaded membership surveys and lectured on the Chapter's virtual PSP courses.

A member of ASIS International since 2017, Rhoden had never previously attended GSX in person. Providing her with the opportunity to attend GSX 2026 gave practical meaning to the Chapter's recognition programme by rewarding service in a way that also supports professional growth.

International Recognition for the Jamaica Chapter

The Jamaica Chapter also arrived at GSX following another important achievement. *ASIS International recognized the Chapter with an Honorable Mention for the 2025 I.B. Hale Chapter of the Year Award.* The acknowledgement reflected continued work in areas such as member engagement, professional development, leadership and chapter operations.



The recognition added further significance to Jamaica's presence at GSX 2026.

ASIS INTERNATIONAL JAMAICA CHAPTER AT GSX 2026

**Leadership • Recognition • Engagement
• Professional Development**

From member recognition, chapter leadership, to international recognition and the ASIS Foundation Fitness Challenge. The Jamaica Chapter's presence in Atlanta reflected a strong contribution to the wider ASIS International Community.

Fitness, Teamwork and Giving Back

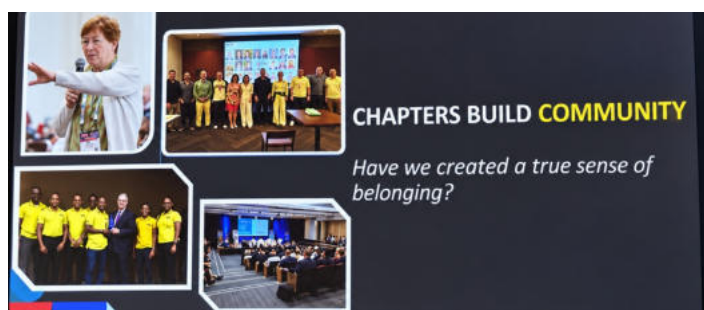
The Chapter was also recognized during GSX for its performance in the ASIS Foundation Fitness Challenge. The Jamaica Chapter received team awards for Most Money Raised and Most Participants, while also placing third overall in the challenge.



GSX recognition of the Jamaica Chapter's Fitness Challenge performance and the Chapter's achievement graphic.

Members collectively recorded 11,573 kilometres, 386,310 footprint points and 5,010 engagement points, while raising US\$875. The results reflected strong participation and the willingness of members to support an initiative that combined wellness, teamwork and giving back to the ASIS Foundation.

Building Community Beyond Awards



At a GSX Chapter leadership discussion, a simple but important question was asked: have we created a true sense of belonging?

The wider GSX experience also raised an important question for professional associations: whether members feel a true sense of belonging. For chapters, recognition, participation and opportunities to contribute can make a meaningful difference in keeping members connected.

The conference also provided exposure to discussions on increasing member value, advancing the security profession, strengthening global operations, building partnerships and supporting digital transformation. These themes are particularly relevant as security professionals continue to respond to changing risks, new technologies and the growing importance of collaboration.



Chapter leaders and presenters exchange ideas during a GSX 2026 session.

Together, these experiences showed that the Jamaica Chapter was not simply attending GSX, but contributing to the wider conversation on chapter development, member engagement and professional growth.

Bringing the Experience Home



The ideas and relationships developed in Atlanta can now help shape future programmes, training opportunities and partnerships in Jamaica.

GSX 2026 gave the Chapter an opportunity to share its work, recognize the people behind its progress and return home with fresh ideas for the year ahead.

The Jamaica Chapter was present, visible and contributing.



Experience is not Enough in Modern Security

Tania Rhoden, CPP, PSP
Placement Chairperson

For decades, Jamaica's private security industry has relied heavily on recruiting former members of the Jamaica Constabulary Force and the Jamaica Defence Force. Their training, discipline and operational experience make them valuable contributors to the security profession. However, the security landscape has evolved, and so too must the standards by which security professionals are recruited and promoted.

A gap remains in how professional qualifications are sometimes recognized across the industry. Recruitment within Jamaica's private security sector has traditionally placed considerable weight on law-enforcement and military experience, while professional security certifications are not always given the same visibility in recruitment and promotion. This can narrow how modern security competence is assessed.

Security today is no longer limited to guarding gates and responding to incidents. Organizations face increasingly sophisticated threats, including cyber-enabled crime, insider threats, workplace violence, terrorism and complex risk-management challenges. Addressing these issues requires professionals with specialized knowledge, strategic thinking and a commitment to internationally accepted best practices.

Professional certifications can add significant value to this development. Credentials such as the Certified Protection Professional (CPP), Physical Security Professional (PSP) and Professional Certified Investigator (PCI) validate knowledge and competence across key areas of security management, physical security and investigations. They also reflect a commitment to professional ethics and continuous learning.

