

TABLE OF CONTENTS

Article: Executive Protection	1
Article: Data Audit & Policy Enforcement	1
Chairman's Message	2
ASIS New Online Membership Directory	3
Notice on CPP, PSP & PCI Examinations in Nov 2008	4
Photographs: ASIS Singapore participates in ASIS International Asia Pacific Conference 2008	5
Photographs: ASIS Singapore Q1 Chapter Meeting	5
Top 10 Reasons to be a CPP	6

ARTICLE SUBMISSION

Do you have an interesting article that you wish to share it with our members? Please email your article and write to the editorial management committee at newsletter@asis-singapore.org.sg

The Security Professional MICA(P) No. 135/03/2008 is published and distributed by the ASIS International (Singapore Chapter).

While every care has been taken to ensure that all information in this newsletter is accurate, the publisher cannot accept and hereby disclaims any liabilities to any party caused by errors or omissions resulting from negligence, accident or any other cause. Statement of facts and opinion are made on the responsibility of authors alone and do not imply an opinion on the part of the editorial management committee or members of ASIS International (Singapore Chapter). The editorial management committee reserve the rights to accept or reject any article submitted for the newsletter.

Editorial Management Committee: ASIS International (Singapore Chapter). Our mailing address is located at: No. 14, Robinson Road, #13-00, Far East Finance Building, Singapore 048545. Email: newsletter@asis-singapore.org.sg.

The ASIS International Logo, CPP™, PSP™ & PCI™ are registered trademarks of ASIS International.

EXECUTIVE PROTECTION

by Leslie Teo

With Singapore's efforts in becoming an international business hub as well as a tourist destination, the island state has become more prominent on the world map. Our future casinos in the IR (Integrated Resort) coupled with several international conferences and high profile events such as the F1 Race and Youth Olympic will attract more VVIPs, high profile personalities as well as high rollers into Singapore. Amidst the backdrop of increasing terrorist activities in South East Asia region, it is predictable that there will be a strong growing demand for Executive Protection service in Singapore.



Executive protection in action, an escorted motorcade (Photo provided by Leslie Teo)

Though Executive Protection (EP) for the private client is similar in concepts when compared to VIP Protection for political figures such as Presidents and Prime Ministers, etc; the execution of EP is more covert and requires one to be more resourceful. Apart from ensuring the safety and security of the client, EP focuses much on value-added services to the client's personal needs and pre-empting (with very little lead time) the principal's next move. This is because there are more impromptu private functions and networking activities for a private client as compared to a Head of State or Government official where almost every event and the principal's movement is mapped out and pre-planned weeks, or sometimes even months, ahead.

Having served two political leaders as the In-Charge of their security details for the past decade, and participated in an Executive Protection operation for a bank Chairman and CEO, I have had the

Continued at page 2

DATA AUDIT & POLICY ENFORCEMENT

by Darren Cerasi

Introduction

In a knowledge-based economy, a business is its data – whether it is customer, employee, product or financial data. Own the data and you own the business.

In an environment full of security threats and compliance requirements, organisations have to go beyond securing their data; they have to continually monitor it by performing a comprehensive data audit followed by policy enforcement.

A data audit can detect unauthorised access to data, prove compliance with organisational policies and improve business processes. Policy enforcement allows organisations to erase any non-compliant data through remediation steps once it has been detected through the audit process.

Data at Risk

Organisations are completely reliant on their data; it is a critical corporate asset and needs to be treated as such. If it is not protected, organisations risk the consequences of non-compliance with legislation which can cost a company its reputation and profits.

The Data Challenge

Due to the ever decreasing cost of storage, data is growing at an incredible rate. Standard laptops

Continued at page 3

Chairman's Message



Dear ASIS Members,

In the heightened security environment of the 21st century, it is ever more important for us all in the security industry to upgrade our professional security skills, keep abreast of security technology, and to remain relevant and effective to deal with evolving security threats and risks. As a leading proactive society, ASIS International has developed its "Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management and Disaster Recovery". More recently, ASIS also contributed to the creation of a voluntary preparedness standards program. Four professional associations: the ASIS, DRII, RIMS, NFPA identified the best practice to comply with the US laws, and their final reports included cross references to other important standards like the ISO/PAS 22399, BS25999, Singapore's TR19:2005 Framework against the US Framework for Voluntary Preparedness etc.

In the first half of this year, ASIS Singapore Chapter presented security practitioners with several good opportunities for professional development. First and foremost, we hosted the Certified Protection Professional[®] (CPP[™]) and Physical Security Professional[®] (PSP[™]) examinations in Singapore. In all, 16 candidates from South East Asia took the ASIS certification exams on 3 May in Singapore. Besides our ever popular CPP Review program held on 28 April to 2 May, our Chapter also successfully organised and conducted the debut PSP Review program on 29 to 30 April. Feedback from course participants for both these certification review programs was very positive and encouraging.

