DEFENCE READY SEMINAR SERIES

DEFENCE RELEVANT DATA: SECURITY FUNDAMENTALS

OVERVIEW

Data security in the Defence supply chain is a long-standing concern for the Defence industry. The protection of "Defence relevant" technical data is a key priority in maintaining technological and strategic advantages over potential adversaries. Government concern for this can be seen in the ever-increasing enforcement of regulation and standards like DISP, NIST 800-171, International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), ISO 27001 and CMMC.

While governments and Defence Primes continue to stress the need for cyber improvements, actual adoption of data security in the defence industrial base remains poor. This can mainly be attributed to two factors 1) nature of the data that needs to be secured and 2) the size of the Defence contractor. The Defence focused workshop looks to address these challenges by taking a data centric approach to information security.

KEY DETAILS

MODE

Virtual

SEMINAR STRUCTURE

- Virtual workshops x 3
- Podcasts x 1

DURATION

3 weeks

WHO SHOULD ATTEND:

- The course is specifically targeted for professionals dealing with IT, Security and Compliance of Defence organisations. However, as data Governance requires close interaction with business and data owners of the company, data owners are highly encouraged to attend this course.

VIEW THE DATES OF THIS COURSE AND REGISTER YOUR INTEREST HERE

DEFENCE RELEVANT DATA: SECURITY FUNDAMENTALS

WHAT TOPICS WILL BE COVERED

Data is the fundamental element that needs to be secured in any organization but most critically within a Defence environment. Data Governance is the process, and procedure organizations use to identify, manage, utilize, and protect their data. The workshop will provide participants with an introductory understanding of data governance and help them develop a Defence relevant framework to securely manage sensitive data..

EXPECTED OUTCOMES:

The workshop will introduce Defence companies on how to identify sensitive Defence relevant data and implement best practice processes, procedures, and technology for proper management of Defence relevant data when dealing with limited resources.

The workshop will provide proprietary data governance and security templates to help participants jump start their data governance strategy. Participant will be taken through various Defence relevant scenarios using these templates and shown how they can be utilized to improve handling of their data assets. The course will also make use of various resources provided by ASD and ACSC as part of the course content and for future reference.

FACILITATOR

RIZWAN MAHMOOD

Rizwan has a passion to solve the human risks to data security and has spent the last 10 years consulting on human factors behind data loss and privacy and designing security systems. He has been engaged in the detection and response of 100s of insider threat cases involving corruption, insider trading, reputational damage, theft for personal gain and accidental loss. Many of which have also become part of OAIC stats.

Rizwan works as Director Data Security and Compliance for e-Safe Systems a UK based security vendor specialising in human risk to data security and compliance, since its inception.

Rizwan has 18 years of experience of designing and management information security and artificial Intelligence-based systems. He holds a Masters in Information Technology Management from Staffordshire University, UK, and is a certified Information Systems Security Professional (CISSP) and Project Management Professional PMP®

During his time with e-Safe Systems he has held several strategic and leadership roles and has been instrumental in growing the business which is now protecting over a million users worldwide.

Prior to migrating to Australia, as Chief Operating Officer he was responsible for establishing e-Safe's R&D and support centre and lead the design and development of e Safe's offerings which include Data loss Prevention, Document Rights Management, File encryption, user behaviour analytics, user activity monitoring, data classification, filtering and e-safety solutions. In his current role as Director Data Security and Compliance, he is responsible for leading the consulting engagements in Australia and is responsible for defining strategic direction for e-Safe's product in light of new challenges and market trends.

FACILITATOR

RAY HARVEY

Ray Harvey is the Internal Threat Business Development Manager for Cider House ICT, a Goal Group Member. Ray is passionate about ensuring that Australian businesses are protecting themselves from evolving cyber threats and are as competitive as they can be in the competitive Defence market.

TIMING	LEARNING MODULE	FORMAT	EST. TIME TO COMPLETE
On demand	**Introduction** ▪ Introduction to seminar and facilitator ▪ Description of seminar bundle incl learning outcomes	Podcast.	30mins

Week 1	**Establishing a Data Governance Approach**
	▪ **Understanding data security risk in a Defence Industry context**
	▪ **What is data governance from a Defence perspective?**
	▪ **Using a data centric approach in practical Defence Industry scenarios.**
	▪ **Determining what Defence relevant data is important? Categories and types of data.**
	  ▪ Data governed by regulations and standards frequently used in Defence Industry.
	  ▪ Data governed by defence regulations like ITAR, NIST 800-171, CMMC.
	  ▪ Data governed by privacy regulations like NDB, PCI DSS and GDPR.
	  ▪ Defence classified information.
	  ▪ Custodial Information.
	  ▪ Data controlled by contractual obligations frequently used in Defence Industry contracts.
	  ▪ Defence Project information.
	  ▪ Defence Project output.
	  ▪ Intellectual Property. Commercially sensitive Defence Industry relevant data.
	  ▪ Engineering design documents.
	  ▪ Customer list.
	  ▪ Internal company processes and procedures.
	▪ **Classifying data**
	  ▪ What is data classification?
	  ▪ Sensitivity of data.
	  ▪ Value of data.
	  ▪ Criticality of data.
	  ▪ Legal requirements.
	  ▪ Data timeline.
	▪ **Understanding Data Retention in Defence**
	  ▪ Determining appropriate record retention timeframe in Defence.
	  ▪ Record retention best practices for Defence
		Virtual Workshop	30min bump in, 60mins, plus 30 - 45 mins of Q&A and chat room participation