Jamaican security companies should recognize these credentials as valuable professional qualifications when recruiting, promoting and developing their workforce. Encouraging employees to earn and maintain relevant

“

Recruitment within Jamaica's private security sector has traditionally placed considerable weight on law-enforcement and military experience, while professional security certifications are not always given the same visibility in recruitment and promotion.

certifications can strengthen professional capability, support client confidence and contribute to the wider development of Jamaica's private security industry.

Professional certification can support a more knowledgeable workforce, give clients additional assurance of competence and encourage practitioners to maintain continuous professional development. The broader goal is not to replace experience, but to complement it with knowledge and competence that have been independently assessed against recognized standards.

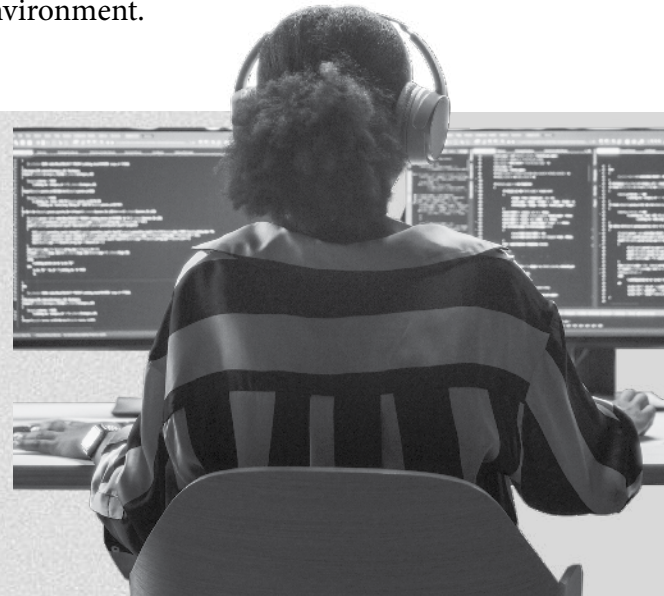
If Jamaica's private security industry is to compete regionally and internationally, professional certification

“

Professional certification can support a more knowledgeable workforce, give clients additional assurance of competence and encourage practitioners to maintain continuous professional development.

should form part of how competence is recognized and developed. Security providers that combine practical experience with verified professional knowledge will be better positioned to meet the demands of a changing security environment.

COMPLETE YOUR SECURITY STRATEGY.



When threats strike from every angle, resilience demands more than vigilance, you need a 360° security strategy. At Global Security Exchange (GSX), powered by ASIS International, you'll discover how to anticipate, assess, and mitigate risks with no gaps, blind spots, or vulnerabilities, just a seamless framework to keep your organization agile and strong.

[REGISTER](#)


Advancing Professional

Whether you're managing a team or preparing for a leadership role, membership provides the tools to sharpen your skills and grow your professional presence.

- **Career HQ** – get access to exclusive career planning resources, including free live and on-demand content
- **Standards & Guidelines** – read our industry-leading guidance on all things security and risk; members get eBook versions for free and discounts on print editions
- **PCI® and PSP® Certifications** – confirm your expertise in investigations and physical security; members receive discounted application fees and prep resources
- **Local Chapters** – connect with security peers in your area for networking, events, and shared learning

AI

POWERING
INFORMATION
INTELLIGENCE

AI CAPABILITIES

-  DATA ANALYTICS
-  PATTERN RECOGNITION
-  PREDICTIVE MODELING
-  NATURAL LANGUAGE PROCESSING
-  REAL-TIME MONITORING
-  DECISION SUPPORT SYSTEMS

CARIBBEAN OVERVIEW

AI technologies enable smarter decisions, real-time insights, and sustainable solutions across the Caribbean.



Technology, AI, and the Future of Guarding in the Caribbean

Warren Smith, CPP, PCI, PSP, CRISC, CISSP
ASIS Member

Across the Caribbean, the guarding sector is entering a period of meaningful change. Advances in technology and artificial intelligence are reshaping how security is delivered and challenging models built primarily around uniformed personnel. Guarding firms now face a practical question: how quickly can they adapt without losing the human judgement on which effective security still depends?

Security services in the region have traditionally been labour-intensive, but technology is increasingly supplementing some of these activities through intelligent video surveillance, remote monitoring centres, biometric access control and AI-enabled analytics that can flag anomalies in real time.

