DECEMBER 2023 | Q4 Issue

SECURITY PROFESSIONAL

ASIS INTERNATIONAL® Singapore Chapter

Contents Page

Chairperson's Note

Dear Members & Colleagues,

As we approach the end of another remarkable year, I want to express my gratitude for your unwavering commitment to advancing the security profession. Your dedication has been the driving force behind the success of this Chapter, and as we look ahead to 2024, I am excited to share some important updates and extend a special call to action.

1. Calling All Members: Step Forward, Volunteer, Lead!
Our community thrives on the collective efforts of passionate individuals like you. I encourage each member to consider stepping forward and contributing your expertise in various capacities. Whether it's becoming a trainer, a mentor, coordinating events, or contributing articles, volunteering your workplace for site visits; your involvement strengthens our network and enriches the experiences of fellow professionals.

2. Save the Date: 2024 ASIS Asia Pacific Conference and Outstanding Security Professional Award
Mark your calendars for the highly anticipated ASIS Asia Pacific Conference in November 2024. This event promises to be a gathering of the finest minds in security, offering a unique platform for knowledge exchange and networking. In conjunction with the conference, we will celebrate excellence with the Outstanding Security Professional Award. Keep a lookout for announcements on how you can participate and make a significant impact.

3. Certification Excellence: CPP, PSP Exam Prep Material Update for 2024
We are committed to ensuring that ASIS certifications remain at the forefront of professional development. In 2024, we will be updating the Certified Protection Professional (CPP) and Physical Security Professional (PSP) exam preparation materials. This enhancement aims to provide you with the knowledge necessary to excel in your security careers. Those aspiring to achieve certification, stay tuned for the release of 2024 exam preparation dates and embark on this rewarding journey.

Your active participation, enthusiasm, and commitment continue to drive ASIS International forward. Together, we will shape the future of the security profession and create a lasting impact on our industry.

Wishing you a joyful holiday season and looking forward to an exciting 2024 ahead!

Sincerely,

YONG Hwee Fong, APP
Honorary Chairperson

Women in Security - Monthly Meetup

Article Contributed by:
By CHOW Keng Fong

Thanksgiving reflections.

I attended a relaxing evening with Women-in-Security on 16 November 2023, where we chatted over food and drinks, forgetting for two hours all our responsibilities as a leader, a worker, a mother, a daughter, a daughter-in-law, a sister, a wife, etc. We were just hanging out, being around the table to draw strength from each other. Ah… I felt that this was a good time for my soul, hence why I kept going back to these meetings. It's time to get inspired by all the people around this table.

Thanks to Marie Hélène MANSARD PARILUSYAN from Axis Communications for hosting these sessions, month after month. Thanks to Hwee Fong Yong, APP and Marie Hélène MANSARD PARILUSYAN who kept this group going despite it all!

The highlight of that evening was listening to Jenny G on how we can care for ourselves and how we can support our peers. As usual, we can't keep our thoughts to ourselves in such times so, a lot of us chimed in our stories, our challenges, and exchanged ideas on how we had been that 'invisible' support to our peers.

Sometimes, our friends need a little nudge, little smile, little hug, little tap, little quiet time, we should be ready to give. But if we felt like we had been giving of ourselves all of this year, here was a very timely reminder.

Jenny reminded me again the safety announcement made on the aircraft, the one about putting on our oxygen mask first before attending to our dependents. Hwee Lee Aw shared similar analogy on lifeguarding in the waters too. 2024 has been a year of many ups and downs, lots of crises, some conflicts personally and I am sure it's the same for many others. Nothing under the sun is new, right? It is the same year-in year-out. Hence this meeting was good timing for me to pause and reflect. "Take care of yourself (again….) then reach out to others". I know my future self will thank me for this.

I also like the lift analogy that Jenny shared, that invention if done early, the rebound back up may be easier. Say, the 10th floor is the normal me. While I am spiralling downwards, I may be unwilling to step off the lift on the 8th floor to seek help or get a breather, thinking I may still be able to bear the burden on my own. If I do get off the 8th floor, I may be able to get back up to the 10th floor easier than if I had got off on the 3rd floor. Perhaps. It is simplified but enough for me, for now. I am encouraged to check in with friends who I had not met up with in a while. It's a good time this year-end to pause and reach out… see how everyone is doing and not be shy to say, "I need help".

I end with this quote from one of my favorite books 'The Boy, The Mole, The Fox and The Horse' by Charlie Mackesy. "What is the bravest thing you've ever said?" asked the boy. "Help," said the horse.

ASX and SEA OSPAs 2023

Article Contributed by:
By LIM Choon Kwang, CPP

The ASIS Thailand Chapter held its 5th regional security conference at the Carlton Hotel, Bangkok on 10 November 2023. It was, as previous years, a pivotal event in the regional security sector, attracting over 100 delegates comprising distinguished speakers, industry thought leaders, security professionals and notable guests from ASIS International. This gathering was notably enhanced by the presence of Peter O'Neil, CEO of ASIS International, and Susan Mosedale, Chief Global Member Engagement Officer, as the guests of honour. Themed "**Fostering Regional Partnerships**", the event unfolded in a dynamic and engaging atmosphere, marking a significant step in advancing security collaboration across the region.

Aaron Le Boutillier, RVP13B, opened the event with a passionate address, with opening remarks that were a fitting precursor to the keynote speech by Peter O'Neil. As the guest of honour, Peter's address was particularly impactful, emphasising the critical role of partnership and collaboration in the security field. This was followed by a series of engaging presentations by several speakers in both corporate and consultancy roles in the security sector.

The conference was immediately followed by the inaugural **Southeast Asia Outstanding Security Performance Awards (OSPAs)** ceremony, sponsored by Singapore-based security system integrator BluOcean Security. This event, having originated in the US, is a celebration of excellence in the security industry with awards presented across multiple categories including '**Outstanding In-House Security Manager/Director**', '**Outstanding Female Security Professional**', and '**Outstanding Security Company**'. These accolades served to highlight the varied talents and significant achievements within the security sector, showcasing the best in the industry and setting high benchmarks for excellence. The ceremony ended with a reception for attendees to reconnect with one another and forge new beginnings.

