IT Risk Management

Session 7

Overview

- Introduction
- Types of Information Technology risk
- Legal Compliances
- IT risk management policies and procedures
- Business continuity planning
- Reducing Information Technology risks

Introduction

Forbes Report

- Only 42% of surveyed executives are confident their organization could recover from a major cyber event without impacting their business
- More than 50% of surveyed organizations have experienced at least one cyber incident in the last three years
- 21% of organizations experienced cyber events due to a non-sanctioned IT resource
- 60% of organizations don't include shadow IT in their threat assessment
- 13% of organizations have lost data or faced downtime due to incidents with their cloud-service provider; 58% of these incidents were security breaches
- 56% of those who suffered losses due to a cloud incident were not compensated by their providers

Forbes


Top 3 Reasons
Shadow IT Occurs
1 Easier to access SaaS-based service
2 IT doesn't have the expertise
3 Departments do have expertise
69%
Currently nearly two-thirds of corporate leadership view Shadow IT as a negative thing
92%
Most respondents said that Shadow IT projects have been turned over to them to manage
Top 5 Opportunities from Shadow IT
1 Business units more engaged with tech
2 IT can focus with their resources
3 Business can go faster
4 More accountability for end users
5 IT can act as an advisor
7.1
The average number of "Shadow IT" projects turned over to IT to manage after being deployed
LANDESK Shadow IT Survey
— Published May, 2015

What is an IT Risk

- If your business relies on information technology (IT) systems such as computers and networks for key business activities you need to be aware of the range and nature of risks to those systems.
- Businesses face many external and internal digital threats that can corrupt hardware and compromise data.
- Your private data and intellectual property could be used in e-crimes or fraud.

Types of Information Technology risk

General IT threats

- Hardware and software failure - such as power loss or data corruption
- Malware - malicious software designed to disrupt computer operation
- Viruses - computer code that can copy itself and spread from one computer to another, often disrupting computer operations
- Spam, scams and phishing - unsolicited email that seeks to fool people into revealing personal details or buying fraudulent goods
- Human error - incorrect data processing, careless data disposal, or accidental opening of infected email attachments.

Criminal IT threats

- Hackers - people who illegally break into computer systems
- Fraud - using a computer to alter data for illegal benefit
- Passwords theft - often a target for malicious hackers
- Denial-of-service - online attacks that prevent website access for authorised users
- Security breaches - includes physical break-ins as well as online intrusion
- Staff dishonesty - theft of data or sensitive information, such as customer details.

Natural disasters and IT systems

- Natural disasters
  - Fire
  - Cyclone
  - Floods

- Damage to buildings and computer hardware can result in loss or corruption of customer records/transactions.