Guarding companies are also diversifying into services such as armed response, cash-in-transit and close protection. While these can create new revenue streams, they often rely on similar cost structures built around personnel, vehicles and compliance. Technology offers another path. Remote operations can oversee multiple sites simultaneously, supported by sensors and analytics

that improve detection and response. This shifts the model away from headcount alone and toward capability and outcomes. As these options become more visible, some clients are beginning to question guard-heavy deployments.

People remain central, but expectations are evolving. The traditional guard role increasingly requires comfort with systems, data and more dynamic decision-making. This applies across guarding and specialised services, where real-time intelligence and communication tools are becoming standard. Upskilling is essential, although cost, access to training and competing operational demands can slow the transition.

“

Technology is increasingly supplementing some of these activities through intelligent video surveillance, remote monitoring centres, biometric access control and AI-enabled analytics that can flag anomalies in real time.

Process discipline is equally important. Effective security operations depend on clear workflows, defined escalation paths and coordination across monitoring and response. This is especially important in areas such as cash-in-transit and armed response, where timing and precision matter. Fragmented or heavily manual processes can limit the value of new capabilities.

Technology creates both opportunity and separation within the market. AI-enabled surveillance, centralised monitoring and tracking tools can reduce reliance on some static posts, improve response times and support more consistent outcomes. These gains, however, depend on sound governance, system integration and appropriate human oversight. They also require investment, which can widen the gap between firms that are able to modernise and those that cannot.

The direction is clear: uniformed guards are not disappearing, but their role is evolving within a more connected security model where physical presence is complemented by digital oversight. In Caribbean

“

AI-enabled surveillance, centralised monitoring and tracking tools can reduce reliance on some static posts, improve response times and support more consistent outcomes. These gains, however, depend on sound governance, system integration and appropriate human oversight.

markets, the pace of that transition will vary with labour costs, infrastructure and firms' ability to invest in technology and training.

For clients, this creates an opportunity to rethink how security is designed. For guarding companies, diversification alone will not be enough. The firms that align their people, processes and technology, while continuing to develop the skills of their personnel, will be better positioned to deliver value in the years ahead.

E-FAST

Emergency First-aid & Safety Training

Blade Design: 1876-465-4785



**Preserving Lives,
Empowering People.**

Services offered include:
Standard First Aid Training
Paediatric First Aid Training
CPR and AED Training

First aid kits available for individual
and corporate clients



Contact Information
emergencyfastja.com
876-281-4772 / 876-830-0792
info@emergencyfastja.com
@efastja EFAST Jamaica

RISK



When the Security Provider Becomes the Risk

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. The difference between resilience and vulnerability often lies not only in the hardware, but in the quality of the partnership behind it.

Organizations sometimes tolerate late responses, vague explanations or transactional attitudes from providers. In a market where supply chains can be fragile and the tropical climate is hard on equipment, weak service can quickly become a security risk. High service-level expectations should therefore be established from the start.

THE "HONEYMOON" TRAP AND EARLY RED FLAGS

Procurement's riskiest stage can be the early implementation period, when attention is focused on technical specifications and implementation while early signs of a weak partnership are missed. Red flags may include a provider who only calls when an invoice is due, repeatedly blames logistics for delays, patches faults without explaining the cause, or cannot outline a credible support roadmap. When the relationship remains purely transactional, the organization may have purchased a system without securing a long-term partner.

THE TRAP OF ENTERPRISE LOCK-IN

Some enterprise security platforms use proprietary protocols or closed ecosystems that can limit an organization's choice of integrators, software or replacement components. If the relationship deteriorates, the organization may be forced to tolerate poor service or replace equipment that still has useful life. Adding secondary systems to compensate can also create a fragmented "Frankenstein" architecture, increasing complexity, response times and training requirements.

THE ROI GAP

Ending a supplier relationship early can be costly. In Jamaica, foreign exchange and importation costs can

“

In a market where supply chains can be fragile and the tropical climate is hard on equipment, weak service can quickly become a security risk. High service-level expectations should therefore be established from the start.

magnify the impact, particularly when NVRs, controllers and specialized sensors remain serviceable. Switching costs may include removal and reinstallation, loss of site-specific knowledge, and operational downtime during transition.

RECOMMENDATIONS FOR “MARRIAGE-READY” PROCUREMENT

Security procurement should move beyond product selection and place greater emphasis on long-term partnership, support and lifecycle value.

- **Prioritize Open Architecture:** Where operationally appropriate, avoid unnecessary dependence on a single dealer or integrator and preserve flexibility for future support.
- **Conduct a “Pre-Nup” Audit:** Speak to long-term clients and ask about response times, parts availability and support after the initial installation period.