The success of both events reflected the generosity of its sponsors, whose support was crucial and which helped to create an environment that not only celebrated current achievements in the security field but also fostered the development of future innovations and partnerships. Their contributions were indispensable in making this conference a landmark event, furthering the cause of regional cooperation and excellence in security.

The next OSPAs ceremony will be held in Singapore around November 2024 in conjunction with ASIS International APAC conference 2024, and members are encouraged to strive for the awards in the respective categories.

Contributed Article

An Introductory Primer to Digital Asset Security for Institutions

Article Contributed by:
Jag Foo, CPP, PSP, PCI

An Introductory Primer to Digital Asset Security for Institutions

When one thinks of security, the conventional approach is the employment of security guards. Additional measures could include the usage of systems such as security cameras, alarm monitoring systems, electronic locks and access control for doors to safeguard their assets from theft. Assets are usually thought of in terms of physical entities such as documents, computers and jewellery.

But as we move to an increasingly digital world, assets that are worth securing are not just limited to physical ones but digital too. With the rise in adoption of major digital assets and stablecoins such as Bitcoin, Ether, Tether and USD Coin, holders of such assets are vulnerable to threats of cyber-attacks and malware which can lead to a catastrophic loss.

The State of Digital Asset Market

Why are digital assets relevant to our lives and worth securing?

We just have to look back at history and the advancement of the digital asset space. Since the creation of the first major digital currency Bitcoin in 2018 by Satoshi Nakamoto as a decentralised internet peer-to-peer cash, we have observed a meteoric rise in popularity of the digital asset class. At its peak, the cryptocurrency market capitalization has reached $3 trillion dollars in 2021.

Use cases of digital assets for the purpose of payment, remittance, insurance, investing and verifiable credentials have sprung up, with increased institutional awareness and usage. Large corporations from Blackrock to Mastercard to Google are entering the digital asset space. Even governments are getting into the act. For instance, Hong Kong has just initiated a new crypto regulatory regime in a bid to nurture a digital-asset hub. Similarly, the Monetary Authority of Singapore has just proposed a framework for designing open, interoperable networks for digital assets. With more active support from the government to provide regulatory clarity, adoption of digital assets and blockchain technology by institutions is set to rise further in the years ahead.

History of Digital Asset Losses

The digital asset landscape is not without its pitfalls. The industry has witnessed several high-profile hacks through the years. For instance, hackers have exploited the databases and private keys (a string of alphanumeric characters used in cryptography to authorise transactions and prove ownership of digital assets). of Mount Gox, a leading Japanese-based exchange at that time, resulting in a massive loss of 740,000 Bitcoins between 2011-2014. It was a devastating blow to the nascent cryptocurrency industry then.

In more recent times, FTX, another well-known exchange, suffered a spectacular collapse amidst allegations of wilful abuse of corporate governance and widespread fraud, wiping out billions of dollars worth of assets.

Losses were not just limited to centralised entities. Numerous Decentralised Finance (DeFi) platforms deployed on smart contracts have suffered from vulnerability exploits through the years. The gaming-focused Ronin network suffered a monumental loss of over $625 million worth of USD Coin and Ether in March 2022. This remains the single largest hack in the history of DeFi.

The Ronin Bridge attack was perpetuated by state-sponsored North Korean hackers via the compromise of the private keys which is the leading attack vector amongst hacking incidents throughout history.

Other major attack vectors that have led to significant asset losses include drained contracts, flash loan attack, signature as well as bug exploits.

Security Options For Institutional Users

Institutions often hold digital assets valued to the tune of millions of dollars. Because of this, they require custodial solutions with highly advanced levels of security. If you are an institution with access to a significant digital asset holding, the question is how do you safeguard your assets against not just external threats but also internal theft?

As part of risk management, it is prudent to ensure that the storage of assets are diversified across different custodians and custody methods. Institutions can choose to custody their assets with centralised providers who assume full responsibility and control over the private keys to their assets.

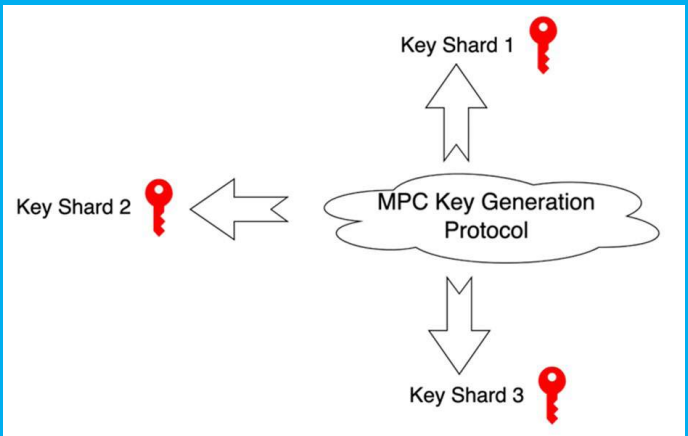
They can also use self-custodial solutions such as smart contract, hardware and Multi-Party Computation (MPC) wallets to retain control over the private keys to their assets while still ensuring a high level of security on the private keys. As the popular saying in the digital asset industry goes, “Not your keys, not your coins.” If you do not own the private keys to your assets, the assets do not truly belong to you.

No particular custody methods are totally risk free. With a diversification in custodial methods across different wallets, should a particular wallet or custodian be compromised, the risk is limited to just the assets held there. And a total obliteration of assets can be avoided.

Users should ensure that centralised custodians and self-custodial solutions have the necessary security certifications such as ISO 27001 and SOC2 and are audited to the highest security standards to be in compliance with the local jurisdiction requirements.

The Role of MPC Wallets in Digital Asset Security

Multi-party computation (MPC) wallets offer a robust solution to digital asset security and is widely considered the gold standard in institutional-grade security solutions. Unlike traditional wallets, which rely on a single private key, MPC wallets distribute the key among multiple parties. This means that even if one party is compromised, the assets remain secure. Decentralised key shard management are vital towards ensuring that there isn’t a single point of failure.