Our Chapter certainly looks forward to hosting the Professional Certified Investigator[®] (PCI[™]) examinations, in

addition to the CPP and PSP exams, on 1 November. We are honoured and proud to announce that our Chapter is the first in Asia Pacific to sponsor the PCI exams in the region. With the PCI certification examinations soon to be available locally, we encourage all interested security practitioners who specialise in investigations to prepare themselves and take up this golden opportunity to be Board certified. Going forward, more security training programs will be offered by our Chapter so that security practitioners can further hone their skills in security management and/or specialised domains, and continue to raise the bar of security professionalism.

On the academic arena, our Professional Diploma in Security Management course, which is jointly awarded by SMA School of Management (SOM) and ASIS Singapore, has proven itself to be a high quality program over time. Students from the 6th Intake of this program have recently graduated in June, and some past graduates have moved on in their careers for the better. As ASIS Singapore members, all of us will enjoy special discounts off the course fees for programs organised by SOM, and our Chapter. Do ensure that you produce your ASIS membership card during registration to enjoy the privilege.

On 27 March, we had a fabulous Chapter Meeting of sixty-over members and guests at The Legends Fort Canning. During the meeting, our members gained security technology insights from a professional presentation on "Meeting Operational Requirements for CCTV System" by 3Si Pte Ltd, a security specialist firm. Besides security networking, our members also enjoyed a sumptuous buffet dinner that evening. We look forward to your participation in our Chapter networking events which are free for all members of ASIS Singapore.

Till we meet,

Anthony Lee, CPP, CBCP
Honorary Chairman
ASIS International
Singapore Chapter

Continued from page 1

privilege of appreciating the two different perspectives of personal security operations. In a security operation for the Head of State/Government, security is rarely compromised and requests for full cooperation from event organizers on access control and security arrangement can be easily expected, and in some cases, even demanded. Resources for security bomb sweeps and advance security deployment are always part of the SOP and access into function venues can easily be sealed and the venue kept 'sterile' with screening checkpoints.

For Executive Protection of a private client, the strategy has to be craftier and constructive. If a client attending a high-risk event is a 'soft' target and certain precautions have to be taken, any request for special security arrangement with the event organizer or site manager has to go through skillful diplomatic negotiations and persuasions. Any attempt that may cause inconvenience to the client or affect the business of the establishment is likely to raise eyebrows. In addition, security is often a cost to the business organizations and any security recommendation is a subject of contention and balancing between risk management and cost management which has to be carefully weighed.

About the author: Leslie Teo is currently an Assistant Vice President in the Corporate Security (based in Singapore) of a US investment bank. An ex-Assistant Superintendent of Police in a VIP protection unit, Leslie has several years of experience in Executive Protection operations. He last served in Criminal Investigation Department before leaving the Singapore Police Force early this year to join the financial institution.

Continued from page 1

come with 160GB hard drives and network-attached storage solutions with terabytes of storage can be purchased for just a few hundred dollars.

The sheer volume of data and locations where it can be stored creates an interesting question, how can an organisation protect and manage its data if it doesn't even know where it is?

Add insider and external threats plus regulatory compliance requirements and it is no wonder that organisations are actively looking at solutions to proactively protect their data.

Data Lifecycle

Data should be protected throughout its lifecycle which includes three stages:

1. **Data at Rest** includes data on desktops, laptops, file and email servers plus other storage media. Scanning these data repositories is called *content discovery* which can identify documents with confidential data on systems where it should not reside.
2. **Data in Motion** is the monitoring of network traffic to identify data being sent across specific communications channels such as email and instant messaging.
3. **Data in Use** is typically addressed by endpoint security solutions that monitor data as the user interacts with it. These solutions can identify when a user attempts to transfer a sensitive document to a USB drive and block that action.

Data Audit

Organisations are defined by their data and by implementing a data audit process, risk can be largely reduced.

Data audit should be an integral part of operations as it enables an organisation to identify who created, changed, deleted or accessed data – when and how. Not only does it augment rigorous perimeter security by actively logging access to data, it also provides invaluable protection inside the perimeter which is where organisations are more vulnerable. *The very existence of data audit capabilities can have a strong deterrent on the insider threat.*

Organisations no longer operate in silos and must collaborate with their partners and customer in order to thrive. It is common for companies to enter into outsourcing contracts or joint ventures during which confidential data such as product plans and designs are shared. Once the contract has ended or the joint venture has reached its course, a proactive data audit of the partner's network would reduce any potential leakage of data and negate any impact on the organisation.

