



ASIS FEATURE

HOMICIDE STATISTICS VS REAL RISK IN JAMAICA

Jamaica stands out in many ways, for music, culture, its people, cuisine, prowess in sports, tourism, and so much more. Sadly, the homicide rate also stands out. If the average person, hoping to visit Jamaica was to look purely at the statistical figures of homicide in Jamaica they would certainly be dissuaded from visiting. Further if they looked at travel advisories from different high commissions in Jamaica they would certainly not want to visit.

- Page 1



Reframing Security: From Cost Center to Business Enabler

Security often gets a reputation as a necessary but heavy expense—much like paying for insurance (apologies to my friends in the Insurance industry). While it is undeniably crucial to protect against threats, this view misses out on what security can really offer.

- Page 9



LEVEL UP YOUR SECURITY CAREER Associate Protection Professional (APP®)

[APPLY FOR APP](#)

Where do you want to go in your security career? The Associate Protection Professional (APP®) certification will help you get there.



23-25 SEPTEMBER 2024
ORLANDO, FL, USA



REGISTER

**Beyond Borders:
Uniting for a Safer World**
ASIS International's Path for Global Growth and Inclusivity

ASIS members, volunteer leaders, and our valued global partners collaborated to define a strategy to grow our community with an emphasis on global outreach to connect the collective brilliance of all security professionals.



READ MORE



Contents

Homicide Statistics vs Real Risk in Jamaica

1

Bridging The Gap Between AI
And Physical Security: An Emerging Nexus
Of Safety And Technology

3

Human Resource Development
And Private Security

6

Navigating Ethical And Moral Challenges
In The Security Industry: Insights From
ASIS International, Jamaica Chapter

8

Reframing Security: From Cost
Center to Business Enabler

11

Resilience Management - Filling the Gap

13



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 or its leadership. References in this newsletter to any specific commercial products, process or service by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply endorsement, recommendation or favouring by ASIS International or its leadership.



Kevin Williams, CPP
ASIS Member

HOMICIDE STATISTICS VS REAL RISK IN JAMAICA

THE AVERAGE MAN CAN FURTHER REDUCE THIS RISK BY APPLYING SECURITY COMMON SENSE

Jamaica stands out in many ways, for music, culture, its people, cuisine, prowess in sports, tourism, and so much more. Sadly, the homicide rate also stands out. If the average person, hoping to visit Jamaica was to look purely at the statistical figures of homicide in Jamaica they would certainly be dissuaded from visiting. Further if they looked at travel advisories from different high commissions in Jamaica they would certainly not want to visit. It is therefore important to take this opportunity to clarify and qualify the statistics being put forward to Jamaicans locally, those in the diaspora as well as foreigners hoping to visit.

The statistics as of 2023 suggest that Jamaica murders 0.0495% off its population every year. Over the last decade the figures have varied from 1000 per year to as high as 1600 and as at the end of 2023 just under 1400. This is alarming when compared to any other country, but it is important to understand the context within which these homicides occur. The police have sought to provide an understanding of the motives that were derived from their investigations to get an appreciation of the underlying reasons for these homicides. They have done this to help the average man to realise what the real risk is to him as he goes about his lawful business. Yet this information often seems to get no further than the police press conference because the real figures and the real understanding rarely ever hits viral social media quite the way bad news does. So, I will attempt to help the average man as well as those intending to visit Jamaica with the analysis.

“

Over the last decade the figures have varied from 1000 per year to as high as 1600 and as at the end of 2023 just under 1400.

As at the end of December 2023 there were 1393 homicides, of that amount 67% or 933 of these murders were reportedly gangsters killing gangsters, 21% or 293 of these murders were interpersonal conflicts that resulted in a homicide, 4% or 60 of these murders were criminal homicides, generally crimes of opportunity gone to its extreme, 1% or 14 of these murders were mob killings (vigilantly groups taking the law into their own hands), not to be confused with gang killings, 7% or 98 of these murders were undetermined, meaning they fell into more than one of the categories mentioned above or the investigations have not been able to determine its classification.

What does this mean to the average man? It means if you are not in a gang your risk of being killed in Jamaica reduces by 67%, if you are self-controlled and have the capacity to manage interpersonal relations and the skill to de-escalate conflicts a further 21% of your risk of being killed in Jamaica also vanishes, unless you commit a crime and leave yourself exposed to being killed by an angry mob then a further 1% is removed from your risk, a further 7% disappears having not

fallen into any of the above categories, this leaves the real risk to the average man at 4% of total homicides. This 4% consists primarily of crimes of opportunity.