In addition, the MPC signing process is computed off-chain. When the protocol is jointly executed, all participating parties will get the same valid signature. No key shard will be exposed during the signing process. Through the entire lifecycle of the private key, it is never exposed or is visible on any physical devices which lowers the probability of it being compromised.

Furthermore, most MPC wallets offer the ability to set transactional policies where approval flows can be customised such that multiple parties are required to review and approve a transaction before it can be executed. No single party can unilaterally approve a transaction without going through a process of check and balance. This helps to strengthen good corporate governance and compliance.

Multi-Layer Security Strategy

As told in the famous Aesop's fable, a single stick is easy to break. But it is tough to break a bundle of sticks. Similarly, a single layer of security is often insufficient to counter sophisticated attacks. Having a multi-layer security strategy with a defence-in-depth approach helps increase the level of difficulty for an attack to take place.

Should the potential reward be not worth the effort and time required, it is unlikely that an attacker would be motivated to make a concerted attempt to steal.

For example, on top of having decentralised key shard management as highlighted earlier to mitigate the risk of a single point of failure on the private key, we could utilise Trusted Execution Environment (TEE) technology which is a secure area of a main processor to form an hardware isolation layer from the rest of the server. This setup guarantees confidentiality and integrity of code and important cryptographic data such as the private keys which are stored inside the secure enclave.

Recovery phrases which are important information that can be used to produce the private keys should be kept securely offline (e.g. security vault or safe deposit services) with strong access control in place.

Additionally, using security solutions like antivirus software, firewalls and VPNs can provide additional layers of protection to data stored on your devices or servers and to keep out inadvertent interactions with malware and trojans. There are also detection tools that are useful for warning users of possible interaction with phishing and known blacklisted websites as well as wallet addresses.

Smart Contract Risks

2022 was by far the record-breaking year in terms of hacks suffered by DeFi protocols which are powered by underlying smart contract codes. Users' assets are often locked into the smart contracts which function as repositories for these funds. Should the smart contract have a bug or vulnerability, losses can occur if they are exploited by attackers.

According to Chainalysis, a blockchain analytics firm, almost $4 billion worth of DeFi assets from bridges, lending contracts, decentralised exchanges and mining pools were stolen, with a vast majority by the attacks originating from state-sponsored actors from North Korea.

In the most recent case in July 2023, the Multi Chain bridge was attacked and suffered a loss in excess of $100M due to a compromised private key. Other common forms of attack vectors on smart contracts include access control exploit, re-entrancy and price oracle attack.

To mitigate risks associated with interactions with smart contracts, users should only use DeFi protocols that have been properly audited by a reputable 3rd party auditor to be in line with industry's best practices. Avoid putting in a significant amount of assets into a DeFi smart contract that has not been battle-tested and stood the test of time.

The Importance of Zero Trust Architecture

Zero Trust Architecture (ZTA) is a security concept that is centred on the approach of "don't trust, always verify", be it outside or inside the perimeters of the organisation. By default, users and devices should not be trusted, even if they are connected to a permissioned network.

In the same vein, it's critical that your custody solution or custodian employs a strong zero trust architecture with measures such as multi-factor authentication (e.g. using hardware tokens, biometric verification etc), remote attestation and What-You-See-Is-What-You-Sign (WYSIWYS) to minimise the attack surface and limit access to sensitive data.

When every step of the wallet and transaction management process is verified, this reduces the risk of malicious actions, thus enhancing security and reliability of the custody infrastructure.

The Security Mindset

Ultimately, the most important tool we have in our arsenal in our fight against security attacks is our security mindset. The digital asset space is revolutionary for bringing about greater ownership and control over one's assets. But with greater power of ownership comes greater responsibility too.

In line with the zero trust concept as highlighted, users should distrust by default. Verify everything such as accessing suspicious links or files from unknown users that come unsolicited. This is especially vital in light of social engineering scams that aim to manipulate you into revealing your credentials or inadvertently signing a transaction which may appear to be genuine.

Institutions themselves play an important role in educating their users in keeping abreast of the latest threats and counter-measures. Regularly conduct training and awareness exercises to prevent complacency from sinking in.

Staff are strongly advised to update their device's operating systems regularly so as to have the latest patches to mitigate against potential zero-day vulnerabilities. Staff have to also take ownership on practising good security hygiene in terms of regularly updating the system with strong passwords (with the help of tools like password managers) as well as reviewing permission and security settings of applications installed on devices to prevent data from inadvertently being leaked.

Summary

In conclusion, an implementation of a strong digital asset strategy for institutional assets involves having an in-depth understanding of threats, vulnerabilities and risk management. It's important to not just have a reliable custody solution and advanced security tools in place, adherence to best practices and having a proactive security mindset amongst users are critical too. Security is an on-going commitment for any institution and is a foundation upon which a sound business can be built on. We are only as strong as our weakest link and it is important to ensure we fortify every aspect of our infrastructure and systems to ensure the security of your assets.

Demystifying Cybersecurity: Identity and Access Management in Simple English

Article Contributed by:
By Daniel Chan, APP

Imagine you are the head of security at a large event. Your job is not just to keep the premises safe but also to ensure that only the right people have access to certain areas. Some may have VIP passes, others are staff, and then there are attendees. In the digital world, this process of identifying and granting access is what we call Identity and Access Management (IAM) - the fourth domain of the CISSP, and a crucial aspect of cybersecurity.

What is Identity and Access Management?
In simple terms, IAM is like the bouncer at a club. It decides who gets in (authentication), where they can go (authorization), and keeps a watchful eye on them (accountability). In cybersecurity, IAM serves to ensure that the right individuals access the appropriate resources at the right times for the right reasons.

Authentication: The Front Gate Check
Picture the process of entering a high-security building. You show your ID, maybe a fingerprint or a retina scan. In the digital world, this is authentication. It is how a system verifies if you are who you say you are. This can be something you know (like a password), something you have (like a security token), or something you are (like your fingerprint).

