Common Sense Security

Denny Nugraha

What is Security?

"Security is the state of being free from danger or threat"

–Google

Security Concepts

- Assurance
- Countermeasure
- Defense in depth
- Risk
- Threat
- Vulnerability
- Exploit

blibli.com
BIG CHOICES BIG DEALS

Security Standards

PCI Data Security Standard V 3.2

ISO 27000 Series

NIST National Institute of Standards and Technology U.S. Department of Commerce

SANS

Security Standards (cont'd)

Standard	Number of Controls
PCI DSS V3.0	228 Controls
NIST SP 800-37 (FISMA)	204 Controls
SANS 20 Critical Control	197 Controls
ISO 27002:2013	114 Controls

blibli.com BIG CHOICES BIG DEALS

Information Overload....

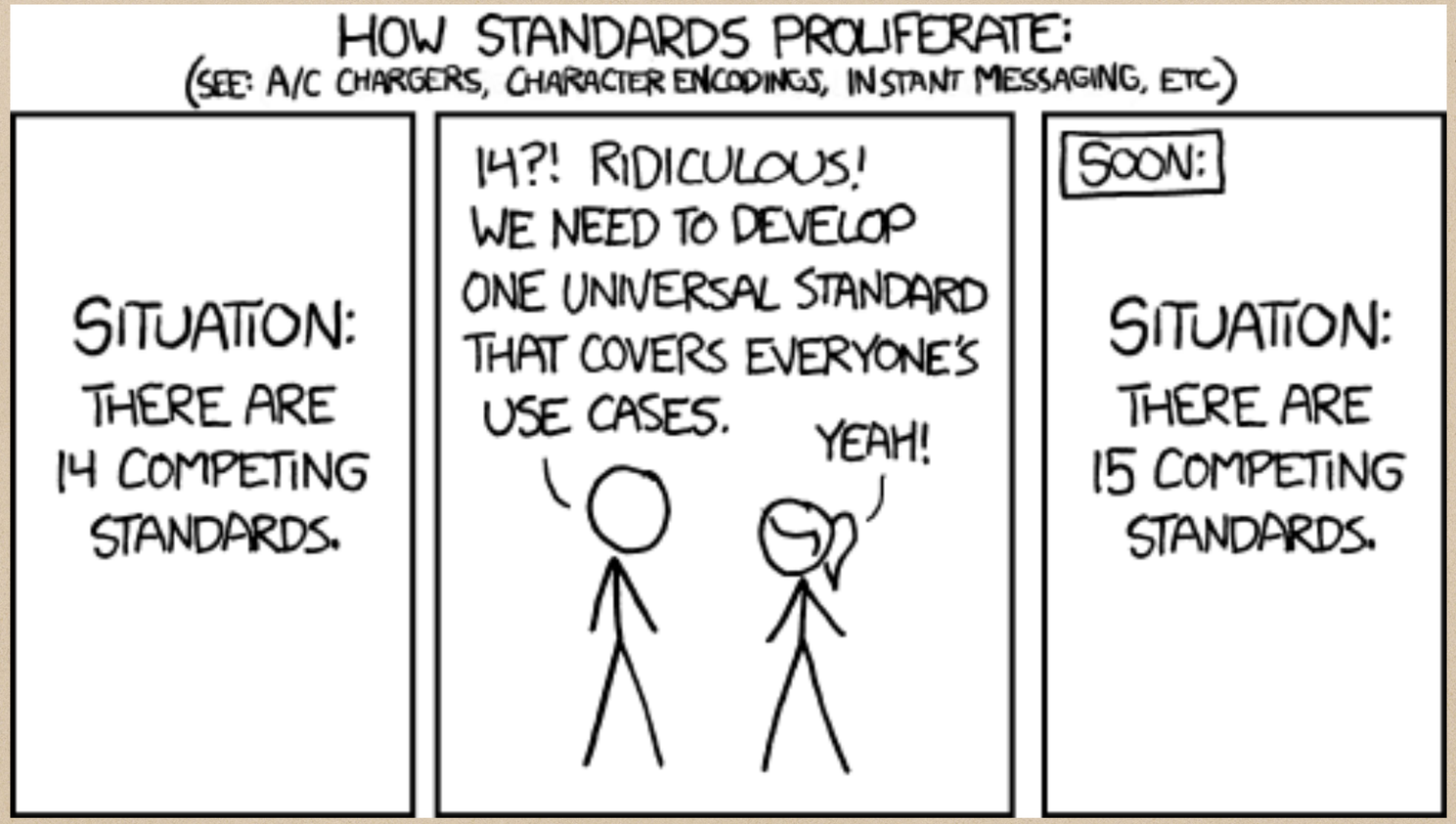
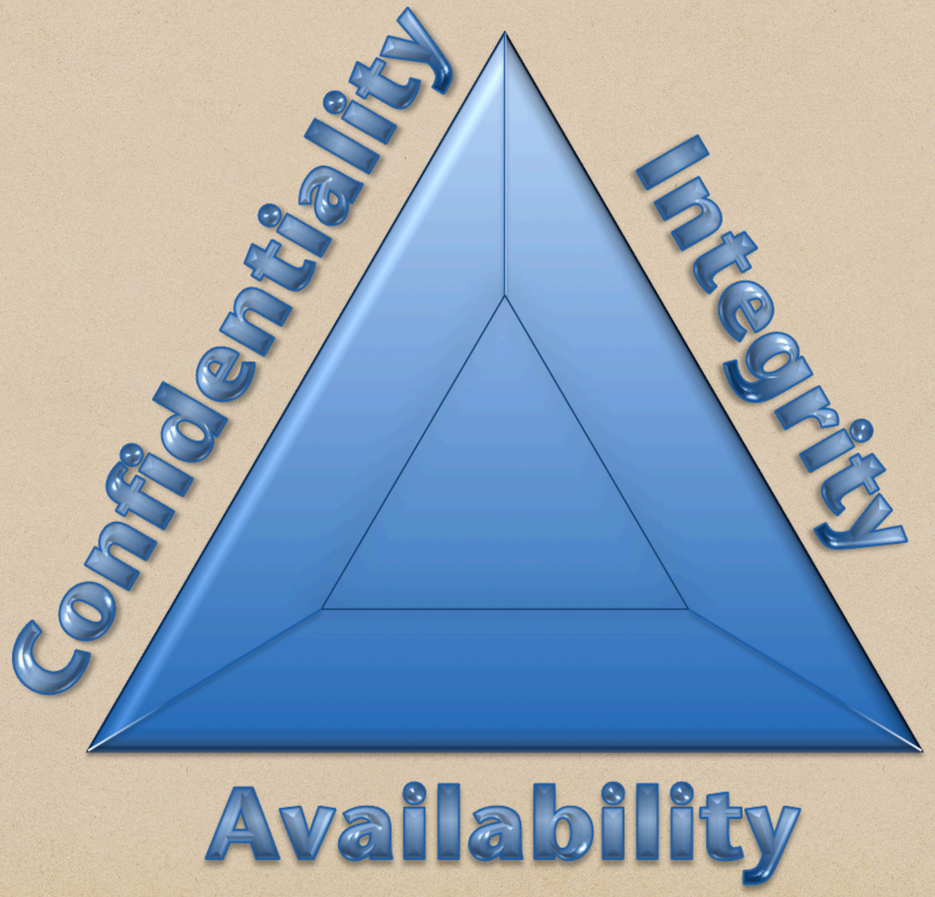
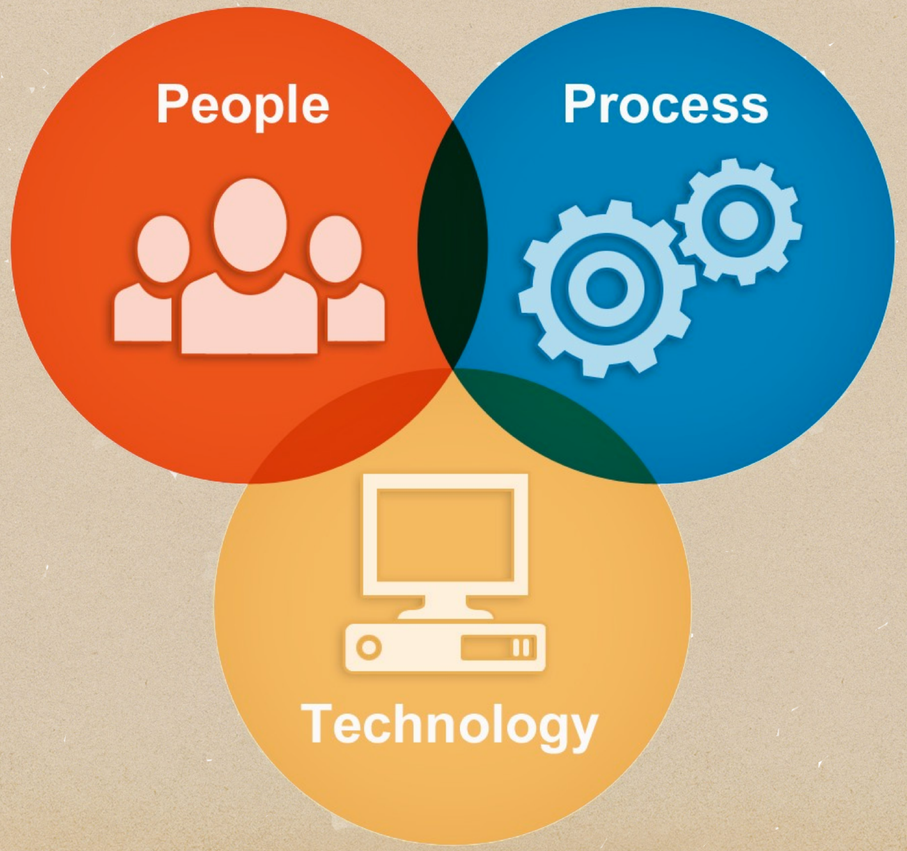


