NETconsent Whitepaper

Addressing the human elements of ISO/IEC 27001

Foreword

Data handling and information security are central to modern business operations. Increased high profile data breaches have heightened awareness among senior executives that failures in information security have a significant negative impact an organisation. Many organisations choose to implement ISO/IEC27001 (ISO 27001), the global standard for information security, in order to improve information security and demonstrate best practice to customers, investors, regulators and other interested parties.

This whitepaper considers the cybersecurity landscape that has led to the need for standards and highlights the human elements that are needed for a successful implementation of ISO 27001.

- Secure communication within the organisation and to interested parties;
- User awareness of the information security policy, their responsibilities and implications of non-compliance;
- Appropriate education and training with evidence of competence;
- Responsibilities of risk owners to control and manage their risks;
- Monitoring and measurement of information security performance and compliance;
- Analysis of non-conformities, corrective action and continual improvement.

Copyright Statement

Introduction

Organisations are handling ever increasing volumes of sensitive and confidential information, the buzzword Big Data has been around for a while. This data is not only valuable to the legitimate holder, but also has a potential commercial value to cybercriminals.

Across every industry and geography cyberattacks are occurring on a daily basis using all sorts of technical and social attack vectors. Readily available tools have reduced the technical knowledge required to undertake destructive cyberattacks.

Recent events (such as Wannacry or the security breach at Zomato, where data of 17 million users have been stolen) have shown that the scales of attack and constantly increasing, so is the damage. Every organisation is at risk of a data breach with the potential to damage brand reputation, revenues and shareholder value.

Yet, information security is still transitioning from an IT problem to a business issue that impacts everyone throughout an organisation and the extended supply chain. It is important that cyber security is viewed as a Board issue[1]

> *"Today's record fine acts as a warning to others that cyber security is not an IT issue, it is a boardroom issue. Companies must be diligent and vigilant. They must do this because they have a duty under law, but they must also do this because they have a duty to their customers."*[2]
>
> *Elizabeth Denham, UK Information Commissioner*

Following a serious security breach data protection and damage limitation quickly become a topic for Board discussion, as seen in the case of telecoms company TalkTalk. CEO, Dido Harding, told a UK parliament committee that she was accountable because cybersecurity is a board issue.[3] After the data breach TalkTalk lost 101,00 customers and £15 million in revenues.[4] Its share value plummeted by 20%[5] and the company has subsequently been handed a record fine of £400,000 from the UK Information Commissioner's Office. Pre-tax profits to 2016 halved to £14 million as exceptional charges rose to £83 million.[6] There is no doubting that information security is a business risk and can have a direct impact on the future sustainability of a company, which suffers a breach.

ISO/IEC 27001

For organisations that are serious about improving their information security posture and reducing cyber risks ISO/IEC 27001 is a widely adopted international standard for information security.

Created by the International Organization for Standardization (ISO), ISO 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) for any organisation, regardless of type or size. Globally

1 https://www.cm-alliance.com/news/2013/02/cyber-security-and-privacy-for-business-executives
[2] https://ico.org.uk/about-the-ico/news-and-events/talktalk-cyber-attack-how-the-ico-investigation-unfolded/
[3] http://www.computing.co.uk/ctg/news/2439321/i-was-responsible-for-security-at-the-time-of-the-hack-says-talktalk-ceo-dido-harding
[4] http://www.telegraph.co.uk/technology/2016/02/02/talktalk-loses-101000-customers-after-hack/
[5] http://www.cityam.com/228714/talktalk-share-price-plunges-twice-as-deep-as-sony-carphone-warehouse-barclays-and-ebay-after-cyber-attacks
[6] https://www.ft.com/content/2144b2f2-1813-11e6-b197-a4af20d5575e

recognised ISO 27001 provides a consistent benchmark to measure information security best practice across different entities.

An ISO 27001 certificate is considered a credible way of demonstrating to clients and stakeholders that an organisation has implemented best-practice information security processes and engenders a level of trust that can generate real competitive advantage.

Key findings from the ISO 27001 Global Report 2016 by IT Governance support this opinion and advise that ISO 27001[7] directly:

- improves an organisation's information security posture (98%);
- creates competitive advantage (56%);
- delivers return on investment (52%).

According to PwC two-fifths of large organisations have been asked by their customers to comply with the ISO.[8] Evidence of its increasing acceptance as a security standard is reflected by a 20% increase in the number of ISO 27001 certificates issued in 2015 from 23,005 to 27,536.[9]

Organisations do not undertake ISO 27001 certification lightly as a great deal of effort is required to document and implement the controls and processes required. The focus of this whitepaper is on sections 7 and 9 of the standard that address the human aspects of ISO 27001 certification, which must be there to support the technical requirements.