Authorization: The VIP Pass
Once you are authenticated, you need the right clearance. In our event analogy, think of authorization as different access levels - backstage, VIP area, general admission. In digital terms, this is about defining what an authenticated user is allowed to do in a system. Does this user have the authority to access certain files, make transactions, or change settings?

Accountability: Keeping an Eye on Things
Now, imagine you have a camera system in your event. It monitors where people go, ensuring they stick to areas they are allowed. In the digital realm, this is accountability. It ensures that all activities can be uniquely traced to a user, often through logs and audit trails.

Directory Services: The Digital Guest List
Imagine having a guest list that tells you who's who at your event. Directory Services in IAM is similar. Similar to a digital Rolodex, it can be likened to holding information about users, what they can access, and their roles. Microsoft's Active Directory is a common example, acting like a central database for user information.

Federated Identity Management: The Event Coalition
Sometimes, events collaborate. Attendees from one event may get access to another without additional checks. Federated Identity Management is similar – it is about trusting identities verified by another system. This method is often used in cloud computing, where services across different platforms trust each other's authentication.

Authentication Methods: More Than Just Passwords

We are all familiar with passwords, but in the world of cybersecurity, there is more. Think of a high-tech lock that opens with a code, a fingerprint, and a voice command. That's multi-factor authentication (MFA), combining something you know (password), something you have (a phone app), and something you are (biometric verification).

Real-World Example: A Breach in the Building

Let us consider a real-world scenario. A company faced a data breach because an employee's credentials were stolen. This is like someone stealing a VIP badge to access restricted areas. The company didn't have MFA, making it easy for the thief. This shows why multiple layers of authentication are crucial.

Why is IAM Important?

In our increasingly digital world, managing identities and access is vital. It is not just about keeping data secure but ensuring the right people have the access they need to work effectively. It is the foundation of a secure digital environment, like having a well-trained security team at your event.

Taking Practical Steps

For those in physical security looking to strengthen their cybersecurity knowledge, understanding IAM is a great start. You might consider:

- Participating in cybersecurity workshops
- Taking courses focusing on digital identity management
- Keeping abreast with the latest in authentication technologies

Conclusion

Identity and Access Management is the backbone of a secure digital environment. Just as a well-managed event ensures safety and enjoyment for all attendees, effective IAM ensures a secure, efficient digital workspace. As security practitioners, expanding our understanding of these digital concepts is not just beneficial; it is essential in our interconnected world.

Insider Threats: An Overview of Types, Motivations, and Mitigation Measures

Article Contributed by:
Perry Peter YEO, CPP

Shane is a HR professional, a rising talent in the company known for his initiatives and can-do attitude. Shane found a new artificial intelligence (AI) website tool online, claiming to be able to use company's personnel data to generate new insights to improve the company's manpower management. In the spirit of efficiency and improving the company, Shane uploads the entire company's personnel list onto the website. A few days later, this same data was found in the public domain. Would Shane be considered an insider? Could the company have mitigated this?

In today's evolving security landscape, companies face an expanding range of security threats. Among these dangers, insider threats stand out as one of the most insidious and difficult challenges to tackle. Unlike external threats, which originate from outside the company, insider threats rear their heads from within the company, from the trusted individuals that we let into the company. Whether you are new to insider risk or a seasoned specialist, let's journey through an overview of insider threats, the different forms it takes, and what companies can do to safeguard valuable assets from within.

What is an Insider threat?
An insider is any individual with privileged access to the company. This includes contractors, business partners, and even former employees. When an insider misuses this access given to them, they become an insider threat. This is regardless of intent or purpose. The potential damage an insider can cause is vast because of the privileged access and information they hold. The damage includes financial and reputational damage, data breaches and compromises of intellectual property. It is important to note that insider threats do not manifest only in the digital domain but in the physical domain as well. The convergence of physical and digital domains means that insider risk mitigation must be holistic in order to provide comprehensive protection from adversaries.

Types of Insider Threats
Insider threats fall into two categories, Malicious and Non-malicious.

Malicious insiders have the intent to harm the company using the privileged access given to them. So, what motivates a malicious insider? For this, we can use the espionage motivational framework of M.I.C.E.

M.I.C.E is a mnemonic device used to generalise the categories of which an individual is motivated to become an inside.

M stands for Money. These insiders are motivated by money to seek financial gain and will steal intellectual property or trade secrets to sell to competitors. They may also exploit financial loopholes within the company's governance system to gain personal financial benefits.

I stand for Ideology. These insiders are motivated by ideology and seek fulfilment in their ideological or political beliefs. They may sway agendas, affiliations, or beliefs in the company to direct more attention to their ideology.

C stands for Compromise. These are insiders that have either been blackmailed or have blackmailed people to betray the company. Often, these insiders have something to hide and are being exploited by their handlers. These include photos of affairs, addictions, or dark secrets.

E stands for Ego. These insiders are motivated by their bruised ego. These include disgruntlement, perceived prejudice against them, or wanting to prove their superiority.

Non-malicious insiders, on the other hand, did not intend to harm the company but did so anyway due to negligence or lack of awareness. Here are some types.

Lack of Knowledge. These insiders do not know that what they have done is damaging to the company. For example, staff may have no knowledge that conducting sensitive financial transactions on unsecured websites is dangerous. (e.g., HTTP) thereby exposing the company data to interception by cybercriminals.

Lack of Awareness. These insiders have the knowledge but fail to be aware of the situations to which it becomes relevant. For example, phishing emails. While we know how phishing emails look, in a moment of folly without checking, we may really think that our IT department urgently needs our password to perform maintenance.

Last but not least, ignorance. These insiders have the knowledge and awareness but choose to ignore them. This could be due to convenience or plain laziness. For example, the premise security guard failing to verify the photo on the security pass with the pass holder because it was not convenient to do so.

So, what can we do about it?
To mitigate insider threats effectively, companies must deploy a holistic strategy involving personnel, physical, technological, and procedural strategies. Some examples are:

1. **Pre-employment screening**: This is the first gate protecting the company. Vet potential employees with background checks and character references. This helps to validate the potential employees' claims and identify any concerning past behaviours.

