

A QUARTERLY NEWSLETTER FROM SISA

IN THIS ISSUE

Leveraging ISO 27005 Risk Assessment -P.1

Forensics: Need of hour - P.2

SISA's view on latest Security breach - P.3

PCI on Cloud - P.3

Industry Update - P.4

SISA UPDATES:

- SISA certifies IBM Daksh on PCI DSS covering 7 locations
- SISA certifies ngpay, the m-commerce platform on PCI DSS
- SISA launches Fast Forensic Services
- SISA launches SMART-RA for PCI Risk Assessment
- SISA launches U.S operations in New Jersey
- SISA conducts PCI awareness seminar with VISA in Nepal and Bangladesh

Leveraging ISO 27005 standard's risk assessment capabilities

Risk assessment (RA) is akin to charting the blueprint for a robust information security strategy. An information gathering exercise performed to determine the right steps to developing a proactive security posture.

The ISO 27005 Risk Assessment acts as enabler for designing effective and efficient controls for organizations.

The ISO 27005 risk assessment standard, first published in June 2008, is based on concepts specified in ISO 27001. The standard does not follow any specific risk analysis tactics, and is methodology free; an approach that is markedly different from other popular standards such as OCTAVE and NIST SP 800-30.

A one-size-fits-all approach to information security is doomed to failure — it's certain to throttle efficiency and productivity.

Risk assessment under ISO 27005

Workflow: Identification, Estimation and Evaluation ISO 27005 brings in considerable structure to risk assessment, in addition to being

methodology free.

Risk identification: This refers to risk characterized in terms of organizational conditions.

1) Asset Identification: ISO 27005 RA classifies assets into primary and supporting assets. Primary assets are usually information or business processes. Supporting assets can be hardware, software and human resources. While a supporting asset is replaceable, ISO 27005 effectively brings out this distinction, enabling organizations to identify valuable assets.

2) Threat identification and profiling: This facet is based on incident review and classification. Threats could be application-based or threats to the physical infrastructure. While this process is continuous, it does not require redefining asset classification from the ground up, under ISO 27005 risk assessment.

3) Identifying existing controls: ISO 27005 risk assessment requires identification of all possible existing controls.

4) Identification of vulnerabilities and consequences: Vulnerabilities must be identified and profiled based on assets, internal and external threats and existing controls, Vulnerabilities unrelated to external threats should also be profiled.



Risk estimation and evaluation: ISO 27005 risk assessment facilitates prioritization. Under ISO 27005, risk can be estimated qualitatively (for example: high, medium, low) or quantitatively (for example: cost in dollars, man-hours).

Risk Assessment is a tedious process. SISA's risk assessment and risk management tool, SMART-RA helps organizations simplify and automate their risk assessments, whilst following a structured and formal methodology.

Based on the ISO 27005 risk assessment methodology, SMART-RA deploys a patent pending methodology to select and implement only the most appropriate and effective controls for a given Asset

Threat combination.

In addition, SMART-RA comes bundled with a database of standard assets, threats and vulnerabilities pertaining to different industry verticals, and compliance environments. This minimizes the need for subject matter expertise from the user.

SMART-RA is automated to the extent that the risk assessment report is generated and ready to sub-

mit within 10% of the time taken using manual or

Generate ROI of up to \$6000 per annum with SMART-RA.

SMART-RA is currently the only tool to offer automated PCI Risk Assessment

spreadsheet driven risk assessments.



To find out how you can benefit from SMART-RA, register for FREE at www.smart-ra.com



SISA workshop conducted in collaboration with VISA in Kathmandu

Computer Forensics— A growing part of Federal cyber security strategy

Computer forensic investigation is not limited to popular crime investigation television shows. As the number of attacks on government system soars, it is becoming more complex for agencies to fit computer based investigations into the cyber-security strategy.

According to US Computer Emergency Readiness Team (US-CERT), the operational arm of the National Cyber Security Division at the Homeland Security Department say, "adding the ability to practise sound computer forensics will ensure the overall integrity and surviv-

ability of its network infrastructure."

Forensics is associated with the scientific collection of evidence for use in legal



procedures and court cases. But as the computer forensics methodology is intensifying in scope, anti-forensic activities are also gaining popularity. Scientific methods used for hiding the data securely in computer devices are very prominent nowadays, and this is directly en-

couraging felons to put up their stands. They attempt to negatively affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis difficult or impossible to conduct.

As the federal government tightens the information security requirements on agencies, it is becoming necessary for security managers not only to systematically investigate security incidents, but also to prove they are complying with computer security laws and best practices.

(Continue to PAGE 4)



SISA PCI-DSS certification workshop conducted in DHAKA.

SISA's view point on the recent card breaches

More than 800 members of the engineering society IEEE received letters informing that their credit card numbers had been stolen, after they registered themselves for a conference.

The attack was targeted at the member database that contained cardholder data. The stolen information included the credit card number, cardholder name, expiration date and the CVV2. This incident raises questions on the IEEE's data storage procedures.

Storing CVV2 is a direct PCI DSS violation and the credit card number, if stored, needs to be encrypted and should be accessible only on a need to know basis.