The average man can further reduce this risk by applying security common sense, avoiding geographic areas that are known to have a high risk of gang activities and applying security measures to fortify their homes and businesses will reduce that 4% risk by a further 2 to 3%. Not attempting to put up resistance if you are being robbed increases your survival rate by 90%. Therefore, the true risk to the average man who goes about his lawful business in Jamaica lies within a 1 to 2% risk of being the victim of a homicide. This real risk therefore would put Jamaica at approximately 27 persons killed annually (as of 2023). With a population of 2.827 million that would equate to approximately 1 homicide per 100,000. While this is certainly still no figure to celebrate because one death is still too much, it would certainly change our ranking in the scheme of things. Even more so, it would change travel

advisories and communicate a more accurate risk factor for visitors to our island. It must be understood that homicide figures by themselves do not communicate the truth about actual risk and it is the risk that they need to know, not the mere number of persons killed.

Case in point, if 1 in 5 persons in the world died from cancer, it would not be accurate to say everyone in the world has a 1/5 chance of dying from cancer. The doctors would be quick to check the history of the family's predisposition to cancer as well as other factors. This is how it should be when communicating crime statistics to the public. It is irresponsible to simply provide only a part of the picture without helping people understand how it impacts them. One's lifestyle contributes significantly to their risk of being a victim of homicide in Jamaica. I challenge security practitioners, police, governments, high commissions and the like to deliver the whole truth and not just homicide statistics. Present the truth about REAL RISK, after all security is about risk management.

E-FAST

Emergency First-aid & Safety Training



**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

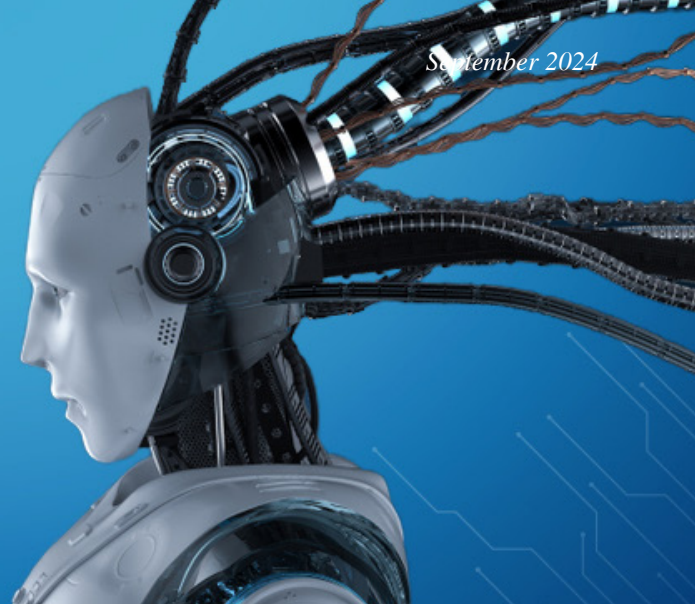


Photo courtesy of: cxotoday.com/specials/navigating-generative-ai-cyber-security-threats/#google_vignette



Bridging The Gap Between AI And Physical Security: An Emerging Nexus Of Safety And Technology

Lt. Col. Oswald J Smiley, MBA, BEng, CPP, PSP
Chairman, ASIS Jamaica Chapter

“The integration of Artificial Intelligence (AI) with physical security systems is transforming the way organizations protect assets, manage risks, and respond to threats.”

Introduction

The integration of Artificial Intelligence (AI) with physical security systems is transforming the way organizations protect assets, manage risks, and respond to threats. Traditionally, physical security has relied on human intervention, mechanical systems, and basic electronic surveillance. However, the rise of AI has opened up new possibilities for enhancing security measures, making them more intelligent, responsive, and adaptive. This article explores the convergence of AI and physical security, examining how AI is reshaping the landscape, the challenges and opportunities this integration presents, and the future trajectory of this evolving relationship.