2. **Access Control**: A robust and updated access control limits individuals from accessing areas and information that they do not need for their work. Keeping access privileges limited and up to date is critical to prevent unauthorised access, especially from employees that have left the company.

3. **Cybersecurity Measures**: Cybersecurity solutions play a critical role in mitigating insider risks. These include Endpoint Security, Data Loss Prevention, and User Behavior Analytics solutions.

4. **Physical Security Measures**: While physical security is never unbeatable, having a strong and robust physical security system will help deter potential insiders. These include Video Surveillance Systems, Security Passes, and Access Control. Physical Security and Cybersecurity must complement each other to ensure that vulnerabilities in both domains are adequately covered.

5. **Security Education and Awareness**: Educating and raising awareness of security threats is fundamental to creating a strong security culture. Some education and awareness efforts include posters, newsletters, incorporating a security module for new-joiners, involving staff in physical red-teaming, and conducting cybersecurity awareness sessions.

Conclusion
It is important to recognize and address malicious and non-malicious insider threats together and address them holistically across all domains. This is a complex and multifaceted topic that cannot be covered adequately in a short article. Nonetheless, I hope this article has provided some insights on the threat, how to identify it, and what you can start doing about it.

If you have any queries on insider threat or other human threat issues, do join the ASIS Human Threat Management (HTM) Community on ASIS CONNECTS and post your questions. We will be more than happy to engage on any human threat topics.

References
PA Consulting Group, & CPNI. (2012). Holistic Management of Employee Risk (HoMER). London; PA Consulting Group and CPNI.

A Buyer's Perspective on Outcome-Based Security Contracting

Article Contributed by:
Azril Ngasiran, CPP

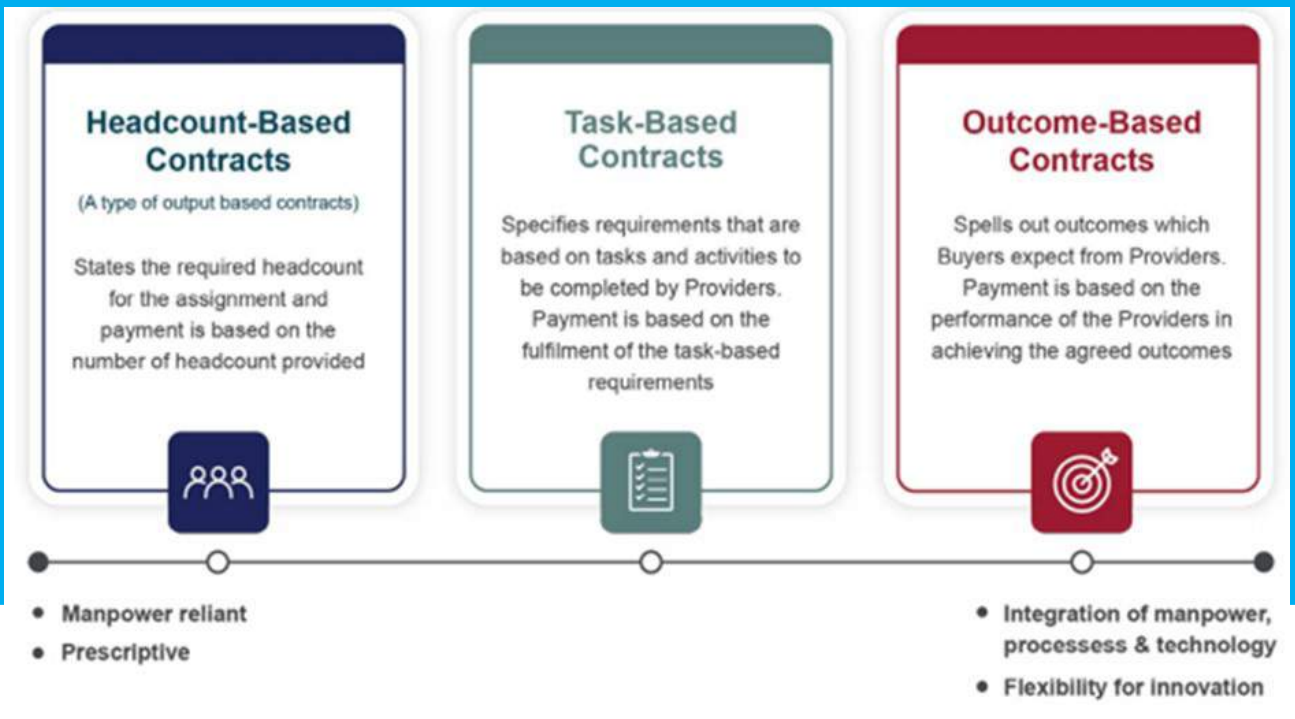
When overseeing security operations, the regular procurement of security services is a familiar task. Traditionally, acquiring security services involved determining the necessary headcounts based on expert judgement of security operations and effective practices.

The emergence of Outcome Based Contracting (OBC) has shifted this paradigm from specifying headcounts to outlining desired outcomes. This shift aligns with the Ministry of Home Affairs' (MHA) Security Industry Transformation Map (SITM), aiming to promote best procurement practices by reducing reliance on manpower and leverage on technology. As service buyers, this shift enables us to manage escalating security service costs resulting from the Progressive Wage Model implementation.

Despite the advantages, implementing OBC may leave service buyers uncertain about success metrics. It's tempting to revert to specifying headcounts for reassurance. When we had to implement OBC for the Central Provident Fund Board (CPFB) in 2019, insights from Jurong Town Corporation (JTC), the Ministry of Manpower, and other Government Procuring Entities (GPE) proved valuable. We referenced MHA's first edition OBC guide, building our approach.

Listing Outcomes instead of Headcounts
Traditionally, Requirement Specifications detailed specific patrols by a set number of officers at designated intervals. With OBC, our specifications shifted to listing desired outcomes, like surveillance during silent hours. This approach empowers service providers to offer blended solutions incorporating manpower and technology to consistently meet outcomes. Concerns arose for key posts like Fire Command Centers requiring 24/7 manning. To address this, we identified critical duty posts that must remain manned, serving as a baseline guide for service providers.

