

*“ Eric is one of the most knowledgeable Information Security practitioners I have worked with. He has extensive and diverse knowledge .... is able to communicate information and concepts well... and provides practical solutions for today's information security challenges. ”*  
Senior Information Security Consultant, Westpac

# Data Security Essentials

## Protecting organisational data and the customer data entrusted to your care

Presented by **Eric Svetcov**



Strong practical focus with extensive class exercises

### Attendees will receive the following sample policies:

- **Data Security** – Comprehensive data security policy – access control, acceptable use, data classification, data ownership, and data lifecycle (creation, usage, transmission, storage, and disposal)
- **Data and Media Disposal** – Policy around disposal of data and media
- **Incident Management** – Policy for managing incidents
- **3rd Party Data Security** – Data handling policy for vendors, partners, and other 3rd parties

Information is your organisation's key resource. Most things can be survived, but the loss of critical enterprise information can be crippling and even unrecoverable. This powerful 2-day course has been specifically designed to comprehensively cover all the key points that you need to understand in order to better protect your most important asset – **YOUR DATA:**

- Better understand the alignment of data security efforts to company strategic goals
- Current technology solutions to drive quick improvements to your data security
- New technology solutions for mitigating the risk of an adverse data disclosure
- Strategies to improve engagement with Information Assurance professionals, internal audit and other risk and compliance groups within your company
- Enhance your data security policies through better alignment with leading governance frameworks
- Expand your data security vision to encompass all company and customer data wherever it might reside
- Know where your company and customer data actually resides and methods for securing it, wherever it might be
- How to better leverage leading frameworks to drive improved data security results
- Tools to help you identify where you are at - the current state of data protection at your organisation



PDA is a member of the ALC Group

Please refer to our website for current dates

# Data Security Essentials

## Protecting organisational data and the customer data entrusted to your care

The enormous growth of the internet and the increasing geographic spread of networking has meant that organisations today have multiple security exposure points, far greater than ever before. Over the past few years the risks have increased substantially.

Information today is the organisation's key resource. Most things can be survived, but the loss of critical enterprise information can be crippling and even unrecoverable.

This 2-day course provides a strong foundation knowledge for anyone responsible for or involved with ensuring security of their organisation's data.

### BENEFITS in attending this workshop

- Gain insight into better alignment of data security efforts to company strategic goals
- Discover new technology solutions that might be helpful in mitigating the risk of an adverse data disclosure
- Improve engagement with Information Assurance professionals to help you and your company achieve your goals
- Integrate your efforts (and create allies) with other departments in your organisation to improve data security efforts
- Enhance your data security policies through better alignment with leading governance frameworks
- Expand your data security vision to encompass all company and customer data wherever it might reside

### What You Will LEARN

- Where your company and customer data actually resides and methods for securing your data wherever it might be
- Who owns the data and who is responsible for managing the data
- How to better leverage leading frameworks to drive improved data security results
- How current technology solutions can help you drive quick improvements to your data security issues
- Strategies for engaging with internal audit and other risk and compliance groups within your company to help you achieve your goals
- About tools to help you identify the current state of data protection at your organisation

### Who Should ATTEND

- IT and MIS managers
- Management and executive staff involved in ensuring corporate security
- IT staff looking to add critical security knowledge to their added-value skill set
- User liaison/support staff responsible for helping the security message permeate the organisation
- Anyone who wants a solid foundation to their understanding of information security

“Eric regularly solicits constructive feedback, asks well-thought-out and well-prepared questions and has a gift of explaining complicated issues clearly and succinctly.”

**Security and Risk Manager, Wesfarmers Insurance**

“Excellent experience sharing and very helpful coordinator.”

**IT Officer, Chief Government Security Office, Malaysia**

## Course Contents

### Day One – Framework and Policy

#### 1. Introduction

- What is data? Where does data live? Who owns it? Who manages it?
- What is data security?
- Why is data security needed?
- What are the expectations of our senior management, executives, board of directors/governing bodies, and customers?