Legal Compliances

Legal obligations

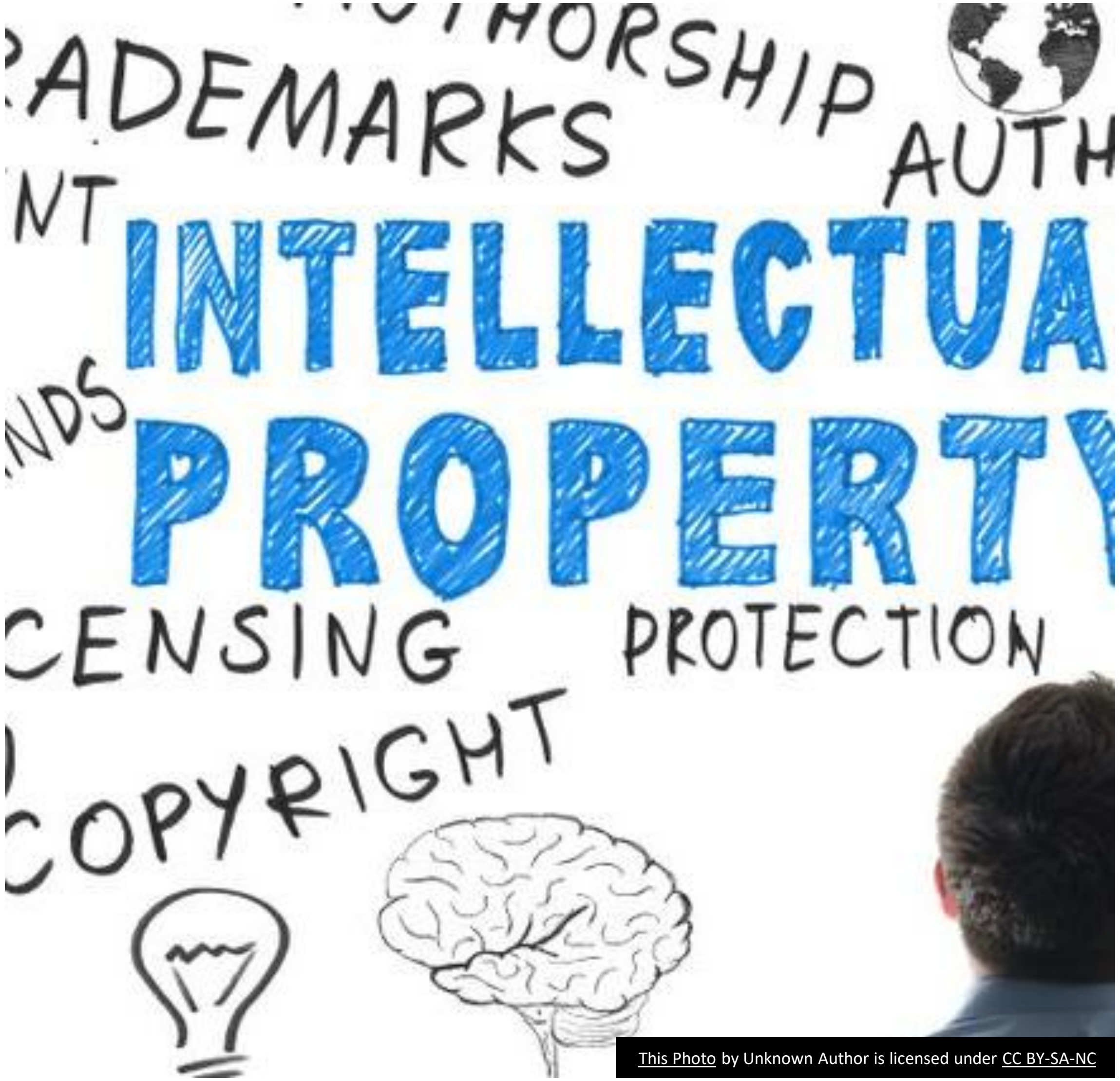
- Privacy
- Intellectual property
- Spam

Privacy

- On 24 August 2017, the Supreme Court of India in a historic judgement declared the right to privacy as a fundamental right protected under the Indian Constitution.
- In declaring that this right stems from the fundamental right to life and liberty, the Court's decision has far-reaching consequences.

Intellectual property

- Patents Act, 1970
- Indian Trademarks Act, 1999
- Indian Copyright Act, 1957
- New Designs Act, 2000
- Geographical Indications of Goods (Registration & Protection) Act, 1999
- Protection of Layouts for Integrated Circuits Act, 2000
- Protection of Plant Varieties and Farmers Rights Act, 2001
- Biodiversity Act, 2002



Spam

- Spam is electronic junk mail.
- It's used to send bulk unsolicited promotional emails indiscriminately to a large volume of email accounts or mobile phone numbers.
- Make sure you adhere to these 3 points:
    - Consent – you must have consent to send messages to your contacts
    - Identify – you must include clear and accurate information about your business, including who is sending the message and how they can be contacted
    - Unsubscribe – you must include an 'unsubscribe' facility to allow recipients to opt out of receiving your messages.

IT risk management policies and procedures

Managing IT risks

- Identify risks
- Assess risks
- Mitigate risks
- Develop response plans
- Review risk management procedures

Policies and procedures

Security policies and procedures can assist your staff training on issues such as:

- Safe email use
- Setting out processes for common tasks
- Managing changes to IT systems
- Responses to IT incidents.

A code of conduct can provide staff and customers with clear direction and define acceptable behaviours in relation to key IT issues, such as protection of privacy and ethical conduct.

List of Suggested Policies

User and Physical Policies

Acceptable Use

Network Architecture

Physical Security

Access Control Policies

Authentication and Access Controls
Encryption

Public Key Infrastructures

External Access Policies

Internet Security

VPN Access

Web and Internet Email

Areas to be protected by a policy

- HARDWARE
- SOFTWARE
- NETWORK EQUIPMENT
- DIAGNOSTIC EQUIPMENT
- DOCUMENTATION
- INFORMATION ASSETS
- PREPRINTED FORMS
- HUMAN RESOURCE ASSETS

Identify from Whom Information or Data is Being Protected

- An important aspect is to define the access for each system and network component.