Performance-based payments
A tiered payment approach linked to performance metrics was adopted, ensuring payments aligned with monthly evaluations. To allow the awarded service provider time to settle in, we assured 100% payment for the first 6 months. This "honeymoon period" allowed for a period of adjustment and familiarisation, empowering the team to transition smoothly and make any necessary recalibrations of their proposal with a sense of security.



Ensuring Continuous Productivity Enhancement

To foster ongoing productivity improvement, contracts with an annual value surpassing $1 million should span a minimum of five years. This extended duration provides service providers with the opportunity to amortise the implemented technology effectively. We mandated one productivity enhancement initiative per contract year, with savings fully awarded to the service provider. This incentivises risk-taking in reducing headcount, while maintaining the flexibility to revert to manpower if needed. The strategic advantage for us lay in the ability to experiment with a lower headcount in subsequent contracts, utilising the current contract as a valuable testing ground for innovations and optimisations.

Quality-focused Evaluation

Defining the requirements marks just the initial phase of the procurement process. Regardless

of the chosen procurement method, the pivotal factor in the success of Outcome Based Contracting (OBC) lies in the comprehensive evaluation of proposals. Recognizing this, we adopted a weighted assessment heavily leaning towards Quality. Our aim was for tenderers to exhibit a profound understanding of OBC, thereby enhancing the likelihood of success. As an evaluative proxy, we meticulously examined:

- The operations plan, scrutinising how their proposal aligns with stipulated outcomes;
- A comprehensive assessment of their understanding of our security environment, conducted through a rigorous Security Risk Assessment;
- Evaluation of frameworks pertaining to continuous improvement and service delivery;
- An appraisal of their track records in executing Outcome Based Contracts (OBC).

The intricacies of each proposal underwent rigorous scrutiny, supplemented by rounds of interviews to ensure tenderers grasped the full scope of their impending commitments. This scrutiny extended to operations plans, relief management strategies, and interviews with key personnel to ensure alignment with our organisational cultural attributes.

Co-creating Innovative Solutions

Upon contract commencement, the implementation of the new Outcome Based Contracting (OBC) approach afforded us a valuable opportunity to reassess our security operations. As a progressive service buyer, an essential practice is adopting a collaborative approach with the service provider to co-create solutions. This new dynamic often results in the service provider suggesting workarounds, technological innovations, or providing insightful feedback on assessed areas. Approaching each proposal with an open mind facilitates a smoother journey, and acknowledges the merits of diverse ideas. It requires placing trust in the expertise of the service provider and allowing them the creative space to propose strategies for reducing headcount and implement technologies, always subject to the final approval of the service buyer. This collaboration not only enhances the partnership but also fosters an environment where innovative solutions can flourish.

Conclusion

The transition from conventional practices to embracing the service provider's proposed solutions in Outcome Based Contracting (OBC) necessitates a profound shift in mindset. This transformation redirects the focus from meticulously accounting for every headcount to placing trust in the service provider's ability to achieve stipulated outcomes through their proposed solutions. This underscores the pivotal importance of conducting a thorough evaluation of the awarded service provider, scrutinising the completeness of their proposed solution and assessing their capabilities.

By sharing a buyer's perspective on OBC, our intent is to assuage concerns and contribute to the broader dialogue on progressive procurement practices. It's heartening to witness the increased adoption of OBC by more service buyers, and with an increasing array of success stories and resources, we extend our best wishes to all those embarking on the journey toward becoming progressive service buyers.

Annual General Meeting 2023

Article Contributed by:
Sujoy Dutta, CPP

It's my first year being part of the ASIS Singapore Chapter Annual General Meeting (AGM) as Hon. Secretary, and oh boy, what great experience it was. It was an honour for me to stand before the members along with our Chairperson and Treasurer to run the AGM.

Over the past year, my role as Hon. Secretary has afforded me the privilege of witnessing firsthand the dedication and hard work of our members and the management committee. Their commitment in advancing the mission of ASIS Singapore has been nothing short of inspiring.

As Hwee Fong Yong, APP, shared the Chairperson's report it raises goose bumps to see how far ASIS Singapore Chapter has come over the years and developed itself to be a truly professional security platform providing growth and learning opportunities for its members. 2023 has been a busy year for us, we tried to maintain our standard events and services in terms of Networking dinners, Field Visits and Professional Development courses while at the same time exploring new horizons in signing of MOUs with SAS and A-CERTS, winning the Chapter Communication award and breaking ground with student membership.

Special call out goes to Women-In- Security (WIS) group this year which started with a mere 4 members in 2021 and grew strong to 25 strong this year, arranging its own networking and educational events for its members.

ASIS Singapore Chapter ideated a concept to build communities for professionals with common interests and provide a platform to share and learn from each other. This led to the formation of the Special Interest Group (SIG) this year. The Special Interest Group was formed in two different domains of Security Operations and Intelligence Analysis.

Edison Koh, our Hon. Treasurer shared the finances of the chapter with its members. It feels good to see we have a strong foundation to move forward in the coming times.

The AGM concluded with the appointment of Aloysius Tan Kim Heng and Eric Lim Thian Beng as Internal Auditors (IA) for 2024.

In closing, I would like to express my gratitude to each member for their contributions, commitment, and dedication. It has been a great opportunity for me to join the ASIS community and together, let us continue to strengthen the bonds that make ASIS Singapore Chapter a thriving community of security professionals.

Q4 Networking Dinner

Article Contributed by:
Collin Chew, Student Member

The ASIS Q4 Dinner started with the chapter signing Memorandums of Understandings (MOU) with Security Association Singapore (SAS) and Association of Companies Emergency Response Teams (A-CERTS). The MOUs form a tripartite that holistically covers the security industry, with the expertise of industry leaders from ASIS and the policies, training, certifications and industry standards of SAS and A-CERTS.

Following the signings, Mr Raj Joshua Thomas shared on the Progressive Wage Model for the industry and its shift towards outcome-based contracting. He also touched on the new minimum wages for security officers, which will be taking effect next year. As the pool of security officers decreases and the cost of labour increases, Mr Thomas further shared how companies can adopt technologies like surveillance systems to help meet their security outcomes.