- **Test Scalability:** Ask how the platform can adapt as operational needs change. A strong partner should be able to demonstrate realistic integration and upgrade paths.
- **Define Exit Strategies:** Include knowledge-transfer requirements in SLAs and ensure the organization retains authorized access to administrative credentials, programming information, system maps and configuration documentation.

CONCLUSION

For managers and entrepreneurs, the lesson is simple: demand high service levels, strategic alignment and a partner capable of growing with the organization. Facility security is not only about locks and cameras; it is about business continuity. The right technology matters, but the partnership supporting it can determine whether the investment remains resilient, scalable and sustainable over time.

Stay ahead of emerging threats with the latest security research.

[Click Here to Read More](#)

FORENSIC
POLYGRAPH SERVICES
Detecting Deception Since 1999

CONTACT

876-383-2754

876-792-0875

🌐 forensicpolygraphja.com

✉ forenpoly@gmail.com

📷 [forensicpolygraphja](https://www.instagram.com/forensicpolygraphja)

**LET US
UNCOVER
THE TRUTH**
FORENSIC POLYGRAPH SERVICES

- ➔ Investigative Polygraph Tests
- ➔ Pre-Employment Polygraph Tests
- ➔ Infidelity Polygraph Tests
- ➔ Behavioural Analysis Interviews
- ➔ Background Investigations



Strengthen your skills. Supercharge your resume.

Advance your security expertise with ASIS certificate courses—focused programs that strengthen your professional skills and knowledge. Designed for both newcomers and experienced practitioners. No prior experience is required, and successful completion earns valuable CPE credits to support your career growth.

GET STARTED

ASIS INTERNATIONAL — JAMAICA



Earn the credential that opens doors.

ASIS BOARD CERTIFICATIONS · CPP · PCI · PSP · APP

20%

higher salary than
non-certified peers



54%

received promotion or
salary increase



55%

of employers prefer
ASIS-certified hires



Source: ASIS International 2019 Certification Survey

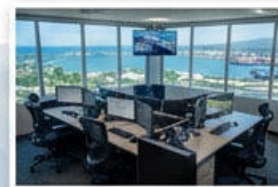
WHICH CERTIFICATION IS RIGHT FOR YOU?

- CPP** Certified Protection Professional · Senior security managers (5–7 yrs exp)
- PCI** Professional Certified Investigator · Investigations specialists (3–5 yrs exp)
- PSP** Physical Security Professional · Physical security experts (3–5 yrs exp)
- APP** Associate Protection Professional · The ideal first step (1+ yr exp)



WHY IT MATTERS IN JAMAICA

Security is one of the most critical industries in our region. Certification tells employers, clients, and the community that you have met the global standard — and that Jamaica's security professionals stand among the best in the world.



Start your certification journey today.

asisonline.org/certification · ASIS Jamaica Chapter

Advancing Security Worldwide®



Are our Facilities Physically Hardened?

Carlos Pipher, CPP, PCI, PSP
Newsletter Editor

In today's security-conscious environment, organizations, corporations and facilities must ask a critical question: Is our facility physically hardened? In the past, physical hardening meant fences, padlocks and watchmen. It now means perimeter intrusion detection systems, electronic access control, power and network resilience, and climate resilience, factoring hurricane-rated buildings and heat-resistant data centres. Physical hardening refers to the deliberate measures taken to protect people, buildings and assets from unauthorized access, environmental hazards, and potential threats. It is the foundation of a comprehensive risk assessment, ensuring resilience against both natural and human-made risks.

Why It Matters

Hardened facilities reduce vulnerabilities, deter adversaries, and strengthen stakeholder confidence. Whether the facility is a corporate office, government agency, or industrial plant, physical resilience protects not only property but also reputation and service continuity. As threats evolve, security managers must regularly assess and reinforce their defenses. Asking "Is our facility physically hardened?" is more than a rhetorical question; it is a call to action. By investing

Physical hardening refers to the deliberate measures taken to protect tangible and intangible assets from unauthorized access.

in layered security, environmental safeguards, and integrated systems, organizations can keep their facilities resilient when unexpected events occur.

A single breach can trigger widespread disruption. If a port's control room is hit by a cyberattack, exports and imports can be disrupted. Physical hardening means preparing for overlapping threats, including the possibility that a hurricane and a cyberattack could strike in the same week. The facilities most likely to withstand these events will be those designed for multiple simultaneous risks, not just isolated incidents. As we move deeper into the Atlantic hurricane season, any facility that has not yet been assessed should now review its structural security measures.

Having a competent, certified security team on board and buy-in from the executive leadership is the precursor to facility hardening. Security professionals certified by ASIS International are trained in security management and physical security principles. Get them on your team to harden your facility.