- An organisation's network may have a system to facilitate the network-based authentication.

Defining Standards

Baselines:

The minimum level of security stated to meet the basic requirements of the policy is known as a **baseline**

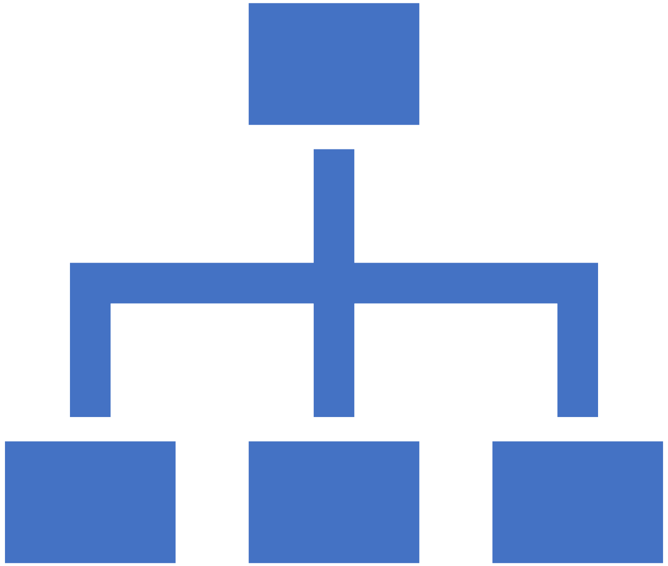
In the case of policies, where there are no technology drivers, standards can be defined which would serve as mandatory mechanisms for policy implementation.

An example of a baseline is to modify the configuration allowing a VPN client to access resources available over the network

Business continuity planning

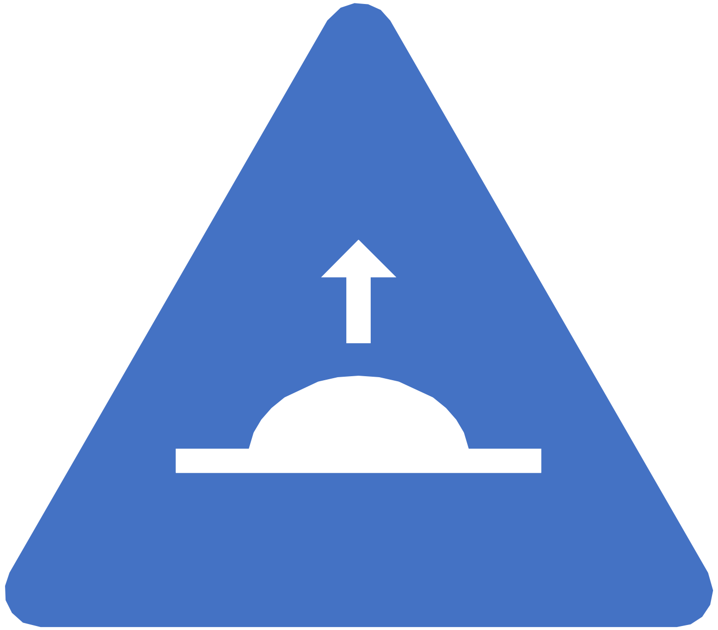
Business continuity plan for key applications and processes:

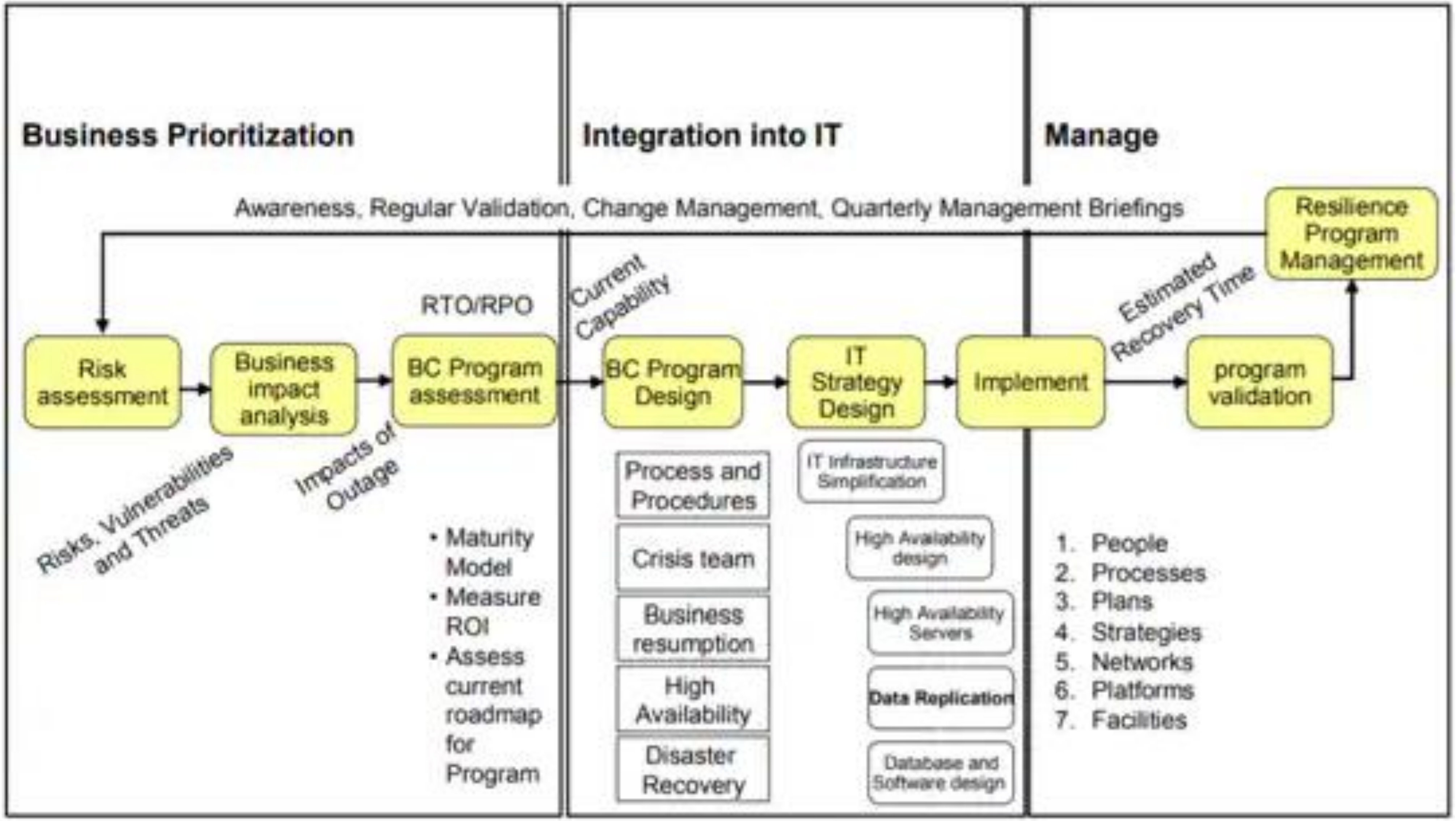
- **High availability**: Provide for the capability and processes so that a business has access to applications regardless of local failures. These failures might be in the business processes, in the physical facilities or in the IT hardware or software.
- **Continuous operations**: Safeguard the ability to keep things running during a disruption, as well as during planned outages such as scheduled backups or planned maintenance.
- **Disaster recovery**: Establish a way to recover a data centre at a different site if a disaster destroys the primary site or otherwise renders it inoperable.



PPRR steps

- **Prevention** - take actions to reduce or eliminate the likelihood or effects of an incident.
- **Preparedness** - take steps before an incident to ensure effective response and recovery.
- **Response** - contain, control or minimise the impacts of an incident.
- **Recovery** - take steps to minimise disruption and recovery times.





**Recovery Point Objective (RPO), Recovery Time Objective (RTO)

Reducing Information Technology risks

Critical Steps

- Secure Computers, Servers And Wireless Networks
- Use Anti-virus And Anti-spyware Protection, And Firewalls
- Regularly Update Software To The Latest Versions
- Use Data Backups That Include Off-site Or Remote Storage
- Secure Your Passwords
- Train Staff In It Policies And Procedures
- Understand Legal Obligations For Online Business.

Secure online presence

- If your business has an online presence, you should assess the security of your website, email accounts, online banking accounts and social media profiles.

- For example, secure socket layer (SSL) technology is used to encrypt transaction data and to send customer and card details to the acquiring bank for authorisation.
- You should ensure any web hosting solution you consider is capable of supporting the SSL protocol.

Q & A

Further Reading

- Perception Gaps in Cyber Resilience: Where Are Your Blind Spots?The hidden risks of shadow IT, cloud and cyber insurance
  Link to PDF:
  https://www.ibm.com/downloads/cas/KDL0MBN0