Data audit can also provide a framework for regulatory compliance and document retention policies, ensuring that data is appropriately monitored and that breaches are reported. Adding data audit to strong policy enforcement protects an organisation much more thoroughly than policy and security alone.

As the need for audit continues to increase, the cost of manual audit outweighs its benefit. Centrally managing and automating the data audit process is a more effective and efficient way to operate.

Policy Enforcement

Once a policy violation is discovered, a number of actions can be taken:

1. **Report** - create an incident for investigation or escalation to the appropriate level.
2. **Warn** - notify the user that they may be in violation of policy.

3. **Restrict** - change access control to restrict access to the file.
4. **Quarantine** - move the file to a secure server and create a recovery request.
5. **Remediate** - erase the file completely from the computer system.

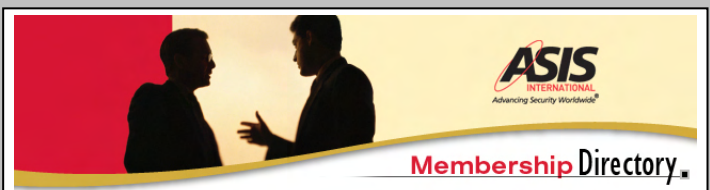
A combination of different policy enforcement options creates a powerful capability for protecting data and supporting the organisation's initiatives.

Data Audit and Policy Enforcement Framework

Auditing an organisation's data and enforcing policies should be approached in a methodical manner and broken down into distinct parts in order to ensure its success.

- Separation of Responsibilities. The audit team must be a distinct entity to avoid possible conflict of interest. This "separation of duty" is a key principle of information security and is used to evaluate compliance with the audit process.
- Independent Audit. The data audit needs to be independent of other business processes and all data collected should be stored in read-only format on a separate server as it may be needed for an internal investigation or litigation purposes.
- Scalability. The data audit solution must accommodate growth and the addition of new data sources.
- Flexibility. Audit requirements change according to organisational needs. A solution that can be deployed on an ad-hoc basis ensures quick response to changes by deploying a flexible audit framework.
- Centralised Management. The data audit process is

Continued at page 4



Membership Directory

It's here... the exclusively online ASIS Membership Directory.

It's enhanced...

- More accurate searches.
- Updates within two full business days, including information about new members.
- Additional search criteria: not only by name, company, and location, but also by certification, chapter or council affiliation, leadership position, lifetime and/or Quarter Century Club status.
- More security: still available only to members in good standing, but with protective measures to thwart those who would use this data for unscrupulous means.

Login!

It's ready...

- To get started, you'll need your ASIS International member number and password.
- The rest is up to you!

Questions?

- Please refer to the FAQs at the top of the page.
- More questions? Contact ASIS Member Services at +1 (703) 519 6200.

Continued from page 3

best controlled from a single point as events can be correlated and analytics can be applied to the whole data set.

- Security. The security of the data audit capability must be guaranteed so as to ensure operational integrity.
- Content Discovery. The process of identifying data across the entire enterprise, a critical step in the data audit process.
- Analysis. The ability to proactively search across desktops, laptops, servers and email at a forensic level by keywords, file extension or active computer process. This deep forensic analysis of data will determine what events took place should an alert be raised.
- Reporting. To use data audit forensically – that is, to determine what happened – requires the ability to view data broadly and in detail. It must be possible to assess any impact on data from the beginning to end of any transaction. In addition, a process should be put in place for the audit team to report its findings to the business leaders.
- Document and Review Policy. Organisations are fluid and adaptive and so should the data audit process. Documentation is important as it articulates the audit

process and is necessary for compliance issues, refinement and improvement of the organisation's policies.

Conclusion

Businesses are answerable to shareholders, partners, customers and staff for the responsible management of data. Unauthorised access, inadvertent data leakage due to poor business processes or theft of data can cost a company its reputation and profits.

A comprehensive data audit capability delivers operational benefits beyond risk management and risk reduction; it complements the whole range of security measures that have already been put in place.

Policy enforcement enables organisations to remediate any non-compliant data and report back to stakeholders with confidence that they are in full compliance.

Organisations need to have a thorough understanding of both the risks inherent in data and the benefits of providing comprehensive data audit and policy enforcement. This will ensure that their single greatest corporate asset – their data – is truly protected.

About the author: Darren Cerasi is Director of I-Analysis Pte Ltd, a company specialised in digital forensics, information security and eDiscovery. He can be reached at this [email](#).