Documented Information

ISO 27001 requires a set of policies and procedures for information security to be defined, approved by management, published and communicated to employees and the relevant stakeholders. Most organisations have policies and procedures in place, but there are a number of areas for improvement, such as:

- Policies and procedures do not reflect how the work is done in practice;
- They are not always readily accessible to all those people who need to refer to them;
- People in the organization do not even know about them, and what their responsibilities are;
- People are not complying with them, and no action is taken.

It's important that information security policies align with an organisation's strategic objectives and operational performance. **P**eople will just look for ways around controls that don't make sense to them, putting an organisation at even greater risk. For this reason, it's crucial that policies are written in a language users understand and their importance emphasised by management. Content must be written in a language that the target audience understands. Too often documents that include technical jargon are shared inappropriately with end users, who just give up.

If policies and procedures are well developed and maintained, over time a library of information can built up, in a structure that is easily navigated, drip fed or available at the point of need. By separating out policies, procedures, guidelines and forms, navigation and readability of documentation is greatly simplified. Adding different media types makes content more interesting and easier to maintain people's attention. Creating and maintaining a centralised library ensures

[7] http://www.itgovernance.co.uk/iso27001-global-report-2016.aspx
[8] PwC Information Security Breaches Survey 2010
[9] http://www.iso.org/iso/iso-survey | http://www.iso.org/iso/the_iso_survey_of_management_system_standard_certifications_2015.pdf

current information is always available in one place when needed. In parallel, a pro-active approach for the management of information security risks is demanded in ISO 27001.

Communication

ISO 27001 puts great emphasis on the communication of information security policy to employees and interested parties, including 3rd party contractors and companies that form part of the supply chain. This requires an easy but efficient distribution process for these documents. It is also inevitably needed to review and update them, and well as re-distribute them when being changed. All this is required by ISO27001 to achieve and maintain the certificate, and therewith information security.

> *"The most-cited privacy priority over the next 12 months is privacy training and awareness, with updating of privacy policies and procedures a close second."* [10]
>
> *PwC, CIO and CSO, The Global State of Information Security® Survey 2017*

A passive approach that simply deposits content into an online library or file share does not guarantee it reaches the eyes, let alone the consciousness of personnel. Neither does it adequately accommodate people external to the organisation. Email notification containing links may indicate notification, but can never prove the link was clicked and the documentation read!

Competence

A requirement of ISO 27001 is to ensure people have the necessary competence to undertake their role in information security. In practice this extends beyond technical personnel to include all staff and often third parties. Face to face induction and annual training is desirable, but not always practical, especially when more and more workers are geographically dispersed and working flexibly. With security threats adapting so quickly, organisations undoubtedly benefit from introducing an on-going education and training program, that people can undertake at their own pace and convenience.

> *"By making small changes to your organisational culture you can make big improvements in the effectiveness of existing security measures."* [11]
>
> *Centre for the Protection of National Infrastructure: Personnel security messages*

Structured campaigns around data handling requirements and best practice information security tips are not likely to overwhelm non-technical staff. It is therefore important to be engaging and keep information security at the forefront of their minds. Automating the delivery of relevant content directly to people's desktop makes such a program less administratively cumbersome and straight-forward for users.

The introduction of short videos or infographics often have a far greater impact on someone's security habits than any ten-page policy document ever could. Such content is freely available on the internet, so is no longer costly to introduce either. Automated approaches make it easier to record

[10] http://www.pwc.com/gx/en/information-security-survey/assets/gsiss-report-cybersecurity-privacy-safeguards.pdf

[11] http://www.cpni.gov.uk/advice/Passport-to-Good-Security/8-Create-a-strong-security-culture-Soft-measures/

levels of voluntary participation, and where necessary are capable of enforcing actions and testing to evidence on-going compliance to management, auditors and regulators.

Internal Audit

Organisations are expected to conduct regular internal audits, which can prove onerous and impact on day to day business activities. An auditor is expected to read through all documented information to ensure there are no non-conformities and confirm that processes are actually being carried out in the manner described. It is therefore crucial that the documentation being referenced is the current version and addresses all necessary aspects. Being able to provide the latest documentation for the information security management system at any point saves wasted time, effort and minimises risk. Clear identification of ownership for each document, and who it affects, makes it much quicker for corrections to be approved and re-communicated to relevant personnel in an efficient and effective manner. Automating this process reduces the time that organisations remain non-compliant and are exposed to risk.