The Evolution of Physical Security

Physical security, at its core, is the practice of protecting people, property, and information from physical threats such as theft, vandalism, terrorism, and natural disasters. Historically, this domain relied heavily on manual processes, such as security patrols, alarm systems, and closed-circuit television (CCTV)

monitoring. While these methods have been effective to some extent, they have limitations, particularly in terms of scalability, real-time response, and the ability to analyze vast amounts of data.

The introduction of digital technologies, such as networked surveillance cameras and access control systems, marked a significant advancement in physical security. However, these systems often generate more data than could be efficiently processed by human operators, leading to information overload and potential security lapses. The gap between the capabilities of traditional security systems and the emerging threats created a demand for more sophisticated solutions, paving the way for AI to enter the scene.

The Role of AI in Enhancing Physical Security

AI brings a new dimension to physical security by offering advanced analytics, automation, and predictive



AI systems are only as good as the data they are trained on, and if this data contains biases, the resulting algorithms can perpetuate these biases, leading to unfair or discriminatory outcomes.

capabilities that surpass human limitations. One of the primary applications of AI in this field is in video surveillance. Traditional CCTV systems rely on human operators to monitor live feeds and identify suspicious activities. However, this approach is prone to human error, fatigue, and bias. AI-powered video analytics can process video feeds in real time, detecting anomalies, recognizing faces, identifying objects, and even predicting potential threats based on patterns of behavior.

For example, AI can be used to identify unauthorized access attempts by analyzing facial recognition data and cross-referencing it with access control databases. In public spaces, AI-driven systems can detect unusual crowd behavior or abandoned objects, triggering alerts for security personnel to investigate. These capabilities not only enhance the effectiveness of security operations but also enable more efficient use of resources by reducing the need for constant human monitoring.

AI is also playing a crucial role in access control and identity verification. Biometric systems, such as fingerprint and iris scanners, have become more sophisticated with the integration of AI, enabling faster and more accurate authentication processes. AI algorithms can analyze biometric data to detect anomalies, such as attempts to spoof biometric systems, enhancing the security of sensitive areas. Furthermore, AI's predictive capabilities are being leveraged to anticipate security threats before they materialize. By analyzing historical data, social media activity, and other relevant information, AI systems can identify potential security risks and recommend proactive measures for mitigation. This shift from reactive to proactive security strategies is a game-changer in the field of physical security.

Challenges in Integrating AI with Physical Security

Despite the numerous benefits that AI brings to physical security, the integration of these two fields is not without

challenges. One of the primary concerns is the issue of privacy. AI-driven surveillance systems often require access to vast amounts of personal data, such as facial recognition profiles, behavioral patterns, and location data. The collection, storage, and analysis of this data raises significant privacy concerns, particularly in regions with strict data protection regulations, such as the European Union's General Data Protection Regulation (GDPR).

Ensuring that AI systems comply with privacy laws and ethical standards is a critical challenge for organizations seeking to implement AI-driven security solutions. This requires robust data governance frameworks, transparency in data usage, and clear communication with stakeholders about how their data is being used and protected.



Photo courtesy of: <https://www.neilsahota.com/ai-in-law-the-positives-and-the-negatives/>

Another challenge is the potential for bias in AI algorithms. AI systems are only as good as the data they are trained on, if this data contains biases, the resulting algorithms can perpetuate these biases, leading to unfair or discriminatory outcomes. For instance, facial recognition systems have been criticized for their higher error rates when identifying individuals from certain demographic groups. Addressing these biases requires careful consideration during the development and training of AI algorithms, as well as ongoing monitoring and refinement to ensure fairness and accuracy.

The integration of AI with physical security also presents technical challenges. Legacy security systems may not be compatible with AI-driven solutions, requiring costly upgrades or replacements. Additionally, the complexity of AI algorithms and the need for high-performance computing resources can strain existing IT infrastructure. Organizations must invest in the necessary hardware, software, and expertise to effectively implement and manage AI-driven security systems.

The Future of AI and Physical Security

As AI continues to evolve, its role in physical security is likely to expand further, leading to more sophisticated and integrated security solutions. One of the most promising areas of development is the concept of “smart security” systems that combine AI with the Internet of Things (IoT). These systems can leverage data from a wide range of sensors, devices, and platforms to create a holistic view of the security environment. For example, IoT-enabled cameras, motion detectors, and access control systems can work in tandem with AI algorithms to provide real-time insights and automated responses to security threats.