Are we Designing Crime Into our Communities?

Renee Watkis
Assistant Newsletter Editor

Most conversations about crime begin after an incident occurs. We ask who committed the offence, how it happened and what punishment should follow. Far less attention is given to a more preventive question: are we designing and maintaining communities in ways that make crime easier to commit?

In my work assessing physical security across sites in Jamaica, I have come to see environmental design as one of the most overlooked tools for reducing opportunities for crime, not after an incident, but before it happens.

Crime Prevention Through Environmental Design, or CPTED, rests on a simple principle: the physical environment can influence human behaviour. The term was introduced by criminologist C. Ray Jeffery in 1971, while architect Oscar Newman's closely related concept of defensible space helped shape its practical application to buildings and communities. Well-designed and properly maintained spaces can discourage offending, support legitimate activity and reduce fear. Neglected environments may provide concealment, weaken community oversight and create easier access for those intending to offend.

Across Jamaica, the warning signs are familiar. A poorly lit roadway forces pedestrians through darkness. An overgrown lot blocks sightlines and creates places of concealment. An abandoned building may provide opportunities for unauthorized occupation and vandalism. A bus stop without adequate lighting, clear visibility or properly defined access points can leave commuters feeling exposed, particularly women, children, older adults and persons with disabilities. These conditions do not cause crime, but they may widen the opportunities available to those willing to offend.

“

An abandoned building may provide opportunities for unauthorized occupation and vandalism. A bus stop without adequate lighting, clear visibility or properly defined access points can leave commuters feeling exposed, particularly women, children, older adults and persons with disabilities.

Community parks often tell the story in reverse, not through one sudden hazard, but through gradual decline. Once lighting fails and damaged equipment remains unrepaired, families may stop using the space. As legitimate activity declines, the “eyes on the street” that once discouraged wrongdoing may also disappear. The park does not become vulnerable overnight; it becomes vulnerable through neglect and attrition.

Housing developments can help reverse this pattern. Clearly marked entrances, visible walkways, maintained landscaping and active communal spaces support natural surveillance and strengthen residents’ sense of ownership. Broken lights, hidden corridors and neglected common areas do the opposite, eroding confidence and making suspicious activity harder to detect.

When I assess a site, the questions rarely begin with cameras or guards. They begin with the environment. Can people see and be seen along every pathway? Are entrances appropriate for the site’s function, clearly defined and capable of being effectively monitored? Does landscaping conceal or reveal? Are public, private and restricted areas clearly separated?

Developers who apply this lens during the planning phase may reduce the need for costly reactive security measures later. Retrofitting security features is often more expensive and disruptive than incorporating them into the original design.

This is not merely theoretical for Jamaica. The Ministry of National Security already has dedicated CPTED leadership, and in May 2025 a two-year, US\$2-million initiative was launched with the Jamaica Constabulary Force, the Pan American Development Foundation

“

The Ministry of National Security already has dedicated CPTED leadership, and in May 2025 a two-year, US\$2-million initiative was launched with the Jamaica Constabulary Force, the Pan American Development Foundation and the United States Embassy to strengthen safety in five communities

and the United States Embassy to strengthen safety in five communities, including Parade Gardens and Majesty Gardens. The Comm-Unity Resilience and Transformation, or CREATE, project combines CPTED training and improvements to community spaces with youth, family and other social interventions.

Jamaica therefore already has the institutional foundation to expand the use of CPTED. What is needed now is for these principles to move from selected communities into standard practice for development projects islandwide. Every major project, whether housing, transportation, recreational or commercial, should confront one essential question: will this design help people feel safer, or will it quietly create opportunities for crime?

That question should be asked before the first brick is laid, not after the first incident occurs.

Sometimes the strongest security measure is not another patrol or another camera. It is a community designed, used and maintained so that crime has fewer opportunities to take root.

Review the Certification Handbook for more details on policies, procedures, eligibility requirements, testing options (test center or remotely proctored exams), and fees for the ASIS certification program. It also contains the domains, tasks, and knowledge statements for all four of our certifications.



ASIS International Board Certification Handbook





DATA ANALYTICS IN SECURITY:

Using Data to Guide Security Strategy and Operations

Karim Campbell
ASIS Member

Part 2: Data Visualisation Techniques in Security Management

This is Part 2 of a series of articles exploring the application of Data Analytics within the Security Department.

In Part 1, we examined the importance of data analytics within the security function and the need to digitise security-related information so that it can be properly captured, analysed, and used to support decision-making within an Enterprise Security Risk Management (ESRM) framework. In Part 2, we focus on data visualisation techniques and their application within the security function.