> SEMINAR MODULES OUTLINE CONTINUED ON NEXT PAGE

TIMING	LEARNING MODULE	FORMAT	EST. TIME TO COMPLETE

Week 1
(Continued)
	Establishing a Data Governance Approach
	(Continued)
	▪ **Roles and responsibilities to be established in Defence suppliers.**
	  ▪ Understanding the importance of data ownership.
	  ▪ The roles and responsibilities of different users in a defence organisation.
	▪ **Developing a classification Scheme for Defence suppliers.**
	  ▪ Introduction to PSPF classification scheme.
	  ▪ PPSPF vs a commercial classification scheme.
	  ▪ Using information markers (Legal, ITAR, CUI, Contractual, Private in Commercial scheme)
	▪ **Developing an asset inventory of defence classified data.**
	  ▪ Mapping data to classification.
	  ▪ Data labelling and marking as required under Defence.
	
	Expected Outcome
	The attendee will gain an understanding of:
	▪ What is Data Governance and its importance from Defence perspective?
	▪ Understand what data-centric approach is and how it is utilised by Defence suppliers.
	▪ How to categorise data and determine what is important for Defence suppliers.
	▪ Understand what is required to build a Defence relevant data classification scheme for your organisation.
	▪ Roles and responsibilities of different users within Defence suppliers.
	▪ Developing an asset inventory of defence classified data.
		Virtual Workshop	30min bump in, 60mins, plus 30 - 45 mins of Q&A and chat room participation

Week 2	**Secure handling of Defence Related Data Assets**
	▪ **What is Data lifecycle from Defence context?**
	  ▪ Create
	  ▪ Store
	  ▪ Use
	  ▪ Share
	  ▪ Archive
	  ▪ Destroy
	▪ **What are data states in Defence?**
	  ▪ Data at Rest
	  ▪ Data in Motion or Transit
	  ▪ Data in Use
		Virtual Workshop	30min bump in, 60mins, plus 30 - 45 mins of Q&A and chat room participation

> SEMINAR MODULES OUTLINE CONTINUED ON NEXT PAGE

TIMING	LEARNING MODULE	FORMAT	EST. TIME TO COMPLETE

Week 2 (Continued)	**Secure handling of Defence Related Data Assets** (Continued)
	▪ **Types of controls.**
	  ▪ Administrative controls in defence
	  ▪ Technical controls in defence
	  ▪ Physical controls in defence
	▪ **Access Control Management as required under Defence.**
	  ▪ User registration and de-registration.
	  ▪ User access authorisation and accountability.
	  ▪ Access restrictions,
	  ▪ Managing privileged user access.
	  ▪ Authentication methods.
	  ▪ Type 1 like passwords, Pass phrase.
	  ▪ Type 2 like token, Mobile APP.
	  ▪ Type 3 biometrics.
	  ▪ Identity management systems.
	  ▪ SSO
	  ▪ LDAP/AD
	  ▪ Data centric access control systems.
	▪ **Auditing Access as required under Defence.**
	  ▪ On-going monitoring and logging.
	  ▪ Review of user access rights.
	  ▪ Removal or adjustment of access rights.
	▪ **Encryption fundamentals as required under Defence.**
	  ▪ Disk based encryption.
	  ▪ Data or File based encryption.
	  ▪ Encryption in communication.
	  ▪ Database encryption.
	▪ **Securing defence data in motion or when shared.**
	  ▪ Email Security
	  ▪ Cloud security
	  ▪ Removable Media
	  ▪ Printing
	  ▪ file transfer applications
	  ▪ Web based communication methods
	  ▪ VPN
	▪ **Auditing data in motion as required under Defence.**
	▪ **Securing Defence related Data at Rest. How to securely store your Defence data?**
	  ▪ File Servers
	  ▪ Mobile devices
	  ▪ Removable media
	  ▪ Cloud storage
	  ▪ Database servers
	  ▪ Data Backups
		Virtual Workshop	30min bump in, 60mins, plus 30 - 45 mins of Q&A and chat room participation

