Information Assurance for Small to Medium Enterprises

Who ‘ya gonna call?

**Key Message**
- Set the Standard
- Measure Compliance
- Improve Assurance Levels
- Monitor

IASME Consortium 2011
Agenda

- Background
- IASME Components
  - Risk Assessment
  - Management Framework
  - Maturity Assessment
  - Certification
- Risk Assessment Workshop
Background

Objectives – improve and recognise SME security

- Consortium
- Research
- Findings
- Development
Consortium Structure

Funding: Technology Strategy Board
           Driving Innovation

Research: University of Worcester

Development: IA Consultancy

Certification: NCC
Research

University of Worcester Research: (Henson)

“This paper reviews the research findings of the University of Worcester on SMEs in 2009 and looks at other recent academic and corporate research on SME data security in the EU and the rest of the world, exploring the unique problems faced by SMEs in securing information. It illustrates the importance of SMEs in the national business infrastructure, and shows that there are significant shortfalls in the protection of SMEs from cyber attack, affecting both their viability and the security of the data which they hold in relation to the larger businesses and government organisations who are often their main customers.”

ICO study: Review of Availability of Security Advice for SMEs (Lacey & James)

“Small and medium sized enterprises (SMEs) face a growing range of information security threats. Few SMEs, however, apply sufficient controls to safeguard their sensitive information. … The result is a growing risk of security breaches of sensitive business or customer data, as well as an exposure for many larger organisations that subcontract work to SMEs.”
SMEs tend to have:

- Staff loyalty
- Small number of well controlled physical spaces
- Clear business focus
- No staff with dedicated IT or security responsibilities
- Little understanding of information security
- No spare cash for non-essentials!
Developing the process

- Develop SME-friendly risk profiling method
  - ENISA model etc.

- Consolidate risk management controls
  - ISO/IEC standards, HMG standards, ICO guidance etc.

- Develop measurement method
  - Carnegie Mellon maturity process
  - Scoring method
## IASME Process

1. **Registration**
   - Tell us who you are.

2. **Orientation visit**
   - We visit you and manage everyone’s expectations – what is your risk profile?

3. **Preparation and self-assessment**
   - Where you collate evidence
   - Preparing any new activities to manage risk

4. **Assessment visit**
   - An intensive day with your assessor to review information security in your business

5. **Reporting and certification**
   - Assessor makes a case for your certification to the independent programme moderator.

6. **Continuous self appraisal**
   - Successful businesses are awarded a bronze, silver, or gold marque

7. **Annual light touch reviews**
   - Is information security maintained and keeping up with your risk profile.
Scalable

Demonstrate good information management

- Business focus
- Uses international security standards
- Core of achievable security measures
- Risk profile determines implementation requirements
- Certification recognises security achievements
- Continuous improvement towards full international standards if required
IASME: Risk Profiling

- Business-focussed balanced scorecard
- No security jargon
- Based on best practice
- Flexible
Risk Profiling Generalisations

- Staff numbers
- Contractor numbers
- Business Locations
- Physical security
- Environmental requirements
- Management responsibility
- Legal issues
- ICT complexity
- Business Change
- Internet use
- Partner access
- Home/remote working
- Risk tolerance
- Threat knowledge
- Information value
- ICT value

Statistically, the more employees and business locations, the greater the overall risk

Affects theft and damage risk

Affects information availability risk

Higher levels of responsibility lowers overall risk

Legal awareness lowers legislative risk

More ICT complexity raises overall CIA risk

Faster change tends to raise overall risk

Increased internet use, partner access and home working tends to increase confidentiality risk

High risk tolerance raises overall risk levels, but lowers security control requirements

Good threat knowledge lowers overall risk levels

The more important the information and ICT facilities to the business, the higher the risk levels
Risk Profiling Outcomes

- Simple Risk Profile
  - Generally low and medium level Risk Factors, with a preponderance of low levels
- Intermediate Risk Profile
  - Mixture of low, medium and high Risk Factors, with a preponderance of medium levels
- Complex Risk Profile
  - Generally medium or high level Risk Factors, or some high risk issues which are business critical
Flexible Assessment

**Policy & Procedures Self Assessment**

Typically used for:
- Simple Risk Profile
- Micro and small businesses
- Quick and simple

**Control Matrix Assessment**

Typically used for:
- Intermediate and Complex Risk Profiles
- 50+ employees
- In addition to P&P Self Assessment
- More detailed, but still flexible and straightforward
Policy & Procedures Self Assessment

- Management Structure (ISMS)
  - Scope and Revisions
  - Owners and Training
  - Creation and Review Dates

- Security Framework
  - Objectives
  - Responsibilities
  - Legislation
  - Framework Details
### Scoring Table

<table>
<thead>
<tr>
<th>Level 0 - <strong>Initial</strong></th>
<th>Little or no evidence available of the security control.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1 - <strong>Minimal</strong></td>
<td>Some evidence of the control, but little or no documentation available.</td>
</tr>
<tr>
<td>Level 2 - <strong>In Use</strong></td>
<td>The control is in use, partially documented and some evidence of use is available.</td>
</tr>
<tr>
<td>Level 3 - <strong>Managed</strong></td>
<td>The control is in use, is fully documented, and some metrics are collected but not fully exploited.</td>
</tr>
<tr>
<td>Level 4 - <strong>Controlled</strong></td>
<td>The control is managed, fully monitored and the metrics are used to improve security.</td>
</tr>
<tr>
<td>Level 5 - <strong>Optimized</strong></td>
<td>The control is managed and leads to optimised security management and forecasting for the business.</td>
</tr>
</tbody>
</table>
Assessment Topics

- Policy and Procedures Management
  - Objectives, Aim & Scope
  - Responsibilities
  - Legislation
- Framework
  - Personnel Security
  - Asset Management
  - Access Management
  - Physical and Environmental Management
  - Computer and Networks
  - Malware
  - Incidents
  - Business Continuity
  - Electronic Commerce
Assessment Exercise

- Demonstrates IASME scope using
  - Assumed Simple Risk Profile
  - Small Business scenario
  - Policy & Procedures Assessment form

- Break into groups
  - Pretend you are the small business undergoing self-assessment
  - Complete the assessment using the supplied scenario
  - Discuss and agree
  - Appoint a spokesperson to report back
Exercise Wrapup

- Outcomes

- Would you award a certificate to this business?

- Gold, Silver or Bronze?

- Could you do this for your business?
Information Assurance for Small to Medium Enterprises

- To register for certification, or to get more information, contact:
  - The IASME Consortium at The National Computing Centre
    The Flint Glass Works, 64 Jersey Street
    Ancoats Urban Village
    Manchester, M4 6JW
  - mailto:info@ncc.co.uk
  - Tel: 0845 519 1055
  - DD: 0161 605 0852