WHY VISUALISE SECURITY DATA

One of the primary purposes of data visualisation is to explain and explore what an organisation's data is telling us. Rather than relying solely on spreadsheets or written reports, visualisations can highlight patterns, relationships, trends, and anomalies that may not be immediately apparent. This gives security managers a different perspective and can provide valuable insight into why certain events or risks are occurring.

Data visualisation is also particularly useful when communicating with senior management and other stakeholders. Complex datasets can be presented through dashboards, charts, maps, and other visual formats that make information easier to understand. Platforms such as Microsoft Power BI and Tableau

allow security departments to combine multiple data sources and create interactive dashboards that support both analysis and communication.

BUILDING A SECURITY DASHBOARD

A security department could use Tableau to create an interactive dashboard highlighting the financial value of assets recovered, vandalised, or stolen over the previous five years, allowing year-over-year comparison.

A bar chart could identify facility types and the relative proportion of associated losses, such as distribution centres or manufacturing sites. A treemap could display the facilities with the highest losses, the size and colour

“

Time-series visualisations can provide another important perspective by showing how security indicators change over time. Such analysis may identify seasonal increases in incidents, unusual spikes, or periods of reduced activity.

of each section proportional to the value measured. A heat map of Jamaica could illustrate the parishes experiencing the greatest losses, while a time-series graph tracks changes over time, revealing seasonal spikes or unusual periods warranting investigation.

One of Tableau's strengths is its ability to apply filters across an entire dashboard. Whether filtering by parish, facility type, year, or another variable, all visualisations update simultaneously. For example, if St. Catherine records significant losses, users can investigate whether those losses are concentrated in one or two facilities or spread across multiple locations. Investigations could also show that a region or facility with the fewest incidents carries significantly greater weight than those recording numerous incidents, and that distinction should be reflected in the risk analysis.

Time-series visualisations can provide another important perspective by showing how security indicators change over time. Such analysis may identify

seasonal increases in incidents, unusual spikes, or periods of reduced activity. An apparent reduction in incidents during a particular year, for example, may be associated with external conditions that changed normal patterns of activity. Recognising such anomalies is important because trends can be misleading when they are viewed without context.

CONCLUSION

Ultimately, data visualisation allows security departments to move beyond simply reporting incidents and losses towards explaining what the data means. By presenting security information in an interactive and accessible manner, dashboards can demonstrate the business impact of security risks, support evidence-based decisions, and help identify patterns, relationships, root causes, and emerging risks. In this way, data visualisation becomes not merely a reporting tool, but an important component of modern security strategy and operations.



Congratulations

Conroy Samuda, CPP, PCI, PSP

The Executive and Members of ASIS International Jamaica Chapter proudly congratulates

Conroy Samuda, CPP, PCI, PSP
For his recent success in the Physical Security Professional exam on July 14, 2026, making him a

Tripple Certificant!




Congratulations

Shanique Hudson, PCI

The Executive and Members of ASIS International Jamaica Chapter proudly congratulates

Shanique Hudson, PCI
For her recent **Exam Success.**

Shanique was successful in the Professional Certified Investigator (PCI) exam on July 2, 2026



Men's Mental Health Webinar:

Analytics for BEYOND "I'M FINE"

The ASIS Jamaica Chapter's Men's Mental Health Awareness Webinar, "Breaking the Silence: Beyond the 'I'm Fine,'" was held virtually on June 30, 2026. Organised by the Chapter's Legislative Committee, the well-attended session was planned and coordinated by Aldean Campbell and her team. Psychologists Dwayne D. Stewart, JP, MA, BA, LAPC, and Dwight Stewart, JP, MA, BA, LAPC, led an interactive discussion on men's mental health, stigma, resilience, help-seeking and healthy relationships.

A pre and post-webinar evaluation showed encouraging results. Nearly 86% of post-webinar respondents said their understanding had improved, while all indicated greater confidence discussing mental health. Before the session, 75% said they were likely or very likely to seek help if they were struggling mentally. After the webinar, every post-webinar respondent said they would be more likely to seek professional help themselves or encourage someone else to do so.

Help-Seeking Responses

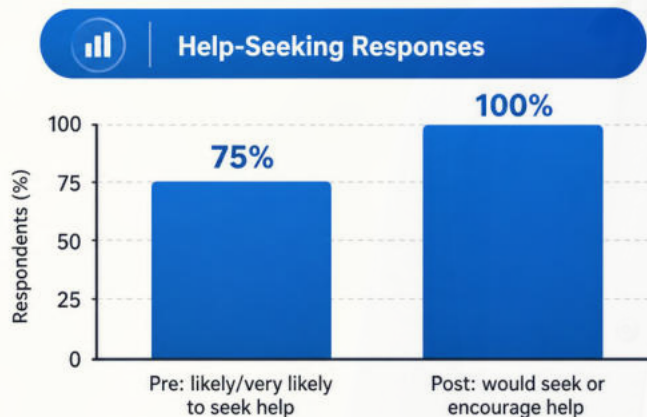
Respondents were more likely to indicate they would seek or encourage help after the webinar.



