WELCOME

ISO/IEC 27001:2017 Information Briefing

Denis Ryan
C.I.S.S.P
NSAI Lead Auditor
Running Order

1. Market survey
2. Why ISO 27001
3. Requirements of ISO 27001
4. Annex A
5. Registration process
6. Questions – discussion
ENISA profile
Survey
UK Department for Digital, Culture, Media 2018

43% of businesses and 19% of charities identified cyber security breaches or attacks in the last 12 months.

42% of micro/small businesses identified cyber security breaches or attacks in the last 12 months.

65% of medium/large businesses identified cyber security breaches or attacks in the last 12 months.

Among the 43% of businesses/19% of charities that identified a breach or attack:

- 22% (25%) had a temporary loss of files.
- 15% (14%) had software or systems corrupted.
- 10% (14%) had their website slowed or taken down.
- 7% (4%) had money, assets, or intellectual property stolen.
- 6% (3%) had a permanent loss of files or personal data.
Figure 5.1: Proportion of organisations that have identified breaches or attacks in the last 12 months

% experiencing a cyber security breach or attack in last 12 months

- Businesses overall: 43%
- Within micro firms: 40%
- Within small firms: 47%
- Within medium firms: 64%
- Within large firms: 72%
- Within finance/insurance: 57%
- Within info/comms: 59%
- Charities overall: 19%

Bases: 1,519 UK businesses; 655 micro firms; 349 small firms; 263 medium firms; 252 large firms; 105 finance or insurance firms; 99 information or communications firms; 569 charities
### Survey

**Q. Have any of the following happened to your organisation in the last 12 months?**

<table>
<thead>
<tr>
<th>Event</th>
<th>Businesses</th>
<th>Charities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraudulent emails or being directed to fraudulent websites</td>
<td>75%</td>
<td>74%</td>
</tr>
<tr>
<td>Others impersonating organisation in emails or online</td>
<td>28%</td>
<td>27%</td>
</tr>
<tr>
<td>Viruses, spyware or malware</td>
<td>24%</td>
<td>24%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>15%</td>
<td>10%</td>
</tr>
<tr>
<td>Unauthorised use of computers, networks or servers by outsiders</td>
<td>15%</td>
<td>5%</td>
</tr>
<tr>
<td>Denial-of-service attacks</td>
<td>12%</td>
<td>13%</td>
</tr>
<tr>
<td>Hacking or attempted hacking of online bank accounts</td>
<td>8%</td>
<td>3%</td>
</tr>
<tr>
<td>Unauthorised use of computers, networks or servers by staff</td>
<td>7%</td>
<td>6%</td>
</tr>
<tr>
<td>Any other breaches or attacks</td>
<td>5%</td>
<td>6%</td>
</tr>
</tbody>
</table>

Bases: 778 businesses that identified a breach or attack in the last 12 months; 218 charities
Figure 5.3: The single most disruptive breach suffered among the organisations that have identified breaches

Q. What was the one cyber security breach, or related series of breaches or attacks, that caused the most disruption to your organisation in the last 12 months?

- Fraudulent emails or being directed to fraudulent websites: 48% (Businesses) 48% (Charities)
- Viruses, spyware or malware: 13% (Businesses) 12% (Charities)
- Others impersonating organisation in emails or online: 10% (Businesses) 12% (Charities)
- Ransomware: 7% (Businesses) 6% (Charities)
- Denial-of-service attacks: 6% (Businesses) 11% (Charities)
- Unauthorised use of computers, networks or servers by outsiders: 4% (Businesses) 11% (Charities)
- Hacking or attempted hacking of online bank accounts: 3% (Businesses) 2% (Charities)
- Unauthorised use of computers, networks or servers by staff: 1% (Businesses) 1% (Charities)
- Any other breaches or attacks: 4% (Businesses) 1% (Charities)

Bases: 778 businesses that identified a breach or attack in the last 12 months; 218 charities
Survey

Figure 6.6: Most common actions following the most disruptive breach of the last 12 months, where breaches had material outcomes

Q. What, if anything, have you done since this (most disruptive) breach or attack to prevent or protect your organisation from further breaches like this?

