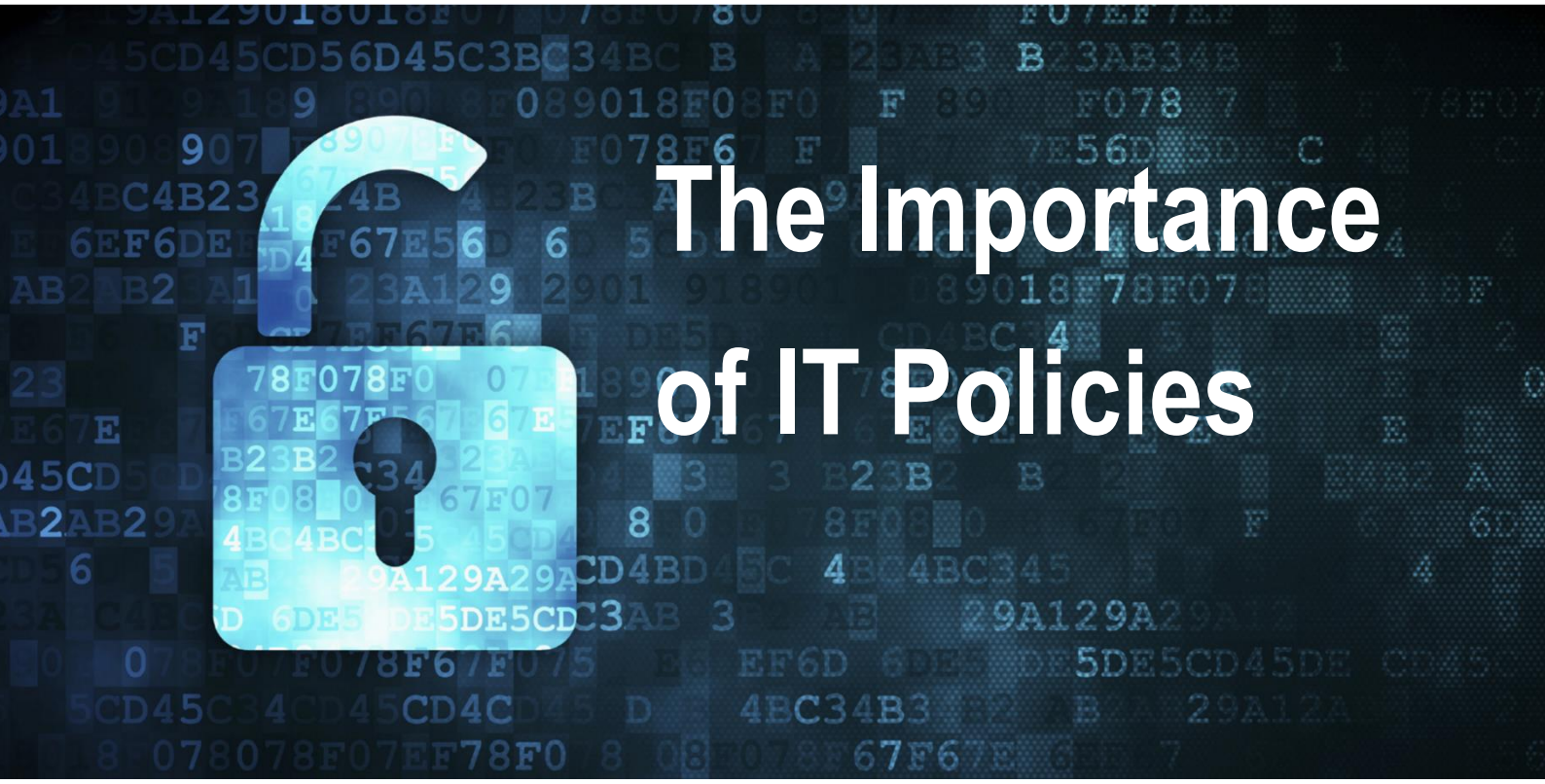
PROTOCOL
POLICY SYSTEMS



The Importance of IT Policies

Table of Contents

Introduction

IT Security Policies play a critical and strategic role in ensuring corporate information is kept safe. This whitepaper answers a number of questions covering the importance of developing and deploying IT Security Policies properly, the business benefits gained, process considerations in terms of stakeholder input, typical policy development shortcomings and ongoing policy management considerations.

Why are IT Policies important?

1. Information security is all about keeping corporate information safe. Policies address the requirement to protect information from disclosure, unauthorised access, loss, corruption and interference and are relevant to information in both electronic and physical formats.

   Information security can be defined by three things:

   - Confidentiality - information must not be made available or disclosed to unauthorised individuals, entities, or processes
   - Integrity - data must not be altered or destroyed in an unauthorised manner, and accuracy and consistency must be preserved regardless of changes
   - Availability - information must be accessible and useable on demand by authorised entities

2. Organisations are beginning to understand the importance of information and communications technology to their business. This may be in support of the activities of the business (financial systems, logistics, inventory, POS systems, CRM etc) or a business channel where customers make purchases or order services - e.g. online shopping portal
3. It is important that these systems are used, operated and managed efficiently and effectively to ensure business continuity and to enable the organisation to meet legal, regulatory and statutory requirements.
4. The organisation must define and communicate its expectations for the appropriate use of these systems so that they remain available for business purposes and their use does not bring the organisation into disrepute.
5. With the proliferation of mobile devices and cloud service offerings, it is more important than ever for organisations to define what they want their IT environment to look like and how their information should be used. Its not just internal systems anymore.
6. Many of the problems around information leakage could have been avoided through appropriate use of information systems. Many outages could have been avoided if systems had been correctly configured and managed.

