# Introduction

## Security

Otago Polytechnic
Dunedin, New Zealand

# Overview

Scary stories

Course information

The problem of security

# Anthem breach

About two weeks ago the health insurance company Anthem announced a security breach that exposed sensitive personal information about up to 80 million people. Costs to Anthem are projected to exceed $100 million USD.

`http://www.zdnet.com/article/anthem-data-breach-cost-likely-to-smash-100-million-barrier/`

`http://www.databreachtoday.com/anthem-health-hit-by-massive-breach-a-7876`

# Target credit card leak

During the Christmas shopping season, the American retailer Target's credit card payment system was compromised. Target's costs related to this event are expected to be in the billions of dollars.

Interestingly, Target had a strong security system in place at the time.

`http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data`

# Not so new vulnerabilities

A 15 year old bug present in all versions of Windows allows remote execution of malicious code.

http://arstechnica.com/security/2015/02/15-year-old-bug-allows-malicious-code-execution-in-all-versions

https://technet.microsoft.com/en-us/library/security/ms15-011.aspx

# Campaign privacy breach

In an effort to demonstrate his use of technology, former Florida governor Jeb Bush accidentally released the personal details of 12,000 people.

`http://www.theguardian.com/us-news/2015/feb/13/`
`jeb-bush-emails-campaign-rushes-to-redact-12000-peoples-social-`

# Facebook API flaw

A programmer identified a vulnerability in a Facebook API that allowed remote deletion of any photos.

Facebook paid a $12,500 USD bounty and fixed the bug.

`http://www.7xter.com/2015/02/how-i-hacked-your-facebook-photos.html`

# Overview

Scary stories

Course information

The problem of security

# Course goals

- This paper will not make you a security expert.
- Instead, we're trying to acquire a baseline level of *security literacy* that every IT professional should have.
- To put it very prosaically, this paper is about "what you need to know about security to avoid screwing up your third year project."

# Course delivery

We will examine a set of security vulnerabilities.

- We will see how to exploit them.
- We will determine their causes.
- We wiil see how to fix them.

# Course delivery

- We can't look at every possible security problem.
- Our intention is to get some experience thinking about and solving security issues.

# Assessments

- Your assessments will be a series of assignments issued approximately weekly.
- There is about a 60/40 split between programming and sysadmin assigments.
- In some cases the distinction will seem a bit arbitrary. Life is funny that way.

# Overview

Scary stories

Course information

The problem of security

# Start at the beginning

- Suppose that you're working on a IT development project.
- What is the process you will follow?

# What about security?

Where, in your project lifecycle, does security come in?

- **Maintenance?**

# What about security?

Where, in your project lifecycle, does security come in?

- Maintenance
- **Acceptance testing?**

# What about security?

Where, in your project lifecycle, does security come in?

- Maintenance
- Acceptance testing
- **Code review?**

# What about security?

Where, in your project lifecycle, does security come in?

- Maintenance
- Acceptance testing
- Code review
- **Unit testing?**

# What about security?

Where, in your project lifecycle, does security come in?

- Maintenance
- Acceptance testing
- Code review
- Unit testing
- **Coding?**

# What about security?

Where, in your project lifecycle, does security come in?

- Maintenance
- Acceptance testing
- Code review
- Unit testing
- Coding
- **Specification?**

# What about security?

Where, in your project lifecycle, does security come in?

- Maintenance
- Acceptance testing
- Code review
- Unit testing
- Coding
- Specification
- **Requirements analysis?**

# What about security?

Security is a consideration at *every* phase of the project lifecycle, and this means that *everybody* needs to be security literate.

- Maintenance
- Acceptance testing
- Code review
- Unit testing
- Coding
- Specification
- Requirements analysis

# Security as a feature

“Engage in security early and often and be sure to have it included in your definition of done.”

– Laura Bell

# Getting started with security

Make security part of your project from the start by identifying risks.

- Look for components of the project where failures would be particularly harmful.
- Look for processes in your project where security problems are more likely.