Bar chart showing top unprompted responses (5% or more):
- Installed, changed or updated antivirus or anti-malware software: 29% (Businesses), 31% (Charities)
- Additional staff training or communications: 14% (Businesses), 19% (Charities)
- Changed or updated firewall or system configurations: 8% (Businesses), 23% (Charities)
- Created or changed policies and procedures: 16% (Businesses), 15% (Charities)
- Hired an outsourced cyber security provider: 11% (Businesses), 3% (Charities)
- No action taken: 10% (Businesses), 12% (Charities)

Bases: 287 businesses that identified a breach or attack with an outcome in the last 12 months; 87 charities
### Public service Survey bsi 2018 (745 org)

**Which security breaches have you suffered in the last 12 months?**

<table>
<thead>
<tr>
<th>Security Breach</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of Service (DoS)</td>
<td>7%</td>
</tr>
<tr>
<td>Ransomware</td>
<td>11%</td>
</tr>
<tr>
<td>Malware</td>
<td>18%</td>
</tr>
<tr>
<td>Staff errors</td>
<td>32%</td>
</tr>
<tr>
<td>Phishing</td>
<td>30%</td>
</tr>
<tr>
<td>Malice from disgruntled employees</td>
<td>2%</td>
</tr>
<tr>
<td>Access from past employees</td>
<td>1%</td>
</tr>
<tr>
<td>No security breaches</td>
<td>23%</td>
</tr>
</tbody>
</table>
Information Security Management Systems

- Framework to protect information such as financial data, intellectual property, sensitive customer information, data, IT.
- Identify risks and implement security measures.
- Continuous review and improvement.
Benefits of implementing ISO 27001

1. Compliance
   - reputational damage caused by ineffective security.
   - Compliance with legislation and stakeholder need and expectations.
   - Enables secure exchange of information.
Benefits of Implementing ISO 27001

2. Marketing

- win new business and retain existing clients.
- increased credibility when tendering for contracts.
- expand into new markets.
- demonstrates best practice.
Benefits of Implementing ISO 27001

3. Structure your business
   - define responsibilities.
   - improved management process and risk strategy.

4. GDPR - EU Data protection regulation
ISO 27001 support of GDPR

- Risk assessment
- Compliance
- Data classification/documentation
- Incident mgmt./breach notification
- Asset management
- Privacy by design
- Supplier relationships
NIS Directive

• EU wide legislation on Cybersecurity.
• National Law May 2018 (transposition in progress)
• Id operator of essential services, Nov 2018
• CSIR response team
Structure of ISO 27001

• ISO 27001 requirements
  – Annex A
    • 14 security categories
    • 114 mandatory controls
Structure of ISO 27001

4 Context
   Interested parties, scope.

5 Leadership.
   Commitment, Policy, roles, responsibilities, authority.

6 Planning
   • Risks assessment, Risk treatment plans, SOA, Objectives and plans

7 Support
   • Resources, Competence, Awareness, Communication, Documented information
Structure of ISO 27001

8 Operation
  • Planning and control, risk assessment, risk treatment

9 Performance evaluation
  • Monitoring, Internal audit, mgmt. review

10 Improvement
  • NC and Corrective action, Continual improvement
Annex A Requirements

A5  Information Security Policies
review of policies

A6  Organisation of IS
Internal organisation- roles and responsibilities
Segregation of duties
Contact with authorities
Contact with special interest groups
I.S in .Project mgmt,
Mobile devices
Policy
Teleworking security measures.
Annex A

A7 Human resource security
Screening
Terms and conditions
Responsibilities of employees and contractors
I.S awareness, education and training
Disciplinary process
Termination or change of employment
Annex A (cont’d)