Another emerging trend is the use of AI in cybersecurity, which is increasingly intertwined with physical security. As more physical security systems become connected to the internet, they become vulnerable to cyberattacks. AI can help identify and mitigate these threats by monitoring network traffic, detecting anomalies, and responding to potential breaches in real time. The convergence of AI, physical security, and cybersecurity represents a comprehensive approach to protecting assets in the digital age.

Furthermore, AI is expected to play a key role in enhancing the resilience of critical infrastructure, such as power grids, transportation systems, and communication networks. By analyzing data from sensors and monitoring systems, AI can predict and prevent potential disruptions, ensuring the continued operation of these vital services. This proactive approach

to infrastructure security is essential in an era where the consequences of security failures can be catastrophic.

Conclusion

The integration of AI with physical security is bridging the gap between traditional security methods and the advanced capabilities offered by modern technology. AI is enhancing the effectiveness, efficiency, and adaptability of physical security systems, enabling organizations to better protect their assets and respond to emerging threats. However, this integration also presents significant challenges, particularly in terms of privacy, bias, and technical implementation. As AI continues to advance, its relationship with physical security will likely become even more intertwined, leading to the development of smarter, more resilient, and more secure environments. Organizations that successfully navigate these challenges and embrace the potential of AI will be well-positioned to lead in the future of security.



“Another emerging trend is the use of AI in cybersecurity”

To see what is happening in AI in other parts of the world...

CLICK HERE



MODERNIZING SECURITY WITH ROBOTICS PROCESS AUTOMATION



READ MORE

HR Policy

Workforce planning

Talent acquisition

HUMAN RESOURCES

Administrative Law

Talent Outreach

Capacity Building

Mobility

Compliance

Performance Management

Photo courtesy of: un.org/management/content/office-of-human-resources



Human Resource Development And Private Security

**Carlos Pipher, BSc (Hons) CPP, PCI, PSP
Newsletter Editor**

“

It is the duty of the Human Resource (HR) department to empower security personnel by organizing, promoting, and evaluating training sessions.

Human resources are the lifeblood of any organization, it is critical that employees are properly trained with the requisite job knowledge to perform efficiently and effectively. The security industry is dynamic and highly compartmentalized. The development of the human capital is crucial for the security provider as well as the client, both stand to gain from well-trained security personnel.

Recruitment

Recruitment of the individual who is job fit is very important for starters, having the right attitude and aptitude for the discipline of security is essential. Job adverts should be clear on the demands of the job and interviewers should focus on the candidate's ability to deliver or even to exceed the job requirements. To attract talented individuals, security organizations should offer competitive salaries, benefits, and opportunities for career advancement. The organization should believe in its employees and their ability to deliver at the highest level. A culture of trust and good representation is important for the good of the industry.

Education and Training

Basic and continuous training programs in general and training programs that are tailored to suit the specific environment where the security officer is deployed are essential. This includes not only technical skills but also security awareness of the latest security threats and best practices, customer service skills, crowd control, and basic self-defence techniques. It is the duty of the Human Resource (HR) department to empower security personnel by organizing, promoting, and evaluating training sessions. Security officers who are more aware because of their disposition will add more value to the team and by extension to the function of asset protection.

If a company cannot retain its skilled security professionals, there will be no benefit from the cost of the security training. However, if those security professionals remain in the industry, then the industry gains from that training. HR should ascertain what drives employee retention and implement policies to address these factors. This may include advanced training, incentives, offering professional development opportunities, recognizing and rewarding achievements, and ensuring a positive work environment.

Talent acquisition

HUMAN RESOURCES

Administrative Law

Compliance and Ethics:

Compliance is responsible for ensuring that employees are aware of and comply with regulatory requirements. This includes security regulations, policy and data privacy some of which can be very complex. Security professionals will encounter situations which call for ethical consideration and they will be expected to make ethical decisions. To properly comprehend this, training in security ethics should be factored in training programs.

Job knowledge alone will not hold the security industry to a high standard, all the other attributes of a professional looking security officer are a factor which will attract others to the industry. Proper training should be invested in the members, conduct and professionalism should be seen at first glance. It is noted that professionally managed security companies will attract better skilled applicants and will also be able to bargain for higher compensation in the negotiating of contracts.