#### Exercise One

*Sets the stage for developing a common understanding of “data”. What is data at your company? Where does data live?*

#### 2. The Role of Corporate/Organisational Governance and IT/Information Security Governance in Building a Data Security Programme

- Corporate/Organisational governance role in data security
- IT and Information Security governance role in data security
- IT/Information Security Governance Frameworks and Standards
  - COBIT 4.1 and data security
  - ISO 27001/27002 and data security

#### 3. Key Players and Roles in the Data Security Programme

- Introduction to RACI Charts
- The business
- IT and Information Security
- Customer
- Government

#### Exercise Two

*Understand how to use tools such as RACI charts to help communicate with senior management and to identify the key players in your organisation. Will help participants understand who they need to work with to improve their data security programme.*

#### 4. Building Your Data Security Programme: A step-by-step approach to building a data security programme that aligns the strategic goals of your organisation with leading IT and Information Security governance frameworks and standards

- Start with a risk assessment
- Understand risks and create risk treatment plan
  - Consider compliance/legal requirements (PCI, SOX, Privacy, etc.) as inputs for the risk treatment plan
- Receive management approval for implementing risk treatment plan
- Implement controls required by risk treatment plan
- Implement solutions to measure effectiveness of controls
- Implement training and awareness programmes
- Implement monitoring and construct procedures for rapid detection of security events and responses to incidents

### Exercise Three

*Movie – “New Face of Cybercrime”. We are now transitioning from theory to practice. This movie places us into the frame of mind of discussing practical, real-world issues and finding solutions to the real data security threats we face. What keeps you up at night? What are your company’s most significant risks? External? Internal? Illegal activity? Mistakes?*

## 5. Writing the Data Security Policy: The strong foundation of your risk treatment plan will be your Data Security Policy

- Leveraging ISO 27001/27002 and COBIT to build a comprehensive policy
- Understanding data as a company asset
- Ownership of data assets
- Access control
- Acceptable use of data assets
- Data classification
- Labeling and handling data assets
- Monitoring and continuous improvement
- Integration with your other Information Security, IT, Risk Management and business policies such as the backup policy, business continuity and disaster recovery, and others

### Exercise Four

*Not all data security policies are the same. Similar industries will face similar risks. In this exercise attendees will review in teams a sample data security policy and craft up to five suggestions on how to improve the policy for their own industry. This group effort will help team members with ideas for improvement of their policy when they return to their organisation.*

## Day Two – Controls, Monitoring and Incident Response

### 6. Data Security Controls – People And Technology

- Current state of many organisations – what’s not working and why?
- Data security and the fallible human being – implementing controls (including training) that limit accidental misuse of data and data disclosure
- Handling internal and external bad actors and why this is a never-ending battle
  - **Case study** – The struggle against phishing attacks and criminal attempts to extract data from SaaS providers (salesforce.com)
- Using public information we will explore what happened during the 2006 phishing attacks, the controls salesforce.com implemented, and additional controls that potentially could further mitigate the risk.
- Multi-layered defenses – preventative and detective controls

### Exercise Five

*Attendees will see they are not alone. All organisations have room for improvement. What are the major control weaknesses for organisations? What is preventing organisations from improving those controls? The list of control weaknesses from this exercise will be mapped to potential solutions discussed in the next section of the course.*

### 7. New Technical Solutions For Improving Data Security

- Just because they are new and “everyone” is implementing one, should you implement one too?