25

percentage point increase

in help-seeking intent post-webinar.



Note: Pre- and post-webinar questions were related but not identical.



Key Takeaway

The webinar was associated with a meaningful increase in the likelihood of seeking or encouraging help.



MEN'S MENTAL HEALTH WEBINAR



86%

Reported improved understanding



100%

Reported greater confidence



100%

Would recommend the webinar

Knowledge Shared, Security Strengthened: Learning Across ASIS International Jamaica Chapter

By The Informer Editorial Team



One of the greatest strengths of a professional association is the opportunity it creates for members to learn from one another. During May, June and July 2026, the ASIS Jamaica Chapter continued that tradition through presentations on emerging threats, cybersecurity and behavioural observation.

In May, Mrs. Keira Hanson-Berry, Accounts Receivable Manager at Atlas Group and a trained criminologist, delivered a presentation entitled “Emerging Threats in the Caribbean with a Focus on Jamaica.” The session encouraged members to consider how the regional threat environment is changing and why security professionals must remain alert to risks that can affect organisations, communities and the wider society.

In June, distinguished cybersecurity expert Mr. Andrew Nooks, B.Sc., CISSP, CISSP-ISSAP, CISM, CISA, CRISC, PCIP, CIPM, focused on the digital environment with

a presentation on current cybersecurity challenges and best practices. As organisations rely more heavily on connected systems and digital platforms, cyber awareness has become an important part of understanding and managing organisational risk.

In July, the Chapter’s Certification Chairperson, Wayne Ballen, CPP, PCI, PSP, presented on “Behavioural Observation in Security: From Profiling to Evidence-Based Risk Evaluation.” His presentation highlighted the importance of moving beyond assumptions and subjective profiling and placing greater emphasis on observable behaviour, indicators and evidence when assessing potential risks.

Taken together, the three presentations highlighted the range of challenges security professionals are now expected to understand, from evolving regional threats and cyber vulnerabilities to the human behaviours that can signal risk. Members were exposed to different

perspectives that can inform how they assess threats, make decisions and strengthen security practices within their organisations.

The sessions also showed the value of the Chapter as a place where members can learn, exchange experiences and take practical ideas back into their workplaces. That is where the real value of knowledge-sharing is seen: when what is discussed in a meeting helps shape better thinking and better security practice afterwards.

Professional membership is therefore about more than attending meetings or building networks. It is also about staying informed, hearing different viewpoints