Complexities in the Global Security Market: 2024 through 2026

- Technology and Services
- Regional Breakdowns
- Employment

Research partner:

How many people work in the security sector worldwide? What is driving growth in the security equipment market? What trends are making the greatest impacts?

For a limited time, available to ASIS International members only. (SIA members, please access through SIA's website).

[READ THE ISSUE](#)

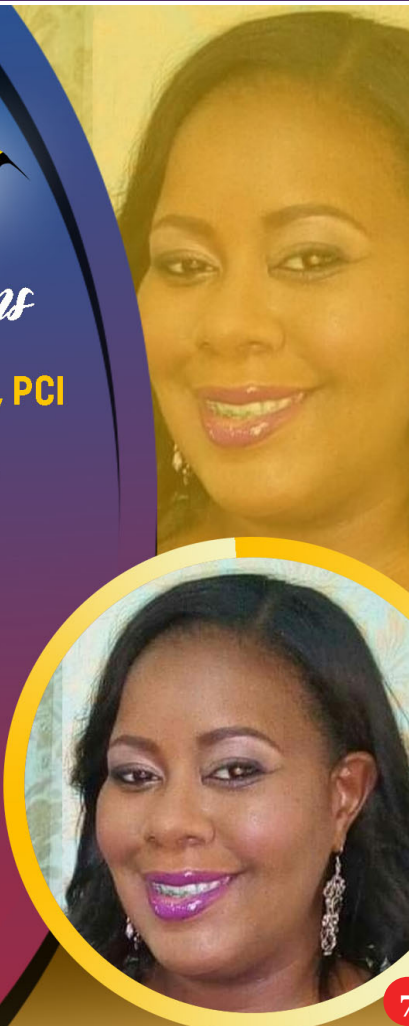


Ms. Rhondene Leslie, CC, PCI

The Executive and Members of ASIS International Jamaica Chapter proudly congratulate

Ms. Rhondene Leslie, CC, PCI
ASIS Member,

for successfully passing the Professional Certified Investigator (PCI®) Exam on July 27, 2024.



ASIS INTERNATIONAL BOARD CERTIFICATION HANDBOOK

[READ THE ISSUE](#)



Photo courtesy of: eagleeye247.com/security-guard-ethics/

Navigating Ethical And Moral Challenges In The Security Industry: Insights From ASIS International, Jamaica Chapter



**Capt. Basil Bewry, CPP, PCI, PSP
Latin America and Caribbean
Regional Board Director**



**Shereen Cox, PhD, Ethicist,
Researcher and Lecturer,
University of Oslo, Norway**

“

When the work culture becomes one that is highly stressful, creating situations where employees find themselves compromising personal morals, witnessing situations that go against their personal integrity or being uncertain of the right thing to do, this creates an environment for moral distress.

Security professionals are an integral part of the society. They are mandated to protect life and property of those who are entrusted to their care. These professionals include military, police as well as those who ply their trade in both the private and public sectors. ASIS International is the largest membership organization for security management professionals and is known as the authority for learning, networking, standards, research and analysis within the security field. ASIS Jamaica is a chapter of ASIS International and has been providing educational support to build competence for its members for over 49 years. To achieve this goal, educational content is delivered through online certification courses, monthly forums, and a quarterly

newsletter. In August, the focus was on the moral and ethical challenges encountered by its members.

Jamaica, unfortunately, has one of the highest intentional homicide rates in the world. ASIS members in the service (police and military) regularly face very stressful and traumatic situations. Over the past year there has been an increase in the number of violent attacks on private security officers. Security personnel are expected to push their personal feelings aside and prioritize the needs of those they serve. Studies have shown that traumatic experiences can lead to compassion fatigue. Crime is only one stressor, other stressors include being underpaid and overworked, lack of cooperation/support from members of the public, internal corruption, and pressure from employers to meet unrealistic targets with limited resources.

At times, security personnel may encounter incidents that go against their personal morals or find themselves losing faith in the justice system and as such compromise what they know to be right procedures to get the job done- with no personal gain. This is often described in the literature as noble cause corruption, a utilitarian concept focused on achieving good ends by questionable means. When the work culture becomes one that is highly stressful, creating situations where employees find themselves compromising personal morals, witnessing situations that go against their personal integrity or being uncertain of the right thing to do, this creates an environment for moral distress. Moral distress is the “physical or emotional suffering that is experienced when constraints (internal or external) prevent one from following the course of action that one believes is right.” It is a concept often explored among health professionals especially nurses but rarely among security professionals. ASIS Jamaica sought to gain insight from its members whether and to what extent they may be facing moral/ethical challenges and the strategies that they may employ to address these challenges.