The evening's sponsor, HID, introduced the use of mobile phones as credentials and being integrated into the access control systems, allowing users to access doors, computer systems, and more through user devices. Leveraging on Bluetooth and NFC technology, the system eliminates the need to issue physical credentials, saving companies time and cost. It also reduces the likelihood of an employee losing their credentials.

Next, the ASIS NextGen Team, composed of students from the Public Safety and Security (PSS) programme at the Singapore University of Social Sciences (SUSS) shared on their upcoming SUSS Career Fair, happening on 23rd January 2024. The fair aims to connect students to organisations and hopes to provide internships and full-time career opportunities.

Since joining ASIS NextGen, I've always looked forward to the quarterly ASIS Networking Dinners as I get to broaden my exposure to new areas of the security industry through the sharings and networking with the industry leaders there. It has been a wonderful experience and I look forward to attending more local chapter events in the coming year!

Open More

with HID Mobile Access®

Open More with HID Mobile Access by using your smartphone or wearable as a credential to access doors, networks, services and more. From banking and finance, educational institutions, global corporate entities and more - we provide the solutions for a mobile-first world, giving you unrivaled convenience, enhanced security and privacy protection, and operational efficiency.

hidglobal.com

Calendar of Events

Field Visit to NUS Campus

The chapter will be organising a field visit to NUS Campus on first quarter of 2024

Please stay tuned to our boardcast over email or visit our ASIS Singapore website.

Q1 Networking Dinner and Lou Hei 2024

Q1 Networking Dinner and Lou Hei 2024 will be held on Feb 2024.

Please stay tuned to our boardcast over email or visit our ASIS Singapore website.

Members' Update

Warm Greetings to the following new ASIS International Singapore Chapter Members!

Mr	Ankit Bhatia		Mr	Patrick Tse	CPP
Mr	Lim Jianhong		Mr	Philip Siow	
Mr	Kayden Kho		Mr	Richard Chan	
Mr	Nathan Masters		Mr	Tan Wen Cheong Kenray	

Congratulation to Newly Certified Members!

Newly Attained CPP

Mr	David Kaye	CPP

Newly Attained APP

Ms	Lim Yan Ling	APP

Members' Update

Certified ASIS International Members

Certified CPP, PSP, PCI members

Mr	Adrian Wong Voon-Ming	CPP, PCI, PSP	Mr	Peter Tan	CPP, PCI, PSP
Mr	Colin J Spring	CPP, PCI, PSP	Mr	Quek Wei Chew	CPP, PCI, PSP
Mr	Jag Foo	CPP, PCI, PSP	Mr	Rajesh	CPP, PCI, PSP
Mr	Koh Shi Sheng	CPP, PCI, PSP	Mr	Shamus Yeo See Yew	CPP, PCI, PSP
Mr	Melvin Pang-Boon-Choon	CPP, PCI, PSP	Mr	Stefan Shih	CPP, PCI, PSP
Mr	Pandian Govindan	CPP, PCI, PSP			

Certified CPP, PSP members

Mr	Abdul Razak Daseran	CPP, PSP	Mr	Melvin Cheng Tze-Hui	CPP, PSP
Mr	Chua Boon-Hwee	CPP, PSP	Mr	Peter Ang Boon Kiat	CPP, PSP
Mr	Eddie Koh	CPP, PSP	Mr	Tan Wee Hock	CPP, PSP
Mr	Ian D Milne	CPP, PSP	Mr	Teo Jon Sheng Johnson	CPP, PSP
Mr	Kagan Gan	CPP, PSP	Mr	Willie Heng Chin-Siong	CPP, PSP
Ms	Kee Ling Min	CPP, PSP	Mr	Xiao Gaoping	CPP, PSP
Mr	Kenneth Lau Yip Choy	CPP, PSP	Mr	Yuen Kin Wai (Dex)	CPP, PSP
Mr	Lee Choon-Wai Anthony	CPP, PSP			

Certified CPP members

Mr	Abdul Redha Bin Abdullah	CPP	Mr	David Kaye	CPP
Mr	Alfian Idris	CPP	Mr	Den Ho Kai-Quan	CPP
Mr	Andrew Fan Tuck-Chee	CPP	Mr	Desmond Ho Kok Tong	CPP
Mr	Anton Chan	CPP	Mr	Dicky Fadly Zaini	CPP
Mr	Azharie B Mohamed Mudakir	CPP	Mr	Edmund Lam	CPP
Mr	Azril Ngasiran	CPP	Mr	Edwin Goh	CPP
Mr	Balasubramaniam Selvam	CPP	Mr	Fabrice Marty	CPP
Ms	Beverly F Roach	CPP	Mr	Firman Latib	CPP
Ms	Cheng Yen Hwa	CPP	Ms	Foong Yi Ling	CPP
Mr	Chia Wai Mun	CPP	Mr	Gan Da	CPP
Mr	Ching Chiu Chiu	CPP	Mr	Glen Martin Balde Arquiza	CPP
Mr	Clement Chan	CPP	Mr	Glenn Koh	CPP
Mr	Damien Lim	CPP	Mr	Hartmut Kraft	CPP
Mr	Daniel Ng	CPP	Mr	Ho Jiann Liang	CPP