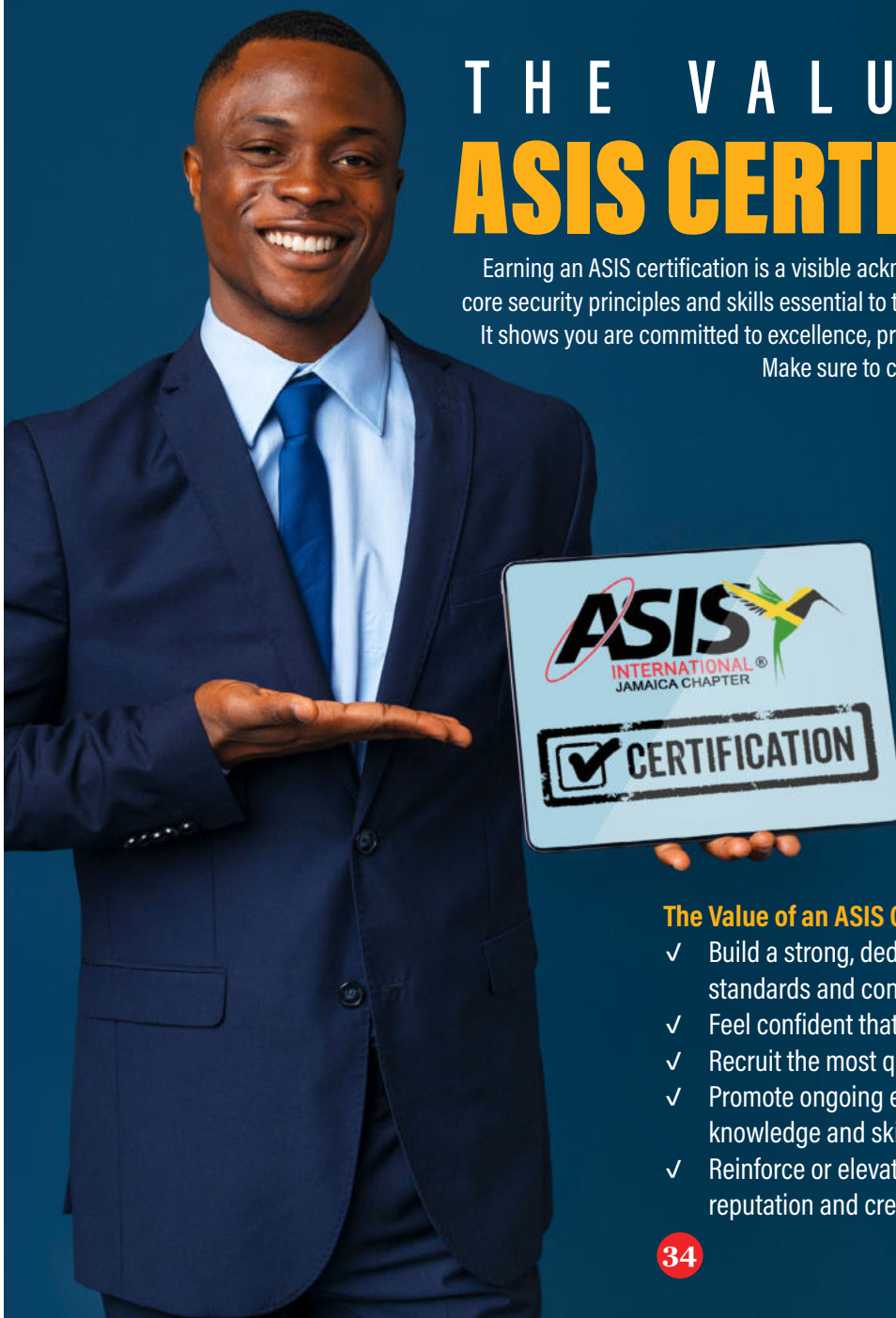
and learning from practitioners with different areas of expertise.

By continuing to bring relevant speakers and practical security topics before its membership, the ASIS Jamaica Chapter is creating meaningful opportunities for members to grow professionally and contribute more effectively within their organisations and the wider security community.

When knowledge is shared, our collective ability to protect the organisations and communities we serve becomes stronger.

THE VALUE OF AN ASIS CERTIFICATION

Earning an ASIS certification is a visible acknowledgment that you possess mastery of core security principles and skills essential to the best practice in security management. It shows you are committed to excellence, professional growth, and a code of conduct. Make sure to choose the certification that's right for you.



Scan here to learn more

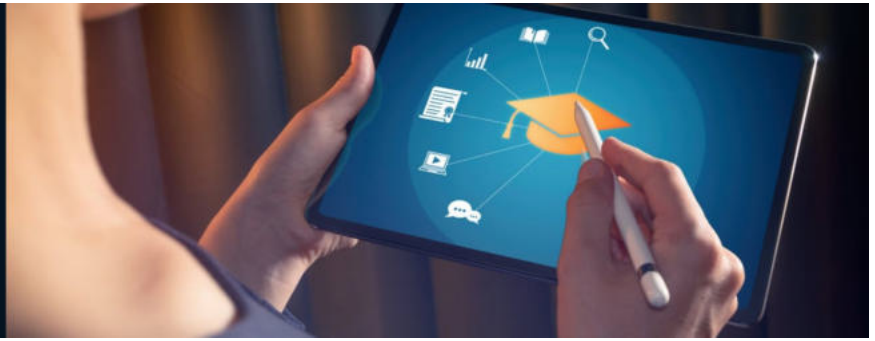
The Value of an ASIS Certification to Your Employer:

- ✓ Build a strong, dedicated team committed to high standards and continuing professional development
- ✓ Feel confident that your staff are using best practices
- ✓ Recruit the most qualified professionals
- ✓ Promote ongoing enhancement of critical job knowledge and skills
- ✓ Reinforce or elevate your organization's reputation and credibility

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. 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



JOIN

34,600

SECURITY PROFESSIONALS

Take your security career to the next level

BECOME A MEMBER



Apply for 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](#)



Jamaica Chapter

For information on ASIS International Jamaica Chapter:
Chairman: suzanne.scarlett@yahoo.com
Treasurer: dapsbusiness@gmail.com
Latin America and Caribbean Regional Board Director: bewryba@gmail.com
Newsletter Editor: carlospipher@gmail.com