A8 Asset management
Inventory of assets
Ownership of assets
Acceptable use of assets
Return of assets
Information classification
Labelling of information
Handling of assets
Management of removable media
Disposal of media
Physical media transfer
Annex A (cont’d)

A9 Access control

Access control policy
Access to networks and services
User registration and de-registration
User access provisioning
Management of privileged access rights
Management of secret authentication
Review of user access rights
Removal or adjustment of access rights
Annex A  cont’d

A9  Access control (cont’d)
use of secret authentication information

System and application
Information access restriction
secure log in procedures
Password management system
use of privileged utility programs
access control to program source code
Annex A (cont’d)

A10 Cryptography

Policy
Key management
Annex A (cont’d)

A11 Physical and Environmental

Physical security
Physical entry controls
Securing offices, rooms, facilities
Protecting against external and environmental threats
Working in secure areas
Delivery and loading areas
Equipment siting and protection
Supporting utilities
Annex A (cont’d)

A11 Physical and Environmental (cont’d)
Cabling security
Equipment maintenance
Removal of assets
Security of equipment and assets off premises
Secure disposal or reuse of equipment
Unattended user equipment
Clear desk and clear screen policy
Annex A (cont’d)

A12 Operations Security
- Procedures and responsibilities
- Change management
- Capacity management
- Development, testing, operational environments
- Protection from malware
- Backup
- Logging and monitoring
- Event log review
- Admin and operator logs
- Control of operational software
- Technical vulnerability
- Restrictions on software installations
Annex A  (cont’d)

A13  Communications security
Network security management
Network controls
Security of network services
Segregation in networks
Information transfer policies and procedures
Agreements on information transfer
Electronic messaging
NDA
A14 System Acquisition Dev and Maintenance
IS in requirements analysis and specification
Securing application services on public network
Protecting Application services transactions
Secure development policy
System change control
Technical review of applications after operating platform changes
Secure system engineering principals
Secure development environment
Outsourced development
System security development
System acceptance testing
Test data
Annex A (cont’d)

A15 Supplier relationships
IS policy for supplier relationships
Security within supplier agreements
Information and communication technology within supply chain
Monitor and review of supplier services
Managing changes to supplier services
Supplier service delivery management
Annex A (cont’d)

A16 IS Incident Management.

- responsibility and procedures
- reporting I.S events
- reporting I.S weaknesses
- assessment of and decision on I.S events
- response to I.S events
- learning from I.S events
- collection of evidence
Annex A  (cont’d)

A17  Business Continuity Management

Planning I.S continuity
Implementing I.S continuity
Verify, review, evaluate I.S continuity
Availability of info processing facilities (redundancy)
Annex A (cont’d)

A18 Compliance

Id of applicable and contractual requirements
Intellectual property rights
Protection of records
Privacy and protection of P.I.I
Regulation of cryptographic controls
Independent review of I.S security
Managers review of f compliance in their area
Technical compliance review
Standard structure

NSAI Website

Self Assessment Checklist
Information in the Cloud

• **ISO 27017**

  Code of practice for information security controls for cloud services.

• **ISO 27018**

  Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
ISO 27001 registration process

1. Familiarise yourself with the requirements of ISO 27001

2. Conduct a self assessment; download self assessment questionnaire from the NSAI website (ISO 27001 webpage)
ISO 27001 registration process

3. Follow system implementation methodology

- ISO 27002 code of practice
- ISO 27003 implementation guidance
- check industry guidance
ISO 27001 registration process

4. Apply for certification
   - Download, complete and return RFQ
   - Sign and return quotation

5. Agree Phase 1 and Phase 2 dates with Lead Auditor

6. Conduct certification audit

7. Certification decision
Resilient Organisation

• Quality (ISO 9001)

• Information Security (ISO 27001)

• Health and Safety (ISO 45001)

• Environment (ISO 14001)

Let's do business!
Thank you.

WWW.NSAI.IE

certification@nsai.ie