Method

An anonymous online survey was created by co-authors Dr. Shereen Cox and edited by Capt. Basil Bewry. The final survey was then reviewed and approved by the Executive of ASIS Jamaica. The survey did not collect any identifiable information and respondents were informed of the purpose. The respondents were asked not to share any identifiable information such as names of place of work or individuals. The survey questions included demographic information, questions related to ethics education, moral challenges in the workplace, moral resilience, strategies to address moral challenges and their views on the effectiveness of ethics education in navigating moral challenges. The survey was made available between August 18 and August 23, 2024.

Results and Discussion

Thirty-three people responded. Many of the respondents were male (76%), married (64%), and over the age of 45. Seventeen worked in private security, law enforcement

FORENSIC
POLYGRAPH SERVICES
Detecting Deception Since 1999

CONTACT
876-383-2754
876-792-0875
forensicpolygraphja.com
forenpoly@gmail.com
forensicpolygraph.ja

LET US UNCOVER THE TRUTH
FORENSIC POLYGRAPH SERVICES

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

9

“

Many of the respondents noted that although it is challenging, they believe it is possible to be both ethical and successful in the security industry.

(4) and military (3) with work experience spanning between 11 and greater than 15 years. The educational level of the majority was a bachelor's or master's degree. Many (85%) noted that they had received ethics education through professional development courses. Only 9% noted having not received any exposure to formal ethics education. Consequently, the majority noted that ethics education was very effective in helping them to navigate moral challenges and their confidence in being able to make morally right decisions under pressure. Many noted a supportive work environment in that they felt completely or somewhat supported. (56%) their ability to speak up or stand firm on their moral values. However, 16% indicated that the work environment somewhat undermines or completely undermines their moral values. In fact, one respondent shared an experience with superiors where his distress was so high that it led to two suicide attempts. However, that respondent indicated that professional counselling was part of his coping strategy. This was an important observation as it indicated that the security professionals can experience significant moral injury to the extent of giving up on life itself. Other strategies included avoidance (39%) and talking to colleagues and supervisors (36%). Respondents noted that they had experienced emotional exhaustion after traumatic incidents and their ability to maintain compassion towards perpetrators was dependent on the crime. Respondents indicated high levels of moral resilience and moral courage i.e., they are unafraid to speak up (moral courage) if necessary, despite the risk

of alienation. One participant noted that it was the nature of the job: “Security is always a function where you have to maintain a separation from colleagues”. When asked their opinion on whether it is ok to compromise ethical values to achieve certain ends, there was an almost 50:50 split. 53% of the respondents indicated that there should not be any compromise while others noted that it depended on the situation. They were of the opinion that if it is a matter of national security and preservation of life, then it may be justified to compromise the means to achieve the ends. This is important for further exploration as it may be an indicator of the existence of noble cause corruption- compromising ethics for the achievement of what is perceived as good outcomes. However, while noble cause corruption may achieve certain immediate ends, the long-term consequences can lead to diminished trust and legal or professional repercussions. Almost all the respondents (90%) noted that ethics education was moderately to very effective in helping them navigate moral challenges on the job.

Conclusion & Recommendations

The survey of ASIS Jamaica Chapter members indicates a strong relationship between ethics education, a supportive work environment and ethical behaviour. Many of the respondents noted that although it is challenging, they believe it is possible to be both ethical and successful in the security industry. Respondents exhibited reasonably good levels of moral resilience and moral courage despite any negative consequences such as alienation. The survey has inherent limitations as the sample size was small. Additionally, many of the respondents were at the managerial/executive level therefore their insights may be based on having more control of their environment. It may be interesting to explore the perspectives of junior security professionals.