7. Documented Policies and procedures take the guess work out of information security and enable an organisation to manage business risk through defined controls that provide a benchmark for audit and corrective action.
8. Without documented policies and procedures each and every employee and contractor will act in accordance with their own perception of acceptable use and system management will be ad-hoc and inconsistent. Staff will be unaware whether they are acting within the organisation's risk appetite or not.
9. Security attacks against organisations are increasing both in number and sophistication and we must ensure our systems can be protected against these threats. The first step in achieving this is to document the rules and guidelines around system management, operation and use. By complying with these rules and guidelines organisations are doing everything they can to protect their systems and their people from a security threat.
10. Effective information security policies protect the staff as much as the organisation.

What are the business benefits?

1. Defining and implementing IT security policies helps an organisation to identify and manage business risks.
2. If you owned a very expensive collectible sports car, worth many thousands of dollars, you probably wouldn't let an 18 year old with no drivers licence take it for a spin? However organisations are happy to let users loose with their computers and corporate information, worth in some cases, millions of dollars, with little or no training in information security and no understanding of the organisation's expectations. The management of these systems is left in the hands of a third or fourth tier manager with little guidance from senior management because they don't understand how technology works or what the threats actually are. Its only when it all goes horribly wrong that they tend to sit up and pay attention and then it's a case of implementing damage control, including policies and procedures and writing out a very big cheque to put things right – that is, if its possible to put it right at all.
3. The business catalyst for implementing information security policies and procedures should not be the ambulance at the bottom of the cliff, but a considered and well thought out approach based on a business impact analysis, risk assessment and risk mitigation strategies and driven from the top of the organisation down.
4. The risks of not defining acceptable use and management standards for information and information systems include:

- misuse or loss of data (yours or customers),
- system unavailability
- law suits (employment and commercial),
- damage to reputation,
- financial repercussions due to remediation and loss of business opportunities.

5. Having well defined policies and procedures that are communicated to staff and reviewed and updated regularly to keep up with changes in the environment include:

    - Providing a security and acceptable use framework for the organisation
    - Helping to protect the information systems and information assets of the organisation
    - Providing a uniform level of control and guidelines for management
    - Promulgating one information security message to all
    - Communicating the IT security and acceptable use policies and guidelines to users
    - Providing a benchmark for monitoring and measurement compliance
    - Assisting with staff issues relating to the misuse of the technology or the information
    - Meeting internal obligations of auditors and risk managers

Who should be involved in the development of IT Policies?

The CIO, IT Manager, Network Administrators and System Administrators should all be involved in the development of the Policies and Procedures. Input from Human Resources and Information Managers is recommended. We also recommend input from Risk and Legal staff if these roles exist within the organisation. Ultimately the Senior Management Team should sign off the policies.

How do organisations manage their policies typically today?

Many organisations have a basic Email and Internet Use Policy and do not comprehensively define their information and information systems management and use expectations. If they have policies they are usually a couple of word documents published somewhere on the organisation's intranet. If policies have been developed they may be out of date, available in hardcopy only and not published in such a way that they are readily available to the wider user community. Email and Internet Use Policies may be handed out by Human Resources during staff induction but there is no reiteration of the policies on an ongoing basis, often no training on information security and typically no ongoing security awareness program.

What shortcomings do you typically see in the area of policy development?

1 Trying to do it yourself. Writing effective policies takes months or even years and therefore it is often put in the too hard basket.

2 Copying a best practice manual often doesn't correlate with how the business operates in practice so the policies are not meaningful and are soon disregarded.

3 Not going through the review process. The first draft provided is a generic policy system taking the time to review and customise the policy statements ensures that they are appropriate for the organisation.

4 Not keeping the policies up to date with changes to operational practices and technology.

5 Not communicating the final policies to staff or publishing the policies so that they are readily available to the wider user community.

How does Protocol Policy System address these shortcomings?

1 The IT Security policies contained within the Protocol Policy System address the need to protect confidential and sensitive information from disclosure, unauthorised access, loss, corruption and interference and is relevant to information in both electronic and physical formats.

2 Purchasing the Protocol Policy System takes the pain away from defining and deploying IT security policies. It will enable organisations to meet their internal risk and audit requirements and does not require much in the way of care and feeding. The CIO or IT Manager is able to focus on other priorities. It is priced to be cost effective and provides a level of cross referencing to best practice standards that would not normally be achieved by the organisation themselves. Feedback from organisations that have been through the process including the 2 day review say it is the best two days they have ever spent as it provides them with an introspective view of their current environment.

3 The Protocol Policy System provides comprehensive IT Security policies and supporting documents in a total solution that only requires a 2 day time commitment from the organisation. It is delivered in a web based format that can be easily deployed on the intranet. It is cross referenced to several best practice standards for compliance purposes. It is platform agnostic and no training is required to get it set up and to use it. A maintenance program is available to keep it up to date. The content is customisable so customers decide the wording and content that is appropriate to their organisation.

What types of organisations use the Protocol Policy System today?

The IT Security policies in the Protocol Policy System are applicable to any organisation that uses Information and Communications Technology in carrying out its business. It is totally scalable, platform agnostic and no training is required to get it set up and to use it. The system caters for customers with less than 20 staff to those with thousands of users. A wide range of customers types use the system including Central Government agencies, Local Government agencies and organisations in sectors including Banking, Finance, Insurance, Infrastructure, Transport, Retail and Education.

Author:

Jackie Krzyzewski,
Policy Development Manager - Protocol Policy Systems.