Image: https://xkcd.com/927/

Look Familiar?



Know Your Business



Identify Your Risk

Security Framework

- Protect Your Application
- Protect Your End-point
- Protect Your Network
- Protect Your Server
- Protect Your Data
- Protect Your Location
- Protect Your People

www.commonsenseframework.org

Protect Your Application

- What's in scope:
  - Web Application
  - Mobile Application
- How do we do it:
  - Secure Coding
  - Document your application security requirement
  - Perform regular assessment

Protect Your End-point

- What's in scope:
  - Workstation
  - Mobile Device (smartphones, tablet, laptops)
  - Removable Media
- How do we do it:
  - Limit who has local admin rights
  - Patch all the things
  - Use anti-malware protection on each device

Protect Your Network

- What's in scope:
  - Wired Network
  - Wireless Network
  - Cloud Network
  - Remote Access (VPN)
- How do we do it:
  - Segmentation
  - Use Strong encryption
  - Multi Factor Authentication for remote access

Protect Your Server

- What's in scope:
  - Application Servers
  - Database Servers
  - File Servers
  - Mail Servers
  - Directory Servers (LDAP)
- How do we do it:
  - Hardening
  - Manage & Monitor Accounts activity
  - Scan and Patch on a regular basis

Protect Your Data

- What's in scope:
  - Data in motion
  - Data at rest
- How do we do it:
  - Enforce the principle of least privilege via periodic user access review
  - Create and test backup for critical data
  - Encrypt all restricted data at stored on disk

Protect Your Location

- What's in scope:
  - Headquarters
  - Branch Office
  - Data Centers
- How do we do it:
  - Restrict access to sensitive area or workplace
  - Keep computing equipment in locked room
  - Require / encourage employee to monitor visitor and challenge strangers

Protect Your People

- What's in scope:
  - Anyone who works for your company
  - Anyone who works with your company
- How do we do it:
  - Perform background checks as needed
  - Provide training and awareness on internal policies, standard, and procedures

"Your security is as strong as the weakest link"

–Google

Thank You

blibli.com

BIG CHOICES BIG DEALS