**YOUR TWO-YEAR MAP
FOR PUBLIC TO PRIVATE
CAREER TRANSITIONS**



READ MORE



Photo courtesy of: nfsecurity.ca/corporate-security-security-personnel-protect-business-covid-19-pandemic/



Reframing Security: From Cost Center to Business Enabler

Warren L. Smith CISSP, CRISC, PMP, PMI-RMP, CPP, PCI, PSP
ASIS Council Liaison

Security often gets a reputation as a necessary but heavy expense—much like paying for insurance (apologies to my friends in the Insurance industry). While it is undeniably crucial to protect against threats, this view misses out on what security can really offer. I, on the other hand, believe it is time we change the conversation around security. Instead of seeing it as just a protective measure, let us start recognizing it as a strategic asset that can drive innovation, build resilience, and give our business a competitive edge.

The Changing Role of Security

Historically, security has been about reacting to risks and safeguarding our assets. These are, of course, important responsibilities, but when we only see security through this lens, we limit its potential within the organization. Today's world is all about digital transformation, globalization, and increasingly sophisticated threats. Security needs to evolve beyond its traditional role. It shouldn't just be considered a cost—security should be seen as a vital contributor to our overall success.

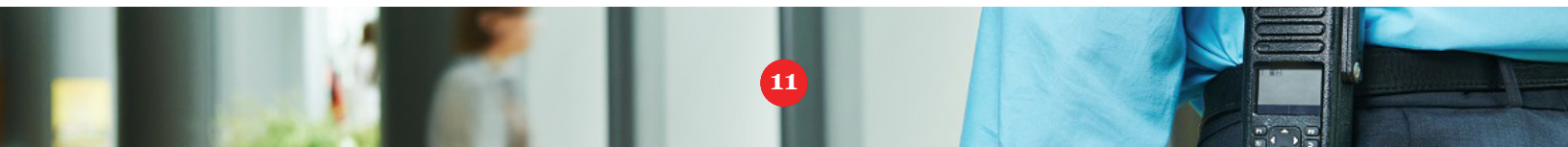


To fully realize these benefits, we need to build strong partnerships with IT, Facility, and Property Management teams, all the pillars that security have fallen into at times...

Security as a Business Enabler

When we think of security as a business enabler, we start to see how it can open new opportunities for innovation and leadership in the market. Take cybersecurity, for example. By proactively investing in it, we're not just preventing breaches; we're also building trust with our customers—a crucial asset in today's digital economy. When customers know their data is secure, they're more likely to engage with us, which leads to increased sales, stronger brand loyalty, and greater market share.

To fully realize these benefits, we need to build strong partnerships with IT, Facility, and Property Management teams, all the pillars that security have fallen into



at times. These teams often have more established infrastructures and better funding, and by working together, we can leverage their technology, expertise, and resources to amplify the impact of our physical security program. When we align our efforts, we create a more cohesive security strategy that tackles both digital and physical threats in a unified way, meeting the expectations of standards like ISO 27001:2022, which emphasizes the importance of physical security controls in protecting tangible assets, including data.

Turning Security into a Competitive Advantage

Security isn't just about protection—it can also set us apart in the marketplace. As regulations tighten and consumers become more aware of privacy and data protection, companies that prioritize security will be better positioned to comply with laws, avoid costly fines, and attract customers who value data integrity. This proactive approach not only reduces risks but also boosts our reputation as a responsible and forward-thinking leader in our industry.

When we integrate security into product development, we can create innovative solutions that meet the demands of an evolving market. In sectors like financial services, healthcare, and technology, where data security is a top priority, embedding security features into the products from the start can give a competitive edge. These security-enhanced products can command higher prices, open new revenue streams, and strengthen our position in the market.

A New Perspective on Security

To truly unlock the potential of security as a business enabler, we need to change the way we talk about it internally. Instead of focusing on minimizing costs, we should see and position security as an investment that drives value. This means integrating security into our broader business goals and making it a fundamental part of our strategic planning.

Just as important is the need to foster collaboration between physical security, IT, and Facility/Property Management teams. By tapping into the strengths of these programs, our security function can become even more effective and play a bigger role in the company's overall strategy. This collaboration ensures that security is considered in every aspect of our business, from product development to customer service, and that all security efforts are aligned towards common goals.

Reframing security as a business enabler isn't just a smart move—it is essential for long-term success in today's fast-paced business environment. By embracing this new approach and building strong partnerships with our stakeholders, we can protect our organization from threats while also unlocking new opportunities for growth, innovation, and competitive advantage. Security is not just a necessity anymore—it is a strategic asset that can help propel an organization to new heights.