It's not clear at this time how IEEE stored the credit card numbers, but the CVV2 value should not have been stored in the first place.

Unfortunately, this not a one off incident. We have seen cases where attackers hacked into the Sony Playstation network, Citi bank stating that more than 200,000 customers' cardholder data has been breached, etc.

The concerned now raised is why has there been a sudden spurt in card breaches?

And are all card breaches actually being detected?

As per the industry studies, the breaches have occurred due to not identifying the key risk areas inside the organization and lack of proactive controls implemented on application protection. Also, the industry estimates that only 2 of the total 10 hacks are

getting detected by the organizations.

As an Information Security Specialist partner, SISA is conducting a one-to-one online educational series on Risk Assessment and how organizations could proactively work in this direction. The

"Information is invaluable. Make sure it is *secure*."

online educational series also includes, steps on how the organization can implement an effective log review process to detect hacks within a network.

The three stripes on the SISA logo represent

- PASSION,
- VALUES,
- DISCIPLINE

the DNA of the organization.

PCI ON THE CLOUD

PCI compliance is possible on cloud. Not many people are optimistic about the security that the cloud offers. Skepticism is about compliance issues in cloud is justified. Quite surprisingly, yes, we can be PCI compliant on the cloud, depending on the cloud service provider and the kind of data stored in there. PCI compliance is all about storing and transmitting cardholder data, hence the best way to work with PCI compliance is not to store cardholder data.

The virtualization guidelines into the payment card industry (PCI) Data Security Standard (DSS) have been introduced in response to the evolving trends in IT. Earlier this month, the PCI Security Standards Council (PCI SSC) added guidelines around PCI-DSS for regulatory compliance within virtualized environments.

The guidelines on cloud computing are focused on the steps the QSA should consider when certifying entities hosting cardholder information in a cloud.

The guidelines from PCI SSC are focused more on the virtualization environment than on cloud computing.

The appendix section provides the virtualization consideration for PCI DSS. The guideline takes the PCI DSS requirements and provides guidance regarding the steps a QSA should consider while assessing a virtual environment. In addition, there are also best practices and recommendations mentioned.

Also, a graphical representation of the responsibilities of the cloud customers and cloud providers is given, explaining who is responsible for data, software, user applications, operating systems,

infrastructure, physical infrastructure and the data center where everything is going to reside.

It will benefit a non-technical person to

understand who is responsible for what in case of



PCI compliance for cloud computing. In short, "the cloud" can be PCI compliant, but it all depends on how "the cloud" has been implemented.

SISA Information Security

SISA House, No. 3029, Sri Sai Darshan Marg,
13th Main Road, HAL II Stage, Indiranagar,
Bangalore—560 008, India
Branch offices in: **Mumbai and New Delhi**
Phone: +91-80-41153769
Fax: +91-80-41153796
E-mail: info@sisa.co.in



International Office:

United States Of America-

SISA Information Security LLC
2711, Centerville Road, Suite 400
Wilmington, Delaware 19808, USA

Bahrain -

SISA Information WLL,
No. 22, Building 1210, Road No 2113,
Manama, Kingdom of Bahrain,
Phone: +973- 39677283

Philippines:

Bloomington Building,
205 Salcedo Street,
Legaspi Village 0731,
Makati City, Philippines.

SISA is a Qualified Security Assessor Company (QSAC) on behalf of Payment Card Industry Security Standard Council (PCI SSC) to certify companies on Payment Card Industry Data Security Standard. SISA is a Qualified Payment Application Security Company on behalf of PCI SSC to certify applications on the Payment Applications: Data Security Standard (PA-DSS).

...Continued from page 2

Computer Forensics growing a part of Federal cyber security strategy

Sensing the need of the hour, SISA launched SISA Fast Forensic Services. The term fast forensic signifies the immediate investigation of security related incidents, to identify how the incident occurred, the impact and the scale of damage it has caused.

Advantages of SISA Fast Forensic Services include helping the victim identify and resolve security incidents faster, accurately assessing the impact caused by an attack or a piece of malicious code.

Subscribing to SISA Fast Forensics helps organizations in quickly and effectively resolving security incidents. A qualified and certified SISA team will be present on-site within 24 hours of the incident occurrence.

Industry Update

SISA Trainings

- SISA [PCI-DSS Implementation Workshop- CPISI Certification Program](#) in Delhi on 4 & 5, August.
- SISA [PCI-DSS Implementation Workshop- CPISI Certification Program](#) in Bangalore on 22 & 23, September.
- OCTAVE Risk Assessment Workshop in Bangalore on November. [Contact us](#) for more information.

For more details on the certification programs and to view our training calendar, click [here](#).

SMART-RA: SISA's Strategic Software Division

- SMART-RA is being showcased at the PCI SSC Community Meetings in [Arizona](#) and [London](#) in September and October, 2011. See you there.
- SMART-RA touches a landmark 100 users. 100 organizations are using SMART-RA to automate and simplify their risk assessments. Access your FREE Edition of smart-ra [here](#).