OMNIRISC
REDEFINING SECURITY

Security Newsletter

JAN 2018 I ISSUE 5

Welcome to the January 2018 edition of the OMNIRISC Security Newsletter where we continue to examine items of interest to the security industry in Macau and security issues elsewhere.

We would like to take this opportunity to wish our readers all the best for a successful, safe and secure 2018.

What we can do to help you

We believe that by being risk conscious and developing a culture of security awareness, we can provide better protection for an organization's people, assets and key infrastructure. To effectively address this issue, OMNIRISC has invested in developing its people in Security Risk Management culture as a focus for operational strategy and risk interventions. We provide bespoke consultations for businesses and organizations on various levels of vulnerability and risk assessments.

About the Author

James Langton is an advisor to "OMNIRISC" with over 40 years of experience in the security and law enforcement industries.

Last year we examined the topics of risk, crisis, hazard, getting ready to deal with emergencies and the relation of these topics to business continuity and resilience. In this issue we will examine the topic of security audits and assessments.

The questions we should be asking about our current security operations should be: Are our security systems and procedures up-to-date? Are they fit for purpose? Are they providing maximum value for investment? And are they adding to and securing the profitability of our businesses? These questions can be answered by conducting effective security audits and assessments.

Throughout 2018, we will examine topics relating to security processes and ways to more effectively provide security services. If you have any areas that you would like to see covered, please let us know and we will try to include them in later issues.

Security News

Macau: Police hunt for $HK 48 million in stolen gambling chips.

Macau police are investigating the theft of $HK48 million in gambling chips from Wynn Casino in Macau. Suspect was said to have worked as a security guard when he joined the casino in 2009 and became a croupier in 2011. It is believed the suspect may be familiar with the control procedures and vulnerabilities who managed to walked away with a loaded cash chips into the bag before leaving the entertainment venue. Two arrests have been made so far and the investigation is continuing.

United States: Hotel Security Changes.

Some hotels in the US are reported to be in the process of eliminating 'Do Not Disturb' signs as part of new security procedures. Instead, they will be replaced with a policy that will require employees to enter each hotel room at least once a day to "ensure guest safety."

Italy: Thieves Steal Qatari Jewels in Brazen Theft at Ducal Palace in Venice.

On the 3rd January at around 10 a.m. at least two thieves disarmed what was purported to be a sophisticated security system and in plain view of closed-circuit cameras one opened the case while the other acted as lookout before disappearing with the jewels into the mass of tourists who daily take over St. Mark's Square. The thieves most likely studied the security measures at the museum before they struck, according to a Venetian police official. New York Times

OMNIRISC SECURITY SERVICE (MACAO) LTD. 26 Avenida De Marciano Baptista, Chong Fok Comercial Centre, 12/H, Macau
Office: +853 28558964 Email: info@omnirisc.com
www.omnirisc.com

Security Audits and Assessments

As we know, the security industry does not exist in a one size fits all environment. All organizations differ in their structures, complexities and security requirements.

These can vary from small single offices with minimal access and security needs to much larger and more complex organizations and facilities with a multitude of security requirements and challenges.

The complexity of the required level of security services also depends on what it is designed to protect. What are the particular vulnerabilities and threats associated with the protected facilities and its contents? Are your security processes keeping pace with current the security risks you face and the development of your business?

We also live in a complex business environment where organizations regularly expand, merge or are taken over by others. This leads to the adoption, combination and restructuring of multiple security systems. With these ever-changing security needs and requirements, how do we know whether our current security systems and procedures are up to date and good enough? How do we know that we are receiving the best value for money from our security processes?

We can answer these questions by conducting effective security audits and assessments (SAAs), a process that can provide a review of the current state of our safety and security programs. So what is an effective SAA? What does it examine? What can it provide?

What can a SAA provide for you?

An effective SAA can provide you with assurance that your security processes are up to date and that they fulfill your organizations stated security objectives. Alternatively, it can provide you with Information that identifies any issues, gaps or vulnerabilities in your security matrix.

It may also satisfy any regulatory or organizational requirement that requires that security auditing be conducted.

What will an SAA Examine?

An effective security audit and assessment can examine some or all of the following:

- Your current vulnerabilities and threats.
- Any previous historical security incidents affecting your organization or your stakeholders or affecting similar organizations globally.
- Any laws, regulations or statutes affecting your particular organization.
- Your current security and safety plans and procedures.
- Security and Safety plans of your key stakeholders.
- The external physical security arrangements for your facility. Including physical barriers, doors, locks, lighting and surveillance.
- Manned guarding, perimeter and internal patrolling.
- Vehicular and pedestrian access control and equipment. Visitor access control procedures.
- Internal security processes for more sensitive areas within the organization.
- Information security processes (not IT)
- Intellectual property protection.
- Key staff protection. Personal security protection.
- Incident response and management.
- Emergency Plans, Fire, Bomb Threat etc
- Evacuation Management.
- CCTV monitoring and control room procedures.
- Security investigations. Inventory security. Staff misconduct.
- Security training and awareness.
- Any other areas that senior management are particularly concerned about.

Internal or External Audits?

There are a number of pros and cons regarding whether or not to conduct an internal or external audit and assessment.

Internal audits are conducted by your own security department which has the advantage of having an intimate knowledge of its own security processes and procedures. There is always a question as to whether the security department has the time and capacity to conduct an audit while dealing with normal day-to-day operations. Experience has also shown that internal audits sometimes have a tendency to just tick the box or accept the status quo as good enough.

External audits have a number of advantages. They are independent and therefore have the ability to examine current practices and processes without operational or organizational bias. They have the time to concentrate on the project without having to deal with daily operational pressures. They bring backgrounds and experiences from a number of outside sources including the experience of the audit personnel themselves and the advantage they have of observing numerous security operations in a wide range of industries.

Security audits and assessments are vital tools in ensuring that security operations, processes and procedures are at optimum levels. Whether you chose an internal SAA or an external SAA depends on whether you want to think inside the box or outside the box. Many organizations choose to utilize a combination of both.

OMNIRISC
REDEFINING SECURITY

Office: +853 28558964 Email: info@omnirisc.com
www.omnirisc.com