3 Steps to Prepare for A New Position in Security Management **READ MORE**

HEART NSTA TRUST DEBATE COMPETITION



Latin America and Caribbean Regional Board Director, Capt. Basil Bewry, CPP, PCI, PSP collects a basket on behalf of the Chapter from event coordinator Susan Scarlett, LLB, PSP.



Capt. Basil Bewry, CPP, PCI, PSP posing alongside the coaches of the winning debate team with their cash prizes.

V FORO WOMEN IN SECURITY LATIN AMERICA 2024



Nichelle Duncan, CPP, PCI, PSP (left) and Alexandria Davis, CPP, PCI, PSP from Puerto Rico.



Nichelle Duncan, CPP, PCI, PSP and Shanna Shirley, CPP, PSP, alongside (L) Cy Oatridge, CPP - President ASIS International Global Board and Pablo Colombes, CPP - Chairman Latin America and Caribbean Regional Board.



Photo courtesy of: odpem.org.jm/odpem_in_the_media/hurricane-deans-3rd-anniversary/



Resilience Management – Filling the Gap

Ian Roberts, PSP
Treasurer



Jamaica is no stranger to hurricanes and to a lesser extent minor earthquakes, which exposes the island to unprecedented disaster events all of which requires SMART preparation.

According to ONSOLVE GLOBAL RISK IMPACT REPORT “Most organizations and agencies don’t have mitigation plans for the threats they are encountering, and fewer than half believe their programs are mature. In addition, most think that their responses are reactive, and few are equipped to be proactive on risks. Key obstacles are not having the right technology, inadequate funding and inappropriately trained or skilled staff”.

When assessing the current state of the technology used for threat and hazard mitigation, the most common types reported by executives and federal, state, and local leaders were the following solutions: mass notification, incident and task management, threat detection, and security.

In my humble opinion, there are preparedness gaps in our security industry and we as security practitioners must focus on “Resilience Management”, through the application of technology and training, which will enable us to withstand not only foreseeable security risks and threats but also natural climatic threats that pose dynamic risks.

According to the World Meteorological Organization (WMO), “heatwaves, floods, droughts, wildfires, and

rapidly intensifying tropical cyclones/hurricanes caused misery and mayhem, upending everyday life for millions, and inflicting billions of dollars in economic losses in 2023”. The National Hurricane Center estimated that we should see at least 25 hurricanes with 4 - 7 major ones during this hurricane season.

Jamaica is no stranger to hurricanes and to a lesser extent minor earthquakes, which exposes the island to unprecedented disaster events all of which requires SMART (Specific, Measurable, Achievable, Reasonable, Time-bound) preparation of our organizations. Technology should be used in the design and execution of mitigation plans for natural disasters. Also, organizational resilience should be a factor in the design to secure tangible and intangible assets which will assist in preventing crimes against the organization after a disaster.

During or after a natural disaster such as a hurricane, there may be looting, vandalism, break-ins on businesses that were not fully or even impacted by the disaster event. Against the afore-mentioned scenario, building resilience is critical for businesses and organizations. Focus should be on crime prevention and quick response to crime post disaster event. This requires risk analysis and evaluation coupled with appropriate training if entities are to be best prepared for any negative event. Let us upgrade our skills and abilities within the industry to meet any negative event and be resilient.

REACH NEW SECURITY HEIGHTS





GLOBAL SECURITY EXCHANGE
23-25 SEPTEMBER 2024
ORLANDO, FL, USA



GSX

GLOBAL SECURITY EXCHANGE

23-25 SEPTEMBER 2024
ORLANDO, FL, USA

REGISTER



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




SECURITY TECHNOLOGY: The Droids You're Looking For

Advanced security robots are no longer just figments of our imagination. They are now patrolling facilities, authenticating visitors, and inspecting hazardous scenes for emergency personnel, changing the way that security practitioners think about deploying human personnel to job sites. Learn more about current security robot applications in the August issue of Security Technology.



**READ THE
ISSUE**



2020-2024 STRATEGIC PLAN

Click Here to Read More

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



Jamaica Chapter

For Information on ASIS International Jamaica Chapter, Contact:

Chairman: ojsmiley@gmail.com
Vice Chairman: swebbwoc@gmail.com
Latin America and Caribbean Regional Board Director: bewryba@gmail.com
Newsletter Editor: carlospipher@gmail.com