> SEMINAR MODULES OUTLINE CONTINUED ON NEXT PAGE

TIMING	LEARNING MODULE	FORMAT	EST. TIME TO COMPLETE

Week 2 (Continued)	**Secure handling of Defence Related Data Assets** (Continued)
	▪ **Using data discovery tools to locate stored Defence data.**
	  ▪ Label based discovery.
	  ▪ Meta data-based discovery.
	  ▪ Content based discovery.
	▪ **Introduction to Defence Data Control Matrix.**
	▪ **Data backup fundamentals as required under Defence.**
	▪ **Data Disposal requirements under Defence.**
	  ▪ Declassifying defence data
	  ▪ Data disposal mechanisms
	▪ **Auditing end of life defence data.**
	▪ **Running scenario using provided defence data control matrix.**
	
	Expected Outcomes:
	The attendee will gain an understanding of:
	▪ Understand different states and lifecycle of data in defence context.
	▪ Understand how to secure defence data in each of its life cycle stages and states.
	▪ Understand how to use defence data control matrix to secure your defence data.
	▪ Gain an understanding of various options available to improve security and secure defence related data.
		Virtual Workshop	30min bump in, 60mins, plus 30 - 45 mins of Q&A and chat room participation

Week 3	**Specific Security Consideration For Defence**
	▪ **What is Insider Threat?**
	▪ **Managing Insider threat in Defence.**
	  ▪ Managing Human error.
	  ▪ User behaviour monitoring.
	▪ **Techniques for controlling defence data when outside of the organisation.**
	  ▪ with suppliers
	  ▪ with ex-employees
	▪ **Working from Home in Defence industry.**
	  ▪ Basic security hygiene when working from home.
	  ▪ Secure ways of handling mobile devices.
	  ▪ How best to handle BYOD (Bring Your Own Device).
	▪ **Cloud Computing fundamentals in Defence industry**
	  ▪ What is cloud and its variations.
	  ▪ Business drivers to adopt cloud. What works and what doesn't for Defence SMEs?
	  ▪ Key Cloud Computing Security considerations in Defence context.
	  ▪ Keeping Defence related data in the cloud. Who is responsible for what? Responsibilities when using a cloud environment.
		Virtual Workshop	30min bump in, 60mins, plus 30 - 45 mins of Q&A and chat room participation

> SEMINAR MODULES OUTLINE CONTINUED ON NEXT PAGE

TIMING	LEARNING MODULE	FORMAT	EST. TIME TO COMPLETE

Week 3 (Continued)	**Specific Security Consideration For Defence** (Continued)
	▪ **Importance of assessments in Defence.**
	  ▪ User vulnerability assessments.
	  ▪ Defence data usage assessments.
	▪ **Running scenario using provided data governance templates**
	
	Expected Outcomes:
	The attendee will gain an understanding of:
	▪ Understand ways to mitigate Insider threat within defence suppliers.
	▪ How to secure devices when working from home.
	▪ How to handle mobile devices and BYOD.
	▪ Understand cloud security considerations in defence.
	▪ Understand defence supplier's role and responsibilities when using cloud providers.
	▪ Importance of assessments in defence.
	▪ Deeper understanding of how to use the data governance templates from defence perspective.
		Virtual Workshop	30min bump in, 60mins, plus 30 - 45 mins of Q&A and chat room participation

TOTAL COURSE DURATION

3 hours instruction / Up to 2.5 hours of Q&A and 1.5 hours of bump in

HOW DOES THIS PACKAGE FIT INTO THE COMPLETE DEFENCE READY SERIES?

- **BD:** Good data security and governance helps businesses comply with various defence legislations and standards. Defence business's ability to showcase that it complies with various defence legislations can be a prime differentiator when bidding for tenders.
- **Legal:** Data security and governance helps to reduce legal exposure that can occur in the event of data loss or breach of contract due to mishandling of data.
- **ISO Standards:** The workshop covers many controls and requirements as stated under ISO 27001 standard.
- **Cyber Security:** Cyber Security workshop is a necessary prerequisite to this course. The Cybersecurity course covers the fundamental security elements that any company should have. Data security workshop extends cybersecurity by focusing on securing the underlying asset itself.
- **Export controls:** The workshop helps to establish controls and processes for proper handling of ITAR and EAR tech data.
- **Introduction to DISP:** The workshop puts in place many of the processes and procedures required for proper handling of data which will be required for companies to attain and maintain DISP levels.

DEFENCE RELEVANT DATA: SECURITY FUNDAMENTALS

COURSE SCHEDULE

EOI cut-off: 02 February

Successful applicants notified: 03 – 10 February

Course joining instructions issued: 10 February

Course timing: 24 February – 10 March 2022 – Weekly 1-hour workshops on a Thursday. Time TBC.

Please note: *please review the delivery timeline for this seminar bundle via the website. It is compulsory to attend the Virtual Workshops at the scheduled times.*

DEFENCE READY SEMINAR SERIES

HUNTER DEFENCE

Australian Government
Department of Defence

GOAL GROUP

AUSTRALIAN INDUSTRY & DEFENCE NETWORK NSW

HUNTERDEFENCE.ORG.AU/DEFENCE READY