Awareness

It is management's responsibility to ensure all employees and, where relevant, third parties, receive appropriate awareness education, training and regular updates to organisational policies and procedures, relevant to their function. To be confident of an organisation's compliance status with regard to these softer security measures, extensive records need to be maintained and reports readily presented. Instead of breaking down summary information by departments or locations to name and shame non-compliant areas of an organisation, such information should be used to motivate business units to improve. Many organisations are now including security objectives in Key Performance Indicators to emphasise its importance throughout the business. Visible leadership from the top and expectation of inclusion in all relevant security awareness education and training activities goes a long way to raising a positive security culture.

Conclusion

Certification against ISO 27001 demonstrates a genuine commitment to best-practice information security processes. A good part of successful certification achieving information security is to keep a library of documents up to date. This can be used to keep interested parties aware of ongoing changes to policies and procedures as soon as they occur and ensure everyone continues to understand their responsibilities in relation to information security. Continuous improvement throughout the year will have a demonstrable impact on reducing security risks and vulnerabilities and avoid the mad dash for compliance as an audit deadline approaches.

Recommendations

It is clear that the human aspects of ISO 27001 are equally important as implementing technical controls. NETconsent therefore recommends that all organisations establish an ongoing policy compliance and communications program in a manner that is sustainable and effective.

1. Use creative media and engaging methods of communication to drive more positive attitudes toward data protection.
2. Engage senior management to promote the strategic importance of information security and participate in security awareness programs.
3. Make information security part of your organisation's DNA e.g. include topic in regular electronic updates, team meetings, non-IT project discussions, KPIs and annual reviews.
4. Assess levels of information security knowledge among employees regularly and plug any gaps identified with new awareness campaigns or revisions to documented information.

5. Ensure help desk and security teams are considered approachable and friendly to encourage reporting of suspicious behaviour, unusual online activities and potential threats.
6. Develop an incident response plan and ensure everyone is aware and understands the part they must play when an incident occurs.

Appendix A – Policies & Procedures

(information from ISO/IEC 27001:2013 Annex A - control objectives and controls)

A.6.2.1 Policy Mobile Device

A.6.2.2 Policy Teleworking

A.7.1.1 Screening

A.7.2.3 Disciplinary Process (communicated)

A.8.1.3 Acceptable Use of Assets

A.8.2.2 Procedures for information labelling

A.8.2.3 Procedures for handling assets

A.8.3.1 Procedures for management of removable media

A.8.3.3 Procedures disposable media

A.9.1.1 Policy Access Control

A.9.2.1 Process User Registration and De-registration

A.9.2.2 Process User access provisioning

A.10.1.1 Policy on the use of cryptographic controls

A.10.1.2 Policy Key Management

A.11.1.5 Procedures for Working in Secure Areas

A.11.2.9 Policy Clear desk and clear screen

A.12.3.1 Policy Back Up

A.12.5.1 Procedures for installation of software on operational systems

A.13.2.1 Policy and Procedures for Information Transfer

A.14.2.1 Policy Secure development

A.14.2.2 Procedures change control

A.15.1.1 Policy for supplier relationships (information security – agreed with every supplier)

A.17.1.2 Procedures for incident response

A.18.1.2 Procedures intellectual property rights

About NETconsent

NETconsent Ltd is a leading vendor of compliance and communications software that automates the policy management life-cycle, delivers e-learning content and promotes user awareness. By making content more visible and enforceable we help public and private sector clients to raise standards of individual accountability and conduct among their employees, contract suppliers and partners.

- Build a *human firewall* to recognise & contain cyber attacks
- Strengthen the *human factor* to raise standards of compliance and governance
- Encourage *human learning* to promote changes in behaviour

NETconsent compliance and communications solutions deliver a pro-active and sustainable approach to handling the policy management life-cycle and other associated documentation, including policies, procedures, guidelines, e-learning modules & forms.

- **NETconsent Policy Manager:** Create legally valid proof of employees having seen, understood & agreed to policies
- **NETconsent Examiner:** Test, monitor, and report employees' understanding of workplace policies
- **NETconsent Reporter:** Analyse, track, present, manage policy & risk management information
- **NETconsent Assessor:** Poll opinions, undertake assessments and analyse employees' feedback & attitudes
- **NETconsent Informer:** Disseminate information on a need-to-know basis
- **NETconsent Alerter:** Communicate important corporate messages direct to user's desktops
- **NETconsent Portal:** Online self-registration for 3rd parties

For more information contact:
Call: +44 (0) 370 013 1600
Email: info@netconsent.com
Visit: http://www.netconsent.com