- Data Leakage Prevention
- Database Logging/Security
  - **Case study** – Explore how privileged users, such as database administrators, can monetize their access to company and customer data at financial institutions.
- This case will identify two scenarios where a database administrator could monetize their access with little risk of discovery for significant personal financial gain, why conventional controls are inadequate, and the potential controls that could mitigate the risk
- Identity and Access Management
- End Point Security
- Network Access Control
- Vulnerability Assessment
- Enterprise Password Management
- Data masking
- Encryption
- Intrusion Detection/Prevention (NIDS/NIPS, HIDS/HIPS, WIDS/WIPS)
- Web application data security
- Patch management

### Exercise Six

*Attendees will have an opportunity to identify one security control which they believe should be implemented in their organisation. Why choose that one? What risk is mitigated? How easy would it be to implement? Attendees will also have an opportunity to learn about controls that they may want to implement in the future.*

### Exercise Seven

*Databases are where much of the company and customer data is stored; however, many organisations do not appropriately test the security of these repositories. This exercise will demonstrate how easy it is to gain an understanding of database security risks. Features hands-on session using Scuba, the Database Vulnerability Scanner from Imperva*

### 8. Testing, Monitoring and Continuous Improvement

- Using ISO 27001 and COBIT to implement appropriate testing, monitoring and continuous improvement
- Following your policy – Testing, monitoring and continuous improvement should be part of your policy
  - **Case study** – Pre-implementation testing as well as real-world regular tests are important. In this short case, a major US collocation provider failed to appropriately test the diesel generators.
- This case will show that when considering your test plans, you should attempt to simulate real-world testing.
- Log aggregation, correlation, alerting, and remediation
- Creating your own metrics
- Managing remediation
- Incident management
- Forensic investigations

### 9. Audit

- The role of Internal Audit and using Internal Audit to improve Data Security
- External Audit – why are they here and what are they looking for?

### 10. 3rd Parties and Outsource Partners

- Building Data Security requirements into outsource agreements
- Understanding the risk of outsourcing
- Creating a framework for assessing potential outsource partners
- Verifying adherence to the data security requirements integrated into outsource agreements

### 11. Summary and Conclusions

## Course Presenter **Eric Svetcov**

Eric is a leading Information Security specialist who focuses on securing key corporate and customer data by understanding of the risks to organisations, aligning business and IT strategies, and creating Information Security solutions that fully align with organisational strategy while maximising operational results and risk mitigation. Eric draws on leading governance frameworks and more than 15 years advising clients on how to protect data placed under his stewardship to craft data security solutions that achieve an appropriate level of risk mitigation and alignment with the goals of the organisation.

Previous roles have included, Information Security and Business Continuity national service leader for KPMG in New Zealand, Information Security Director for salesforce.com in San Francisco, Director of IT and Operations at Grassroots Enterprise, and Manager of Information Systems at Intuitive Surgical.

Eric is a Board Member of the American Board for Information Security and Computer Forensics and a Board Member of the ISACA chapter in Auckland. He is a member of the International Association of Privacy Professionals (IAPP), (ISC)2 and American Board for Certification in Homeland Security (ABCHS). He has an MBA and holds the following certifications: CISSP, CISM, CISA, CIPP, and CHS-III. His articles have been published in Computerworld, SC Magazine, Technology & Learning magazine, School CIO, and Windows NT Systems magazine.

*"Having seen Eric present to large mixed audiences, not only was I impressed by his knowledge and experience... but how he was able to engage the audience, convey the message and do so with hard evidence. He was able to deliver what the IT and security people had to hear to be convinced while relaying the business risks, imperatives and benefits for those C-level execs in the group."*

**Managing Director, Fortify**

Eric has presented training programs in many countries around the world to outstanding reviews and is a regular speaker at industry events such as ComputerWorld's Utility Computing Briefing, the IT Security Summit in Auckland and the Cloud Computing Summit.

A partial list of organisations Eric has worked for: Visa, HSBC, ING, Royal Bank of Scotland, United Commercial Bank, Bank of New Zealand, Westpac, Intuit, US Department of Defense, California Department of Motor Vehicles, New Zealand Ministry of Economic Development, Housing New Zealand, Waikato Institute of Technology, Chevron, Pacific Gas and Electric, Vector, Pacific Bell (now AT&T), ShoreTel, Verio (Now NTT Communications), Google, Cisco, salesforce.com, Plantronics, Xilinx, Autodesk, Intuitive Surgical, Pfizer, Fonterra.