NOTICE OF CPP™, PSP™ & PCI™ EXAMINATION IN NOVEMBER 2008

Warm greetings from the Professional Development Committee, ASIS International Singapore Chapter!

ASIS International (Singapore Chapter) is pleased to sponsor the November 2008 Certified Protection Professional (CPP™), Physical Security Professional (PSP™) & Professional Certified Investigator (PCI™) Examinations in Singapore.

We are proud to highlight that the CPP™, PSP™ & PCI™ designations are the highest recognition in the world accorded to security management professionals. The CPP™ PSP™ & PCI™ conveys professional expertise, demonstrated competency, validated knowledge, and proven skills, all of which translate into a competitive edge in the complex business of security.

Kindly note that the CPP™, PSP™ & PCI™ examinations have been scheduled on **Saturday, 1st November 2008**.

If you are interested to sit for the examination in November 2008, please take note of the important information on registration:-

November 2008 Exam and Deadline Dates

ASIS Headquarters **must** receive all completed and reviewed applications by the deadline date or the exam will be post-poned. Any applications received after the deadline date will be considered and processed for the next exam date.

Exam Date: November 1, 2008
Application Submission Deadline Date: September 1, 2008

For applications and certification information, please visit <http://www.asisonline.org/certification/index.xml>. Click on "How to become a CPP™" or "How to become a PSP™" or "How to become a PCI™" located on the right bar. The application and additional information that will assist you in applying will be at your fingertips.

As a non-profit organisation, ASIS International (Singapore Chapter) has been running the **CPP™ Review Program** for the past few years with great success and had attained good results in terms of high passing rates. We attribute the success to a core team of highly dedicated and professional trainers.

We are also proud to announce that we will also be running the **PSP™ Review Program**. Our primary objective for the CPP™ & PSP™ Review Programs are to provide best-in-class training and value for money for our participants. We strongly encourage you to book early for the CPP™ & PSP™ Review Programs:

For those interested in taking part in the CPP™ & PSP™ Review Programs, please note the following dates:

CPP™ Review Program: Tuesday, 28th October 2008 - Fri, 31st October 2008.

PSP™ Review Program - Thurs, 29th October 2008 - Fri, 31st October 2008

For [immediate reservation and enquiry](#) for the CPP™ & PSP™ Review Program, please visit our chapter website or [email](#) us.

May we wish one and all success in attaining the coveted CPP™, PSP™ & PCI™ designation in 2008!

Best regards.

Paul Rachmadi, Leonard Ong, Henry Ang & Leslie Teo,
Professional Development Committee
ASIS International, Singapore Chapter



ASIS SINGAPORE PARTICIPATES IN ASIS INTERNATIONAL ASIA PACIFIC CONFERENCE 2008



ASIS SINGAPORE Q1 CHAPTER MEETING, IN PARTNERSHIP WITH 3SI PTE LTD

Certified Protection Professional

Top 10 Reasons to be a CPP

1. **Enhance your credibility.** Your CPP designation provides a recognizable status that allows you to be immediately accepted and respected as a reputable security management professional.
2. **Distinguish yourself.** In a competitive job market, your ability to differentiate yourself from the crowd is critical. A CPP raises your profile and broadens your exposure in the profession.
3. **Demonstrate the breadth and depth of your expertise.** Provide evidence that you've mastered the essential body of knowledge that makes up a well-rounded security management professional.
4. **Increase your marketability** with an internationally accepted designation. Your CPP carries the same meaning in all parts of the world and is in demand by multinational corporations
5. **Confirm your leadership abilities.** CPPs are recognized as leaders in the profession. Your CPP identified you as someone with the ability to provide leadership on critical security issues.
6. **Position yourself** for attractive senior-level positions and the income that accompanies them. Demonstrate the full range of your capabilities and let an employer know what you have to offer.
7. **Keep pace with rapid changes** in the security industry through recertification. The stakes are higher now. Continuing education is a lifelong process that's a necessity for career success.
8. **Gain career mobility.** A personally owned credential that's portable across industries and the public and private sectors creates opportunities and offers the option of a flexible career path.
9. **Enjoy liability protection** for yourself and your employer under the SAFETY Act Designation awarded to ASIS International by the U.S. Department of Homeland Security.
10. **Create an expanded network** of professional relationships beneficial to your career. Develop rewarding relationship with CPP colleagues based on a bond of mutual respect.

Will you succeed or fall behind in a 21st century security environment? If you haven't seriously considered the CPP, you owe yourself a look.

Established in 1977, the Certified Protection Professional designation is internationally recognized as the standard of professional competence in security management