Members' Update

Certified ASIS International Members

Certified CPP members

Mr	Isaach Choong	CPP
Mr	James Hammond	CPP
Mr	James Wong Li Ren	CPP
Mr	Jarrod James Nair	CPP
Mr	Jeffrey Yeo	CPP
Mr	JK Wong	CPP
Mr	Jonathan Yap	CPP
Mr	Joseph F. Jasunas	CPP
Mr	Julian Tan	CPP
Mr	Justin Chen Jianan	CPP
Mr	Kan Young Loong	CPP
Ms	Karen Wong	CPP
Mr	Kelvin Koh	CPP
Mr	Ken Ang	CPP
Mr	Ken Tong	CPP
Mr	Koh Kwang Wee	CPP
Mr	Krishnamoorthy Arunasalam	CPP
Mr	Lai Zihui	CPP
Mr	Law Chee Keong	CPP
Mr	Lawrence Tan Jun-Ming	CPP
Mr	Leonard Ong	CPP
Mr	Leong Hoe Meng	CPP
Mr	Leong Keng Weng	CPP
Mr	Lim Choon Kwang	CPP
Mr	Lim Chye Heng	CPP
Mr	Lim Teong Lye	CPP
Mr	Lim Thian Beng	CPP
Mr	Look Kang Yong	CPP
Mr	Lye Kah Meng Joseph	CPP
Mr	Magalingam Veeman	CPP
Mr	Marcus Tan ChongLay	CPP
Mr	Mark Chow	CPP
Mr	Mark Nuttall	CPP
Mr	Mitran Balakrishnan	CPP
Mr	Muhammad Hafiz Bin Rohani	CPP
Mr	Muhammad Iskandar Bin Idris	CPP
Mr	Muhammad Zahed Zulkeplee	CPP
Mr	Muhsin Ben Moasi	CPP
Mr	Nilo S Pomaloy	CPP
Mr	Noriman Salim	CPP
Mr	Ong Kim Poh	CPP
Mr	Pang Jing Chyi	CPP
Mr	Paul Rachmadi	CPP
Mr	Perry Peter Yeo	CPP
Mr	Ramani Matthew Sachi	CPP
Mr	Ren Huajun	CPP
Mr	Richard Goh	CPP
Mr	Rick Wong Soon Wah	CPP
Mr	Sachin Kumar Sharma	CPP
Mr	Sam Wai Peng	CPP
Mr	Sanjay Sharma	CPP
Mr	Shaymentyran Shaem	CPP
Mr	Sheo Boon Chew Winson	CPP
Mr	Sia Wang Ting	CPP
Mr	Simon Tan Eng-hu	CPP
Mr	Soon Koh Wei	CPP
Mr	Stanley Aloysius	CPP
Mr	Sujoy Dutta	CPP
Mr	Surendran Chandra Segaran	CPP
Mr	Taaouicha Mujahid	CPP
Ms	Tam Yuen Yee Jeannie	CPP
Mr	Tan Gwee Khiang	CPP
Mr	Tan Hock Seng	CPP
Mr	Tan Kok Soon	CPP
Mr	Tay Choon Teck	CPP
Mr	Teo Kee Kiat	CPP
Mr	Teo Khai Ming	CPP
Mr	Thirukumaran Sankaran	CPP
Mr	Tony Er	CPP
Mr	Vincent Soh Chee Yong	CPP
Mr	Wayne G Edmonds	CPP
Mr	William Toh	CPP
Mr	Wilson Loh	CPP
Mr	Yeh Ing Kerne	CPP
Mr	Zhou Qinhui	CPP

Members' Update

Certified ASIS International Members

Certified PSP members

Mr	Dion Yeo Lai Ye	PSP	Mr	Low Kay Boon	PSP
Mr	Jeffrey Lam Boon Kee	PSP	Mr	Mayank Sinha	PSP
Mr	Kamlesh Gope Ramchand	PSP	Mr	Soh Wei Jye	PSP
Mr	Kevin Loh	PSP	Mr	Stanley, Tse Chi-Fung	PSP
Mr	Lee Huan Chiang	PSP	Mr	Wee Ting-Jin	PSP

Certified APP members

Mr	Daniel Chan	APP	Mr	Koh Jian Hao	APP
Mr	Eugene Chua	APP	Ms	Lim Yan Ling	APP
Mr	Faizul Salamon	APP	Mr	Ong Poh Tiong	APP
Mr	Francis Zhang	APP	Mr	Soo Wei Lun	APP
Mr	Goh Kwan Way Marc	APP	Ms	Yong Hwee-Fong	APP
Mr	Jason Siow	APP			

Editorial Team

Eddie Koh, CPP, PSP
Editor

Monica Tomer
Editor

Yong Hwee Fong, APP
Contributor

Sujoy Dutta, CPP
Contributor

Chow Keng Fong
Contributor

Lim Choon Kwang, CPP
Contributor

Jag Foo, CPP, PCI, PSP
Contributor

Daniel Chan, APP
Contributor

Perry Yeo, CPP
Contributor

Azril Ngasiran, CPP
Contributor

Collin Chew
Contributor

Calling for Articles

Share your experience and knowledge now and earn up to 9 CPE points

Article should not contain more than 1,000 words in words document with illustrations, diagrams,and/or photos.

We are seeking articles of interest from all members, which may relate to terrorism, physical security, executive protection, investigations, product counterfeiting, supply chain security, crisis management or business continuity management. Articles may relate to current or emerging issues, best practices or challenges faced by security professionals responsible for the protection of people, property, and information in their organisations.

This will be a valuable platform to share your knowledge with fellow Chapter members. CPP/PSP/PCI/APP board-certifi ed members will also be pleased to note that published articles may earn up to 9 CPE credits in recertification.

Interested please email us at memberservices@asis-singapore.org.sg
Submission close on 1 Mar 2024

Management Committee 2023-2024

Honorary Chairperson
Ms. Yong Hwee Fong, APP

Honorary Vice-Chairperson
Mr. Jeffrey Lam, PSP

Honorary Secretary
Mr. Sujoy Dutta, CPP

Honorary Asst. Secretary
Mr. Collin Goh

Honorary Treasurer
Mr. Edison Koh, CPP, PSP, PCI

Honorary Asst. Treasurer
Mr. Lim Chye Heng, CPP

Honorary MC Members
Mr. Anthony Lee, CPP, PSP
Ms. Marie-Helene Mansard
Mr. Mitesh Shah
Mr. Jarrod James Nair, CPP
Mr. Matthew Lee
Mr. Simon Tan, CPP

Registered Mailling Address:
ASIS International (Singapore Chapter)
5 Temasek Boulevard, Suntec Office Tower 5, #17-01, Singapore 038985

Website: www.asis-singapore.org.sg

Email: memberservices@asis-singapore.org.sg