### HOW TO REGISTER

1.		Register Online <b>www.pdatrain.com.sg</b>
2.		Send your details by email <b>learn@pdatrain.com.sg</b>
3.		Fax the Enrolment Form below to: <b>Fax: 6227 2885</b> From any other country <b>65 6227 2885</b>
4.		Any queries please call Customer Service <b>Tel: 6227 2883</b> From any other country <b>65 6227 2883</b>
5.		Post the completed Enrolment Form to: <b>PDA Professional Development Associates Pte Ltd</b> Penthouse Level, Suntec Tower Three, 8 Temasek Boulevard, Singapore 038988

### COURSE DETAILS

<b>FEES:</b> (per delegate)	<b>S\$</b>
<b>Data Security Essentials</b>	
Single delegate	<b>\$1320 + GST</b>
2 or more delegates 10% discount	<b>\$1188 + GST</b>
<b>COURSE INFORMATION:</b> The course is held from 9.00am to 5.00pm with registration from 8.30am on the first day. Upon enrolment you will be sent a confirmation letter giving full details.	
<b>TERMS:</b> The course is of limited class size. To ensure admission, fees must be paid in advance or else an official Purchase Order Number must be supplied. Fees include tuition, lunch, coffee breaks and all course materials. An invoice will be forwarded to you upon receipt of enrolment.	
<b>CITREP FUNDING:</b> (CITREP) is a training incentive programme to equip Singapore infocomm professionals with critical and emerging skills thus enabling them to enhance their employability and to improve their organisations' competitive advantage. The Enhanced CITREP supports up to 80% of the course and exam fees for courses and certifications commencing between 1 April 2009 and 31 March 2011. Organisations who sponsor their employees for training can benefit from "Absentee Payroll" support. Terms and conditions apply. Please visit <a href="http://www.ida.gov.sg/citrep">www.ida.gov.sg/citrep</a> for more information or email PDA at <a href="mailto:learn@pdatrain.com.sg">learn@pdatrain.com.sg</a>	
<b>CANCELLATIONS:</b> Cancellations will be accepted up to 10 working days before the course. After that time no refunds can be given but substitutions can be sent at any time.	

### ENROLMENT FORM - Data Security Essentials



A Member of  
The ALC Group

PDA Professional Development Associates Pte Ltd is a member of the ALC Group ([www.alc-group.com](http://www.alc-group.com)), providing leading-edge training in IT and management for business and government in Australia, Hong Kong, Indonesia, Malaysia, New Zealand and Singapore. ALC has no affiliation with vendors of software or hardware and provides completely independent unbiased training.

	NAME	<input checked="" type="checkbox"/> SELECT	COURSE NAME + DATE	
1	Mr/Mrs/Miss/Ms (as per NRIC)	<input type="checkbox"/> Course + Exam <input type="checkbox"/> Course only CITREP Sponsorship: <input type="checkbox"/> Company <input type="checkbox"/> Self <input type="checkbox"/> None		
	Position			Mobile
	Email			
2	Mr/Mrs/Miss/Ms (as per NRIC)	<input type="checkbox"/> Course + Exam <input type="checkbox"/> Course only CITREP Sponsorship: <input type="checkbox"/> Company <input type="checkbox"/> Self <input type="checkbox"/> None		
	Position			Mobile
	Email			

TRACK CODE: A B C D R

Organisation: \_\_\_\_\_

Address: \_\_\_\_\_

Postcode: \_\_\_\_\_ Phone: ( ) \_\_\_\_\_ Fax: ( ) \_\_\_\_\_

1.  Cheque payable to *PDA Professional Development Associates Pte Ltd*    2.  Purchase Order No.: \_\_\_\_\_

<b>Person Making Booking:</b>	Mr/Mrs/Miss/Ms	<b>Send Invoice To:</b>	Mr/Mrs/Miss/Ms		
	Position		Phone	Position	Phone
	Email		Email		